UNIVERSIDAD DE CUENCA

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

CARRERA DE CONTABILIDAD SUPERIOR Y AUDITORÍA.

“Auditoría de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCI DSS aplicada a CORAL HIPERMERCADO, RACAR PLAZA con corte a Junio de 2015.”

TRABAJO DE TITULACIÓN PREVIA
A LA OBTENCIÓN DEL TÍTULO
DE CONTADOR PÚBLICO AUDITOR.

AUTORAS:

PATRICIA MARÍA BENENAULA LITUMA.

ESTEFANÍA LISETH ORTEGA LÓPEZ.

DIRECTOR:

ING. PAÚL ADRIÁN OCHOA ARÉVALO.

CUENCA-ECUADOR

2016

RESUMEN

Coral Hipermercado GO es una empresa dedicada a la comercialización de diversos productos de consumo masivo. Debido a la demanda que mantienen y el nivel de transacciones que realizan en ventas diariamente, <para comodidad de sus clientes ofrece diversas formas de pago entre ellas las tarjetas de pago, mismas que por la actual situación del auge de los sistemas informáticos y de la necesidad de la seguridad de los datos ante actos maliciosos las marcas de tarjetas de crédito han visto necesaria la implementación obligatoria (tanto en comercios como en las entidades intermediarias) de la Normativa PCI DSS. De esta manera, el servicio que brindan a los tarjetahabientes a más de ser mejorado, sea seguro en todas sus instancias.

A través de nuestra investigación se obtuvo conocimiento de que la empresa Coral Hipermercado GO no ha realizado anteriormente una auditoria de la Normativa PCI DSS, por lo que la implementación de la Normativa podría no ser completa o apropiada, las políticas de la empresa pueden no contener los procesos y procedimientos que se deben llevar a cabo, haciendo que la seguridad de accesos a los datos de los titulares de tarjetas se vean vulnerables, de igual manera el manejo de las autenticaciones y la infraestructura de la seguridad física, misma que permite el resguardo de los equipos y por ende de la información.

Se observó en la auditoría realizada a los requerimientos 7, 8, 9 de la Normativa PCI DSS que la misma no ha sido socializada en su totalidad, existen falencias en su implementación ya que el uso de las autenticaciones, accesos a los datos y seguridad física no son correctos, viéndose expuesta la información de los datos de los titulares de tarjetas de pago y la posibilidad de incurrir en pérdidas debido a probables actos maliciosos que se podrían encontrar expuestos en un futuro.

Es imperativo mencionar que la norma ayudara al cumplimiento de los objetivos siempre y cuando se logren disminuir las falencias de su

implementación o caso contrario se procederá a dar las recomendaciones necesarias respecto a los problemas encontrados para posteriores correcciones de forma que se mejore la gestión de la empresa.

PALABRAS CLAVES

NORMATIVA PCI DSS

REQUERIMIENTOS

CONTROL DE ACCESO

COMERCIALIZACIÓN

DEMANDA

TARJETAS DE PAGO

SISTEMAS INFORMÁTICOS

TARJETAHABIENTES

AUDITORIA

PROCESOS

PROCEDIMIENTOS

SEGURIDAD DE ACCESOS

AUTENTICACIONES

INFRAESTRUCTURA DE SEGURIDAD FÍSICA

IMPLEMENTACIÓN

GESTIÓN DE EMPRESA

ABSTRACT

Coral Hypermarket GO is a company dedicated to marketing of various massive consumer products. Due to demand that maintain and the level of transactions carried out on daily sales, for the convenience of its customers it offers various forms of payment including payment cards, same as for the current situation of the rise of computer systems and the need for data security against malicious acts brands of credit cards have seen necessary the mandatory implementation (both in stores and intermediary entities) of the PCI DSS Normative. Thus, the service they provide to cardholders, besides being improved, being safe in all instances.

Through our research knowledge that the company Coral Hypermarket GO has not previously conducted an audit of the PCI DSS Normative was obtained, so that the implementation of the Normative may not be complete or appropriate, the company policies may not contain processes and procedures to be carried out, making the security access to data cardholders look vulnerable, likewise, authentications handling and physical security infrastructure, same that allows the safeguarding of equipment and therefore information.

It was noted in the audit conducted of requirements 7, 8, 9 of the PCI DSS Normative that it has not been socialized as a whole, there are shortcomings in implementation since the use of authentications, access to data and physical security they are not correct, looking exposed information data of holders payment cards and the possibility of incurring in losses due to probable malicious acts that could be found exposed in the future.

It is imperative to mention that the standard will help the meeting of the goals as long as they manage to reduce the shortcomings of their implementation or otherwise will proceed to make the necessary

recommendations regarding the problems encountered for subsequent corrections so as to improve the management of the company.

KEYWORDS

PCI DSS

REQUIREMENTS

ACCESS CONTROL

COMMERCIALIZATION

DEMAND

PAYMENT CARDS

INFORMATION SYSTEMS

CARDHOLDERS

AUDIT

PROCESSES

PROCEDURES

SECURITY ACCESS

AUTHENTICATIONS

PHYSICAL INFRASTRUCTURE SECURITY

IMPLEMENTATION

MANAGEMENT COMPANY

ÍNDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS.

ÍNDICE DE ABREVIATURAS

- **PCI DSS:** "Payment Card Industry Data Security Standard".
- **GO:** Grupo Ortiz.
- **IBM:** International Business Machines Corp.
- **SI:** Sistema Informático.
- **ASV:** Proveedor Autorizado para escanear
- **SAQ:** Cuestionario anual de autoevaluación.
- **QSA:** Asesores de Seguridad Calificados.
- **ERP:** Enterprise Resource Planning.
- **AIX:** Advanced Interactive Executive.
- **CVV:** Código de seguridad de la tarjeta.
- **VLAN:** Red de área virtual local.
- **VPN:** Red privada virtual.
- **LINUX:** Sistema Operativo que provee el software necesario para el ordenador del computador.
- **POS:** Sistema electrónico de puntos de venta.
- **TI:** Tecnología de la información.
- **LED:** Light- emitting diode (diodo emisor de luz).
- **MALWERE:** Malicious Software.
- **SDLC:** Controlador de Enlace de Datos Síncrono

Universidad de Cuenca
Clausula de derechos de autor

Yo, Patricia María Benenaula Lituma, autora del trabajo de titulación "Auditoria de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCIDSS aplicada a CORAL HIPERMERCADO, RACAR PLAZA con corte a Junio de 2015", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Contador Público Auditor. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autora.

Cuenca, 13 de Junio de 2016.

Patricia María Benenaula Lituma

C.I: 0105360747

Universidad de Cuenca
Clausula de propiedad intelectual

Yo, *Patricia María Benenaula Lituma,* autora de la tesis "Auditoria de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCIDSS aplicada a CORAL HIPERMERCADO, RACAR PLAZA con corte a Junio de 2015", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autora.

Cuenca, 13 de Junio de 2016.

Patricia María Benenaula Lituma

C.I: 0105360747

Universidad de Cuenca
Clausula de derechos de autor

Yo, Estefanía Liseth Ortega López, autora de la tesis "Auditoria de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCIDSS aplicada a CORAL HIPERMERCADO, RACAR PLAZA con corte a Junio de 2015", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Contador Público Auditor. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autora.

Cuenca, 13 de Junio de 2016.

Estefanía Liseth Ortega López

C.I: 0105688774

Universidad de Cuenca
Clausula de propiedad intelectual

Yo, *Estefanía Liseth Ortega López,* autora de la tesis "Auditoria de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCIDSS aplicada a CORAL HIPERMERCADO, RACAR PLAZA con corte a Junio de 2015", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autora.

Cuenca, 13 de Junio de 2016.

Estefanía Liseth Ortega López

C.I: 0105688774

Agradecimiento

"Nada te turbe, Nada te espante, Todo se pasa, Dios no se muda,
La paciencia todo lo alcanza,
Quien a Dios tiene nada le falta, Solo Dios Basta."
Madre Teresa.

A Dios gracias por permitirme realizar mis sueños, por su sabiduría en los buenos y malos momentos, este reto es gracias a él y es una bendición.

A mi hermano mayor por estar siempre a mi lado, por su confianza en mí, su apoyo, por motivar mi crecimiento profesional, sentó en mí las bases de responsabilidad, y deseos de superación.

A mis hermanos, a mis cuñados, sobrinos y personas especiales que siempre son mi compañía en los momentos grises, frente a obstáculos han sido mi apoyo, gracias por cada impulso.

A Dios gracias por mi familia por mantenerse unidos, acompañándome en todo este trayecto hasta con una palabra de aliento, sé que al final del día siempre estarán conmigo.

A mi compañera gracias por su paciencia y gentileza, Dios nos permitió compartir este trabajo, aprender y conocer cosas nuevas, nos brindó fortaleza para culminar con éxito nuestras carreras.

Agradecimiento especial a nuestro Profesor Ing. Paul Ochoa Arévalo que como Director de este trabajo, nos ha orientado, apoyado y compartido sus conocimientos con un interés y entrega que han sobrepasado las expectativas que como alumnas depositamos en su persona.

A mis profesores de la Universidad de Cuenca, gracias por su tiempo, por sus conocimientos y experiencias transmitidas en este largo camino lo que permitió el desarrollo de mi formación profesional y personal en varias ocasiones.

A Coral Hipermercado por permitirnos ser parte de esta experiencia enriquecedora, a su personal, y en especial a los Ingenieros Humberto Cedillo y Paulino Quinde por toda su comprensión y apoyo.

Patricia Benenaula L.

Dedicatoria

Con mucho amor a mis padres, que son el motor de mi vida,
Por su trabajo y sacrificio en todos estos años,
Gracias a ustedes me he convertido en lo que soy, me amaron, apoyaron y enseñaron a luchar para lograr lo que solo con esfuerzo se alcanza.
En especial a mi madre ejemplar, me ha enseñado a no desfallecer ni rendirme ante nada y perseverar siempre a través de sus consejos y todas sus fuerzas para que siga adelante a pesar de los obstáculos. A mi padre por enseñarme a sostener mi palabra, y a cuidar de mis responsabilidades.
A Dios gracias por tenerlos junto a mí.

"Solo se fracasa cuando se deja de intentar"
Patricia Benenaula L.

Agradecimiento

Agradezco primero a Dios, por bendecirme y brindarme la oportunidad de llegar a cumplir una meta más en mi vida, por iluminarme cada día guiándome siempre por el camino correcto.

A mis padres, Johnny y Mirian, que me han brindado su apoyo, compresión y amor incondicional, por enseñarme buenos valores que me ayudan a ser una persona de bien, por otorgarme la oportunidad de estudiar para ser una excelente

profesional y dar siempre lo mejor de mí.

A mis hermanas y a Mauricio, por apoyarme en este trabajo a lo largo del año, brindándome su compresión, alegría y ayuda.

Al Ingeniero Paúl Ochoa por creer en nosotras y brindarnos la oportunidad de realizar el presente trabajo de titulación.

A la empresa Coral Hipermercado por ayudarnos con información necesaria para realizar el presente trabajo de titulación.

Estefanía Ortega L.

Dedicatoria

A Dios por permitirme cumplir una meta más en mi vida y a mi padres por brindarme la oportunidad de estudiar todos estos años y así ser una persona de bien con valores y ética profesional.

Estefanía Ortega L.

INTRODUCCIÓN

En la actualidad gran parte de los comercios usan tarjetas de pago, por esa razón muchas de ellas se han visto involucradas en fraudes, dadas estas circunstancias seis grandes marcas (MasterCard, Visa, American Express, Discover y JCB Internacional) crean la Normativa PCI DSS como el conjunto de normas para la seguridad de los datos de las tarjetas de pago, que mejora y fomentan la seguridad de los datos del titular de la tarjeta y de esa manera protegen los mismos. La norma PCI DSS se aplica para todos los comercios que almacenan, procesan o transmiten datos relacionados con las tarjetas de pago.

Por lo mencionado anteriormente, el presente trabajo de titulación se enfoca en la Auditoria de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCI DSS aplicada a Coral Hipermercado Racar Plaza con corte a junio del 2015, este tema surge a partir de que la empresa desconoce el nivel de cumplimiento de los requerimientos 7, 8, 9 ya que no se ha realizado una auditoria desde el momento de la implementación de la norma. La empresa debe evaluar el nivel de cumplimento de los requerimientos de la Normativa PCI DSS por estar comprendido el negocio dentro de los comercios a Nivel 4 según MasterCard y Nivel 2 según American Express en el caso de que no se tenga listo este cumplimiento en las fechas predeterminadas la empresa podría incurrir en multas de incumplimiento, mayor costo al procesar transacciones con tarjetas de crédito o perder el permiso de realizar transacciones con las mismas en caso de un compromiso de datos a más de no fomentar ni mejorar la seguridad de datos de los titulares de tarjetas pudiendo encontrarse la empresa vinculada a posibles casos de fraude, en caso de fuga de información, lo que disminuiría la confianza de los clientes al no contar la organización con el estándar de seguridad, ocasionando perdida al negocio.

El desarrollo del contenido del trabajo de titulación llamado “Auditoria de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCI

DSS aplicada a CORAL HIPERMERCADOS, RACAR PLAZA con corte a junio de 2015.” Se encuentra dividido de la siguiente manera:

Capitulo uno: Describe los antecedentes de la empresa Coral Hipermercado como: historia de la empresa, misión, visión, objetivos, planes estratégicos, valores, nivel de comercio de la organización, actividades que realiza, organigrama, estructura funcional, productos que ofrece, sucursales y la tecnología implementada en la empresa.

Capitulo dos: En este capítulo se detalla los fundamentos del proceso de la auditoria de sistemas el cual contiene: definición de auditoria de sistemas, objetivos de la auditoria de sistemas, importancia de la auditoria de sistemas, tipos de auditoria de sistemas, riesgo de auditoria, tipos de riesgos de auditoria, control interno, además se detalla el procesos de auditoria compuesto por: planificación, ejecución, reporte, seguimientos. También describe la normativa PCI DSS donde se observará la historia e PCI DSS, patrocinadores, objetivos de PCI DSS, nivel de comercio, cuestionarios de autoevaluación, alcance de PCI DSS, requerimientos que mayoritariamente se cumple y el conocimiento de los requerimientos 7, 8, 9.

Capitulo tres: Se da la evaluación del nivel de cumplimiento de la norma en los requerimientos 7, 8, 9, aquí se desarrolla: el entendimiento de la empresa Coral Hipermercado, universo auditable, formalización de la auditoria, ejecución de la auditoria donde se efectúa los programas de auditoria de los requerimientos 7, 8, 9 con sus respectivos papeles de trabajo, además se realiza el informe de auditoría.

Finalmente el capítulo cuatro: se presenta las conclusiones y recomendaciones, en el cual se da a conocer los aspectos más significativos del trabajo de titulación.

CAPÍTULO I.

1. ANTECEDENTES GENERALES DE LA EMPRESA.

1.1. Historia de la empresa Coral Hipermercados.

Una de las compañías más exitosas de la ciudad de Cuenca tuvo sus inicios en las instalaciones de una caseta en el mercado 10 de Agosto, en donde la señora Luz María del Carmen Cornejo la atendía, mientras el señor Gerardo Ortiz su esposo creaba un naciente comercio.

Este negocio funcionó hasta que se empezó a levantar el mercado 10 de Agosto, por lo que debieron alquilar una tienda en la calle Juan Jaramillo, fue el primer logro para el desarrollo de los locales comerciales. Luz María del Carmen Cornejo llevaba a las ferias de Chuquipata, Biblián y Azogues variada mercadería entre ellas: productos comestibles, artículos del hogar, artículos de ferretería, bazar, juguetes, prendas de vestir, licores, plásticos, entre muchos otros.

Esta pareja se adaptó perfectamente al mundo de los negocios, junto a sus hijos quienes aprendieron desde muy pequeños a perseverar con honestidad, responsabilidad y disciplina.

Uno de los primeros negocios de éxito de Gerardo Ortiz es la fábrica del Café Cubanito que fue colocada junto a la residencia en la Virgen de Fátima, la cual procesa el café de Zaruma y de zonas altas de la provincia de Loja. Este producto llega al mercado nacional apetecido por toda la provincia, hoy en día tiene instalaciones modernas y tecnología de punta.

En la década de los 60 todos los hijos ya se encontraban involucrados en el negocio, por lo que la pareja Ortiz Cornejo levantó el primer edificio de puestos de ventas, en la calle Miguel Ullauri, después instalarían más tiendas en las calles General Torres y Tarqui. Los esposos Ortiz Cornejo en 1976 entregaron a manos de sus hijos el negocio familiar para que continuaran con este legado.

Los tres hijos del matrimonio Ortiz Cornejo (Ángel, Patricio y Rosa) fundaron Grupo Gerardo Ortiz e Hijos Cía. Ltda., hoy en día conocido como GRUPO GO, para ampliar las actividades llevando al negocio al campo industrial. Los centros comerciales de Ortiz Cornejo fueron situados en sus inicios en la calle Huayna Capac a principios de los 90 y luego el Coral Centro en las Américas, poco después el Mall del Río en el 2004, Monay Shopping en el 2009, más adelante el centro comercial Racar Plaza.

Además dentro del Parque Industrial de Cuenca, muchos de sus espacios están ocupados por Grupo Ortiz como por ejemplo, Lamitex, Ecuaespumas, Dinastic, Telartec entre otras fábricas, las mismas dan trabajo a miles de obreros que elaboran productos con modernas maquinarias.

La señora Luz Carmen asumió la responsabilidad al momento de la muerte de Gerardo Ortiz (16 de abril de 2007), manteniendo la unión familiar y dando consejos a los hijos y nietos.

A partir del fallecimiento de su madre el 4 de Noviembre del 2010, Grupo Ortiz actualmente se encuentra liderado por Ángel Ortiz. No obstante a pesar de esta pérdida sus hijos siguen con sus metas de emprender varios proyectos que servirían para el desarrollo local de la Ciudad sin embargo el negocio se va extendiendo aún más a nivel nacional, con la apertura de la Sucursal de uno de sus negocios más grandes de comercio CORAL HIPERMERCADO en la Ciudad de Manta.

(RevistaAvance, 2010)

1.2. Misión.

Gerardo Ortiz e hijos Cía. Ltda. Tiene como misión, “Satisfacer las necesidades actuales de nuestros clientes, apoyados en el más amplio surtido de productos, en las mejores marcas, al mejor precio, con calidad de servicio y con atención personalizada.”

(Corporación Gerardo Ortiz, 2010)

1.3. Visión.

La visión de la compañía Gerardo Ortiz e hijos es de “Ser una empresa reconocida por exceder las expectativas de nuestros clientes mediante liderazgo, innovación y desempeño sobresaliente de largo plazo.”

(Corporación Gerardo Ortiz, 2010)

1.4. Objetivos.

1.4.1. Objetivo general.

- Ser el líder del mercado.
- Generar mayores utilidades.
- Lograr una mayor participación en el mercado como Coral Hipermercado.
- Ser reconocido por la frase “de todo y más barato”.
- Incrementar la cadena de Coral Hipermercados a nivel nacional.

(Quinde & Cedillo, 2015)

1.4.2. Objetivos específicos.

- Aumentar las ventas mensuales en un 20%.
- Obtener una rentabilidad anual del 25%.
- Lograr una participación de mercado del 20% para el segundo semestre del 2016.
- Producir un rendimiento anual del 14% sobre la inversión.
- Abrir la tienda Coral Hipermercado en Manta para el segundo semestre del 2016.
- Abrir 3 tiendas adicionales en el país para el cuarto trimestre del 2017.

(Quinde & Cedillo, 2015)

1.5. Valores.

- **Disciplina**

Es el principal valor del corporativo Gerardo Ortiz, está enfocado a seguir un trazado a conciencia, en donde se proponga un objetivo para luchar hasta alcanzarlo, separa lo personal del trabajo, respetando los recursos del negocio y tener la convicción de terminar y las cosas que sean importantes para la propia formación de un proyecto exitoso.

- **Autocrítica**

Aceptar que como personas y seres humanos se tiende a errar y que de dichos errores salen nuevas experiencias y conocimiento esencial para evolucionar tanto personalmente así como empresa.

- **Pro actividad**

Esta es la característica que ha dado éxito a la corporación Gerardo Ortiz, la toma de acciones sobre las oportunidades que se presentan a diario; prever, intuir, y actuar de manera positiva sobre todos los problemas que puedan ocurrir en el negocio y en el país, reaccionar de forma instantánea y eficaz.

- **Disponibilidad al Cambio**

Con el cambio cotidiano y evolución tanto de las personas, negocios y tecnología, la corporación Gerardo Ortiz requiere de mucho temple, y sobre todo tener por entendido que existirá la necesidad de estar siempre dispuesto al cambio, sean estos ajustes pequeños o grandes que harán que el camino tome un nuevo rumbo; Gerardo Ortiz mantiene la disponibilidad y la capacidad de entender que las cosas no siempre salen como se prevé.

- **Responsabilidad**

Cuando Gerardo Ortiz inició el negocio adquirió un sin número de responsabilidades, tanto de índole personal como de índole social; Gerardo Ortiz está consciente de entender que se deben respetar una

serie de lineamientos y reglas, además de contribuir en el crecimiento y la armonía del entorno en el que nos desenvolvemos y con las personas que interactuamos.

- **Aprendizaje**

Como todo buen empresario, la gerencia tiene claro que todos los días se aprende algo, además de tener la motivación empresarial. Las técnicas y recursos necesarios para el buen manejo de un negocio ha sido el atributo esencial. La empresa que no evoluciona está destinada a la desaparición, razón por la cual solo queda la preparación y el aprendizaje diario.

(Quinde & Cedillo, 2015)

1.6. Políticas estratégicas.

- La empresa debe estar en constante innovación y desarrollar nuevas practicas administrativas.
- Ser éticos y honestos en todas las transacciones y actividades que se realicen.
- Ofrecen un servicio de calidad en el momento de la compra ya que el cliente es su prioridad.
- Tienen constante innovación y adecuación de las instalaciones y servicios, con la adaptación de nuevas tendencias y tecnologías.

(Quinde & Cedillo, 2015)

1.7. Nivel de comercio.

Desde el punto de vista de las marcas Visa, MasterCard y American Express se pudo determinar cuáles es el nivel de comercio de la empresa Coral Hipermercado (GO), para esto se debe observar los criterios que expone la normativa PCI DSS, además se debe analizar los tipos de tarjetas que acepta la empresa al momento de brindar sus bienes y servicios, de esa manera se compara y se determina el nivel de comercio según lo establecido en PCI DSS, por lo que se llegó a la conclusión que

la empresa Coral Hipermercado se encuentra ubicada en el nivel 4 según MasterCard y en el nivel 2 según American Express, porque procesan 33.398 de transacciones de MasterCard llegando a lo requerido; además procesan 54.798 de transacciones de American Express llegando así a lo expuesto en la norma, lo anteriormente mencionado se analizará a fondo y se determinará en el capítulo 2 y 3 respectivamente.

1.8. Actividades.

Gerardo Ortiz se encuentra dedicado a la venta de una gran variedad de productos en varias líneas entre ellas Textil, Plástica, Hogar, Construcción, Ferretería, maquinaria y equipo, licorera, etc., en sus centros de distribución a nivel nacional con su línea de comercio altamente conocida como CORAL HIPERMERCADO con sucursales en Quito, Ambato, Guayaquil, Cuenca y próximamente Manta.

Una vez que se funda (GRUPO GO) ¨Gerardo Ortiz e Hijos Cía. Ltda.¨ se amplían las actividades iniciales al negocio de la fabricación en el Parque Industrial de Cuenca. Sus fábricas elaboran productos con modernas maquinarias, cuentan con plantas de producción integradas por 17 empresas productivas. Actualmente tienen una diversidad productiva que ensambla y fabrica cocinas de inducción, teléfonos celulares, autoradios, televisores, bicicletas, juguetería, plásticos, textiles, tejidos, tela toalla, pintura, barnices e insumos para la construcción. Entre las fábricas más destacadas están:

- **ECUACYCLO Y MIDEA**

Ecuacyclo produce cuatro tipos de modelos de bicicletas, de la marca GTiBikes, fabricando 400 unidades al día por otro lado Midea se encarga de la producción de cocinas encimeras de inducción. Ambas fábricas funcionan en el sector de Racar, se ensamblan desde 300 encimeras al día con implementos nacionales y otros importados desde China.

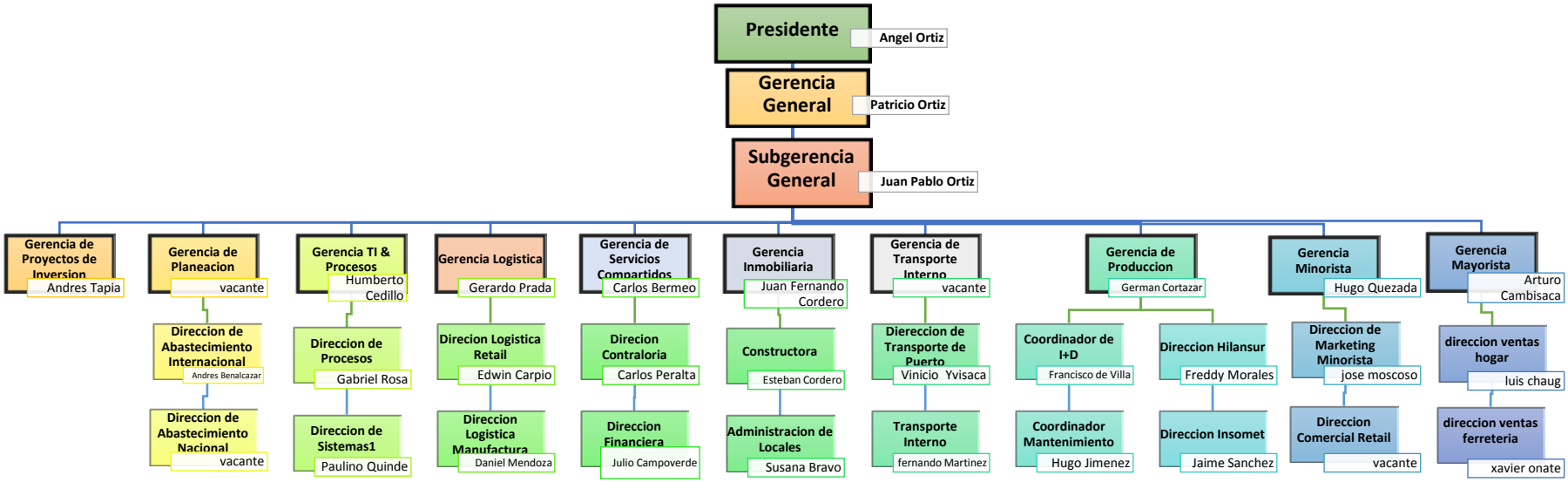
- **HILANSUR**

Se encuentra funcionando en el Sector Sur de Cuenca en la parroquia Yanuncay, su objetivo principal es la fabricación con hilo para la confección de telas para la obtención de productos finales entre ellos sabanas, edredones, colchones, manteles ofreciendo un costo menor que el de la competencia. Está compuesta por 5 naves industriales mismas que en su totalidad son automáticas.

Dentro de las actividades del Grupo Ortiz también está el arrendamiento de locales comerciales aquí podemos mencionar que Grupo Ortiz es propietario del centro comercial más grande de la ciudad "Mall del Rio" considerado un gran aporte para el progreso local ya que ayuda a generar trabajo mediante el comercio y la industria.

El objetivo de Grupo Ortiz es lograr el abastecimiento de las necesidades del sector mayorista comercial así como a pequeños y medianos comercios. Los clientes de esta manera encuentran en un único lugar amplio un surtido para sus negocios, gracias a la capacidad operativa y distributiva Grupo Ortiz ha logrado llegar a posicionarse como el principal referente comercial.

1.9. Ilustración 1 Estructura Organizacional Coral Hipermercado (GO)



Fuente: Coral Hipermercado Racar Plaza (GO)
Elaborado por: Autoras.

1.10. Estructura funcional

- **Presidente:** Es el encargado de representar a la junta directiva de la empresa y a la empresa en si, por lo que toma las decisiones financieras y verifica que se cumplan los objetivos y metas planteados.
- **Gerente del Hipermercado:** Es el que administra el Hipermercado, coordina con los jefes departamentales y dentro de sus funciones esta informar al Presidente la situación de la empresa logrando un buen trabajo en equipo.
- **Subgerente General:** Debe mantener todos los procesos bajo control y supervisión.
- **Director de Auditoria:** Responsable de que los activos de la organización estén seguros.
- **Gerencia Minorista:** Administra los procesos comerciales de los negocios minoristas.
  - ✓ **Dirección Comercial Retail:** Responsable de la operación comercial del Retail.
  - ✓ **Director Ventas Retail:** Responsable de las ventas del Retail.
  - ✓ **Director Marketing Minorista:** Es su responsabilidad el desarrollo de estrategias para lograr el posicionamiento de la organización permitiendo la generación mayores ingresos.
- **Gerente Mayorista:** Administración de los procesos comerciales y ventas de los negocios mayoristas.
  - ✓ **Director Ventas Hogar:** Responsable de las ventas y comercialización de los productos de su categoría.
  - ✓ **Director Ventas Ferretería:** Responsable de las ventas y comercialización de los productos de su categoría.

- ✓ **Director Exportaciones:** Responsable de las ventas y comercialización de los productos que se exportan en cada fábrica.
- ✓ **Director Adheplast:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Consuplast:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Insomet:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Hormiazuay:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Licsur:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Lamitex:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Sintecuero:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Motsur:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Embuandes:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Ress:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Ecuacyclo:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Piedrahuasi:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Impubli:** Responsable de las ventas y comercialización de los productos de la fábrica.
- ✓ **Director Marketing Mayorista:** Desarrollar estrategias para el posicionamiento de la Organización y la generación de mayores ingresos.

- **Gerente de Planeación:** Responsable de la planificación de la demanda y el abastecimiento de la Corporación, maximizando el nivel de servicio al consumidor y optimizando los niveles de inventarios.
  - ✓ **Director Abastecimiento Internacional:** Responsable de la gestión de abastecimiento internacional de productos.
  - ✓ **Director Abastecimiento Nacional:** Responsable de la gestión de abastecimiento nacional de productos.
  - ✓ **Director de Planeación:** Planificar la demanda y el abastecimiento de la Corporación, mediante las mejores prácticas de Cadena de Abastecimiento de Retail, para maximizar el nivel de servicio al consumidor y optimizar los niveles de inventarios.
- **Gerente de TI & Procesos:** Gestionar la plataforma tecnológica para la mejora e innovación de procesos y servicios de la Organización.
  - ✓ **Director de Procesos:** Responsable de la optimización de recursos mediante el diseño de procesos eficientes.
  - ✓ **Director de Sistemas:** Responsable de la administración tecnológica de la Organización.
- **Gerente Logística:** Programar, coordinar, ejecutar y controlar el abastecimiento oportuno de bienes materiales y prestación de servicios que requieren las unidades funcionales de la Organización, a fin que dispongan de los bienes materiales para cumplir su misión.
  - ✓ **Director Logística Retail:** Responsable del funcionamiento logístico en el Retail.
  - ✓ **Director CD:** Responsable del funcionamiento logístico en el Centro de Distribución.
  - ✓ **Director Logística Manufactura:** Responsable del funcionamiento logístico en fábricas de manufactura.

- **Gerente Transporte Interno:** Responsable del transporte interno y externo de los productos
  - ✓ **Director Transporte de puerto:** Responsable del transporte de productos desde y hacia el puerto.
  - ✓ **Gerente de Servicios Compartidos:** Brindar apoyo en gestiones administrativas de toda la Organización.
  - ✓ **Director Financiero:** Responsable de elaborar el plan financiero estratégico de la Organización mediante la implementación y supervisión del registro adecuado de las operaciones financieras y contables.
  - ✓ **Director de Seguridad Industrial:** Responsable de los procesos de seguridad y salud ocupacional en la Organización.
  - ✓ **Director Legal:** Responsable de la administración de procesos legales dentro de la Organización.
  - ✓ **Director de Talento Humano:** Responsable de la gestión de Talento Humano de toda la Organización.
- **Gerente Inmobiliario:** Responsable de la planificación, organización y control de los proyectos inmobiliarios.
  - ✓ **Director Constructora:** Responsable de la construcción de proyectos inmobiliarios.
  - ✓ **Director Administración de locales:** Responsable de la construcción y ajustes en locales.
- **Gerente de Producción:** Responsable de planificar, organizar y controlar las actividades de producción de cada fábrica.
  - ✓ **Coordinador de I+D:** Responsable de la investigación y gestión de proyectos de desarrollo productivo
  - ✓ **Coordinador de Mantenimiento:** Responsable del mantenimiento de maquinaria e infraestructura de las fábricas.
  - ✓ **Director Diseño y Producción de piezas y partes:** Responsable de fabricar y abastecer piezas y partes a las diferentes fábricas de la Organización.

- ✓ **Director Producción Adheplast:** Responsable de la producción de la fábrica Adheplast.
- ✓ **Director Producción Consuplast:** Responsable de la producción de la fábrica Consuplast.
- ✓ **Dirección Producción Hilansur:** Responsable de la producción de la fábrica Hilansur.
- ✓ **Director Producción Insomet:** Responsable de la producción de la fábrica Insomet.
- ✓ **Dirección Producción Telartec:** Responsable de la producción de la fábrica Telartec.
- ✓ **Director Producción Licsur:** Responsable de la producción de la fábrica Licsur.
- ✓ **Director Producción Ecuaespumas:** Responsable de la producción de la fábrica Ecuaespumas.
- ✓ **Director Producción Lamitex:** Responsable de la producción de la fábrica Lamitex
- ✓ **Director Producción Fimitex:** Responsable de la producción de la fábrica Fimitex.
- ✓ **Director Producción Sintecuero:** Responsable de la producción de la fábrica Sintecuero.
- ✓ **Dirección Producción Motsur:** Responsable de la producción de la fábrica Motsur.
- ✓ **Director Producción Embuandes:** Responsable de la producción de la fábrica Embuandes.
- ✓ **Director Producción Hormiazuay:** Responsable de la producción de la fábrica Hormiazuay.
- ✓ **Director Producción Ecuacyclo:** Responsable de la producción de la fábrica Ecuacyclo.
- ✓ **Director Producción Ress:** Responsable de la producción de la fábrica Ress.
- ✓ **Director Producción Impubli:** Responsable de la producción de la fábrica Impubli.

1.11. Conociemiento de Coral Hipermercado.

- **Historia de Coral Hipermercado.**

CORAL HIPERMERCADO es uno de los negocios principales del matrimonio Ortiz Cornejo, tuvo sus inicios con una tienda de abarrotes en el mercado 10 de agosto hoy en día es la cadena más grande de supermercado se ha expandido a nivel local con varias sucursales y a nivel nacional ubicados en la ciudad de Guayaquil y Quito, se ofrecen numerosos productos que elaboran en sus propias fábricas las cuales están la mayor parte en el Parque Industrial de Cuenca, esto ayuda a brindar productos a bajos costes siendo accesibles para todas las personas, lo que ha logrado el éxito de este negocio.

- **Racar Plaza Coral Hipermercado.**

El centro comercial de la cadena Coral Hipermercado recientemente se construyó en una antigua ladrillera que se encuentra ubicado en Racar, presta modernos servicios a los clientes como: Servicios de bancos, almacenes de ropa, artefactos eléctricos, menajes domésticos, ferreterías, patio de comidas y variedad de equipamientos y servicios.

La gigantesca construcción tiene más de cincuenta mil metros cuadrados, que da capacidad en su estacionamiento para 1.200 automóviles, la construcción demoró tres años y estuvo bajo la responsabilidad de Esteban Cordero, arquitecto que diseñó y dirigió la obra.

Racar Plaza cuenta con un centro de distribución mayorista de productos, así como una red de transporte para que los compradores reciban luego el producto en cualquier lugar de la cuidad.

Además en el centro comercial Racar Plaza se encuentran ubicadas las oficinas de la Corporación Empresarial Grupo Ortiz Coral Hipermercado,

podemos decir que es aquí en donde se lleva a cabo la gestión empresarial de todo el Grupo.

(RevistaAvance, 2014)

- **Tipos de productos:**

CORAL HIPERMERCADO ofrece variedades de productos de un supermercado como Alimentos, Electrodomésticos, Muebles, Cristalería, Juguetería, Ropa, y un sin fin más de productos accesibles por sus cómodos precios.

- **Sucursales:**
  - ✓ Mall del Rio
  - ✓ Monay Shopping
  - ✓ Sucre y Huayna Cápac
  - ✓ Racar Plaza
  - ✓ Tarqui y Sucre
  - ✓ Av. De las Américas
  - ✓ Guayaquil: Sucursal en la Av. Carlos Julio Arosemena Km 11/2. Y otra sucursal en la Vía a Daule Km 10. ½.
  - ✓ Quito: Av. Shyris y Tomas de Berlanga.
- **Tipos de transacciones:**
  - ✓ Pagos en efectivo.
  - ✓ Tarjetas de crédito.
  - ✓ Pagos a crédito directo.

1.12. Tecnología Implementada.

- **Arquitectura del SOFTWARE:** Es desarrollada internamente por la organización, detallamos a continuación y lo veremos con más amplitud en el Capítulo III de este trabajo.

- ✓ Cliente- Servidor: Aplicación Oracle[1], Forms 6i[2] y Oracle ápex 4.1[3]
- ✓ Bases de datos: Oracle 11g[4]
- ✓ Sistema Operativo: IBM AIX, LINUX

- **Interfaz Pago de Tarjetas**

Utilizan el Switch transaccional adquirido al Banco Internacional, por el cual se procesan todas las tarjetas afiliadas al establecimiento excepto las tarjetas Cuota fácil para la cual usa el sistema de autorización tradicional llamado P.O.S. (Medianet, Datafast, P.O.S del banco del Austro), además el software propio de la empresa se encarga de enrutar la solicitud de crédito hasta el Switch transaccional y hasta el toda la información es encriptada; lo que sucede luego del Switch transaccional y como vaya la información no está bajo la responsabilidad de la empresa.

(Corporación Gerardo Ortiz, 2010)

[1] **Aplicación Oracle:** según (ORACLE, 2008) es una herramienta cliente servidor desarrollada por Oracle Corporación para la gestión de base de datos, vendido a nivel mundial aunque por su precio y tecnología se encuentra en su mayoría solo en empresas grandes y multinacionales.

[2] **Forms 6i:** según (ORACLE, 2008) es la misma herramienta de Oracle Corporación para la gestión de base de datos solo que su adicional cometido es que permite el desarrollo más rápido de aplicaciones, funcionando la versión 6i funciona en web aparte de un cliente servidor**.**

[3] **Oracle ápex 4.1:** según (ORACLE, 2008) Herramienta que se basa en un navegador web que permite el desarrollo más rápido y seguro de aplicaciones web para las Bases de datos Oracle.

[4] **Oracle 11g:** según (ORACLE, 2008) Base de datos que representa una estructura múltiple, facilita la consolidación de las bases de datos y la administración en la nube, ofrece un desempeño analítico innovador así como nuevos niveles de seguridad, y desempeño.

CAPÍTULO II.

2. FUNDAMENTACIÓN DEL PROCESO DE LA AUDITORIA DE SISTEMAS, Y CONOCIMIENTO DE LAS IMPLICACIONES NORMATIVAS Y SUS REQUERIMIENTOS.

2.1. Definición de Auditoria.

Existen múltiples definiciones de lo que se conoce como auditoria, se mencionaran las más relevantes para el estudio del tema de investigación.

Según Carlos Muñoz Razo "Auditoria es la revisión independiente que realiza un auditor profesional, aplicando técnicas, métodos y procedimientos especializados, a fin de evaluar el cumplimiento de las funciones, actividades, tareas y procedimientos de una entidad administrativa, así como dictaminar sobre el resultado de dicha evaluación." (Muñoz Razo, 2002)

ISACA define a la auditoria como "Un proceso sistemático por el cual un equipo o una persona competente e independiente (auditor[5]) obtiene y evalúa objetivamente la evidencia respecto a las afirmaciones acerca de un proceso con el fin de formarse una opinión sobre el particular e informar sobre el grado de cumplimiento de dicha afirmación." (ISACA, 2014).

2.1.1. Concepto de Auditoria de Sistemas.

Como hemos podido conocer sobre la auditoria ahora nos adentramos a la auditoria de sistemas.

[5] **Auditor: ''**Del latín auditor. Persona capacitada para realizar auditorías en empresas u otras instituciones". (Muñoz Razo, 2002)

¨La auditoría de SI[6] puede definirse como cualquier auditoria que abarca la revisión y evaluación parcial o total de los sistemas automatizados de procesamiento de información, procesos relacionados no automatizados y las interfaces entre ellos.¨ (ISACA, 2014)

- **Objetivos de la Auditoria de Sistemas.**

La evaluación de sistemas computacionales, proyectos informáticos, seguridad de los sistemas, y lo relacionado presenta los siguientes objetivos:

- ✓ Emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área de informática.
- ✓ Evaluar que los sistemas de procesamiento, sistemas operativos, los lenguajes, programas y paqueterías de aplicación y desarrollo, instalación y desarrollo de nuevos sistemas, se estén aprovechando adecuadamente.
- ✓ Evaluar que se estén cumpliendo los planes, programas, estándares, políticas, normas y demás lineamientos que ayudan a la regularización de las funciones, actividades y sistemas de procesamiento de información, del personal y usuarios de la misma.
- ✓ Evaluar las áreas, actividades y funciones de la empresa con el apoyo de los sistemas computacionales, programas especiales de auditoria y paquetería de soporte para el desarrollo de auditorías por medio del computador.

(Muñoz Razo, 2002)

[6] **SI**: Es un sistema informático que consta de hardware, software y el personal que integra esta área; el sistema informático permite almacenar y procesar la información de la organización.

2.1.2. Importancia de la Auditoria

Para el desarrollo de las actividades de una organización hoy en día el uso de la tecnología es una parte esencial del negocio. Permite el procesamiento y presentación de informes para la contabilidad, información sobre fabricación, venta y distribución de productos, en si todas las actividades básicas de un negocio se basan en el uso de la tecnología en cierta medida.

La tecnología ha evolucionado no solo apoyando un proceso de negocio sino en varios casos se encarga de controlar el proceso, en resultado los controles internos de procesos y actividades son basados en su mayoría de la tecnología, deficiencias en la misma y falta de integridad en su apoyo afectaría las operaciones de la organización y el objetivo del negocio de manera significativa.

Vivimos en un entorno competitivo donde la gestión ha aumentado las expectativas de las TI y sus funciones para una mayor calidad, funcionalidad y facilidad de uso, reduciendo tiempos de entrega, mejoras continuas en el servicio a menores costes.

A su vez las empresas necesitan asegurarse de que la tecnología de la información esté siendo eficiente para ayudar al logro de los objetivos de la organización es por ello que las auditorías a las tecnologías del negocio se hacen cada vez más necesarias de forma que permiten al negocio identificar falencias e ir moldeando el uso de las TI a beneficio de la organización, sin olvidar el papel importante que juega la auditoria al momento de realizar un control del cumplimiento de las normas, políticas, manuales o como en nuestro caso la Normativa PCI DSS aportando para que las empresas logren dar seguimiento a que sus actividades vayan desarrollándose de acorde a lo establecido por varias organizaciones que brindan una guía, apoyo, y control mediante normativas para la toma de decisiones, así como para el logro de los objetivos.

2.1.3. Tipos de Auditoria en Sistemas.

- **Revisión.**

Una revisión brinda una seguridad limitada acerca de una afirmación lo que en realidad se lleva a cabo es solo un trabajo de revisión enfocado más a procesos, o adecuación de tareas por lo que las pruebas de auditoría son prácticamente limitadas o no se hacen al igual que la verificación, ya que el nivel de evidencia que se recoge es mucho menor que en una auditoria, como resultado no incluye dictámenes de auditoría y las conclusiones pueden ser muy generales.

(ISACA, 2015)

- **Examen**

La exanimación es un proceso sistemático en la cual una persona competente, independiente evalúa de manera objetiva la evidencia obtenida con respecto a una afirmación sobre un evento dado, con la finalidad de proporcionar una opinión a través de un reporte. Este tipo de trabajo ofrece una mayor seguridad ya que abarca la recolección y evaluación de evidencia suficiente, competente y realiza pruebas y otros procedimientos.

(ISACA, 2015)

- **Procedimientos acordados**

En este tipo de trabajo una tercera parte y el auditor acuerdan los procedimientos específicos que se van a realizar para obtener evidencia en la cual el tercero está dispuesto a confiar como base para una conclusión, por lo que el pactado nivel de evidencia puede ser limitado o extenso.

(ISACA, 2015)

2.2. Riesgo de Auditoría

Según (ISACA, 2014) el riesgo de auditoría es alcanzar una conclusión errónea o incorrecta basada en los resultados de auditoría. El riesgo de auditoría está compuesto por tres componentes, estos son, Riesgo de control, Riesgo de detección, Riesgo inherente y al considerar cada componente se puede determinar el riesgo general de auditoria.

2.2.1. Tipos de Riesgos de Auditoria.

El riesgo de auditoría se clasifica en:

2.2.1.1. Riesgo Inherente:

El riesgo inherente es propio de la naturaleza del negocio que estamos auditando, por esa razón hay que conocer el entorno del mismo y ver cuáles son los posibles riesgos de la organización auditada, en este riesgo no se toma en consideración el sistema de control ya que puede originarse por las susceptibilidades de que las operaciones, sistemas, programas tengan errores o irregularidades.

El Riesgo inherente según (ISACA, 2014) “se refiere a la susceptibilidad de errar en un área de auditoría de forma que pueda ser importante, individual o en combinación de otros errores, siempre y cuando no exista controles internos relacionados”. Esto quiere decir que son riesgos propios del negocio.

- **Factores del riesgo inherente:**

✓ Uno de los factores que puede influenciar al riesgo inherente es la naturaleza del negocio que son las operaciones que realizan de manera cotidiana.
✓ La naturaleza del producto, a lo que se refiere en los volúmenes de producción.
✓ La estructura financiera de la empresa.
✓ El plan de organización.
✓ La estructura humana por la que se encuentra organizada la empresa.

- ✓ Así como la dotación de materiales. (Peña G. , 2013)
- ✓ Otro factor más importante que influye en el riesgo inherente es la integridad de la gerencia y la calidad de recursos.

2.2.1.2. Riesgo de Control:

El riesgo de control es cuando la organización cuenta con un sistema de control débil incapaz de detectar o evitar errores o irregularidades que puedan existir en la organización, esto quiere decir que en la organización no exista un sistema de control efectivo.

El riesgo de control es la incapacidad para detectar o evitar errores, amenazas o vulnerabilidades significativas de manera oportuna para la toma de decisiones.

El Riesgo de control según (ISACA, 2014) se refiere al riesgo que no sea prevenido, detectado y corregido oportunamente por el sistema de control interno, por esta razón puede darse errores que podrían ser material, individual o una combinación con otros errores.

El auditor de SI debe evaluar el riesgo de control como alto en el caso de que la organización no tenga controles internos que sean identificados, evaluados con efectividad y que se pruebe y demuestre que funcionan adecuadamente.

- **Factores de riesgo de control:**

- ✓ El más importante de los factores de riesgo de control es que la organización cuente con una estructura de control débil haciendo de esa manera que aumente el riesgo.

2.2.1.3. Riesgo de Detección:

El riesgo de detección es la probabilidad de que el proceso, técnicas pruebas sustantivas, etc. no detecten errores o irregularidades haciendo de que la organización este expuesta a posibles amenazas o

vulnerabilidades, el riesgo de detección puede ser controlado por el auditor, mientras que los dos anteriores son parte de la empresa.

Por lo que el riesgo de detección depende de la experticia[7] del auditor, además se debe tener claro los objetivos o alcance, también debe existir una planificación efectiva de los recursos, el auditor debe tener un conocimiento previo de la organización a ser auditada y tiene que tener un conocimiento de técnicas de auditoría.

El Riesgo de detección según (ISACA, 2014) "se refiere al riesgo de que los procedimientos sustantivos realizados por los auditores de SI no detecten un error que podría ser material, individual o una combinación con otros errores".

- **Factores del riesgo de detección:**

✓ Existe una ineficacia de los procedimientos de auditoría.
✓ Además que hay una mala aplicación de procedimientos de auditoría.
✓ Otro de los factores de riesgo de detección es cuando el auditor tiene problemas para definir el alcance y la oportunidad.

2.3. Control Interno

Los controles son desarrollados para proveer una certeza razonable a la gerencia de que se alcanzaran los objetivos de negocio y de que se prevendrán o detectaran y corregirán los eventos de riesgo.

Según (IT Control Objectives ISACA, 2014) ¨El control interno es un proceso para asegurar el logro de los objetivos de la empresa para la eficacia y la eficiencia operativa, informes confiables, y el cumplimiento de las leyes, reglamentos y políticas. El control interno es un concepto amplio que abarca todos los aspectos de la gestión y control del riesgo al que se enfrentan las empresas¨.

[7] **Experticia:** Según (BBVA, 2013), significa "habilidad o conocimiento especial" o la "habilidad o conocimiento de un experto".

Según (Echenique Garcia), “El control interno comprende el plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus actividades, verificar la razonabilidad y confiabilidad de su información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescritas por la administración”.

- **Objetivos del Control según** (IT Control Objectives ISACA, 2014)

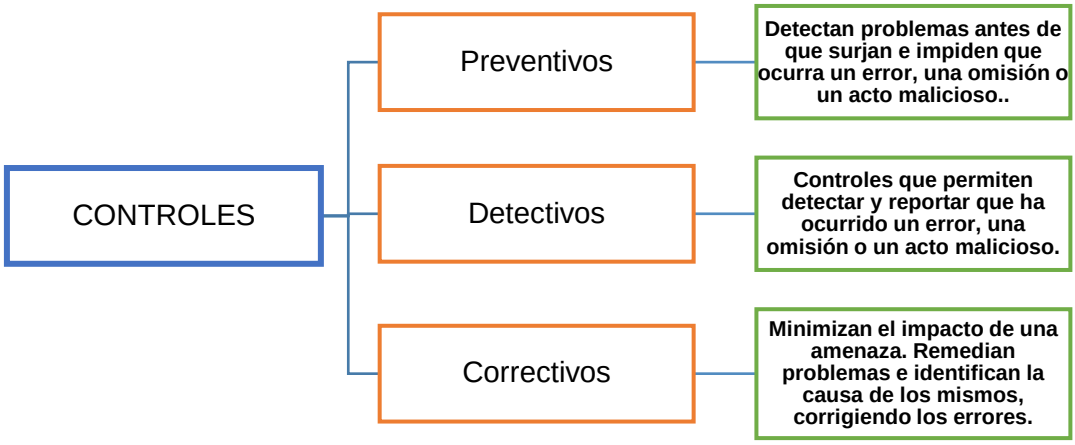
Los controles proporcionan una seguridad razonable de la obtención de los objetivos planteados por la administración con relación a una determinada aplicación.

- **Características del control:**
  - ✓ Integridad: los procesos de todas las operaciones y su Información están completas.
  - ✓ Precisión: las transacciones son procesadas de forma precisa y según lo previsto, por lo que el resultado es una información exacta.
  - ✓ Validez: solo se procesan las transacciones válidas.
  - ✓ Autorización: solo aquellas transacciones debidamente autorizadas son procesadas.
  - ✓ Separación de funciones: la aplicación brinda y apoya para una apropiada separación de funciones y responsabilidades definidas por la dirección.
- **Clasificación de los controles:** Los controles según su ámbito se clasifican en los controles generales y los de aplicación para el tema a investigar nos adentraremos en los controles de aplicación sin dejar de mencionar de forma breve los controles generales:
  - ✓ **Controles generales:** Se aplican a todos los componentes de sistemas, procesos y datos.
  - ✓ **Controles de aplicación**: Son aquellos relacionados con el ámbito de los sistemas de aplicación entre ellos se encuentran:

Los controles de aplicación que forman parte de los controles internos se relacionan con las aplicaciones del sistema y la información que se maneja por esa aplicación debe ser precisa, oportuna, información confiable para la toma de decisiones. De los sistemas de aplicación depende la información, debiendo ser puntual, exacta y fiable para generar, procesar, almacenar y reportar la información.

- ✓ **Preventivos:** impiden que se produzcan los errores, basándose en reglas ya sea de lógica empresarial o de negocio predefinidas que son ejecutadas en su mayoría en las transacciones antes de las acciones que hayan sido confirmadas. (ej.: validación de ingreso en RRHH sin el código sin el sueldo asignado).
- ✓ **Detectivos:** detectan errores basándose en la lógica predefinida del negocio o de sus reglas. Se ejecutan después de una acción que ha tenido lugar y cubren un grupo de transacciones. Implican actividades de revisión manual.
- ✓ **Correctivos:** suelen ser más eficientes y eficaces sobre todo cuando se detectan y corrigen los errores dando lugar a costos adicionales. Pueden ser más fáciles de automatizar que los controles de detección.

Ilustración 2 Tipos de Controles de Auditoria.



Fuente: (Auditoria en Sistemas Computacionales, 2002)
Elaborado por: Autoras.

2.4. Proceso de la Auditoria de Sistemas

Con la finalidad de llevar a cabo una auditoría de sistemas correctamente elaborada para una eficaz toma de decisiones se requiere de una serie de etapas y actividades que se detallará a continuación:

- Etapa 1: **La planificación.**
  - ✓ Entendimiento del negocio.
  - ✓ Universo auditable.
  - ✓ Evaluación del riesgo.
  - ✓ Formalizar el plan de auditoría.
- Etapa 2: **Ejecución.**
  - ✓ Redefinir la comprensión y el alcance de TI.
  - ✓ Probar la eficacia del diseño de control de los objetivos de control clave.
  - ✓ Probar el resultado de los objetivos de control clave.
  - ✓ Documentar el impacto de control y debilidades.

- Etapa 3: **Reporte.**
  - ✓ Estructura del reporte.
  - ✓ Contenido del Reporte de SI.
  - ✓ Proceso de escritura de un reporte.
- Etapa 4: **Seguimiento.**
  - ✓ Procedimientos de actividades de seguimiento.
  - ✓ Factores a considerar al determinar los procedimientos adecuados para la etapa de seguimiento.

2.4.1. La Planificación.

El proceso de planificación en la auditoria nos permite identificar cuáles son las áreas más vulnerables e importantes y los potenciales problemas del examen, de forma que se evalué el nivel de riesgo y se programe la obtención de evidencia que se necesite para examinar los componentes de la entidad a ser auditada.

Se planifica en auditoria para determinar de forma efectiva y eficiente la manera de lograr la obtención de datos necesarios e informar a la entidad acerca de su gestión, naturaleza y alcance de la planificación, misma que puede variar según el tamaño, volumen de operaciones, nivel organizacional de la entidad así como del nivel de experiencia del auditor.

Existen varias definiciones de la Planificación pero a continuación citaremos algunas más relevantes para el tema a investigar:

Según (Contraloria General del Estado, s.f.) ¨La planificación permite identificar lo que debe hacerse en una auditoría, por quién y cuándo.¨

Según (Muñoz Razo, 2002) “Es el proceso de establecer metas y elegir medios para alcanzar dichas metas”.

Beneficios de realizar la auditoria:

- ✓ Garantiza el diseño de una estrategia adaptada a las condiciones de cada entidad.

- ✓ Permite organizar todo el trabajo de auditoria de forma que las personas implicadas, tareas a realizar, recursos necesarios, objetivos, y programas a aplicar entre otros.
- ✓ Garantiza también que la etapa de la ejecución se lleve a cabo con éxito.
- ✓ Permite establecer objetivos específicos y factibles de alcanzar en cuanto a las áreas determinadas para la evaluación de riesgo.
- ✓ Mediante una buena planificación se logra la obtención de un correcto programa de trabajo, optimizando el uso de los recursos disponibles para la auditoria.

Para lograr entender la etapa de la planificación a continuación se dará a conocer algunos pasos que seguiremos para lograr la auditoria y una correcta aplicación de la planificación:

2.4.1.1. Entendimiento del Negocio.

La tecnología existe para apoyar y promover los objetivos de la organización y si sus resultados fracasan esto implica un riesgo debido a la imposibilidad de lograr el objetivo del negocio.

Por lo tanto es necesario:

- ✓ Entender los objetivos de la organización, las estrategias, modelo de negocio, y la importancia de la tecnología como apoyo para la empresa.
- ✓ Identificar los riesgos encontrados en las tecnologías utilizadas y determinar cómo cada uno de estos puede intervenir en el logro de un objetivo, al realizar esto las evaluaciones serán más significativas y útiles para la gestión.
- ✓ Familiarizarnos con el modelo de negocio de la organización es vital, su misión, conjunto de metas y objetivo de negocio propios de la entidad. El modelo de negocio ayuda a identificar los productos o

servicios que la organización ofrece, su base de mercado, canales de suministro, fabricación y generación de productos, procesos y mecanismos de entrega.

- **Entorno de funcionamiento**

Al entender los objetivos necesitamos comprender como los procesos de negocios están estructurados para alcanzarlos, se pueden utilizar diferentes recursos internos para identificar y entender las metas y objetivos de la organización y familiarizarnos con la misma, incluso:

- ✓ Conocer la misión, visión y valores.
- ✓ Los planes estratégicos.
- ✓ Planes de negocios anuales.
- ✓ Cuadros de mando integral de rendimiento de Gestión.
- ✓ Informes y suplementos anuales de los Accionistas.
- ✓ Prestaciones regulatorias.

Se procede a identificar los procesos críticos para el éxito de los objetivos:

Para esto se debe entender como cada proceso de negocio difiere dentro de las unidades de operación, funciones de apoyo y los grandes proyectos de la organización, la forma en como estos se relacionan y se enlazan a los objetivos de la entidad.

"Un proceso se considera clave si su fracaso impide a la organización lograr plenamente el objetivo estratégico al que está atado".

Dentro de las unidades operativas están:

- ✓ Los procesos básicos: Son con los que la empresa logra sus objetivos primarios (Ej. Distribución y ventas).
- ✓ Funciones de apoyo (procesos de gestión) son soporte de las funciones operativas.
- ✓ Funciones operativas (cumplimiento de actividades, finanzas, recursos humanos, tesorería, etc.)

Se delinean las aplicaciones importantes y la infraestructura informática crítica (por ejemplo, bases de datos, sistemas operativos, redes, y entorno físico) que apoyan estas aplicaciones y estas a su vez apoyan los procesos de TI como los ciclos de vida de desarrollo de sistemas, el cambio gestión, operaciones y actividades de seguridad.

- . **Factores Ambientales de TI.**

Nos ayudaran a comprender el entorno operativo y sus riesgos:

- ✓ **El grado de centralización del sistema (Distribución de los Recursos de TI).**

El modelo de negocio de la organización determina la función de TI, su estructura y modelo de entrega.

Al operar con unidades de negocio descentralizadas se tiene autonomía para tomar decisiones operativas de ti, aplicaciones y productos implementados, mientras que al realizar el mismo trabajo de forma centralizada se da una alineación en la rendición de cuentas de gestión.

- ✓ **Las tecnologías desplegadas**

La necesidad de conocimientos técnicos dentro de auditoria y el número de áreas a ser revisadas se determinan a través de la arquitectura de sistemas de la organización, esta puede estar en cualquier y todos los niveles de la tecnología, los componentes clave de una aplicación de infraestructura única, incluyendo su código de programa, base de datos, sistema operativo, y la infraestructura de red.

"El grado de riesgo se basa en la criticidad de la actividad empresarial que la tecnología apoya y permite, y en la configuración y despliegue de la misma. Por lo tanto a más variedad en cada una de estas, mayor es el perfil de riesgo de la organización". [8]

- ✓ **El grado de personalización.**

[8] (Security, 2013): Fragmento relacionado con La norma PCIDSS 2013.

Si las aplicaciones, sistemas operativos u otro software de soporte se modifican para adaptarse a una organización, una gran cantidad de la propiedad es riesgo asumido.

Se debe realizar un análisis coste-beneficio a la hora de tomar la decisión de personalizar software de terceros y considerar los aspectos de control puesto que las implementaciones añaden complejidad a la gestión de activos de TI.

- ✓ **El grado de formalización de las políticas y normas de la empresa**

Las políticas son declaraciones generales a largo plazo, ayudan a guiar el desarrollo de las reglas de negocio para situaciones específicas; pudiendo interpretarse y apoyarse por las normas, controles y directrices. Para TI pueden proporcionar altas directivas de gestión en áreas como derechos de propiedad intelectual, protección de datos, retención y privacidad para asegurar el cumplimiento con las leyes y reglamentos y la salvaguardia eficaz de los datos de activos.

Las normas en cambio proporcionan más dirección en procesos de negocio o procedimientos, estándares de TI que nos ayudan a definir como debe ser implementada la misma.

La organización debe mantener un proceso de actualización de todas las políticas y últimos mandatos regulatorios de forma que mejore la gestión, actividades y riesgos de TI a través del propio Gobierno de TI.

- ✓ **El grado de regulación y cumplimiento.**

Los requisitos reglamentarios de la organización se deben considerar según el perfil de riesgo y el universo de auditoria de ti. Las organizaciones altamente reguladas en general tendrán un perfil de alto riesgo debido a posibles consecuencias de incumplir las exigencias reglamentarias.

- ✓ **El grado y forma de la contratación externa.**

La externalización de TI es cada vez más frecuente en muchas organizaciones debido al alto costo y la experiencia necesarios para ofrecer servicios.

Se debe considerar los diferentes riesgos derivados de la externalización a la hora de elaborar el plan de auditoría de TI. La administración de Factores que incluyen supervisión y monitoreo de papel, la madurez de la disposición (por ejemplo, la transición frente a un proceso de trabajo establecido), riesgos específicos de cada país, así como la integridad de los planes de continuidad de negocio de la organización y del proveedor.

- ✓ **El grado de estandarización operativa.**

El nivel de estandarización operativa puede afectar a la fiabilidad e integridad de la Infraestructura de TI y sus activos. Las organizaciones que adoptan procesos estandarizados en todas sus funciones de prestación de servicios aumentan su capacidad para operar como una organización de alto desempeño.

- ✓ **El nivel de dependencia tecnológica**

Varias organizaciones son usuarios intensivos de tecnología o la utilizan para diferenciarse de sus competidores. Si bien la tecnología puede mejorar los controles internos generales con el uso de los controles de aplicación automatizados, los procesos operativos y de gobernanza internos se convierten en más importantes cuando la dependencia de TI aumenta.

Las organizaciones dependen más de la disponibilidad e integridad de la funcionalidad de TI para habilitar las operaciones de negocio y cumplir con sus objetivos. La importancia de las TI aumenta los riesgos en el perfil general de riesgo de la organización.

2.4.1.2. Universo Auditable.

Definición de Universo de Auditoria de TI.

Se necesita determinar qué es lo que se va a auditar, que áreas de la entidad provenientes de los procesos del negocio. El objetivo del plan de auditoria de TI es cubrir adecuadamente las áreas que tienen mayor riesgo y donde la auditoria puede agregar mayor valor a la organización, proporcionando una adecuada garantía sobre el nivel de gestión de riesgos de la organización, todo esto requiere un profundo conocimiento de objetivos, modelo de negocio y modelo de soporte de servicios de TI de la empresa.

- ✓ **Al examinar el modelo de negocio**

Las organizaciones pueden estar compuestas por diferentes unidades operativas y funciones de apoyo para llevar a cabo sus objetivos los mismos que cuentan con procesos de negocio que enlazan las actividades para el logro de los mismos.

Es importante entender el entorno de TI de la empresa, identificando los procesos críticos para el éxito de cada unidad, utilizando un enfoque de arriba hacia abajo para comprender la organización, estructura y actividades.

- ✓ **Papel de las Tecnologías de Apoyo**

La identificación de tecnologías de TI de infraestructura de soporte es un proceso sencillo si se detectan actividades empresariales que se basan en aplicaciones clave.

Las tecnologías de apoyo existen porque la organización les obliga ya que un fracaso en estos servicios y productos pueden dificultar la capacidad de la organización para cumplir su misión por lo que las tecnologías clave de apoyo aunque no estén directamente asociados con una aplicación o procesos de negocio, deben ser identificadas en el universo de las áreas auditables.

- ✓ **Planes de Negocios Anual**

También es importante tener en cuenta las estrategias y planes de negocio anuales de la organización. Con los datos de los planes se pueden ofrecer importantes cambios y proyectos que pueden realizarse al siguiente año puede requerir la participación de una auditoria convirtiéndose en sujetos para el universo de auditoria de TI.

Todo proyecto o iniciativa de la empresa va a requerir de la intervención de TI beneficiarse de la utilización de componentes de TI críticos que necesitan a su vez de la auditoria en cuanto a controles de acceso, sistemas de gestión, conexiones de red, limitando siempre el acceso a los recursos de TI necesarios.

- ✓ **Funciones de TI Centralizada y Descentralizada.**

Incluyen el diseño de redes y administración de la seguridad, la administración del servidor, la base de gestión de datos, actividades de servicio o mesa de ayuda y de operaciones mainframe.

Hay varias ventajas en la identificación de áreas de auditoría centralizada.

- Uso efectivo de los recursos de auditoria de TI, esto permite que el equipo de auditoría pueda centrarse en un área, utilizar técnicas de muestreo, y obtener una gran cantidad de la cobertura en una sola auditoría.
- Transferencia de eficiencia de auditoría interna a otras auditorías, debido a que áreas centralizadas que ya han sido cubiertas pueden ser excluidos del alcance de otras auditorías.
- La organización es auditada minuciosamente una única vez y no se afecta cuando las aplicaciones se revisan individualmente.

Las organizaciones centralizan su función de TI de manera diferente. Varias suelen crear una red de función de apoyo que administra su diseño de la red y la seguridad. Estas funciones deben ser revisadas al menos anualmente.

En las funciones descentralizadas de ti cada ubicación física puede representar un tema independiente de auditoria. Esto depende el tamaño de la ubicación, así la auditoria seria sobre los controles generales y técnicos para cada capa de la infraestructura.

- ✓ **Cumplimiento Normativo**

Existen diferentes leyes y regulaciones en todo el mundo que ordenan que existan controles internos y gestión de riesgo así como privacidad de información personal identificable. Así también exigen que se proteja la información de clientes en la industria de tarjetas de crédito, seguridad de la información personal. Hacen referencia a un entorno de TI debida y adecuadamente controlado y seguro.

Como auditores se debe determinar si la organización tiene procesos rigurosos y si estos están operando de manera efectiva de forma que se garantice el cumplimiento de las normas.

- ✓ **Definir áreas de estudio de auditoría**

El objetivo es saber cómo dividir el medio ambiente de una manera que proporcione auditorías eficientes y eficaces, para esto el área de estudio no debe ser excesivamente amplia ya que podría dar lugar a un ámbito de aplicación imprevisto, ni tampoco debe ser sobrecargada es decir si el plan contiene numerosas pequeñas auditorias se puede pasar mucho tiempo administrando la relación de las auditorias.

Para encontrar el tamaño de la auditoria se puede tener una base en las prácticas y cultura de auditoria de la organización, esta debe ser coherente con prácticas históricas aceptadas.

La responsabilidad de la gestión debe estar determinada para evitar problemas de quien recibirá el informe de auditoría y será responsable de remediar las deficiencias encontradas. Finalmente el alcance de la

auditoria debe ser establecido con claridad para que la comunicación de los resultados sea clara.

- ✓ **Aplicaciones de Negocios**

Las aplicaciones de negocio se pueden incluir como parte de la auditoria de Universo de TI, las funciones de auditoria interna que las aplicaciones del negocio junto con los procesos de negocio que estas apoyan deben ser auditadas ya que brindaría seguridad a los controles automatizados y manuales para los procesos examinados, minimizando las brechas y esfuerzos de auditoria y determinando lo que se incluye en el alcance del trabajo de auditoria.

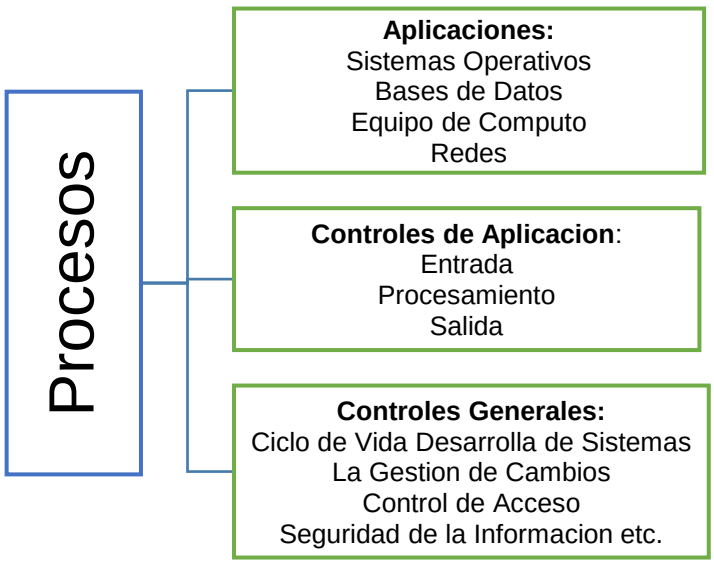
Aunque las aplicaciones de negocio se mantengan separadas del universo de auditoría de TI, los sujetos individuales de auditoría pueden crear dentro del universo de auditoría de TI a gran escala aplicaciones que se utilizan de múltiples funciones para múltiples procesos, tales como los sistemas ERP.

2.4.1.3. Evaluación del Riesgo

Después de haber definido el universo de TI, se realiza la evaluación de riesgos.

En la evaluación de riesgo se necesita examinar la estructura, aplicaciones y las operaciones informáticas o componentes que proyectan la mayor amenaza a las habilidades de la organización para asegurar el sistema y los datos disponibles, confiables, íntegros y confidenciales.

Ilustración 3 Proceso de Evaluación de Riesgo



Fuente: (ISACA, 2014)
Elaborado por: Autoras.

- **Proceso de Evaluación de Riesgos:**

a) Identificar y Entender los Objetivos del Negocio

Para la evaluación de riesgos es primero fundamental el entendimiento de los objetivos del negocio de la organización y conocer cómo se usa la TI para lograr el alcance de los mismos.

Los procesos de gestión de riesgo deben tener cinco objetivos claves:

- ✓ Riesgos que se deriven de las estrategias y actividades del negocio tienen que ser identificados y priorizados.
- ✓ Se debe determinar el nivel de riesgo aceptable para la organización.
- ✓ Se necesita actividades de mitigación de riesgo que sean designadas e implementadas.
- ✓ Se necesitan llevar a cabo actividades de monitoreo continuo para

gestionar el riesgo.

- ✓ El directorio y la administración necesitan recibir reportes de procesos de gestión de riesgo periódicamente.

b) Identificar y entender las estrategias de la TI

El plan estratégico de TI debe vincularse a los objetivos de la organización y proporcionar una dirección clara de cómo se vinculan a esos objetivos, este debe identificar las acciones tácticas a ser desarrolladas, dentro de un periodo definido de tiempo, el cual está diseñado para apoyar el alcance de los objetivos de la organización.

c) Identificar el Universo de TI

Se necesita conocer los componentes claves de un entorno computacional y así determinar qué áreas necesitan ser revisadas desde la perspectiva de riesgo y control, algunas organizaciones en cambio dividen los universos de TI en tres principales subcategorías: infraestructura, sistemas operativos y aplicaciones.

- ✓ **Infraestructura:** Son todos los componentes computacionales que soporta el flujo y el proceso de información, como servidores, routers, puentes, mainframes, líneas de comunicación, impresoras, centro de datos, equipos de red, software de antivirus y escritorios.
- ✓ **Sistemas Operativos:** Procesos y controles que administra el ambiente computacional.
- ✓ **Aplicaciones:** El software usado por la organización para procesar, archivar y reportar transacciones del negocio.

d) Nivel de Riesgo

Se debe asignar un nivel de riesgo al universos auditable estas deben clasificarse en base al impacto que tengan sus objetivos en la organización y las probabilidades de ocurrencia (riesgo) de las mismas. Se necesita determinar que puede salir mal en cada área y como la

organización puede ser afectada si los controles para administrar o mitigar el riesgo no están operando efectivamente.

De acuerdo a la Evaluación de Riesgo, tres tipos de factores de riesgo son comúnmente usados:

1. “Factores de riesgo subjetivos: para medir el riesgo y su impacto se requiere una combinación de experticia, habilidades, imaginación y creatividad”. (Rehage, Hunt, & Nikitin, 2008)

2. “Factores de riesgo objetivo o histórico: medir la tendencia de factores de riesgo puede ser útil en organizaciones con operaciones estables”. (la información objetiva actual es útil en la medición del riesgo). (Rehage, Hunt, & Nikitin, 2008)

3. “Factores de riesgo calculados: un subconjunto de datos de factores de riesgo objetivos es la clase de factores calculados a partir de la información objetiva o histórica”. (los más débiles de todos los factores a usar porque son factores derivados del riesgo que es histórico o pasado). (Rehage, Hunt, & Nikitin, 2008)

Debido a estos factores de riesgo, los auditores deben diseñar y usar un modelo de impacto de riesgo que se ajuste a sus organizaciones.

Un método de clasificación simplista que usa las categorías alta (H), media (M) y baja (L).

Tabla 1 Escala de Modelos de Impacto de Riesgo.

ESCALA DE IMPACTO (FINANCIERA)		
H	3	El potencial para el impacto material sobre las ganancias de la organización, bienes, reputación o las partes interesadas es alto
M	2	El potencial para el impacto material sobre las ganancias de la organización, bienes, reputación o las partes interesadas

		puede ser significante para la unidad auditada, pero moderada en términos de toda la organización.
L	1	El impacto potencial sobre la organización es menor en tamaño o limitado en alcance.

Fuente: (Developing The IT Audit Plan , 2008)
Elaborado por: Autoras.

La tabla 2 muestra los rangos de puntuación y sus correspondientes frecuencias de audiciones o revisiones basadas en la disponibilidad de recursos de la organización.

Tabla 2 Rangos de puntuación y sus correspondientes frecuencias de auditorías o revisiones.

NIVEL	RANGO DE PUNTUACIÓN DE RIESGO COMPUESTO	CICLO ANUAL RECOMENDADO
H	35 – 54	Cada 1 a 2 años
M	20 – 34	Cada 2 a 3 años
L	6 – 19	Cada 3 a 5 años

Fuente: (Developing The IT Audit Plan , 2008)
Elaborado por: Autoras.

2.4.1.4. Formalizar el Plan de Auditoría.

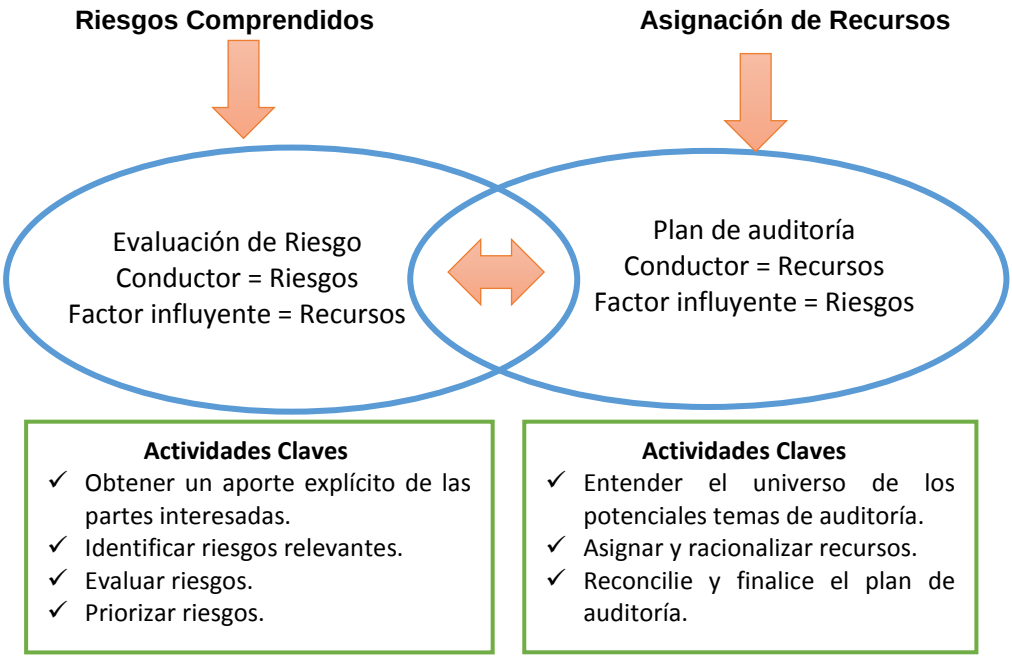
Se deberá crear un plan de auditoria de TI dentro de los límites de presupuesto y recursos disponibles.

El plan de auditoría de TI debe ser creado como parte de los procesos de la planificación estratégica de las funciones de auditoría. Este proceso de planificación debe ser cíclico y puede ser entendido bajo el ciclo de la administración clásica “plan, hacer, chequear y actuar”. Así, mientras el plan es el habilitador de la clave para implementar el proceso, este delinea como buscar objetivos de auditoría y metas. Como resultado, esto debe incluir una lista de actividades de auditoría como en el cronograma,

dependencias y recursos asignados necesarios para buscar las metas de auditoría.

En el plan de auditoria se define como objetivo la revisión de las áreas de mayor riesgo a las cuales se les asignan los recursos disponibles, por lo tanto la vía para la revisión son los recursos y la influencia es el riesgo.

Ilustración 4 Objetivos para la Evaluación de Riesgos Planes de Auditoria.



Fuente: (Developing the IT Audit Plan , 2008)
Elaborado por: Autoras

- **Contenido del Plan de Auditoría de TI**

El contenido del plan de auditoría de TI debe ser un reflejo de la evaluación de riesgo. El plan también debe tener tipos diferentes de auditorías de TI, por ejemplo:

- ✓ Procesos de auditorías de negocios integrados.
- ✓ Proyectos de negocio (o empresariales) y auditorías de iniciativas de TI, incluyendo revisiones del ciclo de vida de desarrollo de software (SDLC).
- ✓ Revisiones de control de aplicaciones.
- ✓ Revisiones de red (por ejemplo, revisiones de la arquitectura de la

red, pruebas de penetración, evaluaciones de vulnerabilidades y evaluaciones de desempeño).

- **Integración del Plan de Auditoría**

Un aspecto clave del proceso de planificación es determinar el nivel de integración del plan de auditoría con las actividades auditadas distintas de TI.

Diferentes opciones para integrar el plan de auditoría:

- ✓ **Plan de baja integración:** Está generalmente aislado de las actividades auditadas distintas de TI e incluye la revisión de las aplicaciones. Las actividades de auditoría distintas de TI no incluyen ninguno de los componentes de TI dentro del alcance.
- ✓ **Plan de auditoría parcialmente integrado:** Estos planes proporcionan un conjunto adicional de compromisos (o contratos) planificados, generalmente referidos o conocidos como revisiones de las aplicaciones, las cuales son distribuidas a través de otros equipos de auditoría distintos de TI y coordinados con otras revisiones de procesos de negocio.
- ✓ **Un plan de auditoría altamente integrado:** A menudo, las actividades de auditoría de TI son planificadas bajo la responsabilidad de un equipo multidisciplinario que tiene un conjunto de habilidades equilibrado, incluyendo experiencia de auditoría de TI.

Dado que un sistema de control interno típicamente incluye controles automáticos y manuales, con más dependencia de los controles de aplicación, la habilidad para alcanzar una auditoría que abarque todos los controles es esencial para proporcionar una evaluación integral del ambiente de control. Una completa auditoría de negocio, incluyendo una revisión de todos los componentes de TI, proporciona la oportunidad para evaluar si existe una apropiada combinación de controles para mitigar los riesgos de negocio.

Tabla 3 Auditoría de TI y Auditoría Integrada

UNIVERSO AUDITADO	PLAN DE AUDITORÍA POCO INTEGRADO	PLAN DE AUDITORÍA PARCIALMENTE INTEGRADO	PLAN DE AUDITORÍA ALTAMENTE INTEGRADO
Procesos de negocio ✓ Operacional ✓ Financiero ✓ Cumplimiento	Auditoría no de TI	Auditoría no de TI	Enfoque integral
Sistemas de aplicación ✓ Controles de aplicación ✓ Controles generales de TI	Auditoría de TI	Enfoque integral	Enfoque integral
Controles de infraestructura de TI ✓ Base de datos ✓ Sistemas operacionales ✓ Red	Auditoría de TI	Auditoría de TI	Enfoque integral

Fuente: (Developing The IT Audit Plan , 2008)
Elaborado por: Autoras.

- **Comunicar, ganar apoyo ejecutivo y obtener aprobación del plan.**

Se debe presentar el Plan de Auditoria a la alta dirección, ya que la aprobación recibida por ellos es de suma importancia para el éxito del ejercicio de la planificación de auditoría y permitirá los auditores entender mejor el ambiente de negocio, identificar riesgos y seleccionar las áreas de auditoría.

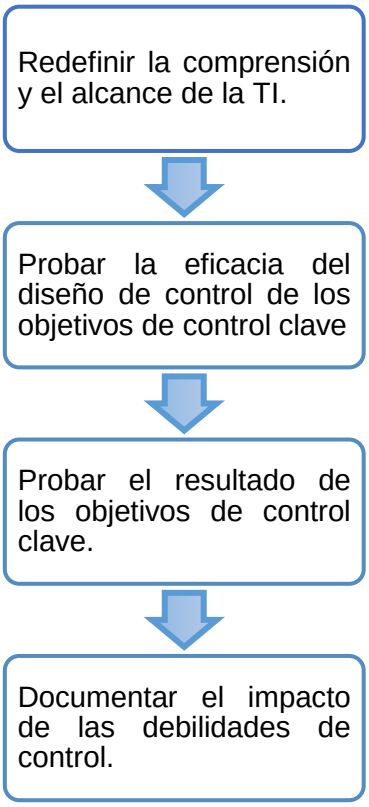
Cuando se habla del plan de auditoría, los auditores deben hacerlo de una manera que sea apoyado por los ejecutivos claves de TI, administradores y el personal. Ganando la comprensión, coordinación y apoyo del equipo de TI hará el proceso de auditoría más efectiva y eficiente.

2.4.2. Ejecución de Auditoria.

Una de las etapas del proceso de auditoría de sistemas es la ejecución, se realizan las acciones programadas, se aplican los instrumentos y herramientas determinadas en la planeación, ya que se realiza las acciones programadas en esta etapa. Se identifica y elabora los documentos de desviación encontrados, también se realiza el dictamen preliminar para presentar a discusión y se integra los papeles de trabajo.

En la ilustración 5 se describe una guía a seguir para ejecutar la auditoría.

Ilustración 5 Guía a seguir para la ejecución de la Auditoría.



Fuente: (IT ASSURANCE GUIDE , 2007)
Elaborado por: Autoras.

2.4.2.1. Redefinir la comprensión y el alcance de TI.

En la etapa de la planificación el auditor comprende el negocio mientras que en la primera etapa de la ejecución debe redefinir la comprensión del entorno en el que se realiza la prueba.

Esto implica el conocimiento de la organización por parte del auditor para seleccionar correctamente el alcance de la auditoría de aseguramiento de TI y los objetivos. Se debe establecer las estrategias, el alcance y enfoque que deben ser finalizados en base a los objetivos, el enfoque óptimo de las pruebas y el riesgo evaluado en la etapa de la planificación. Los procesos, los recursos y la selección de los objetivos de control de la TI se deben ajustar según se requiera. La documentación necesaria y el enfoque de la prueba deben determinarse para garantizar la cobertura más eficaz y eficiente de los objetivos de aseguramiento.

Para poder tener resultados en esta etapa se debe observar:

- ✓ Quién, donde y cuando se realiza el trabajo de auditoría.
- ✓ Los insumos necesarios para realizar la auditoría.
- ✓ Los procedimientos establecidos para la realización del trabajo de auditoría.

Además que el auditor debe realizar:

- ✓ Entrevista y uso de la lista de actividades además de los gráficos RACI[9].
- ✓ Colectar y leer la descripción de procesos, políticas, insumos/resultados, problemas, actas de reuniones, reportes de aseguramiento pasados, recomendaciones de aseguramiento pasadas, reportes de negocios, etc.
- ✓ Preparar el alcance del trabajo de auditoría (objetivo de los procesos, metas y medidas del proceso a ser revisadas).
- ✓ Construir una comprensión de la arquitectura de la TI de la empresa.

2.4.2.2. Probar la eficacia del diseño de control de los objetivos de control clave.

Se debe evaluar el diseño de los controles, así como verificar el funcionamiento y evaluar la eficiencia operativa, por lo que el auditor puede aplicar diferentes tipos de pruebas:

Tabla 4 Tipos de prueba de auditoria.

Preguntar y Confirmar:	Al momento de realizar esta prueba el auditor busca las desviaciones y las examina, investiga eventos que se encuentran fuera de la rutina, verifica, comprueba, determina si algo fuera de lo común ha ocurrido, además que debe confirmar las declaraciones de fuentes independiente, el auditor

[9] **RACI:** Una gráfica RACI identifica quién es Responsable, que persona debe rendir cuentas, quién debe ser Consultado e Informado.

	debe evaluar, entrevistar al personal y hacer preguntas a la administración para poder obtener respuestas que ayuden a confirmar los hallazgos.
Inspeccionar:	El auditor debe revisar planes, políticas, procedimientos, buscar registros de problemas, además que debe inspeccionar físicamente la documentación y comprobar los hallazgos actuales con los esperados.
Observar:	Se debe observar y describir el proceso, los procedimientos y comparar el comportamiento actual con el esperado.
Volver a realizar o recalcular:	Otra prueba que debe realizar el auditor es desarrollar y estimar los resultados esperados, además que se debe comparar el valor y el comportamiento esperado con el valor actual.
Revisar la evidencia recolectada.	Además el auditor debe recolectar datos, usar módulos de auditoría, analizar datos usando técnicas de auditoría, etc.

Fuente: (IT ASSURANCE GUIDE , 2007)
Elaborado por: Autoras.

2.4.2.3. Probar el resultado de los objetivos de control clave.

Las medidas de aseguramiento a realizarse afirman que las medidas de control están trabajando según lo prescrito, llegando a la conclusión que el mecanismo de control se encuentra idóneo.

Para poder llegar al resultado final el auditor busca evidencia directa e indirecta del impacto del control de la calidad de los resultados del proceso, además debe obtener evidencia directa o indirecta de períodos seleccionados para asegurar que el control que se examina está

funcionando con eficacia mediante la aplicación de una selección de técnicas de prueba.

2.4.2.4. Documentar el impacto de control y debilidades.

Las deficiencias de control encontradas deben estar documentadas, teniendo en cuenta su naturaleza confidencial, además, se requiere un cuidado especial para analizar correctamente y evaluar la gravedad de las deficiencias observadas y el impacto potencial para el negocio que puedan tener.

Se debe analizar más detalladamente cuando:

- ✓ No están en su lugar las medidas de control
- ✓ Los controles no están funcionando como se esperaba
- ✓ Los controles no se aplican consistentemente

Tabla 5 Cuando exista un impacto significativo.

Análisis de causa efecto.
Ilustrar el impacto y que no más afectaría.
Ilustrar el impacto de las debilidades de control con los números y los escenarios de los errores, ineficiencias y el mal uso.
Aclarar las vulnerabilidades y amenazas que son más propensos con los controles que operan ineficazmente.
Documentar el impacto de las debilidades de control actuales comparando con el impacto esperado.
Señalar consecuencia de la falta de cumplimiento de los requisitos regulatorios y acuerdos contractuales.
Documentar el costo (es decir, el cliente y el impacto financiero) de los errores que podrían haber sido evitados por controles efectivos.
Medir y documentar el costo de la reanudación (por ejemplo, la relación de la reanudación de trabajo normal) como una medida de la eficiencia afectada por debilidades de control. Mostrar el ahorro de costes de controles efectivos.

Fuente: (IT ASSURANCE GUIDE , 2007)
Elaborado por: Autoras.

Papeles de Trabajo que se utilizan comúnmente en la auditoría.

1. **Hoja de identificación:** Aquí se encuentra la empresa responsable de la auditoria, identificación de papeles de trabajo, periodo de evolución, nombre y cargo el responsable de auditoría, fecha de emisión del dictamen.
2. **Dictamen preliminar (borrador):** Es un borrador que me da a conocer el resultado inicial de la evaluación de auditoría, contiene las desviaciones encontradas durante la revisión y me permite preparar el informe final.
3. **Resumen de desviaciones detectadas:** Este documento considera las desviaciones encontradas, la causa y sus posibles soluciones.
4. **Situaciones encontradas. (situaciones, causas y soluciones):** Se coloca las situaciones encontradas, las causas que originaron, posibles soluciones, la fecha de solución y quien será el responsable de la solución encontrada.
5. **Guía de auditoría:** Indica cada uno de los puntos que debe evaluar el auditor, formas de evaluar, técnicas que se deben usar, métodos y herramientas, deben ser diseñados previamente; la guía de auditoría se debe guardar ya que ayuda a las próximas auditorias.
6. **Inventario de software:** Se debe documentar el inventario de programas, lenguajes, paqueterías, sistemas operativos, y cualquier otro software que se utilice en la empresa para el procesamiento de la información y operaciones del sistema.

Instrumentos de recopilación de información de una auditoria en sistemas.

1. **Entrevistas:** Es la recopilación de la información que se realiza cara a cara, donde se interroga a los entrevistados sobre aspectos de lo que se va auditar, haciendo una serie de preguntas bien

elaboradas que me permitan sacar información útil para la auditoria.

2. **Cuestionarios:** El cuestionario son fichas impresas donde el encuestado responde según su criterio, de esta manera el auditor obtiene información útil.
3. **Encuestas:** La encuesta es una de las herramientas más utilizadas por los auditores en sistemas, sirve para averiguar opiniones acerca de aspectos informáticos como servicio, actualización, comportamiento de los sistemas, etc.
4. **Observaciones:** Permiten recolectar directamente la información necesaria sobre el comportamiento, el área, las funciones, actividades y operaciones del sistema, el auditor debe observar con cuidado el área auditada.
5. **Muestreos:** El muestro es escoger un grupo pequeño de población, una parte representativa de la población que me permita obtener información necesaria y relevante para sacar mejores resultados.

2.4.3. Reporte

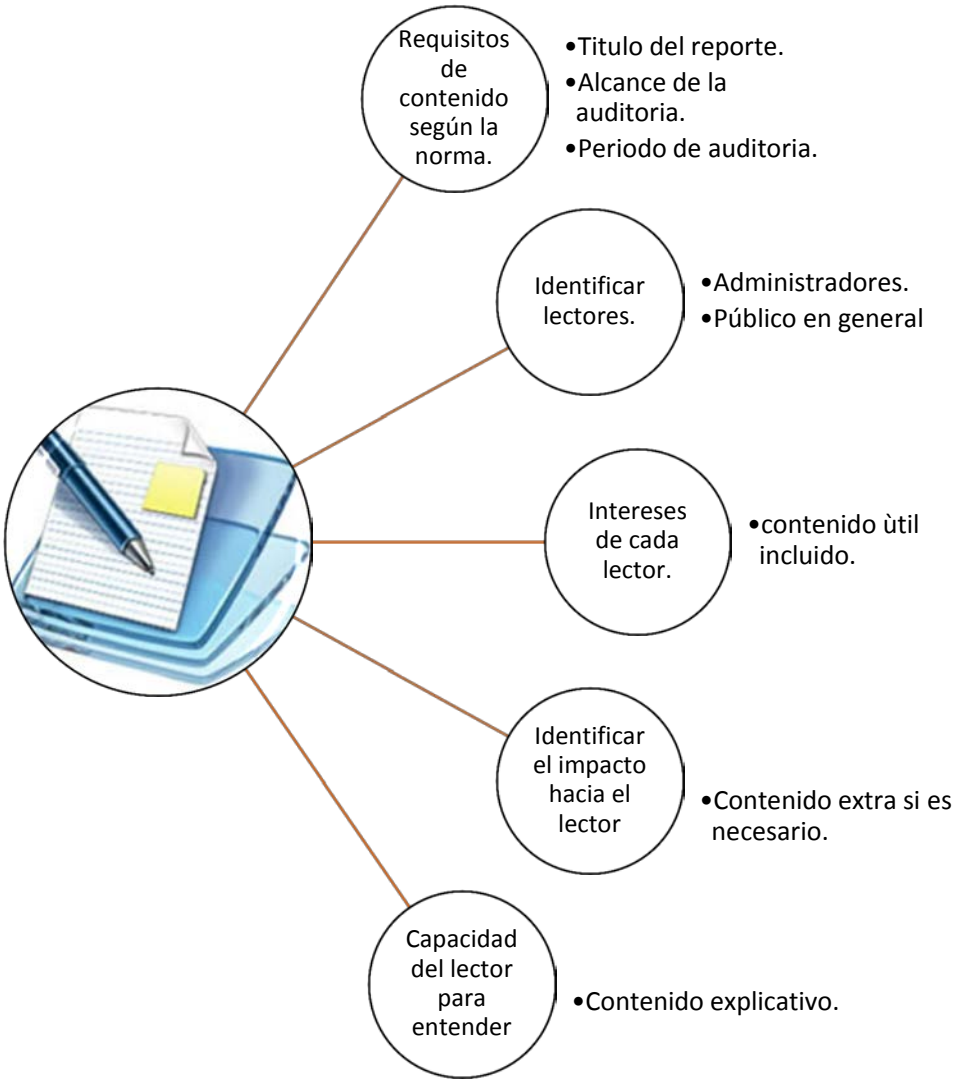
El reporte es la etapa final de la auditoria que comunica los resultados a la empresa auditada, estos resultados de auditoría deben estar presentados de forma clara, concisa y completa, el contenido del reporte puede variar dependiendo del tipo de trabajo que se esté haciendo.

- **Objetivo del reporte.**

El reporte de auditoría se elabora con el objetivo de que el auditor presente formalmente los resultados finales de la auditoria, además debe proporcionar información donde identifique las áreas que necesiten acciones correctivas y recomendaciones; el reporte ayuda al auditor a registrar los hallazgos de la auditoria con la finalidad de dar recomendaciones para realizar las correcciones respectivas.

El reporte debe tener la capacidad de comunicar el alcance de la auditoria, objetivo, resultado y recomendaciones, así como también tiene la capacidad para entregar información que ayude a reducir el riesgo, lograr los objetivos de la empresa y tomar acciones correctivas, por esta razón el reporte debe ser comprensible para todos los usuarios que necesitan la información.

Ilustración 6 Estructura del Reporte.



Fuente: (ISACA, 2015)
Elaborado por: Autoras.

- **Contenido del Reporte de SI.**

Muchos reportes de auditoría de SI incluyen las siguientes secciones, además que algunos elementos son obligatorios según los estándares ISACA[10]:

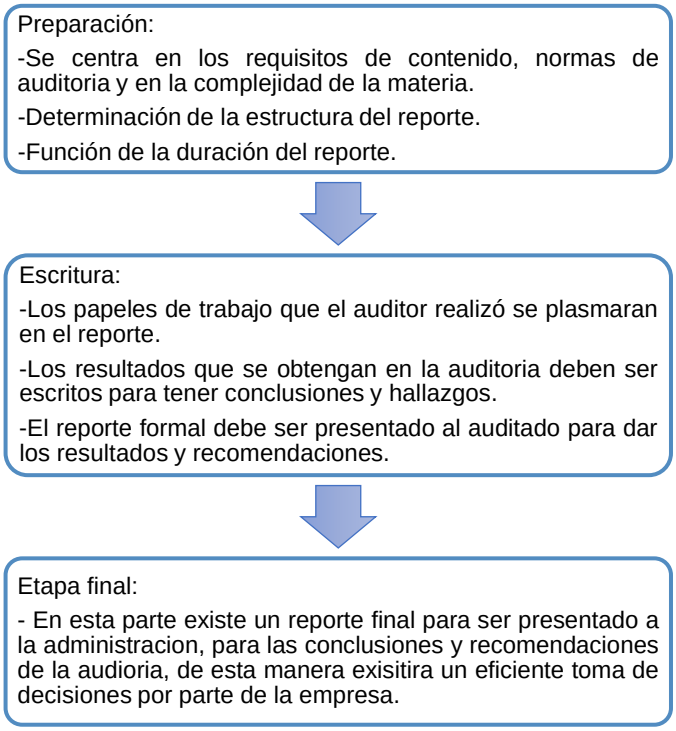
- ✓ Título de la página (la identificación del reporte es obligatorio)
- ✓ Persona que firma y página de transferencia (la firma es obligatoria)
- ✓ Tabla de contenidos (opcional)
- ✓ Introducción (opcional)
- ✓ Resumen Ejecutivo (opcional dependiendo de la extensión y complejidad del reporte)
- ✓ Alcance de Auditoría (obligatorio)
- ✓ Objetivo/s de Auditoría (obligatorio)
- ✓ Metodología de la Auditoría (obligatorio)
- ✓ Resultados de la Auditoría (obligatorio dependiendo de los resultados de la auditoría)
- ✓ Conclusión u Opinión de la Auditoría (obligatorio)
- ✓ Recomendación (obligatorio dependiendo de los resultados de la auditoría)
- ✓ Respuesta de la Administración (obligatorio dependiendo de los resultados de la auditoría)
- ✓ Respuesta del Auditor (opcional)
- ✓ Apéndice (opcional)

- **Proceso de escritura de un reporte.**

El proceso de escritura de un reporte se podrá observar en la ilustración 7.

[10] (Estándar de auditoría y aseguramiento de SI 1401 Reportes, 2014)

Ilustración 7 Proceso de Escritura de un Reporte.



Fuente: (ISACA, 2015)
Elaborado por: Autoras.

2.4.4. Seguimiento.

Es el proceso mediante el cual se determina “la adecuación, efectividad y tiempos de las acciones tomadas por la gerencia sobre las observaciones y recomendaciones informadas” (ISACA, 2014) incluyen las realizadas por auditores externos y otros.

El establecer un proceso de seguimiento permite a la empresa tener una garantía razonable sobre el beneficio óptimo que brinda la revisión realizada por los profesionales cuando las conclusiones de las mismas hayan sido implementadas y la organización reconozca el riesgo de atrasar las recomendaciones al no cumplir su compromiso de implementarlas.

Cabe mencionar que la Gerencia puede o no aceptar el riesgo de corregir la situación que le ha sido informada, sin embargo en caso de aceptación

la Gerencia Ejecutiva debe documentar, aprobar formalmente y comunicar a los encargados del gobierno.

Procedimientos de actividades de seguimiento:

- ✓ Debe existir un rango de tiempo para que la gerencia responda a las recomendaciones.
- ✓ Realizarse una evaluación de las respuestas de la Gerencia dadas.
- ✓ Verificar que las respuestas sean adecuadas.
- ✓ Seguimiento del trabajo, si es adecuado.
- ✓ Comunicar las respuestas excepcionales y no satisfactorias y/o acciones para la Gerencia o encargados del Gobierno.
- ✓ Proceso que permita que la Gerencia acepte el riesgo asociado en caso de que la acción correctiva no se proponga para implementarse o sea retrasada. por parte de la gerencia.

Factores a considerar al determinar los procedimientos adecuados para la etapa de seguimiento:

- ✓ Importancia e impacto de hallazgos y recomendaciones.
- ✓ Cambios en el entorno de SI que afecten la importancia e impacto de hallazgos y recomendaciones.
- ✓ Complejidad que se presenta para corregir la situación reportada.
- ✓ Para corregir la situación reportada se debe tener en cuenta el tiempo, coste y esfuerzo necesarios.
- ✓ En caso de fallar la situación reportada considerar el efecto de la misma.

La gerencia debe ser responsable de implementar las acciones recomendadas en particular cuestiones de alto riesgo y acciones correctivas con plazos de entrega largos, para esto deben actualizar periódicamente a los profesionales.

2.5. Normativa PCIDSS.

2.5.1. Historia de PCIDSS.

Debido a la inseguridad que existe para resguardar los datos como: débiles contraseñas, programas inseguros y numerosos fraudes relacionados con la industria de tarjetas, las seis más grandes marcas de tarjetas de pago (MasterCard, Visa, American Express, Discover y JCB Internacional) colaboraron para crear en el 2004 un conjunto de normas para prácticas seguras de transacciones donde se usan tarjetas de pago. Por lo que formaron el Council de PCI.[11] (Security, 2013)

Al formar el Council de PCIDSS en el 2004 como resultado se obtiene el estándar de seguridad de tarjetas de pago conocido como PCIDSS que ayuda a la protección y resguardo de los datos de las tarjetas de pago; en junio del 2005 debido a los números fraudes relacionados con la industria de tarjetas. El Council de PCI impuso fecha de cumplimiento de la norma para grandes comercios que almacenaban, procesaban y trasmitían datos de tarjetas. (Security, 2013)

Hoy en día debido a las nuevas vulnerabilidades de red y amenazas, el estándar PCIDSS ha evolucionado, mejorado y actualizado para poder combatir con las nuevas vulnerabilidades y amenazas por lo que ahora se aplica en todo tipo de comercios grandes, medianos o pequeños pero que realicen transacciones con tarjetas de pago. (Almacenan, procesan o transmiten datos de tarjetas de pago).

Todos aquellos que juegan un rol en la transacción son responsables de proteger los datos de tarjetas, a través de los requerimientos que presenta

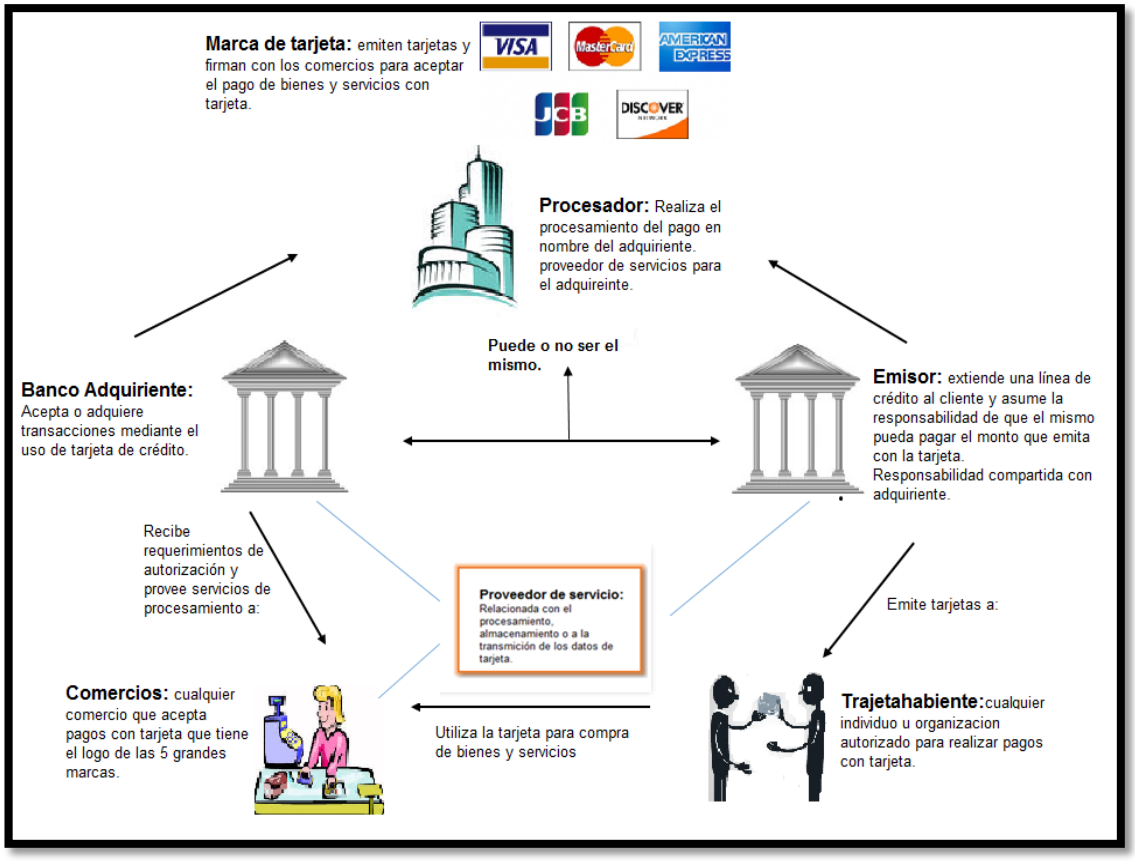
[11] Council de PCI: Según (Security, 2013) “Es el ente responsable de gobernar y crear el estándar de PCI, en donde las organizaciones que manejan pagos con tarjetas y cualquier comercio que acepta tarjetas deben cumplir con esto. “

la norma, las marcas que ayudaron a crear PCIDSS exigen a los comercios el cumplimiento estricto y en caso de incumplimiento tendrá un costo como: penas regulatorias y penalidades, multas de incumplimiento, mayor costo al procesar transacciones con tarjetas de crédito, etc. (Security Awareness, 2013)

2.5.2. Patrocinadores de PCI

La ilustración 8 explica cuáles son los patrocinadores de PCI y que funciones cumplen.

Ilustración 8 Patrocinadores de PCI



Fuente: (Security Awareness, PCIDSS EDUCATION SERIES , 2013)
Elaborado por: Autoras.

2.5.3. Tarjetas de pago.

Las tarjetas de pago o tarjetas de crédito tienen datos que me permiten realizar transacciones, estos datos pueden ser de almacenamiento permitido, los cuales tienen protección requerida y almacenamiento no permitido, los mismos se encuentran ilustrados en el Tabla 5.

Tabla 6 Partes de una Tarjeta de pago o de crédito.

Almacenamiento permitido.	**Almacenamiento no permitido.**
PAN: Es el número de cuenta o número exclusivo de una tarjeta de pago. Generalmente de 16 dígitos.	Banda magnética: Información confidencial, no debe ser almacenada en el sistema del comercio.
Nombre del tarjetahabiente: Individuo autorizado para utilizar la tarjeta.	Código del servicio: Se utiliza para la diferenciación entre intercambios nacionales e internacionales e identificar restricciones de uso.
Fecha de expiración: Evita fraudes.	Código de validación: Es único y está asociado con la tarjeta y el número de tarjeta.

Fuente: (Security Awareness, PCIDSS EDUCATION SERIES , 2013)
Elaborado por: Autoras.

Los datos de almacenamiento permitido deben ser protegidos y resguardados, para poder evitar posibles fraudes y daños al tarjetahabiente, además que se debe evitar que los datos que no son de almacenamiento permitido lleguen a manos de personas malintencionadas ya que son muy valiosos debido a que les permite generar tarjetas de pago falsas y crear transacciones fraudulentas. En la ilustración 9 se puede ver con mayor detenimiento las partes de una tarjeta de crédito.

Ilustración 9 Partes de una Tarjeta de Pago o Crédito.

Fuente: (Security Awareness, PCIDSS EDUCATION SERIES , 2013)
Elaborado por: Autoras.

- **Transacciones con tarjetas de pago**

Según (Security Awareness, 2013) para poder realizar transacciones con tarjeta de pago o de crédito se realiza el siguiente proceso:

- ✓ El tarjetahabiente que es el autorizado para realizar pagos presenta dicho documento al comercio encargado de brindar bienes o servicios para su compra.
- ✓ El comercio desliza la tarjeta por el POS e ingresa el monto y trasmite la autorización necesaria hacia el banco adquiriente,
- ✓ El banco adquiriente envía la información hacia el procesador.
- ✓ El procesador pasa la información al banco emisor y determina si tiene los fondos suficientes para que se realice la transacción rechazando o aprobando la misma.

- ✓ Luego se reenvía del procesador al banco emisor y este hacia el banco adquiriente.
- ✓ El banco adquiriente reenvía la respuesta a la base de datos haciendo que el comercio reciba el número de autorización o rechazo para que se proceda a completar la transacción con la obtención de la firma del tarjetahabiente entregándole una copia del voucher.
- ✓ Se deposita el voucher original con el banco adquiriente el cual acredita o deposita a la cuenta del comercio.
- ✓ El banco adquiriente envía electrónicamente la transacción para el pago a través del procesador.
- ✓ El procesador hace que el banco adquiriente reciba el dinero del banco emisor.
- ✓ Por último el procesador pide al banco emisor que debite de la cuenta del tarjetahabiente el monto de la venta.

Por todo lo mencionado anteriormente se creó el estándar de seguridad de los datos PCI DSS el cual tiene como objetivo, mejorar la seguridad de los datos del titular de la tarjeta de pago, de esta manera se crea un entorno más seguro para todos los que procesan, almacenan o transmiten información de tarjetas, pero en el caso de que no se cumpliera con la norma puede existir para los comercios, penas regulatorias, multas de incumplimiento, mayor costo al procesar transacciones con tarjeta de crédito e incluso se podría perder el permiso de realizar transacciones con tarjeta, además que se mancharía la reputación del negocio y la confianza del tarjetahabiente, por lo que la norma establece requerimientos que se deben cumplir.

Estos requerimientos se encuentran plasmados dentro de seis objetivos los cuales se mostraran en la tabla 6.

Tabla 7 Objetivos de PCI DSS.

Objetivo 1.- Desarrollar y Mantener una red segura.	
Requisito 1:	Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas.
Requisito 2:	Los parámetros de seguridad y contraseñas de sistemas provistos por los proveedores no utilizarse.
Objetivo 2.- Proteger los datos del titular de la tarjeta.	
Requisito 3:	Proteja los datos que fueron almacenados del titular de la tarjeta.
Requisito 4:	La transmisión de los datos de los titulares de tarjetas codificar a través de redes públicas abiertas.
Objetivo 3.- Desarrolle un programa de administración de vulnerabilidad.	
Requisito 5:	Utilice y actualice regularmente el software o el antivirus.
Requisito 6:	Desarrolle y mantenga sistemas y aplicaciones seguras.
Objetivo 4.- Implemente medidas sólidas de control de acceso	
Requisito 7:	Conforme la necesidad de conocer que tenga la empresa restrinja el acceso a los datos de los titulares de las tarjetas.
Requisito 8:	A cada persona que tenga acceso a equipos asigne una ID única.
Requisito 9:	Restrinja el acceso físico a datos de titular de tarjetas.
Objetivo 5.- Supervise y pruebe las redes con regularidad.	
Requisito 10:	Rastree y supervise todo acceso a

	los recursos de red y datos de titulares de tarjetas.
Requisito 11:	Pruebe con regularidad los sistemas y procesos de seguridad.
Objetivo 6.- Mantenga una política de seguridad de la información	
Requisito 12:	Mantenga una política que aborde la seguridad de la información para empleados y contratistas.

Fuente: (Norma PCI DSS, Noviembre 2013)
Elaborado por: Autoras.

Estos requerimientos deben ser cumplidos por todos los negocios que se realicen transacciones con tarjeta de pago sin importar el tamaño; los comercios se clasifican desde el Nivel 1 que son los más grandes hasta el Nivel 4 que considerados como pequeños.

- **Nivel 1.**

Según (Domínguez Torres, 2007) en el nivel 1 se considera cualquier comercio que procese más de 6 millones de transacciones por año, de acuerdo a Visa y MasterCard, y 2.5 millones de transacciones, según American Express, además que haya sufrido algún tipo de daño donde los datos quedaron comprometidos o cualquier comercio que Visa, MasterCard y American Express considere como nivel 1.

Según (Security Standar, Noviembre 2013) todos los comercios de este nivel deben tener un Reporte de cumplimiento, este se consigue mediante las Auditorias de seguridad anuales y los escaneos trimestrales de vulnerabilidades los cuales se hablaran más adelante, además que el reporte de cumplimiento debe ser revisado por un QSA[12] o también se puede hacer una Auditoria interna, por lo que el Auditor interno antes de

[12] **QSA:** Según (Security, Standards Council, s.f.) son organizaciones que han sido calificados por el Consejo para evaluar el cumplimiento de la norma PCI DSS Asesores de Seguridad Calificados, son empleados de estas organizaciones que han sido certificados por el Consejo para validar el cumplimiento de una entidad con el PCI DSS."

realizar su trabajo debe tomar el entrenamiento adecuado y estar certificado por el Council de PCI. Para poder proceder a la auditoria interna el reporte debe estar firmado por el oficial de la compañía y el banco adquiriente debe estar de acuerdo.

- **Nivel 2.**

Se clasifica como nivel 2 según los criterios de Visa y MasterCard todos los comercios que realicen entre 1 millón y 6 millones de transacciones por año sin importar el medio por el cual se reciba y según American Express se clasifican como comercio de nivel 2 los que procesan entre 50,000 a 2.5 millones de transacciones.

Según (Security Awareness, PCIDSS EDUCATION SERIES , 2013) todos los comercio de nivel 2 deben realizar un cuestionario anual de autoevaluación, realizar escaneos trimestrales de vulnerabilidades, realizar una auditoria externa y debe estar firmada por el oficial de la compañía, todas estas actividades hace el comercio de nivel 2.

- **Nivel 3.**

Los comercios de nivel 3 se les consideran a cualquier negocio que realice 20.000 a 1 millón de transacciones por año según Visa y MasterCard, mientras que American Express nos dice que se considera como nivel 3 cualquier comercio que procese entre 50.000 transacciones al año.

Los de nivel 3 deben cumplir los mismo requisitos que los de nivel 2, cuestionarios anules de autoevaluación, escaneos trimestrales de vulnerabilidad y auditorías internas firmadas por el oficial de la compañía.

- **Nivel 4.**

Se considera de nivel 4 el resto de comercios que no se encuentre entre las cantidades de transacciones mencionadas en los niveles anteriores, que procesen menos de 20.000 transacciones al año con MasterCard E-Commerce y menos de 1 millón de transacciones con MasterCard.

Los comercios de nivel 4 deben realizar un cuestionario anual de Autoevaluación que debe ser completado internamente y firmado por el oficial de la compañía, además se realizará el escaneo trimestral de vulnerabilidades.

El escaneo trimestral de vulnerabilidades debe ser obligatorio para todos los niveles de comercios, este debe ser elaborado por un Proveedor Autorizado para escanear (ASV)[13].

Según los niveles anteriormente mencionados los comercios tienen que hacerse responsables de presentar ciertas evaluaciones como:

- **Escaneos de vulnerabilidades.**

Son utilizados para determinar si es que existe alguna debilidad en las conexiones de internet o sitios Web de los comercios, busca cualquier problema de seguridad de los datos que puedan traer problemas mayores como fuga de información, entre otros, además el escaneo de vulnerabilidades revisa que los sistemas se encuentre configurados adecuadamente para que resguarden los datos de tarjetas.

- **Cuestionarios de Autoevaluación (SAQ)**

Como pudimos observar todos los niveles de comercio deben realizar el cuestionario anual de autoevaluación para poder cumplir con la normativa PCIDSS, este cuestionario se debe realizar según las circunstancias que se presenten por lo que existe varias versiones del mismo.

[13] **Proveedor Autorizado para escanear (ASV):** Según (Security, Standards Council, s.f.)"Son organizaciones que validan los requisitos de PCI DSS mediante la realización de análisis de vulnerabilidades de Internet, frente a los entornos de los comerciantes y prestadores de datos."

Existen 5 versiones del cuestionario de autoevaluación (SAQ) y para poder usarlos de manera adecuada se debe conocer cuál es el modelo de negocio que se va observar, si se identifica correctamente la versión que se utilizará, el comercio puede reducir el número de preguntas que debe contestar.

- **Versiones de SAQ:**

SAQ A: El cuestionario de autoevaluación A, se debe usar solo en los casos de que las transacciones con tarjetas de pago no se realicen cara a cara con el cliente, cuando los proveedores realicen procesos de datos de tarjetas y que estos cumplan con PCI, por último se utiliza este cuestionario cuando la información de los datos de tarjetas se imprimen y no son electrónicos.

SAQ B: Se elaboran este tipo de cuestionario los comercios que utilizan impresoras conectadas a internet, cuando los datos de tarjetas no sean transmitidos por la red, además solo deben retener copia de los voucher o reportes ya que no almacenan datos de manera electrónica si no física.

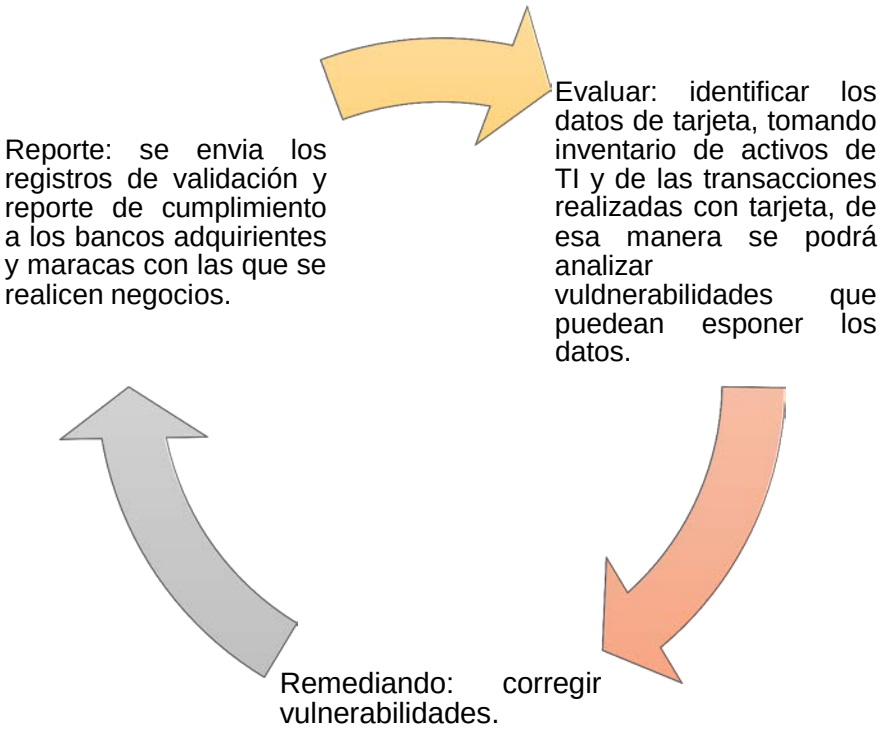
SAQ C-VT: Se debe utilizar este cuestionario de autoevaluación cuando los datos sean procesados en lectores virtuales de tarjetas de crédito o terminales virtuales, los mismo deben ser obtenidos de un proveedor de servicios que se encuentre autorizado por PCI DSS, además debe estar conectado una computadora y no debe estará en otra ubicaciones o sistemas dentro de la organización, quiere decir que debe ser una solo ubicación no debe rotar, también se debe utilizar cuando los comercios no tengan programas que almacenen datos de tarjetas, no debe existir almacenamiento electrónico de los datos de tarjetas de pago.

SAQ C: Cuando se utiliza una aplicación de pago que esté conectada a internet se debe realizar este tipo de cuestionario, además los comercios no deben almacenar los datos, solo retienen copias de los voucher o

recibos, por ningún motivo deben almacenar los datos de manera electrónica y el negocio utilizará técnicas seguras para las aplicaciones de pago.

SAQ D: Contienen un conjunto de requerimiento de PCI, deben ser validados por los QSA.

Ilustración 10 El Ciclo de cumplimento de PCI DSS



Fuente: (Security Awareness, PCIDSS EDUCATION SERIES , 2013)
Elaborado por: Autoras.

2.5.4. Alcance de PCI DSS

La mayoría de los aspectos de PCI DSS son ya una mejor práctica de seguridad y no es cierto que sea difícil de cumplirlos. La norma es un sistema eficaz para las empresas, comerciantes y procesadores que aseguren toda la información sensible.

Requerimientos de seguridad de PCIDSS:

- ✓ El ambiente de datos de tarjeta es la parte de la red que posee datos de tarjeta o datos de autenticación sensibles.
- ✓ PCI DSS como las marcas de tarjetas de crédito han recomendado no almacenar los datos de las tarjetas de crédito tanto a comercios como procesadores. No es permitido el almacenamiento de datos de la banda magnética de la tarjeta en caso de necesariamente necesitar el almacenamiento de los datos de una tarjeta estos deberían estar encriptados o ilegibles.

A medida que son desarrolladas las aplicaciones forman parte de la certificación de PCI. La marca visa indicó en el 2010 que todas las aplicaciones de pago "of the shelf"[14] deben ser certificadas por PCI DSS

PCI DSS no se usa a las aplicaciones de pago proveída en los módulos que incluyen una "línea base" en caso de que es el único que realice funciones de pago (debe ser revisada por un PA QSA). Si los módulos realizan funciones de pago PCI DSS se aplica a esos módulos.

PCI DSS no se aplica a las aplicaciones de pago desarrolladas por los comerciantes y proveedores de servicios si se utiliza solo en la casa (no se vende, distribuye, o con licencia a un tercero), ya que esta aplicación de pago está cubierta dentro de la certificación de PCI del comercio o proveedor de servicios.

- ✓ Se define al alcance como el sistema en el que se "almacena, proceso o transmite" datos de tarjeta y sistemas interconectados. Se cree erróneamente que al dejar de almacenar datos se evita el problema del cumplimiento pero el hecho de que los sistemas interconectados también están dentro del alcance, y estos forman parte de los activos a ser revisados por lo que no se trata solo del almacenamiento de los datos de los tarjetahabientes.

[14] **Aplicaciones de pago Of the Shelf:** Son aplicaciones de pago que se venden, distribuyen o licencia a terceros y se instalan "Off the Shelf", es decir sin demasiada personalización por proveedores de software.

- ✓ El tiempo invertido al desarrollar un diagrama de flujo preciso y detallado hará la certificación y cumplimiento más relajado, rápido y barato.
- ✓ Los comercios son los responsables que los proveedores en caso de outsourcing[15] de los servicios estos cumplan con PCIDSS.
- ✓ Hay datos que por lo general ni se conoce que están almacenados por lo que se corre el riesgo que sean robados ya que una gran variedad de herramientas (comerciales y libres) están disponibles para ayudar a localizar datos de tarjeta, mismas que se pueden correr periódicamente sobre todos los sistemas de la red de la organización, incluyendo los que estén fuera del alcance para verificar que no se tengan almacenados datos inapropiadamente.
- ✓ No almacenar datos es un excelente medio para reducir el riesgo. Pero según las estadísticas aún es posible para los ladrones robar datos de tarjeta, lo que trae como consecuencia por que los sistemas están en el alcance y por qué no se debe almacenar datos de tarjeta.

Minimizar el alcance y sus beneficios

Las mejores prácticas contenidas en PCI DSS son pasos que todos los negocios deben implementar para proteger los datos sensibles y la continuidad de operaciones. Si bien es cierto existen muchos productos y servicios disponibles para cumplir los requerimientos de seguridad y cumplir con PCI sin embargo las personas dicen que PCI es muy difícil pero en realidad es porque quieren decir que no es barato pero los costos de no cumplir y los riesgos del negocio pueden exceder el costo de implementar PCIDSS ya que estos costos pueden incluir penalidades, comisiones legales, decremento en el precio de las acciones, y pueden perder el negocio. Implementar PCI DSS en el negocio debe ser la forma en que la empresa logra una estrategia de

[15] **Outsourcing:** Tercerizar, es cuando una empresa transfiere recursos hacia otra empresa externa a través de un contrato con, la finalidad de que la compañía subcontratada desarrolle actividades en nombre de la primera empresa.

seguridad empresarial por lo que las acciones de PCI deben ser normales para la operación del negocio.

Del cumplimiento de PCIDSS

Los consultores de seguridad y el staff de cumplimiento de los bancos trabajan conjuntamente para asegurar que los hallazgos se han remediado de manera correcta para su cumplimiento. En caso de que se trabaje con un QSA ellos serán los únicos que pueden generar el reporte de cumplimiento.

- ✓ Identificar lo que se requiere para cerrar los hallazgos identificados.
- ✓ Reportar los planes y las fechas apropiadas de remediación.
- ✓ Cambios a los proceso
- ✓ Cambio en las políticas
- ✓ Documentación adicional
- ✓ Eliminación de datos
- ✓ Cambios en las configuraciones de los sistemas
- ✓ Cumplimiento continúo.

Proceso anual donde se da seguimiento a que todos los requerimientos siguen cumpliéndose.

- ✓ Cumplir por primera vez no significa que se cumpla siempre, el cumplimiento es un proceso continuo que se debe validar y rectificar siempre como buena práctica.
- ✓ Deben existir procesos de monitoreo de forma que siempre se pueda estar al tanto del progreso de cumplimiento que tiene la normativa.
- ✓ Cuando el cumplimiento del negocio es constante la inclusión a nuevas versiones de PCI será más sencillo.

- ✓ Se evitaran las certificaciones fallidas al estar en cumplimiento constante.

PCIDSS por que aplicarlo y para que nos sirve.

El cumplimiento de los programas de las marcas de tarjetas es mucho más que un proyecto con un principio y final es un proceso continuo de evaluación, remediación y presentación de informes, el cumplimiento se resuelve mejor por un equipo multidisciplinario ya que en caso de compromisos con las tarjetas de pago o de los datos se llegaría a impactos financieros y la percepción negativa de la marca, que afecta de toda la organización.

Responsabilidades de un QSA

Se dice que cada vez que se cumple con PCIDSS se requiere una evaluación por un asesor de seguridad calificado QSA, muchos contratan a un QSA con el fin de beneficiarse de su experiencia y conocimiento especializado en PCIDSS durante la visita en sitio y evaluación de la seguridad. El QSA también hace que sea más fácil de desarrollar y obtener la aprobación para un control de compensación. PCIDSS ofrece la opción de un comerciante realice una evaluación interna, con la firma de un oficial en el cumplimiento si el banco adquiriente y/o banco del comercio está de acuerdo.

Las amenazas de seguridad con continuas y cada vez más fuertes, por lo que se van haciendo más sofisticadas cada día, por lo que los esfuerzos de cumplimiento de PCI deben ser un proceso continuo de evaluación y remediación para garantizar la seguridad de los datos de los tarjetahabientes.

De los compromisos detectados.

Los compromisos son en su mayoría detectados por un tercero y cuando mejoramos las tecnologías de detección de incidentes mejora el tiempo para responder ante el mismo.

Por qué no almacenar datos de tarjeta.

Cuando los datos de los tarjetahabientes no son almacenados los atacantes solo puede reunir una cantidad mucho menor de estos datos pero los datos en movimiento aún se capturan a menudo mediante el uso de programas de malware[16].

Después de un compromiso de datos las marcas de tarjetas afectadas los bancos de transformación o de organizaciones de salud, solicitan la investigación de la empresa para ofrecer una ventana de exposición de datos. Todas las cuentas afectadas (las transacciones) que fueron procesadas por la entidad comprometida se entregan a la empresa investigadora para generar un número muy cercano al real y cuantificar el número verdadero de cuentas comprometidas.

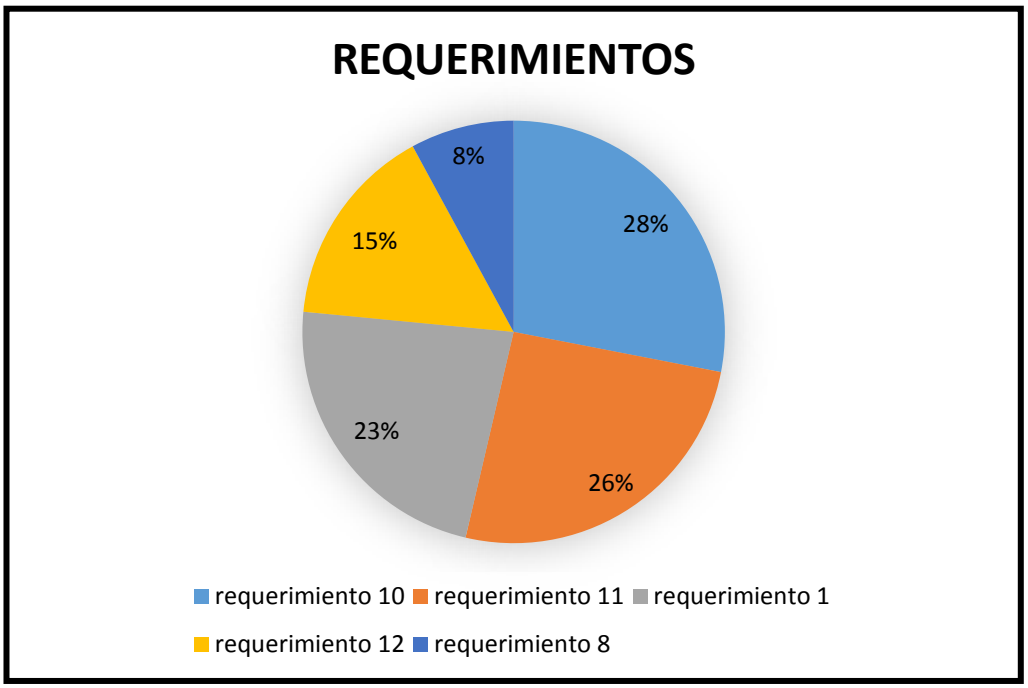
Requerimientos que mayoritariamente los comercios no cumplen

- ✓ "Req. 10: Rastrear y supervisar todos los accesos a los recursos de red y de datos de los titulares de tarjetas de pago. 99.2%
- ✓ Req. 11: Probar con regularidad los sistemas y procesos de seguridad. 98.4%
- ✓ Req. 1: Instalar y mantener una configuración de firewalls que proteja los datos de los titulares de tarjetas. 97.5%
- ✓ Req. 12: Mantener una política que permita abordar la seguridad de la información para todo el personal.95.1%
- ✓ Req. 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora. 92.6%."

(Security Awareness, PCI DSS EDUCATION SERIES, 2013)

[16] **Malware:** "Malicious software", todo tipo de programa que engloba los programas y códigos informáticos maliciosos que dañan un sistema o causan un mal funcionamiento.

Ilustración 11 Requerimientos que mayoritariamente los comercios no cumplen.



Fuente: (Security Awareness, PCI DSS EDUCATION SERIES, 2013)
Elaborado por: Autoras.

Si bien cómo podemos observar en el grafico anterior dentro de los requerimientos que mayoritariamente las empresas no logran cumplir se encuentra el requerimiento 8. “Asignar una ID exclusiva a cada persona que tenga acceso por computadora.” Mismo que nos encontramos analizando por lo que podríamos decir que tenemos una prueba más de lo imperativo de llevar a cabo el cumplimiento solido de la asignación de una identificación única a cada empleado (persona) que tenga el acceso a computadores de la empresa u organización de esta forma se garantizara

que cada una de estas personas sean responsables propias de cada uno de sus actos.

2.5.5. Requerimientos 7, 8, 9 De PCI DSS

2.5.5.1. Requerimiento 7: Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.

Este requerimiento asegura a la empresa que a los datos importantes de las tarjetas solo pueda acceder personal autorizado, además el acceso a los mismos debe ser de acuerdo a la necesidad de conocer[17] y según la responsabilidad que tenga el usuario según su cargo.

PCI crea este requerimiento en la normativa con la finalidad de que se restrinja el acceso a personas no autorizadas de los datos de los titulares de tarjetas, ya que si no se hace esta limitación existirá más riesgo de uso malicioso de los datos, además las personas autorizadas deben de tener una limitación de acceso a los datos debido a que se puede dar un mal manejo por falta de experiencia o por otro tipo de fines.

Tabla 8 Requerimiento 7 "Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa".

7.1 Limite el acceso a los datos de tarjeta.	• El personal debe tener una restricción para el acceso. • Por seguridad no se debe permitir acceder a toda la información. • Acceso de acuerdo a sus necesidades.
7.2 Restringir el acceso "Need to know"	• Establezca un sistema de control de acceso que restrinja el acceso en base a

[17] **Necesidad de conocer:** Según (Security Awareness, PCIDSS EDUCATION SERIES , 2013) "la necesidad de conocer es cuando se otorga derechos a la menor cantidad de datos y privilegios necesarios para realizar una tarea".

	la necesidad del usuario de conocer.
7.3 Documentar las políticas y procedimientos operativos de seguridad.	• De forma que se restrinja el acceso a los datos del titular de la tarjeta. • Todas las partes afectadas tengan conocimiento.

Fuente: (Norma PCI DSS, Noviembre 2013)
Elaborado por: Autoras.

2.5.5.2. Requerimiento 8: Identificar y autentificar el acceso a los componentes del sistema.

Este requerimiento, trata acerca de que se debe asignar una ID exclusiva y única para cada usuario que se encuentra laborando dentro del comercio, de manera que cada uno se hará responsable de sus actos, por lo tanto el usuario poseerá una contraseña única, segura e intransferible de eso modo una vez que ingresa el ID y contraseña, el sistema podrá verificar que los datos ingresados pertenecen a dicho usuario, evitando actos maliciosos de terceros. Así como también el desarrollo métodos de seguridad por parte del comercio para evitar que durante la transferencia y almacenamiento de datos estos puedan ser robados.

Tabla 9 Requerimiento 8 "Identificar y autentificar el acceso a los componentes del sistema."

8.1 Proveer un único usuario.	Implementar políticas y procedimientos para la correcta administración de la identificación de los usuarios al momento del ingreso al sistema. (Asigne una ID única).
8.2 Autenticar a todos los usuarios.	Correcta administración de IDs y contraseñas, usando: ✓ Contraseña o frase de seguridad. ✓ Tarjeta inteligente o dispositivo token[18]

[18] **Token:** Según (Security, Standar Council, 2010) "un token es un grupo de caracteres proporcionado por un hardware o software que funciona con un servidor de autenticación".

	✓ Rasgo biométrico como por ejemplo la palma, huella, etc**.**
8.3 Implemente doble factor de autenticación para usuarios remotos.	Se requiere la autenticación a través de dos métodos (contraseña, tarjeta inteligente y/o rasgo biométrico) cuando se requiera el acceso desde una red externa.
8.4 Documentar y Comunicar los procedimientos y políticas de seguridad a todos los usuarios	• Lineamientos y sugerencias para la selección del método de autenticación. • Protección de credenciales de autenticación. • Instrucción para no seleccionar contraseñas usadas anteriormente. • Cambio de contraseña cada 90 días y ante la sospecha de posible robo.
8.5 No permitir el uso de IDs y contraseñas de grupo.	No deben ser compartidas ni genéricas para ninguna actividad dentro del sistema y una vez detectada esta situación se deberá desactivar y/o eliminarse dichos IDs y contraseñas.
8.6 Otros mecanismos de autenticación.	Pertenecer a una sola cuenta y no compartirse entre varias, implementar controles físicos y lógicos que garanticen el correcto uso de dichos métodos de autenticación.
8.7 Restricción de acceso a cualquier base de datos que contengan datos del titular de la tarjeta.	Se logra a través de una correcta autenticación de los usuarios, de esta manera se prevé el ingreso no autorizado o malintencionado a bases de datos; de esta autenticación se excluye a los

	administradores de las bases de datos (DBA) ya que estos podrán accederlas directamente.
8.8 Políticas y procedimientos de información deben estar documentados e implementamos	Deben estar documentados e implementados, además que sean de conocimiento para todo el personal y usuarios.

Fuente: (Norma PCI DSS, Noviembre 2013)
Elaborado por: Autoras.

2.5.5.3. Requerimiento 9: "Restrinja el Acceso Físico a los Datos del Titular de la Tarjeta"

Se debe tener en consideración que accesos físicos a datos o sistemas que almacenen datos de titulares de tarjetas corren el riesgo de que existan accesos a sus dispositivos y datos, eliminación de sistemas o copias en papel y deben ser restringidos correctamente.

Para esta restricción es necesario hacer una diferenciación entre:

Empleados: Personal que está presente en las instalaciones de la entidad y labora tiempo completo, parcial o temporal, además de contratistas y consultores.

Visitante: Personas que necesiten ingresar a la organización durante un corto tiempo, por lo general no más de un día, entre estos proveedores, invitados de algún empleado, personal de servicio o cualquier otra persona.

Medios: Todos los medios que contienen datos de titulares de tarjeta ya sean estos en papel o electrónicos.

Tabla 10 Requerimiento 9: "Restringir el acceso físico a los datos del titular de la tarjeta".

9.1 Utilizar controles	Para limitar y supervisar el acceso físico a

de acceso a las instalaciones.	los sistemas del entorno de datos de titulares de tarjetas, utilice controles de entrada a la empresa apropiados.
9.2 Identificación del personal	Desarrollar procedimientos que permitan distinguir fácilmente a los empleados y a los visitantes sobremanera en las áreas donde se pueda acceder a datos de titulares de tarjetas.
9.3 Gafetes a todos los visitantes	Controle el acceso físico de los empleados a las áreas confidenciales.
9.4 Utilice bitácoras para los visitantes	Implemente procedimientos para identificar y autorizar a los visitantes su permiso previo el ingreso a la organización y a las diferentes áreas.
9.5 Almacene los respaldos en un lugar seguro	Proteja físicamente todos los medios.
9.6 Asegure todo los medios impresos y digitales	Lleve un control y proteja físicamente todos los medios ya que si no se protegen los datos de titulares de tarjetas mientras están en medios extraíbles o portátiles son susceptibles de revisiones copias o análisis no autorizados.
9.7 Mantener un control de distribución de medios	Lleve un control estricto sobre la distribución interna o externa de cualquier tipo de almacenamiento y la accesibilidad de medios que contenga datos de titulares de tarjetas.
9.8 Requiere aprobación para	Destruya los medios cuando ya no sea necesario guardarlos por motivos

mover el medio	comerciales o legales. Asegurarse que la gerencia apruebe todos los medios que contengan datos de titulares de tarjetas que se muevan desde un área segura.
9.9 Mantener control sobre el almacenamiento de medios	Proteja los dispositivos[19] que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta para proporcionar contra alteraciones y sustituciones Lleve un control estricto sobre el almacenamiento y accesibilidad de los medios.
9.10 Destruya los medios que contengan datos de tarjeta	Destruya los medios que contengan datos de titulares de tarjetas cuando ya no sea necesario para el negocio o por motivos legales.

Fuente: (Norma PCI DSS, Noviembre 2013)
Elaborado por: Autoras

[19] **Dispositivos:** Un dispositivo de almacenamiento de datos es un accesorio que se utiliza para grabar o almacenar datos electrónicos. Un dispositivo de almacenamiento de datos genérico utilizado en una computadora puede ser o no extraíble. Los dispositivos de almacenamiento de datos que se utilizan con un equipo generalmente incluyen una unidad de disco duro y una grabadora de CD/DVD. Otros tipos de dispositivos de almacenamiento de datos incluyen una unidad de memoria extraíble, una unidad de disquete y una unidad de cinta. (www.wordforence.com).

CAPÍTULO III

3. EVALUACIÓN DEL NIVEL DE CUMPLIMIENTO DE LA NORMA EN LOS REQUERIMIENTOS 7, 8, 9 DE CORAL HIPERMERCADO RACAR PLAZA.

Carta de Auditoria a Coral Hipermercado Racar Plaza.

Cuenca, 1 de Octubre del 2015.

Señor Ángel Ortiz
PRESIDENTE
CORAL HIPERMERCADO.

Estimado señor:

En mi carácter de Director de Auditoria, tengo el agrado de poner a su disposición el servicio profesional para satisfacer las necesidades de la empresa vinculadas con la Auditoria de Sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCI DSS de Coral Hipermercado Racar Plaza con corte a junio 2015.

El objetivo del trabajo consistirá en emitir una opinión sobre el Nivel de cumplimiento de la Normativa de seguridad de los datos de los titulares de las tarjetas de pago (PCI DSS) de los requerimientos 7, 8, 9 de manera que permita a la empresa lograr el efectivo resguardo de la información, además de mejorar la gestión y toma de decisiones.

El examen para tal propósito será realizado de acuerdo a las Normas de Auditoria en sistemas de ISACA, la cual requiere que la auditoria sea planeada y ejecutada para verificar el cumplimiento de los requerimientos de la norma PCI DSS.

El trabajo se realizará en las siguientes etapas:

Etapa 1: **La planificación: se efectuará:**

- ✓ Entendimiento del negocio de Coral Hipermercado.
- ✓ Universo auditable de los sistemas de Coral Hipermercado.
- ✓ Evaluación del riesgo del universo auditable de Coral Hipermercado.
- ✓ Formalizar el plan de auditoría.

Etapa 2: **Ejecución: se realizará:**

- ✓ Programas de auditoria de los requerimientos 7, 8, 9.
- ✓ Papeles de trabajo de los requerimientos 7, 8, 9.

Etapa 3: **Informe Final: se presentará:**

- ✓ Resultados de la auditoria al cumplimiento de los requerimientos 7, 8, 9 de la norma PCI DSS a Coral Hipermercado.
- ✓ Conclusiones y recomendaciones.

Agradeciendo la oportunidad para presentar esta propuesta, anexamos una copia de esta carta para poder contar con su aprobación.

Atentamente,

Ing. Paúl Adrián Ochoa Arévalo.
Director de Auditoria.

3.1. Planificación de la Auditoria a Coral Hipermercado Racar Plaza.

3.1.1. Entendimiento del negocio de Coral Hipermercado Racar Plaza.

Coral hipermercado es uno de los supermercados más grandes a nivel nacional, a más de proporcionar variedad de productos a precios accesibles para mayoristas y personas naturales en general brinda varios servicios dentro de sus centros comerciales lo que caracteriza a la empresa con un alto grado de efectividad y éxito.

Dentro de sus objetivos organizacionales constan:

- **Objetivo general.**
  - ✓ Ser el líder del mercado.
  - ✓ Generar mayores utilidades.

- ✓ Lograr una mayor participación en el mercado como Coral Hipermercados.
- ✓ Ser reconocido por la frase “de todo y más barato”.
- ✓ Incrementar la cadena de Coral Hipermercados a nivel nacional.

- **Objetivos específicos.**

  - ✓ Aumentar las ventas mensuales en un 20%.
  - ✓ Obtener una rentabilidad anual del 25%.
  - ✓ Lograr una participación de mercado del 20% para el segundo semestre del 2016.
  - ✓ Producir un rendimiento anual del 14% sobre la inversión.
  - ✓ Abrir la tienda Coral Hipermercado en Manta para el segundo semestre del 2016.
  - ✓ Abrir 3 tiendas adicionales en el país para el cuarto trimestre del 2017.

(Quinde & Cedillo, 2015)

- **Misión.**

Gerardo Ortiz e hijos Cía. Ltda. Tiene como misión, “Satisfacer las necesidades actuales de nuestros clientes, apoyados en el más amplio surtido de productos, en las mejores marcas, al mejor precio, con calidad de servicio y con atención personalizada.”

(Corporación Gerardo Ortiz, 2010)

- **Visión.**

La visión de la compañía Gerardo Ortiz e hijos es de “Ser una empresa reconocida por exceder las expectativas de nuestros clientes mediante liderazgo, innovación y desempeño sobresaliente de largo plazo.”

(Corporación Gerardo Ortiz, 2010)

- **Planes de negocios anuales y futuros.**

La empresa Coral Hipermercado se proyecta en un futuro, mantener el uso del Switch transaccional[20] porque es más eficiente contratar este servicio que el disponer de un dispositivo POS por cada punto de venta. La exigencia bancaria les ha solicitado hasta enero del 2016 que las transacciones se puedan realizar con la tecnología EMV (tarjetas con chip), para ello se está desarrollando una nueva versión de aplicaciones para el punto de venta con tecnología JAVA[21] como Front End.

- **Proceso crítico:**

Uno de los procesos de Coral Hipermercado que se necesita analizar con profundidad es el de cómo realizar una venta segura a través de las tarjetas de pago.

1. Los encargados de realizar el cobro con tarjeta de pago son los cajeros:

Son los que tienen que asegurarse de que el dueño siempre esté presente durante la transferencia, además de solicitar la entrega por parte del cliente de un certificado de identidad, el voucher debe estar firmado, con el número de cédula y el teléfono, también deben verificar que las tarjetas no estén rotas o adulteradas y que la firma del voucher sea igual al de la cédula.

2. Existen dos opciones para el cobro con tarjetas de pago dentro de la empresa:

El P.O.S: Compuesto por Medianet, Datafast y el P.O.S del Banco del Austro, los cajeros utilizan cuando el Switch transaccional, que fue creado

[20] **Switch transaccional:** Es capaz de realizar transacciones, cuyos resultados es el depósito del dinero a la empresa participante, maneja el concepto de servicio, ya que se configura para brindar servicios al tarjetahabiente.
[21] **JAVA:** Según (JAVA , 2015) "es la base para prácticamente todos los tipos de aplicaciones de red, además del estándar global para desarrollar y distribuir aplicaciones móviles y embebidas, juegos, contenido basado en web y software de empresa. Java le permite desarrollar, implementar y utilizar de forma eficaz interesantes aplicaciones y servicios."

por la empresa, no funciona, está en mantenimiento o se paga con tarjeta Cuotafácil.

El procedimiento al utilizar el P.O.S es:

- ✓ Insertar la tarjeta en la ranura del P.O.S.
- ✓ Al insertar la tarjeta si es que esta tiene chip, no se debe retirar o mover mientras se haga la venta o podría ocasionar transacción fallida o se anulará, el P.O.S le indicará cuando debe retirarse la tarjeta.
- ✓ Si existe algún error en el proceso de lectura de chip el P.O.S se solicitará que se deslice por el lector de banda y se continuará con el proceso habitual.
- ✓ Se ingresa los cuatro últimos dígitos de la tarjeta y pulse ENTER.
- ✓ Se ingresa el código de seguridad de la tarjeta.
- ✓ Se ingresa la base imponible (0%, 12%) y pulse ENTER.
- ✓ Esperar la respuesta del P.O.S

(Corporación Gerardo Ortiz, 2010)

El Switch Transaccional: Este software es creado por la empresa y acepta tarjetas afiliadas al establecimiento excepto la tarjeta Cuotafácil que solo puede ser procesa por Medianet como se mencionó anteriormente.

El proceso que se debe realizar para una transacción con el Switch transaccional es:

- ✓ Seleccionar la opción otros bancos dentro del sistema autorizador.
- ✓ Ingresar el número de BIN de la tarjeta.
- ✓ Ingresar el CVV o código de seguridad de la tarjeta, luego seleccionar aceptar.
- ✓ Aparecerá un mensaje que indique si se debe o no deslizar la tarjeta por el Switch.

- ✓ En la ventana del sistema autorizador aparece el valor de la factura.
- ✓ Se debe verificar si el monto de pago con la tarjeta es parcial o total.
- ✓ Se coloca el valor y presionamos aceptar.
- ✓ Se selecciona tipo crédito (corriente o diferido).
- ✓ Si se selecciona diferido se habilita el botón plan pagos que les permite colocar cuantos meses de diferido desea. (tres meses sin intereses, 6 meses hasta 24 meses con intereses).
- ✓ Seleccionar el botón enviar.
- ✓ Se espera la respuesta del autorizador, en caso de ser aprobada se imprime el voucher y se hace firmar por el cliente el original y se entrega la copia.

(Corporación Gerardo Ortiz, 2010)

- **Modelo de Negocio.**

El modelo de negocio determina la función que tiene TI en la empresa, su estructura y el modelo de entrega.

La tecnología para Coral Hipermercado es de suma importancia debido a que la mayoría (casi todos) de sus procesos y procedimientos para el logro de los objetivos mencionados, dependen en gran medida del apoyo y uso efectivo, adecuado de la tecnología, sus procesos tanto de ventas, distribución y comercialización se encuentran apoyados por las TI.

La dependencia tecnológica para Coral hipermercado es única y necesaria en absoluto para el modelo de negocio que esta organización mantiene, ya que para sus ventas físicas en sus centros comerciales la transaccionalidad de estas operaciones a nivel de todas las sucursales debe mantener un control contable, así como para las ventas que realizan a través de la web, para sus comercializaciones a nivel local y sobre todo nacional, el sistema que brindan las TI permiten que se encuentren bajo control todas las operaciones y se consoliden, de modo que permite el

logro de los objetivos mejorando la toma de decisiones de forma rápida y efectiva ante cualquier eventualidad.

- **Grado de centralización del sistema de Coral Hipermercado (Distribución de los Recursos de TI).**

La infraestructura de TI se encuentra implementada en cada uno de los corales, sin embargo al finalizar las labores diarias de cada sucursal, la información se centra para hacer replica por batch en la noche, logrando que sea consolidada en una matriz, la administración, sus políticas y normativas se rigen para toda la organización, esto nos permite definir que el Sistema de Coral Hipermercado es centralizado.

- **Las tecnologías desplegadas.**

Coral Hipermercado Racar Plaza, cuenta con un software desarrollado internamente, se encuentra implementado en un entorno cliente- servidor con Oracle Forms y Reports. Para el almacenamiento de los datos se utiliza una base de datos Oracle 11g, esta base de datos se encuentra en IBM AIX para la centralización y Linux para cada Coral.

La empresa utiliza FORMS 6i para todo el ERP y para la parte web utiliza Ápex 4.1, como vimos anteriormente cuenta con una base de datos en cada coral pero al finalizar el día los datos se transfieren a una central que se encuentra en Coral Hipermercado Racar Plaza.

En cada base de datos remota existe una réplica en Standby que se usa como contingente en caso de pérdida de la misma (el tiempo máximo de cambio es de 5 minutos). Las bases de datos están montadas sobre plataforma Linux y AIX (Linux para los servidores de aplicaciones y AIX para base de datos).

- ✓ **Conexión entre las diferentes bases de datos y sucursales:**

La conexión cuando se trata de sucursales regionales es con VPN contratado con Punto Net, mientras que en las locales es a través de fibra óptica[22] contratado con Etapa o conexiones de enlaces inalámbricos propios de la empresa.

- ✓ **Los puntos de venta:**

Se usa POS IBM, certificados por PCI desde la construcción, los cuales utilizan sistema operativo Windows Embeded[23] creados propiamente para los POS de IBM.

- ✓ **Software de los puntos de venta:**

Las aplicaciones están desarrolladas en Forms6i de Oracle con la reportaría en Reports6i.

- ✓ **Interfaz para el pago de tarjeta:**

En el caso que se quiera realizar pagos con tarjetas la corporación cuenta con un Switch transaccional adquirido en el Banco internacional, cuando tienen inconvenientes con los enlaces de los bancos a través de este Switch, se utiliza Medianet, Datafast y Banco del Austro.
Cuando se utiliza el Switch transaccional que se encuentra conectado a las cajas (El software propio de la empresa) este se encarga de enrutar la solicitud de crédito hasta el Switch transaccional donde toda la información se encuentra de forma encriptada.

- **El grado de personalización.**

[22] **Fibra óptica:** se emplea habitualmente en redes de datos y telecomunicaciones para la transmisión, es un hilo muy fino, por el que se envía pulsos de luz que representan los datos.
[23] **Windws Embeded:** "Es un equipo con un propósito determinado que se integra en el sistema que controla".

Todos los sistemas que manejan Coral Hipermercado son desarrollados por la misma organización por lo que no cabría la determinación de algún grado de personalización.

- **El grado de Formalización:**

Coral Hipermercado desarrolla sus propias políticas, procedimientos y normas de acuerdo a su realidad y características de la empresa, estas ayudan a establecer el ambiente de control de TI, permitiendo que la organización mantenga un programa de gobierno de TI efectivo: el cuál debe ser comunicado, entendido, monitoreado y actualizado.

Las políticas que Coral Hipermercado ha implementado dentro la organización apoyan para mitigar el riesgo al que se ve expuesta, tiene como objetivo estandarizar y contribuir al desarrollo informático de las diferentes áreas del negocio.

Las políticas y manuales de procedimiento se rigen para todos los centros comerciales de Coral Hipermercado (Grupo Ortiz).

- **El grado de regulación y cumplimiento.**

Para poder determinar cuál es el nivel de comercio y de esta manera el nivel de cumplimiento de la norma PCI DSS de Coral Hipermercado (Grupo Ortiz), se debe observar los criterios que Visa, MasterCard y American Express exponen dentro de PCI DSS, además se tiene que analizar los tipos de tarjetas que acepta la corporación en sus transacciones, se compara y se determina el nivel de comercio según lo establecido en la norma.

Tabla 11 Niveles según clasificación de Visa, MasterCard y American Express.

NIVEL	N. TRANSACCIONES	TIPO DE TARJETA
Uno	Más de 6 millones. Taque que comprometió datos.	MasterCard
	Más de 2.5 millones.	American Express.

Dos	Entre 1 millón y 6 millones.	Visa o MasterCard.
	Entre 50,000 a 2,5 millones	American Express.
Tres	Menos de 20,000 a 1 millón.	MasterCard.
	Entre 50,000.	American Express.
Cuatro	Menos de 20,000. Menos de 1 millón.	MasterCard E- Commerce. MasterCard.

Fuente: (Norma PCI DSS, Noviembre 2013)
Elaboración: Autoras.

Tarjetas que usan en la corporación Gerardo Ortiz para el pago de bienes y servicios:

- ✓ **MAESTRO.**

Es una tarjeta de la línea MasterCard, donde el cliente puede acceder a cuenta corriente y de ahorros sin necesidad de llevar dinero en efectivo ya que le permite pagar las compras de bienes y servicios en cualquier establecimiento que se encuentre afiliado sin ningún costo por transacción.[24]

Tabla 12 Número de transacciones de Coral Hipermercado (GO), (Maestro).

MAESTRO	2,00
MAESTRO	8,00
MAESTRO	5,00
MAESTRO	1,00
MAESTRO	10,00
MAESTRO	1,00

[24] http://www.mastercard.com/co/consumidores/maestro.html

TOTAL	27,00

Fuente: Coral Hipermercado Racar Plaza.
Elaboración: Autoras.

- ✓ **PACIFICARD.**

Este tipo de tarjetas son emitidas por el Banco del Pacífico y muestran el logo de Visa o MasterCard son utilizadas por el tarjetahabiente en cualquier establecimiento que porte los logos anteriormente mencionados sea dentro o fuera del país, no se limita solo a las redes afiliadas por el banco del Pacífico en Ecuador, si no que existe otras redes afiliadas.[25]

Tabla 13 Número de transacciones de Coral Hipermercado (GO), (PACIFICARD).

PACIFICARD	993,00
PACIFICARD	48,00
PACIFICARD	1.224,00
PACIFICARD	4.560,00
PACIFICARD	3.790,00
PACIFICARD	3.531,00
PACIFICARD	8.488,00
PACIFICARD	5.741,00
PACIFICARD	4.996,00
TOTAL	33.371,00

Fuente: Coral Hipermercado Racar Plaza.
Elaboración: Autoras.

- ✓ **VISA.**

"Visa es la red comercial de pagos electrónicos más grande del mundo y es una de las marcas de servicios financieros globales más reconocidas en el ámbito internacional. Visa facilita el comercio global a través de la transferencia de valores e información entre instituciones financieras,

[25] https://www.pacificard.com.ec/establecimientos.aspx

comercios, consumidores, compañías y entidades gubernamentales." (VISA, 2014)

Tabla 14 Número de transacciones de Coral Hipermercado (GO), (VISA).

VISA AUSTRO	1.038,00
VISA AUSTRO	186,00
VISA AUSTRO	1.294,00
VISA AUSTRO	608,00
VISA AUSTRO	1.127,00
VISA AUSTRO	4.284,00
VISA AUSTRO	16.816,00
VISA AUSTRO	9.717,00
VISA AUSTRO	263,00
VISA B.BOLIVARIANO	73.943,00
VISA B.BOLIVARIANO	36.549,00
VISA B.BOLIVARIANO	84.136,00
VISA B.BOLIVARIANO	56.071,00
VISA B.BOLIVARIANO	1.079,00
VISA B.BOLIVARIANO	18.123,00
VISA B.BOLIVARIANO	17.617,00
VISA B.BOLIVARIANO	11.332,00
VISA B.BOLIVARIANO	48.504,00

VISA PICHINCHA	4.718,00
VISA PICHINCHA	7.251,00
VISA PICHINCHA	13.226,00
VISA PICHINCHA	9.508,00
VISA PICHINCHA	1.189,00
VISA PICHINCHA	79,00
VISA PICHINCHA	1.674,00
VISA PICHINCHA	1.898,00
VISA PICHINCHA	4.675,00
TOTAL	428.803,00

Fuente: Coral Hipermercado Racar Plaza.
Elaboración: Autoras.

- ✓ **AMERICAN EXPRESS.**

Es comúnmente conocida como Amex y facilita el pago de la compra de bienes y servicios, con la finalidad de que el tarjetahabiente no porte dinero en efectivo.

Tabla 15 Número de transacciones de Coral Hipermercado (GO), (AMERICAN EXPRESS).

AMERICAN EXPRES	2.022,00
AMERICAN EXPRES	148,00
AMERICAN EXPRES	2.842,00
AMERICAN EXPRES	7.760,00
AMERICAN EXPRES	3.704,00
AMERICAN EXPRES	6.707,00
AMERICAN EXPRES	18.072,00
AMERICAN EXPRES	11.807,00
AMERICAN EXPRES	1.736,00
TOTAL	54798

Fuente: Coral Hipermercado Racar Plaza.
Elaboración: Autoras.

Con la información expuesta podemos concluir que la empresa Coral Hipermercado de Grupo Ortiz se encuentra ubicada en el nivel 4 según MasterCard y en el nivel 2 según American Express, porque procesan 33.398 transacciones de MasterCard llegando a lo requerido que es menos de 1 millón de transacciones, además procesan 54.798 transacciones de American Express encontrándose en lo establecido por la norma donde indica que en este nivel se procesan entre 50.000 a 2.5 millones de transacciones con esta tarjeta.

- ✓ **Nivel 4 según MasterCard.**

Coral Hipermercado como comercio a nivel 4 debe realizar un cuestionario de autoevaluación anualmente que debe estar completado internamente y firmado por el representante de la compañía.

Requieren ayuda de un QSA externo para tener un punto de vista experto.

- ✓ **Nivel 2 según American Express.**

Coral Hipermercado necesita llenar el cuestionario de autoevaluación anualmente. Este debe ser completado internamente y firmado por el representante de la compañía.

Las compañías como Coral Hipermercado que son muy grandes pueden requerir un QSA externo para un punto de vista profesional.

- **El grado y forma de la contratación externa de Coral Hipermercado (Grupo Ortiz).**

Coral Hipermercado (Grupo Ortiz) mantiene un sistema desarrollado en casa (Inhouse), denominado ERP y mantiene una parte WEB, por lo que se llegó a la conclusión de que no tercerizan, debido a que su sistema es elaborado dentro de la organización.

- **El grado de estandarización operativa.**

Se mantienen procedimientos para varias actividades, tareas que se deben llevar a cabo en la continuidad del negocio, por ejemplo como el cobro en ventas con tarjetas de pago para ello se basan en el Marco de PCI DSS que establecen las marcas de tarjetas de crédito, Procedimientos para la debida y adecuada eliminación de la información que ya no es necesaria en la organización, cada departamento según la actividad a realizar debe basarse en los procedimientos que han sido establecidos en su totalidad se podría decir que el nivel de las operaciones se encuentran estandarizadas a en todas las sucursales así como en la matriz en casi un 100%.

- **El nivel de dependencia tecnológica.**

Como se observó la empresa Coral Hipermercado es totalmente dependiente de la tecnología debido a que en todos procesos operativos del negocio se utiliza la tecnología, la empresa no podría realizar sus actividades diarias, especialmente transacciones que tengan algún vínculo con las tarjetas de pago.

3.1.2. Universo Auditable.

Como pudimos observar en la tecnología desplegable de la empresa, los sistemas que manejan datos de tarjetas de crédito son los puntos de ventas, los cuales están compuestos desde la facturación hasta el momento en que los datos llegan a su etapa final en el Switch transaccional, a raíz de todo esto hemos determinado que el universo auditable que se analizará posteriormente es:

Sistemas Operativos: Base de datos ORACLE 11g, UNIX. Base central replica por batch en la noche.

- ✓ Interfaz: FORMS6i
- ✓ La Conexión entre las diferentes bases de datos y sucursales son:

a. Con las sucursales regionales con VPN contratada con Punto Net.
b. Con las locales tienen con fibra óptica contratada con etapa o conexiones de enlace inalámbrico propio de la empresa.
c. Internamente las conexiones son con fibra óptica con una alterna de cobre como contingente.
d. Las redes están segmentadas tanto por sucursal como local, para el caso se usan Vlan's independientes.

Los puntos de venta: Existen P.O.S IBM con sistema operativo Windows Embeded.

El software de los puntos de venta:

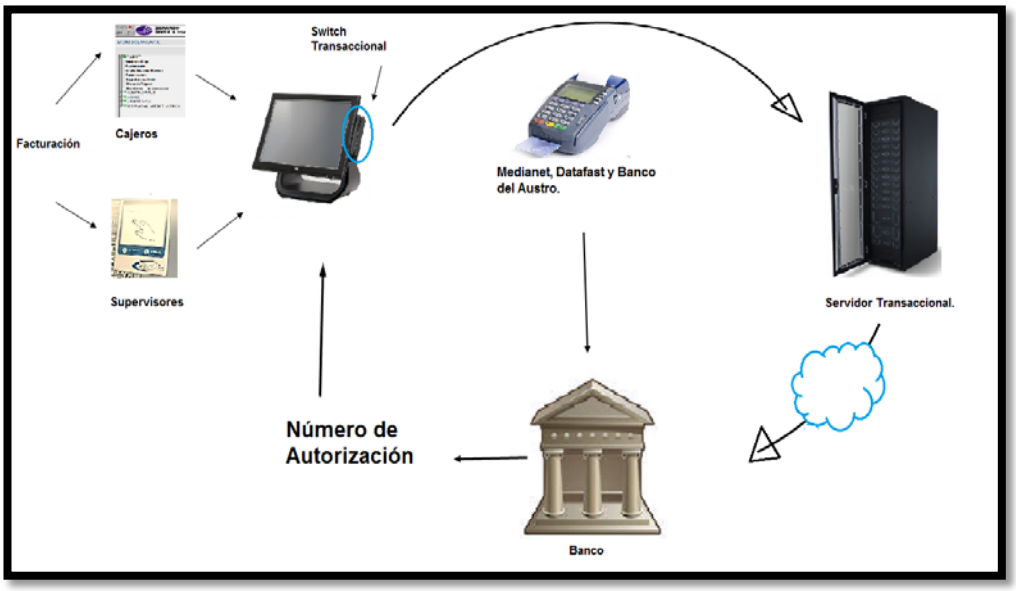
- ✓ Las aplicaciones están desarrolladas en Forms6i de Oracle con la reportería en Reports6i.
- ✓ Cuando se cobra con tarjeta de crédito se levanta un servicio adicional que ofrece el Switch transaccional para tomar la transacción, fue adquirido a Banco Internacional y por el pasan todas las tarjetas afiliadas, a excepción de las tarjetas Cuota fácil para la que se usa el sistema de autorización tradicional.
- ✓ El software propio de la empresa se encarga de enrutar la solicitud de crédito hasta el Switch transaccional y hasta él toda la información es encriptado.

En resumen el Universo Auditable para la presente auditoria se vería compuesto por:

- ✓ Sistemas operativos: Base de datos ORACLE, UNIX,
- ✓ Computadores: cajas registradoras, computadores, Racks, POS.
- ✓ Red de enlace que sale del Switch.
- ✓ Sistema de facturación.
- ✓ Servidor transaccional.

- ✓ Sistema que maneja la empresa (IBX).

Ilustración 12 Universo Auditable.



Fuente: Coral Hipermercado Racar Plaza.
Elaborado por: Autoras.

3.1.3. Evaluación de Riesgo.

Tabla 16 Evaluación de Riesgos

VARIABLES CLAVE	VALOR DESCRIPTIVO (1 BAJO A 5 ALTO)	SISTEMAS					
		FACTURACIÓN		SERVIDOR TRANSACCIONAL		SISTEMAS OPERATIVOS (BASE DE DATOS ORACLE, UNIX)	
		PESO	VALOR AMPLIADO	PESO	VALOR AMPLIADO	PESO	VALOR AMPLIADO
CARÁCTER DE LA ACTIVIDAD	Considerar: Actividad principal = 4 a 5 Unidad de negocio = 2 a 3 Sistema local = 1	30	120	40	200	30	60
RETROCEDER	Considerar: 2 Plan de continuidad de negocio 2 Planes de recuperación de desastres. 2 Procedimientos manuales 2 Sistema antiguo 2	20	40	20	40	10	20
ALCANCE DE SISTEMA, PROCEDIMIENTO Y PROCESO DE CAMBIO	Considerar: La extensión de la reingeniería: Reingeniería importante = 4 a 5 Reingeniería moderada = 2 a 3 Reingeniería menor = 1 No hay procedimientos = 4 a 5 Procedimientos locales = 2 a 3 Procedimientos corporativos = 1	20	40	10	30	30	120
COMPLEJIDAD	Considerar: El volumen de transacciones. Número de usuarios. Centralizado o Descentralizado. Número de interfaces Muy complejo = 4 a 5 Moderadamente compleja = 2 a 3 Sencillo = 1	30	150	30	120	30	150
	TOTAL	100	350	100	390	100	350

Elaborado por: Autoras.

3.1.4. Formalización de la Auditoria.

Tabla 17 Cronograma de la Formalización de la Auditoría

ACTIVIDADES	SEMANA I							SEMANA II							SEMANA III							SEMANA IV						
	1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7
1. Programa de auditoría del Requerimiento 7.																												
2. Recolección de evidencia.																												
3. Elaboración de papeles de trabajo requerimiento 7.																												
4. Programa de auditoria del Requerimiento 8.																												
5. Recolección de evidencia.																												
6. Elaboración de papeles de trabajo requerimiento 8.																												
7. Programa de auditoría del requerimiento 9.																												
8. Recolección de evidencia.																												
9. Elaboración de los papeles de trabajo requerimiento 9.																												
10. Conclusión y recomendaciones.																												
11. Informe de auditoría.																												

Elaborado por: Autoras.

3.2. Ejecución de la Auditoria de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCIDSS aplicada a CORAL HIPERMERCADO, RACAR PLAZA CON CORTE A JUNIO DE 2015.

La empresa Coral Hipermercado desconoce el estado actual del cumplimiento de los requerimientos 7, 8, 9 establecidos en la norma PCI DSS, por lo que se procede a realizar la auditoria de sistemas al cumplimiento de la misma.

Después de realizar un conocimiento amplio del negocio, saber cuáles es el universo que se debe analizar y después de haber evaluado las áreas con mayor riesgo, procederemos a cumplir con lo propuesto en el cronograma realizado.

3.2.1. PROGRAMA DE AUDITORIA DEL REQUERIMIENTO 7. Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.

Tabla 18 Matriz de fortalezas y debilidades del Requerimiento 7

Matriz del requerimiento 7: Restricción al acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.			
Empresa Auditada:	Coral Hipermercado Racar Plaza (GO).		
Responsable:	Estefanía Ortega		
Supervisa:	Patricia Benenaula L.		
Aplicativo:	**Fecha de estudios:**		Periodo 2015 con corte a Junio.
Requisitos de PCI DSS	**FAD**	**FORTALEZA**	**DEBILIDAD**
Observar las limitaciones del acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de acceso.	**A**	La política de control de acceso de Coral Hipermercado abarca la mayor parte de los parámetros que se necesita para cumplir el requerimiento descrito en el papel de trabajo 001 de la norma PCI DSS, la empresa a más de eso en la práctica también lo aplica.	La empresa Coral Hipermercado, en el caso de anulación de voucher no tiene definida en los manuales de funcionamiento quien debe realizar esa labor, se le designa al supervisor sin ninguna aprobación documentada, además en el caso de los encargados del servidor transaccional no hay manual de funcionamiento por lo que no se sabía con exactitud cuáles eran las funciones que se deben realizar, pero según las entrevista efectuadas, ellos tiene acceso a otros componentes del sistema que no están dentro de su labor.
Observar el sistema de control de acceso establecido para los componentes del sistema que restrinja el acceso según la necesidad del usuario de conocer y que se configure para "negar todo", salvo que se permita específicamente.	**D**	Se mantiene implementado un sistema de control de acceso para los empleados en los sistemas de Facturación y supervisión.	No se tiene un correcto sistema de control de acceso para los servidores transaccionales se debería mejorar el ingreso mediante la seguridad del acceso remoto con clave única y no con clave conjunta como se lleva a cabo actualmente.

Verificar que las políticas de seguridad y procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta estén documentados, implementados y sean de conocimiento para todas las partes afectadas.	**A**	Mantienen normas debidamente documentadas sobre el acceso a los datos y como restringir el mismo.	La norma no se encuentra socializada a todos los empleados, no se realizan capacitaciones periódicas para mantenerlos actualizados.

Referencias:	
F	Fuerte
A	Aceptable
D	Débil
PT	Papeles de Trabajo

Elabora por: Autoras.

Tabla 19 Programa de Auditoría del Requerimiento 7.

Requerimiento 7: Restricción al acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.						
Empresa Auditada:	Coral Hipermercado Racar Plaza (GO).			**Fecha de estudios:**		
Responsable:	Estefanía Ortega					
Supervisa:	Patricia Benenaula					
Objetivos a evaluar	**FAD**	**Nº**	**Procedimiento**	**Comentario**	**Recomendación**	**Referencia a PT**
Observar las limitaciones del acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de acceso.	**A**	7.1	Solicitar y revisar las políticas escritas para el control de acceso de Coral Hipermercado Racar Plaza y verificar que estas: * Definan las necesidades de acceso y asignación de privilegios de cada función. * Restrinjan el acceso de usuarios con IDs privilegiadas a la menor cantidad de privilegios. * Asignen los accesos según la tarea, clasificación y la función de cada persona.	Las políticas de administración de control de acceso de Coral Hipermercado cumple en un gran mayoría con la norma PCI DSS, ya que abarca casi todos puntos del requerimiento descrito en el papel de trabajo 001, además la empresa aplica la política en la práctica diaria, pero cuando se trata de aprobación	Se recomienda actualizar los manuales de funcionamiento de la empresa, colocando las funciones del supervisor según el trabajo que realiza y elaborar un manual de funcionamiento para el encargado del servidor transaccional y de esa manera se defina bien cuáles son con	**PT001**

			*Que tenga aprobación documentada de las partes autorizadas que estén incluidas la lista de los privilegios.	documentada no cumplen con todo lo necesario, debido a que en la anulación de Voucher de la tarjeta de pago, en el manual no se especifica quien debería realizar esta función, el supervisor lo hace directamente sin que se encuentre dentro del manual de funcionamiento de los supervisores. La empresa no tiene un manual de funcionamiento para los encargados del servidor transaccional por lo que no se	Exactitud las funciones necesarias que tienen para que puedan realizar su trabajo.	
		7.1.1	Seleccionar una muestra de las funciones para verificar que las necesidades de acceso de cada función estén definidas e incluyan: * Componentes del sistema y recursos de datos que necesitan para realizar su trabajo. * Se Identifique los privilegios necesarios para que puedan desempeñar sus funciones.			

		7.1.2	Entrevistar al personal encargado de asignación de los accesos para verificar que el acceso de usuarios con ID privilegiadas cumplan con: * Asignación solamente a las funciones que específicamente necesitan acceso privilegiado. * Que esté restringido a la menor cantidad de privilegios que sean necesarios para llevar a cabo las responsabilidades del trabajo.	sabe con exactitud que funciones debe cumplir, pero según las entrevistas y observaciones realizadas ellos tienen acceso a componentes del sistema y recursos de datos fuera de lo expuesto por la empresa. Todo lo mencionado podría ser perjudicial porque el acceso no es controlado y no se limita según sus necesidades y funciones.		
			Seleccionar una muestra de las ID de usuarios privilegiados y entrevistar al personal de administración encargado con la finalidad de verificar que los privilegios asignados respeten: * Ser necesarios para el trabajo del usuario. * Estén restringidas a la menor cantidad de privilegios que sean necesarios para llevar a cabo las responsabilidades del trabajo.			

		7.1.3	Seleccionar una muestra de las ID de usuarios y entrevistar al personal administrativo responsable para poder verificar que los privilegios se asignen según la tarea, clasificación y función de cada persona.			
		7.1.4	Seleccionar una muestra de las ID de usuarios y comparar con la aprobación documentada para verificar que exista una aprobación documentada, además que las partes autorizadas aprobaron el documento y Los privilegios especificados en la documentación coinciden con los roles asignado a la persona.			
7.2. Observar el sistema de control de acceso establecido para los componentes del sistema y verificar que restrinja el acceso según la necesidad del usuario de conocer y que se configure para "negar todo", salvo que se permita	**D**	7.2	Evalué los parámetros del sistema y la documentación del proveedor para verificar que el sistema de control de acceso se implemente de la siguiente manera:	El sistema de control de acceso que ha implementado Coral Hipermercado para el manejo de los componentes y parámetros del sistema si mantiene un acceso restringido según el usuario sobre todo para el sistema de	Se recomienda que para el Sistema de Servidores transaccionales su ingreso al sistema sea mediante una clave única de tal forma que permita la distinción de los ingresos a las bases tanto para	**PT002**
		7.2.1	Confirmar que los sistemas de control de acceso se implementen en todos los componentes del sistema.			

específicamente.		7.2.2	Confirmar que los sistemas de control de acceso sean configurados de tal manera que los privilegios asignados a una persona se realicen según la clasificación del trabajo y la función que desempeñan.	Facturación y supervisión, sin embargo presenta falencias para los servidores transaccionales debido a que se mantiene una clave para el manejo de varias personas para soporte del sistema y accesos remotos.	soporte como para monitorios.	
		7.2.3	Confirme que los sistemas de control de acceso cuenten con la configuración predeterminada de "negar todos".			
7.3. Asegurar que las políticas de seguridad y procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta estén documentados, implementados y sean de conocimiento para todas las partes afectadas.	**A**	7.3	Solicitar y revisar la documentación, entrevistar al personal y verificar que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta cumplen con: - Están documentados. - Están implementados. -Son de conocimiento para todas las partes afectadas.	Al conversar con los empleados, facturación, supervisores, y servidor transaccional de Grupo Ortiz de Coral Hipermercado se nos dio a conocer que no se tiene conocimiento sobre una política de seguridad se encuentra documentada e implementada pero no existe un conocimiento general o una socialización de la normativa. Cabe mencionar	Las políticas que mantienen Coral Hipermercado sobre la restricción de accesos a los datos de titulares de tarjetas deberían ser socializadas a todo el personal, por lo que se recomienda realizar capacitaciones, evaluaciones periódicas para actualizar los conocimientos en cuanto a	**PT003**

				que el personal de facturación nos ha indicado que se les realiza una capacitación cada 3 meses por parte del departamento de crédito para el manejo adecuado de pagos con tarjetas de pago pero esto no implica el conocimiento de una normativa ni del proceso de seguridad de accesos a los datos.	estas normativas.		

	Referencias:	
	F	Fuerte
	A	Aceptable
	D	Débil
	PT	Papeles de Trabajo

Elabora por: Autoras.

3.2.2. PROGRAMA DE AUDITORIA DEL REQUERIMIENTO 8. "Identificar y autentificar el acceso a los componentes del sistema."

Tabla 20 Matriz del requerimiento 8: Identifique y autentifique el acceso a los componentes del sistema.

Matriz del requerimiento 8: Identifique y autentifique el acceso a los componentes del sistema.			
Empresa Auditada:	Coral Hipermercado Racar Plaza (GO).		**Fecha de estudios:**
Responsable:	Estefanía Ortega		
Supervisa:	Patricia Benenaula		
Aplicativo:			
Requisitos de PCI DSS	**FAD**	**FORTALEZA**	**DEBILIDAD**
Verificar que se haya definido e implementado las políticas y procedimientos para garantizar la correcta administración de la identificación de todos usuarios, en los componentes del sistema.	**D**	*Los empleados cesantes son inhabilitados en el momento de su salida, autoriza recursos humanos.	*En la política de autentificación no hay algún parámetro que indique, cuales es número determinado de intentos y por cuanto tiempo debe permanecer bloqueada en el caso de que se intente ingresar con contraseñas incorrectas, tampoco existe ninguna política o procedimiento acerca de que se debe inactivar el sistema en el caso de que pase sin ser usado un lapso de 15 minutos o menos. *Los encargados del servidor transaccional no reciben una contraseña para cada uno si no esta es compartida. *No existe monitoreo de las cuentas de acceso remoto por parte de la empresa. *En las pruebas realizadas no se bloqueó la cuenta cuando se hizo más de seis intentos de inicio de sesión no válidos.

Evaluar que exista una correcta administración de autenticación de todos los usuarios en los componentes del sistema y que se usa al menos algo que el usuario sepa (contraseña, o frase de seguridad), algo que el usuario tenga (dispositivo token, tarjeta inteligente) y algo que el usuario sea (rasgo biométrico).	**D**	*Las contraseñas de los usuarios cajeros y supervisores son a través de la huella digital y el número de cédula, es una forma más segura de resguardar los datos porque es un rasgo biométrico único. Esta información es almacenada de manera encriptada y no se puede realizar copia a otro usuario. *Los encargados del servidor tienen contraseñas de 16 dígitos combinados con números y letras.	*La empresa no aplica procedimientos de autentificación para el cambio de credenciales de autenticación. *No describen todos los métodos de autenticación dentro de la política. *Los encargados del servidor transaccional no hacen cambios en su contraseña, mantienen la misma contraseña que se les otorgó cuando ingresaron a la organización. *En el caso de los cajeros y supervisores, no pueden cambiar su contraseña debido a que es su huella digital, pero las personas encargadas de resguardar estos datos mantienen la misma contraseña sin hacer ningún cambio.
Observar que se incorpore la autenticación de dos factores para el acceso remoto a la red desde fuera de la misma por parte del personal	**D**		Existe un solo método de autentificación cuando hay acceso remoto.
Verificar que se documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios y que esta incluya lineamientos para seleccionar una credencial de autenticación sólida, además de como los usuarios deben proteger las credenciales, instrucciones para no seleccionar contraseñas utilizadas anteriormente e	**A**	Coral hipermercado cuenta con una política de autenticación y claves que está compuesta por lineamientos que ayudan a proteger las credenciales de autenticación y tener contraseñas seguras difíciles de adivinar.	La empresa no reparte la política de autenticación a los usuarios, además no tiene ningún lineamiento que ayude al cambio de contraseñas para no usar las mismas.

instrucciones para cambiar la contraseña si es necesario.			
Evaluar que no se utilice ID ni contraseñas de grupo, compartidas ni genéricas.	**D**	Todos los usuarios tiene ID exclusivas.	Los usuarios encargados del servidor transaccional y de los que reguardan los datos de las huellas digitales, mantienen la misma contraseña que se les otorgó al momento del ingreso a la organización.
Verificar que en el caso de que se use otros mecanismos de autenticación estos se asignen a una sola cuenta y no compartirlos entre varias, además verificar que se implementen controles físicos y lógicos para garantizar que solo la cuenta deseada usa esos mecanismos para acceder.	**D**		No se usa mecanismos de autentificación como tokens, tarjetas inteligentes y certificados.
Observar que se restrinjan todos los accesos a cualquier base de datos que tengan datos del titular de la tarjeta por lo que cualquier consulta y acción se realicen mediante métodos programáticos, solo los administradores de la base de datos puedan acceder, solo las aplicaciones pueden usar las ID de aplicaciones.	**A**	Los cajeros y los supervisores tienen una ID y contraseña única. *Los 7 encargados de acceder a la base de datos solo pueden acceder a información básica del titular de la tarjeta (Nombre, número de factura, valor adquirido, número de voucher y número de lote) así como lo específica la norma.	Los 7 encargados de acceder a la base de datos tienen una misma contraseña.

Verificar que las políticas de seguridad y los procedimientos operativos de identificación y autenticación estén documentados y sean de conocimiento para todas las partes.	**D**	La empresa si tiene política de seguridad documentada al igual que procedimientos.	La política de seguridad no se encuentra implementada del todo además que no está completa debido a que los usuarios realizan algunas actividades que no se encuentra dentro de la política por ejemplo en el caso de la autentificación de los cajeros y supervisores, este método no está establecido en la política de autentificación y claves, además que la política no es conocida por todas las partes afectadas.

Referencias:	
F	Fuerte
A	Aceptable
D	Débil
PT	Papeles de Trabajo

Elabora por: Autoras.

Tabla 21 Requerimiento 8: Identifique y autentifique el acceso a los componentes del sistema.

Requerimiento 8: Identifique y autentifique el acceso a los componentes del sistema.						
Empresa Auditada:	Coral Hipermercado Racar Plaza (GO).				**Fecha de estudios:**	
Responsable:	Estefanía Ortega					
Supervisa:	Patricia Benenaula					
Aplicativo:						
Objetivos a evaluar	**FAD**	**Nº**	**Procedimiento**	**Comentario**	**Recomendación**	**Referencia a PT**
Verificar que se haya definido e implementado las políticas y procedimientos para garantizar la correcta administración de la identificación de todos usuarios, en los componentes del sistema.	**D**	8.1	Solicitar, revisar los procedimientos y confirmar que estos definan los procesos para los siguientes puntos: Todos los usuarios tengan asignada una ID exclusiva para tener accesos a los componentes del sistema o los datos del titular de la tarjeta. Que las ID de usuarios y las ID de usuarios privilegiados se hayan implementado solamente con los privilegios especificados en la aprobación documentada.	Coral Hipermercado tiene un bajo nivel de cumplimiento de este requerimiento de la norma PCI DSS, porque las políticas y procedimientos de autenticación no se encuentran del todo completas, en el caso del acceso remoto la empresa no especifica en ninguna norma o procedimiento como debe ser un el acceso remoto. Además la empresa no menciona que debe ocurrir en el caso de que el sistema esté inactivo en un lapso de 15 minutos, también otra de las debilidades es que los encargados del servidor transaccional usan una	Se recomienda a la empresa Coral Hipermercado, que se realice un ajuste en la política de autenticación así como también un ajuste en la configuración del sistema en la parte de las contraseñas y de esa manera corregir las falencias mencionadas para un mejor funcionamiento de la seguridad de los datos del titular de la tarjeta y de la tarjeta mismo.	**PT001**

			Las ID, tarjetas inteligentes, tokens, etc., de los usuarios cesantes se hayan desactivado o eliminado de las listas de acceso.	misma contraseña para los siete designados, al tener una contraseña compartida puede existir inconvenientes en el hecho de que no se mantiene una responsabilidad individual, si es que suceda algún inconveniente no se sabría de quien es la responsabilidad. La empresa al no monitorear el acceso remoto se puede tener dificultades ya que se accedería en el momento que se desee y sin vigilancia de que se pueda hacer algún acto que exponga los datos del titular de la tarjeta o de la tarjeta. La empresa no tiene bloqueo de cuenta en el caso de que se haga varios intentos de inicio de sesión no válidos, al no tener implementado este requerimiento corre el riesgo de que algún individuo con intensiones maliciosas intente adivinar la clave. Como se mencionó anteriormente		
			Además que los usuarios inactivos se eliminen o inhabiliten en el caso de que tengan más 90 días inactivos.			
			Que las cuentas de los proveedores se inhabiliten cuando no se usan, se habiliten cuando el proveedor las necesita y monitorear las cuentas de acceso remoto de los proveedores mientras se utiliza.			
			Los parámetros de autentificación se encuentren configurados de manera que se bloquee la cuenta de todos usuarios después de realizar, como máximo seis intentos de			

			inicio de sesión no válidos.	Coral Hipermercado no tiene parámetros que le permita inactivar el sistema en el caso de que pase un lapso de 15 minutos sin utilizar, esto puede causar que algún individuo se lleve datos del titular de la tarjeta en el momento de que el usuario se aleje del computador.		
			También que los parámetros de las contraseñas se encuentren configurados de manera que al bloquear la cuenta de un usuario, esta permanezca bloqueada un mínimo de 30 minutos o hasta que el administrador del sistema la restablezca.			
			Y que se inactive el sistema en el caso que pase sin ser usado un lapso de 15 minutos o menos.			
		8.1.1	Entrevistar al personal administrativo para confirmar que todos los usuarios tengan asignada una ID exclusiva para tener accesos a los componentes del sistema o los datos del titular de la tarjeta.			

		8.1.2	Tomar una muestra de ID de usuarios privilegiados e ID de usuarios generales, evalúe las autorizaciones asociadas y observe los parámetros del sistema a fin de verificar que todas las ID de usuarios y las ID de usuarios privilegiados se hay implementado solamente con los privilegios especificados en la aprobación documentada.			
		8.1.3	Seleccionar una muestra de los usuarios cesantes en los últimos seis meses y revisar las listas de accesos de usuarios actuales tanto para accesos local y remoto, de esa manera se verificará que las ID de dichos usuarios se hayan desactivado o eliminado de las listas de acceso, además se debe verificar que todos los			

			métodos de autentificación físicos (tarjetas inteligentes, tokens) se hayan devuelto o desactivado).			
		8.1.4	Observar las cuentas de usuarios inactivos y verifique que se eliminen o inhabiliten las que lleven más de 90 días inactivas.			
		8.1.5	Entrevistar al personal administrativo y observar los procesos de administración de cuentas que usan los proveedores para acceder, respaldar o mantener los componentes del sistema a fin de verificar que las cuentas de los proveedores cumplan con lo siguiente: se inhabilitan cuando no se usen, se habilitan cuando el proveedor las necesita; además se debe observar los procesos para verificar que se			

			monitoreen las cuentas de acceso remoto de los proveedores mientras estos utilizan.			
		8.1.6	Seleccionar una muestra de los componentes del sistema para inspeccionar los parámetros de configuración del sistema para verificar que los parámetros de autentificación se encuentren configurados de manera que se solicite el bloqueo de la cuenta de usuarios después de realizar como máximo seis intentos de inicio de sesión no válidos.			
		8.1.7	Seleccionar una muestra para verificar que los parámetros de las contraseñas se encuentren configurados de tal manera que permanezca bloqueada la cuenta de usuario, mínimo 30 minutos o hasta que el administrador del sistema la			

			restablezca.			
		8.1.8	Seleccionar una muestra de los componentes del sistema para inspeccionar los parámetros de configuración del sistema para verificar que las funciones de tiempo máximo de inactividad del sistema se encuentren establecidos en 15 minutos o menos.			
Verificar que exista una correcta administración de autenticación de todos los usuarios en los componentes del sistema y que se usa al menos algo que el usuario sepa (contraseña, o frase de seguridad), algo que el usuario tenga (dispositivo token, tarjeta inteligente) y algo que el usuario sea (rasgo biométrico).	**D**	8.2	Solicitar documentos que describa métodos de autentificación para revisarlos, comprar con los componentes del sistema y verificar que estos funcionen de manera coherente.	Las contraseñas utilizadas en Coral Hipermercado para los usuarios cajeros y supervisores son a través de la huella digital y el número de cédula, es una forma más segura de resguardar los datos porque es un rasgo biométrico único. Estas información es almacenada de manera encriptada y no se puede realizar copia a otro usuario, haciendo más segura la información, además los encargados del servidor tienen contraseñas de 16 dígitos	Se recomienda implementar procedimientos de cambios de autenticación siguiendo los estándares de la norma, además que se debe reformar los parámetros de configuración de las contraseñas para que pida cambio de la misma al menos cada 90 días como indica la norma.	**PT002**
		8.2.1	Solicitar y evaluar la documentación del proveedor y los parámetros de configuración para verificar que las contraseñas se protejan durante la transmisión y el			

			almacenamiento mediante una criptografía sólida. Tomar una muestra de los componentes de sistema y revisar archivos de contraseñas para verificar que estas sean ilegibles durante el almacenamiento. Además se debe tomar una muestra para revisar la transmisión de datos de contraseñas para verificar que estas sean ilegibles durante la transmisión. Observar los archivos de los proveedores para: verificar que las contraseñas de los clientes sean ilegibles durante el almacenamiento Y para verificar que sean ilegibles durante la transmisión.	combinadas con números y letras como lo indica la norma pero la empresa tiene inconvenientes que pueden costar los datos del titular de la tarjeta y de la tarjeta mismo, como: Los métodos de autenticación de los cajeros y supervisores no se encuentran registrados en la política de autenticación, además no aplican los procedimientos de autenticación para el cambio de credenciales de autentificación ya que no se ha hecho ningún cambio de la contraseña desde que ingresaron a la organización, esto hace que una persona malintencionada se le proporcione más tiempo para descubrir la contraseña.		

		8.2.2	Revisar los procedimientos de autenticación que sirven para modificar las credenciales de autenticación y observar al personal de seguridad que revise la identificación del usuario antes de modificar la credencial ya sea por teléfono, correo electrónico, internet u otro método no personal.			
		8.2.3	Seleccionar una muestra de los componentes del sistema de usuarios y usuarios proveedores e inspeccionar los parámetros de configuración del sistema para verificar que los parámetros de la contraseña del usuario se encuentren configurados de una longitud mínima de siete caracteres y una combinación de caracteres numéricos y alfabéticos.			

		8.2.4	Tomar una muestra de los usuarios y usuarios proveedores para poder inspeccionar los parámetros de configuración de las contraseñas y verificar que estos se encuentren configurados de manera que se le solicite al usuario cambiar su contraseña al menos cada 90 días.			
		8.2.5	Seleccionar una muestra de los componentes del sistema de usuarios y usuarios proveedores para verificar que los parámetros de configuración de las contraseñas se encuentren configuradas de tal manera que no se puedan repetir con las cuatro últimas contraseñas.			

		8.2.6	Solicitar una muestra de los parámetros de configuración de las contraseñas de nuevos usuarios y contraseñas restablecidas para usuarios existentes con el fin de que el personal de seguridad verifique que se configuren en un valor único para cada usuario y se cambie después del primer uso.			
Observar que se incorpore la autenticación de dos factores para el acceso remoto a la red desde fuera de la misma por parte del personal.	**D**	8.3	Revisar la configuración del sistema para los servidores y sistema de acceso remoto (acceder desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar, a través de una red local o externa) y verificar que se exija la autentificación de dos factores (tokens, contraseñas, etc.) en el caso de que se	Existe un solo método de autenticación para el acceso remoto, solo se ingresa la contraseña y el usuario que está en un computador fuera de la red puede realizar el acceso, esto podría exponer los datos del titular de la tarjeta porque es más fácil el ingreso al computador con un método que con dos métodos e autenticación.	Se recomienda cambiar la configuración del acceso remoto para que pida dos métodos de autentificación en el caso de que se quiera acceder, además se debe implementar procesos para el acceso remoto y se debe tener un control cuando se realice el mismo.	**PT003**

			quiera ingresar con acceso remoto tanto para el personal como para proveedores y terceros que quieran brindar mantenimiento. Observar a un grupo de empleados que se conecte de manera remota a la red para verificar que se use al menos dos formas de autenticación			
Verificar que se documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios y que esta incluya lineamientos para seleccionar una credencial de autenticación sólida, además de como los usuarios deben proteger las credenciales,	**A**	8.4	Revisar los procedimientos de autentificación y entrevistar al personal para verificar que los procedimientos y las políticas de autentificación se distribuyen a todos los usuarios. además se debe verificar que estas incluyan:	Coral hipermercado cuenta con una política de autenticación y claves que está compuesta por lineamientos que ayudan a proteger las credenciales de autenticación y tener contraseñas seguras difíciles de adivinar. La empresa no reparte la política de autenticación a los usuarios, además	Se recomienda una actualización de la política donde se incluya los lineamientos de cambio de contraseña, además que se capacite al personal para que tengan conocimientos de la política y que se les reparta la misma.	**PT004**

instrucciones para no seleccionar contraseñas utilizadas anteriormente e instrucciones para cambiar la contraseña si es necesario.			Lineamientos sobre cómo seleccionar credenciales de autenticación sólidas. (para ayudar al personal a colocar una contraseña que sea difícil de adivinar Lineamiento de como los usuarios de ben proteger las credenciales de autenticación. Instrucciones a los usuarios para que no utilicen contraseñas que ya estaban anteriormente. Instrucciones para cambiar las contraseñas en el caso de que se corra riesgo. Entrevistar a un grupo de usuarios para verificar que conozca los procedimientos y políticas de autenticación.	no tiene ningún lineamiento que ayude al cambio de contraseñas para no usar las a anteriores, esto afecta a la empresa debido a que el personal no tiene conocimiento de la política que le ayudará a entender y cumplir de manera correcta la misma, la empresa tampoco tiene definida un lineamiento que ayude al cambio de contraseñas, puede existir la posibilidad de que esta deje de ser segura y no podrá prevenir que usuarios mal intencionados utilicen una contraseña legítima para obtener acceso no autorizado.		
Evaluar que no se utilice ID ni contraseñas de grupo, compartidas ni	**D**	8.5	Seleccionar una muestra de los componentes del sistema, y revisar las listas de ID de	Según los dato otorgados todos los usuarios tiene ID exclusivas, pero al momento de realizar entrevista y	Se recomienda realizar una reforma en las ID y contraseñas de los encargados del servidor	**PT005**

genéricas.			usuarios y verificar que: .Las ID de usuarios genéricas sean desactivadas o eliminadas. .Además se debe revisar que no exista ID de usuarios compartidas para realizar actividades de administración del sistema y demás funciones críticas. .Las ID de usuarios compartidas y genéricas no se deben utilizar para administrar componentes del sistema. Solicitar y revisar las políticas y procedimientos de autentificación para verificar que las contraseñas y las ID de grupo y compartidas u otro método de autenticación parecidos, estén prohibidos.	observaciones los usuarios encargados del servidor transaccional tienen ID y contraseñas compartida, además las contraseñas que son las mismas que se les otorgó cuando ingresaron a la empresa, esto hace que la empresa se responsabilice por las acciones de una persona ya que cualquier persona del grupo puede haber realizado la acción, por lo tanto no se sabría sobre quién debe caer la responsabilidad.	transaccional, de tal manera que no se les permita usar una grupal sino que cada uno tenga exclusividad, además se debe realizar una configuración de los parámetros de contraseñas, pidiendo al usuario que debe cambiar obligatoriamente pasado los 30 días.	

			Se debe entrevistar a los administradores del sistema para verificar que las contraseñas de grupo y compartidas no se distribuyan, incluso en el caso que se solicite.			
		8.5.1	Revisar que las políticas y los procedimientos de autenticación y entrevistar al personal para verificar que se utilicen diferentes métodos de autentificación para acceder a la cada proveedor.			
Verificar que en el caso de que se use otros mecanismos de autenticación estos se asignen a una sola cuenta y no compartirlos entre varias, además verificar que se implementen controles	**D**	8.6	Revisar las políticas y procedimientos de autentificación para verificar que los procedimientos que usan mecanismos de autentificación (tokens de seguridad, tarjetas inteligentes y certificados) estén definidas dentro de la política y	La empresa Coral Hipermercado no usa tokens, tarjetas inteligentes y certificados, esto hace que no se identifiquen usuarios no autorizados, haciendo que puedan acceder usando mecanismos de autentificación compartidos y con total libertad.	Se recomienda implementar mecanismos de autenticación más seguros, además que se debe reformar la política de autenticación para resguardar los datos relacionados con las tarjetas de pago y así evitar actos maliciosos.	**PT006**

físicos y lógicos para garantizar que solo la cuenta deseada usa esos mecanismos para acceder.			procedimientos, además estos mecanismos deben ser asignados a una solo persona y no ser compartida y con los controles físicos y lógicos garantizan que la cuenta deseada es la única que usa ese mecanismo para acceder. Se debe entrevistar al personal de seguridad y se debe examinar los parámetros de configuración del sistema y los controles físicos para verificar que se implementen controles a fin de garantizar que solo la cuenta deseada usa esos mecanismos para acceder.			
Observar que se restrinjan todos los accesos a cualquier base de datos que tengan datos del titular de la tarjeta por lo que	**A**	8.7	Revisar los parámetros de configuración de la aplicación y de la base de datos para verificar que todos los usuarios estén autentificados antes de acceder.	Los cajeros y los supervisores tienen una ID y contraseña única, además solo pueden acceder a información básica del titular de la tarjeta (Nombre, número de factura, valor adquirido, número de voucher y	Se recomienda reformar los métodos de autenticación y los parámetros de autenticación dentro del sistema, además que se debe asignar una contraseña individual, de esa manera la	**PT007**

cualquier consulta y acción se realicen mediante métodos programáticos, solo los administradores de la base de datos puedan acceder, solo las aplicaciones pueden usar las ID de aplicaciones.			Revisar los parámetros de configuración de la base de datos y de la aplicación para verificar que el acceso de todos los usuarios, consultas del usuario y acciones del usuario en la base de datos se realicen únicamente mediante métodos programáticos.	número de lote). Los siete encargados de acceder a la base de datos solo pueden acceder a información básica del titular de la tarjeta (Nombre, número de factura, valor adquirido, número de voucher y número de lote) así como lo específica la norma, pero los Siete tienen la misma contraseña para acceder, esto hace que se incremente el riesgo de que puedan realizar actos maliciosos con los datos del titular de la tarjeta.	responsabilidad será individual.	
			Evaluar los parámetros de control de acceso de la base de datos y los parámetros de configuración de la aplicación de la base de datos y verifique que el acceso directo del usuario a la base de datos, o las consultas a esta, esté limitado a los administradores de la base de datos.			
			Revisar los parámetros de control de accesos de la base de datos, los parámetros de configuración de la aplicación			

			de la base de datos y las ID de aplicaciones relacionadas para verificar que solo las aplicaciones pueden usar las ID de la aplicación.			
Verificar que las políticas de seguridad y los procedimientos operativos de identificación y autenticación estén documentados y sean de conocimiento para todas las partes.	**D**	8.8.	Revisar la documentación y entrevistar al personal para verificar que las políticas de seguridad y los procedimientos estén documentados, implementados y sean conocidos para todas las partes afectadas.	La empresa si tiene política de seguridad documentada al igual que procedimientos, pero no se encuentra implementada del todo además que no está completa debido a que los usuarios realizan algunas actividades que no se encuentra dentro de la política por ejemplo en el caso de la autenticación de los cajeros y supervisores, este método no está establecido en la política de autenticación y claves, además que no es conocida por todas las partes afectadas, el personal debe conocer y respetar siempre las políticas y procedimientos operativos para que pueda administrar la identificación y la autorización.	Se recomienda realizar una reforma total de la política, después de eso se debe realizar capacitaciones al personal para que se distribuya y se conozca de la misma.	**PT008**

	Referencias:					
	F	Fuerte				
	A	Aceptable				
	D	Débil				
	PT	Papeles de Trabajo				

Elaborado por: Autoras.

3.2.3. PROGRAMA DE AUDITORIA DEL REQUERIMIENTO 9. Restringir el acceso físico a los datos del titular de la tarjeta.

Tabla 22 Matriz del Requerimiento 9: Restringir el acceso físico a los datos del titular de la tarjeta.

Matriz del Requerimiento 9: Restringir el acceso físico a los datos del titular de la tarjeta.			
Empresa Auditada:	Coral Hipermercado Racar Plaza (GO).		
Responsable:	Estefanía Ortega		
Supervisa:	Patricia Benenaula		
Requisitos de PCI DSS	**FAD**	**FORTALEZA**	**DEBILIDAD**
Verificar que se utilicen controles de entrada a la empresa para limitar y supervisar el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta.	**A**	Se mantiene cámaras de seguridad para la entrada y salida, monitoreo de todo el local de Coral Hipermercados, lo que brinda seguridad a los clientes y personal.	Sin embargo no se mantiene un debido control mediante filmaciones con cámaras a los cómputos que almacenan RACKs[26], sistemas de placas o leds en varias oficinas, centros de cómputo, redes, cableados, telecomunicaciones.
Verificar que se desarrollen procedimientos que permitan distinguir fácilmente a los empleados y a los visitantes.	**D**	Existe una diferenciación de empleados y visitantes pero no es una seguridad fuerte puesto que existen varias falencias.	Entre las falencias que se presentan esta que la política para distinción entre empleados y visitantes no se encuentra documenta, no existe un registro de ingreso y salida de las instalaciones, no se cambian los requisitos de acceso para visitantes, no existe un procedimiento claramente definido para el ingreso de los mismos.

[26] **RACK:** Es un sistema de almacenaje de datos, sirve para aplicaciones con un alto volumen de almacenamiento, ayuda al montaje de servidores facilitando la distribución de espacios en centros de datos de igual manera para el cableado de los datos.

Observar que se controle el acceso físico de los empleados a las áreas confidenciales mediante, accesos autorizados según el trabajo de cada persona, finalizar el acceso después de terminado el trabajo y desactivar todos los mecanismos de acceso físico como claves, tarjetas de acceso verificar que se devuelvan.	**F**	Existe un procedimiento documentado en la normativa para la seguridad de los datos del titular de la tarjeta que se mantiene realizándose en su mayoría.	Coral Hipermercado no almacena Datos de tarjetas, sin embargo los datos básicos que se registran para el control de transacciones se encuentran monitoreados, pero se recomienda que se mantengan formatos de autorización de accesos (formulario) que especifique las responsabilidades de los mismos al tener acceso al entorno de datos de titular de tarjetas (caso de facturación y servidores por el acceso remoto).
Verificar que se hayan implementado procedimientos para identificar y autorizar a los visitantes.	**D**	Existe identificaciones que se otorgan a los visitantes en su ingreso a las instalaciones mediante la entrega de un documento de identificación (cedula).	No se cumple con lo que manda la política de seguridad, los visitantes no siempre van acompañados, no se maneja una autorización física para las visitas, los carnet que se otorgan para la diferenciación entre empleados y visitantes no son adecuados y no registran fechas de vencimientos como pide la normativa PCI DSS, no se lleva un registro de los visitantes ni de su ingreso así como de su salida.
Comprobar y observar que se protejan físicamente todos los medios.	**F**	Se mantiene protección de los medios de Coral Hipermercado mediante el apoyo del departamento de seguridad y vigilancia.	Se recomendaría en caso de mejorar aún más la seguridad implementar cámaras de video en todos los departamentos (RACKs), señalización de las oficinas en donde se encuentran los medios de uso privado, exclusivo, y solo para personal autorizado.
Observar que se lleve un control estricto de la distribución interna o	**A**	No se almacenan datos de titular de tarjeta en medios.	Monitorear el aseguramiento del resto de medios que contiene otro tipo de información como bases de datos.

externa de todos los tipos de medios y realizar lo siguiente:			
Verificar que se lleve un control estricto del almacenamiento y la accesibilidad de los medios.	**D**	No se encontraron fortalezas.	La política no menciona información alguna sobre el monitoreo periódico de los inventarios de medios, se mantiene un registro de medios pero el personal desconoce del mismo y de sus responsabilidades sobre los equipos asignados.
Comprobar que se destruyan los medios cuando ya no sea necesario guardarlos por motivos comerciales o legales.	**F**	Coral hipermercados no almacena datos del titular de la tarjeta en ningún medio sin embargo si mantienen documentada la normativa sobre la destrucción de medios.	Se debería socializar la política de destrucción de medios a todo el personal pero en especial para aquellos que manejan datos confidenciales para la organización y los clientes (Vouchers en el departamento de Crédito).
Observar que se protejan los dispositivos que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta para proporcionar protección contra alteraciones y sustituciones.	**D**	No se encontraron fortalezas.	No se encuentra documentada la normativa sobre la protección de dispositivos, existe un procedimiento que es socializado de forma verbal, no se mantiene un listado de los dispositivos, el personal desconoce de estos registros, no se les capacita periódicamente sobre la prevención en riesgos que existen con el mal manejo de los dispositivos y a mas no se realizan inspecciones prioridad contra posibles alteraciones.

Referencias:

F	Fuerte
A	Aceptable
D	Débil
PT	Papeles de Trabajo

Elaborado por: Autoras.

Tabla 23 Requerimiento 9: Restringir el acceso físico a los datos del titular de la tarjeta.

Requerimiento 9: Restringir el acceso físico a los datos del titular de la tarjeta.						
Empresa Auditada:	Coral Hipermercado Racar Plaza (GO).			**Fecha de estudios:**	Periodo 2015 con corte a Junio	
Responsable:	Patricia Benenaula					
Supervisa:	Estefanía Ortega					
Objetivos a evaluar	**FAD**	**Nº**	**Procedimiento**	**Comentario**	**Recomendación**	**Referencia a PT**
9.1 Verificar que se utilicen controles de entrada a la empresa para limitar y supervisar el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta.	D	9.1	Verificar la existencia de controles de seguridad física para cada sala de informática, centro de datos y otras áreas físicas con sistemas en el entorno de datos del titular de la tarjeta: *Verificar que se controle el acceso con lectores de placas de identificación u otros dispositivos, placas autorizadas y llave y candado. *Observar un intento de algún administrador del sistema para iniciar sesión en las consolas	Hemos concluido que no se mantiene un adecuado sistema de seguridad que sea estricto para los entornos de sistemas de redes, dispositivos manuales, comunicaciones y líneas de telecomunicaciones puesto que se encuentran al acceso fácil de personas ajenas a la entidad, no están debidamente señalizados mediante letreros que prohíban el	Se recomienda que el control del ingreso de personal a áreas confidenciales sea para personal estrictamente autorizado ya sea centros de cómputo, redes, videos de cámaras de seguridad y a su vez estas instancias se encuentren monitoreadas a través de cámaras de seguridad para prevenir malas intenciones.	**PT001**

			de sistemas seleccionados de forma aleatoria en un entorno de titulares de tarjetas y verificar que estén asegurados y se impida el uso no autorizado.	ingreso y no mantienen cámaras de seguridad de acceso a centros confidenciales como el monitoreo de las cámaras de seguridad y los RACKs.		
		9.1.1 a	Verificar que las cámaras de video y otros mecanismos de control de acceso sean usados para supervisar los puntos de entrada y salida de áreas confidenciales.			
		9.1.1 b	Verificar que estas cámaras de video y otros mecanismos de control de acceso se encuentren protegidos contra alteraciones o desactivaciones.			
		9.1.1 c	Verificar que se controlen las cámaras de video y otros mecanismos y que los datos de los mismos se almacenen durante al menos tres meses.			

		9.1.2	Entrevistar al personal responsable y observar las ubicaciones de las conexiones de red de acceso público para verificar que se hayan implementado controles físicos o lógicos a fin de restringir el acceso a estas conexiones.			
		9.1.3	Verificar que haya restricción del acceso físico a los puntos de acceso inalámbricos, gateways, dispositivos manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones.			
9.2 Verificar que se desarrollen procedimientos que permitan distinguir fácilmente a los empleados y a los	**D**	9.2 a	Revisar los procesos documentados para verificar que los procedimientos se definan de manera tal que se pueda realizar una identificación y distinción entre empleados y visitantes	Se concluyó en que primero no existen procesos documentados que permitan socializar la distinción entre empleados y visitantes, por lo que no se puede saber si los	Se recomienda establecer procedimientos en la normativa sobre la identificación de empleados y visitantes, documentarlos e implementarlos mediante	**PT002**

visitantes de forma que: ***Se identifiquen empleados o visitantes nuevos (mediante la asignación de placas).** ***Existan cambios en los requisitos de acceso.** ***Se revoquen las identificaciones de empleados cesantes y las identificaciones vencidas de visitantes (placas de identificación).**			los procesos deben incluir: *Identificación de empleados o visitantes nuevos. *Cambio de requisitos de acceso. *Revocación de identificaciones de empleados cesantes y las identificaciones vencidas de visitantes.	requerimientos que se solicitan para el ingreso a las instalaciones son los más adecuados, si se revocan o no las identificaciones cesantes o quien realiza el manejo de los carnets que se entregan y que existan o no las autorizaciones debidas ya que según lo que se nos ha informado en las entrevistas realizadas al personal administrativo todo el procedimiento que se sigue para visitas es verbal, se sigue las actividades que se han venido haciendo desde tiempo atrás.	socializaciones a todo el personal de forma que disminuya el riesgo de posibles infiltraciones. Se puede mejorar la seguridad para las instalaciones. Solicitar una autorización u oficio previo para el ingreso sería de gran ayuda, mantener un registro de visitas, y sobretodo asignar un acompañante para los visitantes hasta verificar que lleguen al lugar que han indicado dirigirse y con la persona que solicitan.	
		9.2 b	Observar los procesos para identificar y distinguir entre empleados y visitantes y verificar que: *Los visitantes están claramente identificados. *Es fácil la distinción entre empleados y visitantes.			
		9.2 c	Verificar que el acceso al proceso de identificación este limitado solo al personal autorizado (ej. Proceso de sistema de placas).			

		9.2 d	Revisar los métodos de identificación implementados y verificar que identifiquen claramente a los visitantes, y que sea fácil realizar una distinción entre empleados y visitantes.			
9.3 Observar que se controle el acceso físico de los empleados a las áreas confidenciales mediante, accesos autorizados según el trabajo de cada persona, finalizar el acceso después de terminado el trabajo y desactivar todos los mecanismos de acceso físico como claves, tarjetas de acceso	**F**	9.3 a	En el caso de un grupo de empleados con acceso físico al entorno de datos del titular de la tarjeta, entreviste al personal responsable y observe las listas de control de acceso y verificar que: *Se autoriza el acceso al entorno de datos. *La persona necesita acceder para realizar su trabajo.	Coral Hipermercado de Grupo Ortiz no almacena datos de tarjetas sin embargo los datos básicos que se almacenan por control de registro de transacciones de los titulares de las tarjetas mantienen un procedimiento previamente documentado en la normativa.	Se recomendaría que el mismo sea monitoreado, actualizado y verificar que sea de conocimiento de todo el personal, puesto que varios accesos no cuentan con las debidas autorizaciones solo se realiza por medio verbal, pero no se realiza el llenado de un formato de autorización previamente firmado y autorizado como respaldo. Se debería realizar actualizaciones	**PT003**
		9.3 b	Observe el acceso del personal al entorno de datos del titular de la tarjeta para verificar que todo el personal tenga			

verificar que se devuelvan.			autorización antes de que accedan.		periódicas, obtener respaldos que comprometan al personal a mantener la debida responsabilidad en el manejo de los datos del titular de la tarjeta (ej. formato de autorizaciones).	
		9.3 c	Seleccionar un grupo de empleados que hayan dejado de trabajar recientemente y revisar las listas de control de acceso para verificar que no tenga acceso físico al entorno de datos.			
9.4 Verificar que se hayan implementado procedimientos para identificar y autorizar a los visitantes. Los	**F**	9.4	Verificar que los controles de acceso y las autorizaciones de los visitantes se implemente de la siguiente forma:	Coral Hipermercado de Grupo Ortiz no mantiene un adecuado control de ingreso de los visitantes existen varias falencias	Se recomienda que se implementes procedimientos para permitir el ingreso de visitantes, que se lleve un	**PT004**

procedimientos deben incluir:		9.4.1 a	Observar los procedimientos y entrevistar al personal para verificar que los visitantes reciben autorización antes de acceder a áreas de procesamiento o almacenamiento de datos de titular de tarjeta y estén siempre acompañados.	como la falta de registros de ingresos y personal que autoriza las visitas (formularios no se encuentran debidamente firmados y autorizados por un superior), no existen placas de identificación con fecha de vencimiento y que permitan la adecuada diferenciación de visitantes así como el proceso de administración al permitir que el visitante ingrese sin la compañía en todo momento de un empleado tal como manda la normativa PCI DSS.	registro de los visitantes de su ingreso y salida de las instalaciones, fechas, tiempos así como el departamento al que indico dirigirse y quien le estuvo acompañando durante la visita como el autorizante esto es de suma importancia para futuros eventos en donde se necesite evidencias para auditorias en caso de eventos o sucesos de fraudes.	
		9.4.1 b	Observe el uso de placas para visitantes u otro tipo de identificación a fin de verificar que estas identificaciones no permitan el acceso sin acompañantes a áreas físicas donde se procesan o conservan datos del titular de la tarjeta.			

		9.4.2 a	Observar las personas dentro de las instalaciones y verificar que usen placas para visitantes u otro tipo de identificación y que los visitantes se puedan distinguir fácilmente de los empleados que trabajan en la empresa.			
		9.4.2 b	Verificar que las placas de visitantes y otro tipo de identificación tengan vencimiento.			
		9.4.3	Observar la salida de los visitantes de las instalaciones para verificar que entreguen la placa u otro tipo de identificación al partir o al momento del vencimiento.			

		9.4.4 a	Verificar que se implemente un registro de visitantes para registrar el acceso físico a las instalaciones así como las salas de informática y los centros de datos donde se almacenan o transmiten los datos del titular de la tarjeta.			
		9.4.4 b	Verificar que el registro incluya: *Nombre del visitante *Empresa representada *Empleado que autoriza el acceso físico.			
		9.4.4 c	Verificar que el registro se conserve durante al menos tres meses.			
9.5 Observar que se protejan físicamente todos los medios.	**A**	9.5	Verificar que los procedimientos para proteger los datos del titular de la tarjeta incluyan controles para el resguardo seguro de todos los medios (entre estos:	Coral Hipermercado de Grupo Ortiz no mantiene dispositivos o medios de almacenamiento de datos de los titulares de tarjetas, se manejan, los		**PT005**

			computadoras, dispositivos electrónicos extraíbles, recibos e informes en papel y faxes).	computadores del sistema de facturación, Switch o Medianet por donde se realiza el pago con tarjetas de pago, y demás sistemas de red por donde se realiza toda la transaccionalidad del negocio, según lo observado se ha podido comprobar que se mantiene una seguridad contra posibles vulneraciones de personas externas a la organización mal intencionados.		
		9.5.1 a	Observar y verificar que la seguridad física del lugar de almacenamiento para confirmar que el almacenamiento del medio de la copia de seguridad este protegido.			
		9.5.1 b	Verificar que la seguridad del lugar de almacenamiento se revise al menos una vez por año.			
9.6 Observar que se lleve un control estricto de la distribución interna o externa de todos los tipos de medios y realizar lo	**A**	9.6	Verificar que exista una política para controlar la distribución de medios y que dicha política abarque todos los medios distribuidos incluso aquellos que se distribuyen a personas.	Coral Hipermercado no almacena datos de titular de tarjetas por lo tanto no existe el riesgo de almacenamiento de este tipo de información en	A pesar de que Coral Hipermercado no registre riesgo en la distribución de información mediante medios puesto que no se almacenan datos de	**PT006**

siguiente:		9.6.1	Verificar que todos los medios se hayan clasificado para poder determinar la confidencialidad de los datos.	medios o dispositivos, sin embargo para otro tipo de información que se respalden en medios, como por ejemplo las bases de datos como se puede evidenciar en el fragmento de la política que si se mantiene documentada se detallan las precauciones de ser el caso para el manejo de las bases de datos y según lo informado por el personal administrativo para la distribución se utiliza la conexión mediante acceso	tarjetas, se recomienda revisar el respaldo de los medios de bases de datos, el acceso a las mismas mediante accesos remotos al personal que lo realiza entregar una contraseña única de forma que se pueda monitorear el ingreso de los usuarios a la misma.	
		9.6.2 a	Entrevistar al personal y revisar los registros para verificar que todos los medios enviados fuera de la empresa estén registrados y se envíen por correo seguro u otro método que se pueda rastrear.			
		9.6.2 b	Seleccionar una muestra actual de varios días de registros de seguimiento externos de todos los medios y verificar que se documenten los detalles de seguimiento.			

		9.6.3	Seleccione una muestra actual de varios días de registros de seguimientos externos de todos los medios. Mediante la evaluación de los registros y las entrevistas al personal responsable, verificar que se cuente con la debida autorización de la gerencia cuando sea necesario trasladar los medios desde un área segura.	remoto, en esta instancia existe una falencia en cuanto a las credenciales de los usuarios de confianza ya que para el ingreso a la base de datos se mantiene una contraseña conjunta.		
9.7 Verificar que se lleve un control estricto del almacenamiento y la accesibilidad de los medios.	**A**	9.7	Obtener y revisar la política para controlar el almacenamiento y el mantenimiento de todos los medios y verificar que la política requiera inventarios periódicos de medios.	Se concluyó que si se mantienen políticas para el mantenimiento de los medios, pero no se nos permitió observar el registro de inventariado de los medios del almacenamiento y accesibilidad de los	Se recomienda socializar con el personal acerca de los medios que se encuentran a cargo de estos, el registro que se mantiene de los mismos y realizar inventarios periódicos que permitan conocer sobre el estado de	**PT007**

		9.7.1	Revisar los registros de inventarios de los medios para verificar que se conserven los registros y se lleven a cabo inventarios de medios al menos una vez al año.	mismos pero según nos informó personal administrativo no se les han realizado un monitoreo o inventario periódico de los medios que se encuentran a cargo de los empleados y estos desconocen de que existan registros de estos medios.	los mismos y si se encuentran funcionando o si ha existido algún tipo de atentado mal intencionado contra los mismos	
9.8 Comprobar que se destruyan los medios cuando ya no sea necesario guardarlos por motivos comerciales o legales de la siguiente manera:	**F**	9.8	Revisar periódicamente la política de destrucción de medios y verificar que abarquen todos los medios y que mantengan los siguientes requisitos: *Los materiales de copias en papel se deben cortar en tiras, incinerarse o convertirse en pulpa para cerciorarse de que no puedan reconstruirse. *Los contenedores de	Coral Hipermercado como se había mencionado con anterioridad no almacena datos del titular de la tarjeta lo que minimiza prácticamente todo el riesgo que contempla este requerimiento y además la empresa a pesar de no requerir el cumplimiento de este requerimiento si contemplan como un		**PT008**

			almacenamiento que se usan para los materiales que se destruirán deben ser protegidos. *Los datos del titular de la tarjeta guardados en medios electrónicos deben permanecer irrecuperables mediante un programa con la función de borrado seguro o mediante la destrucción física de los medios.	refuerzo procedimientos para la destrucción de medios e información confidencial para empresa.		
		9.8.1 a	Entrevistar al personal y revisar los procedimientos para verificar que los materiales de copias en papel se corten en tiras, se incineren o se conviertan en pulpa para que no se puedan reconstruir.			
		9.8.1 b	Revisar los contenedores de almacenamiento utilizados para los materiales que se			

			destruirán y verificar que dichos contenedores estén asegurados.			
		9.8.2	Verificar que los datos del titular de la tarjeta guardados en dispositivos electrónicos sean irrecuperables mediante un programa con la función de borrado seguro de acuerdo con las normas aceptadas por la industria para lograr una eliminación segura o bien destrúyalos físicamente.			
9.9 Observar que se protejan los dispositivos que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta para proporcionar	**D**	9.9	Revisar las políticas y los procedimientos documentados para verificar que se realice: *Conservar una lista de los dispositivos. *Inspeccionar los dispositivos periódicamente para buscar intentos de alteración o sustitución.	Coral Hipermercado no mantiene un procedimiento de seguridad documentado para los dispositivos sin embargo si hay un conocimiento general por parte de los empleados debido a capacitaciones recibidas al ingresar a	se recomienda desarrollar un procedimiento para el manejo de la seguridad de los dispositivos y que se documenten en la normativa de manera que se socialice a todo el personal y en especial al personal de Facturación.	**pt009**

protección contra alteraciones y sustituciones.			*Capacitar al personal para que detecten comportamientos sospechosos e informen la alteración o sustitución de dispositivos.	laborar en la organización pero estas deberían estar primero documentadas y según lo requiere el cumplimiento de la normativa implementadas con capacitaciones periódicas. No se mantiene un registro de dispositivos, el personal desconoce de listado de dispositivos y su responsabilidad ante la seguridad de estos. El personal debido a la experiencia que van adquiriendo mantiene seguridad ante los dispositivos pero esto no es suficiente para minimizar el riesgo que implican los dispositivos que si bien mantienen	Se deberían realizar inspecciones periódicas para controlar que no hayan sufrido alteraciones o intento de sustituciones, mantener capacitado al personal para que pueden defenderse y detectar intentos de alteraciones, sustituciones, autorizaciones no permitidas a personal que intente dar soporte sin previo aviso de la gerencia, se necesita disminuir el riesgo ante manejos mal intencionados de los dispositivos.	
		9.9.1 a	Revisar la lista de los dispositivos y verificar que incluya: *Marca y modelo del dispositivo. *Ubicación del dispositivo (dirección de la empresa o la instalación donde se encuentra el dispositivo) *Número de serie del dispositivo u otro método de identificación única.			
		9.9.1 b	Seleccionar una muestra de dispositivos de la lista y observar la ubicación del dispositivo para verificar que la lista sea exacta y está			

			actualizada.	contacto directo con las tarjetas de pago.		
		9.9.1 c	Entrevistar al personal para verificar que la lista de dispositivos se actualice cuando se agreguen reubiquen, desactiven, etc., dispositivos.			
		9.9.2 a	Revisar los procedimientos documentados para verificar que estén definidos para incluir: *Procedimientos para inspeccionar los dispositivos. *Frecuencia de las inspecciones.			
		9.9.2 b	Entrevistar al personal responsable y observar los procesos de inspección para verificar: *El personal conoce los procedimientos para			

			inspeccionar los dispositivos. *Todos los dispositivos se inspeccionan periódicamente para buscar indicios de alteraciones y sustitución.			
		9.9.3a	Revise el material de capacitación para el personal que trabaja en los puntos de venta para verificar que en la capacitación se incluya. *Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de otorgarles autorización para acceder y modificar un dispositivo o solucionar algún problema. *No instalar, cambiar ni devolver dispositivos sin verificación. *Estar atentos a			

			comportamientos sospechosos cerca del dispositivo (por ej. personas desconocidas que intentan desconectar o abrir el dispositivo). *Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ej. a un gerente o encargado de seguridad).			

		9.9.3 b	Entrevistar a un grupo del personal del punto de venta para verificar que hayan recibido capacitación y que conozcan los procedimientos para: *Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de otorgarles autorización para acceder y modificar un dispositivo o solucionar un problema. *No instalar, cambiar ni devolver dispositivos sin verificación. Estar atentos a comportamientos sospechosos cerca del dispositivo (por ej. personas desconocidas que intentan desconectar o abrir el			

			dispositivo). *Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ej. a un gerente o encargado de seguridad).			

	Referencias:	
	F	Fuerte
	A	Aceptable
	D	Débil
	PT	Papeles de Trabajo

Elaborado por: Autoras.

INFORME FINAL

"Auditoría de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCI DSS aplicada a CORAL HIPERMERCADO, RACAR PLAZA con corte a Junio de 2015."

Cuenca- Ecuador 2016.

Cumplo con informar el resultado de la auditoría realizada al cumplimiento de los Requerimientos 7, 8, 9 de la norma PCI SS aplicada a Coral Hipermercado Racar Plaza con corte a Junio de 2015.

Saluda atentamente,

---------- ----------
Patricia Benenaula L. Estefania Ortega

Objetivos de la Auditoria:

- **Objetivo General**

Verificar el nivel de cumplimiento de la seguridad de los datos de los titulares de las tarjetas de pago por medio de una auditoria de sistemas de manera que permita a la empresa tener información veraz y efectiva, además se logrará el apropiado resguardo de la información de las tarjetas de pago para un correcto desenvolvimiento y toma de decisiones de la empresa.

- **Objetivos Específicos**

✓ Verificar que se restrinja el acceso a los datos de los titulares de tarjetas según la necesidad de saber que tenga la entidad.

✓ Comprobar que se identifique y autentique el acceso a los componentes del sistema.

✓ Observar que se restrinja el acceso físico a los datos del titular de la Tarjeta.

Alcance de Auditoría

Validar el cumplimiento de los requerimientos 7. “Restringir el acceso a los datos del titular de la tarjeta según las necesidades de saber que tenga la empresa”, 8 “Identifique y autentifique el acceso a los componentes del sistema”, 9 “Restringir el acceso físico a los datos del titular de la tarjeta” de la norma PCI DSS, aplicada a Comercio Nivel 4 según MasterCard y Nivel 2 según American Express.

Metodología de la Auditoría

La revisión fue en conformidad con la Norma de Seguridad de Datos de Titulares de Tarjetas de pago PCI DSS, incluyo pruebas de validación y otros medios técnicos considerados necesarios en las circunstancias.

Esta metodología fue alineada con el marco a nivel mundial, ISACA conocido como la asociación internacional de mayor apoyo para las actividades de auditoría.

Resultados de la Auditoría

Luego de haber realizado la auditoria a los Requerimientos 7, 8, 9 de la Normativa de Seguridad de Datos de Titulares de Tarjetas de pago PCI DSS se obtuvieron los siguientes resultados que detallaremos a continuación:

Requerimiento 7: Restricción al acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.

7.1. En este punto se observó las limitaciones del acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de acceso, se obtuvo como resultado:

- ✓ La empresa Coral Hipermercado, en el caso de anulación de voucher no tiene definida en los manuales de funcionamiento quien debe realizar esa labor, se le designa al supervisor sin ninguna aprobación documentada.
- ✓ Los encargados del servidor transaccional no tienen manual de funcionamiento por lo que no se sabía con exactitud cuáles eran las funciones que se deben realizar, pero según las entrevistas efectuadas, ellos tiene acceso a otros componentes del sistema que no están dentro de su labor.

7.2 Se observó el sistema de control de acceso establecido para los componentes del sistema que restrinja el acceso según la necesidad del usuario de conocer y que se configure para "negar todo".

- ✓ La política de seguridad de accesos se encuentra documentada pero presenta falencias para los servidores transaccionales debido a que se mantiene una clave para el manejo de varias personas para soporte del sistema y accesos remotos.
- ✓ Los sistemas de control de acceso para los servidores transaccionales no cuentan con la configuración predeterminada de "negar todos", se pudo realizar una observación y verificar que al ingresar varias claves el sistema no se bloquea de forma automática como debería después de varios intentos fallidos.

7.3 Se verificó que las políticas de seguridad y procedimientos operativos que restringen el acceso a los datos del titular de la tarjeta estén

documentados, implementados y sean de conocimiento para todas las partes afectadas.

- ✓ La Política de Seguridad en cuanto a la restricción de accesos de datos de los titulares de tarjetas no se encuentra socializada a todos los empleados, no se realizan capacitaciones periódicas para mantenerlos actualizados. Cabe mencionar que el personal de facturación indicó que se les realiza una capacitación cada 3 meses por parte del departamento de crédito para el manejo adecuado de pagos con tarjetas de pago pero esto no implica el conocimiento de una normativa ni del proceso de seguridad de accesos a los datos.

Requerimiento 8: Identifique y autentifique el acceso a los componentes del sistema.

8.1. Se verificó que se haya definido e implementado las políticas y procedimientos para garantizar la correcta administración de la identificación de todos usuarios, en los componentes del sistema, el resultado fue:

- ✓ En la política de autentificación no hay algún parámetro que indique, cuales es número determinado de intentos y por cuanto tiempo debe permanecer bloqueada en el caso de que se intente ingresar con contraseñas incorrectas.
- ✓ No existe ninguna política o procedimiento acerca de que se debe inactivar el sistema en el caso de que pase sin ser usado un lapso de

15 minutos o menos.

- ✓ Los encargados del servidor transaccional no reciben una contraseña para cada uno si no esta es compartida.
- ✓ No existe monitoreo de las cuentas de acceso remoto por parte de la empresa.

- ✓ En las pruebas realizadas no se bloqueó la cuenta cuando se hizo más de seis intentos de inicio de sesión no válidos.

8.2. Se evaluó que exista una correcta administración de autenticación de todos los usuarios en los componentes del sistema y que al menos se use algo que el usuario sepa (contraseña, o frase de seguridad), algo que el usuario tenga (dispositivo token, tarjeta inteligente) y algo que el usuario sea (rasgo biométrico), y se determinó que:

- ✓ La empresa no aplica procedimientos de autentificación para el cambio de credenciales de autenticación.
- ✓ No describe todos los métodos de autenticación dentro de la política.
- ✓ Los encargados del servidor transaccional no hacen cambios en sus contraseñas, mantienen la misma que se les otorgó cuando ingresaron a la organización.
- ✓ En el caso de los cajeros y supervisores, no pueden cambiar su contraseña debido a que es su huella digital, pero las personas encargadas de resguardar estos datos mantienen la misma contraseña sin hacer ningún cambio.

8.3. Se observó que se incorpore la autenticación de dos factores para el acceso remoto a la red desde fuera de la misma por parte del personal y los resultados de esta evolución fueron:

- ✓ Existe un solo método de autentificación cuando hay acceso remoto, pero según la normativa debería existir dos métodos de autenticación cuando existe acceso remoto.

8.4. Se verificó que se documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios y que esta incluya lineamientos para seleccionar una credencial de autenticación sólida, además de como los usuarios deben proteger las credenciales, instrucciones para no seleccionar contraseñas utilizadas anteriormente e

instrucciones para cambiar la contraseña si es necesario y de este análisis se obtuvo:

- ✓ La empresa no reparte la política de autenticación a los usuarios.
- ✓ No tiene ningún lineamiento que ayude al cambio de contraseñas para no usar las anteriores.

8.5. Se evaluó que no se utilice ID ni contraseñas de grupo, compartidas ni genéricas, los resultaron fueron:

- ✓ Los usuarios encargados del servidor transaccional y de los que reguardan los datos de las huellas digitales, mantienen la misma contraseña que se les otorgó al momento del ingreso a la organización.

8.6. Se Verificó que en el caso de que se use otros mecanismos de autenticación estos se asignen a una sola cuenta y no compartirlos entre varias, además verificar que se implementen controles físicos y lógicos para garantizar que solo la cuenta deseada usa esos mecanismos para acceder, se obtuvo:

- ✓ La empresa no se usa otros mecanismos de autentificación como tokens, tarjetas inteligentes y certificados.

8.7. Se observó que se restrinjan todos los accesos a cualquier base de datos que tengan datos del titular de la tarjeta por lo que cualquier consulta y acción se realicen mediante métodos programáticos, solo los administradores de la base de datos puedan acceder, solo las aplicaciones pueden usar las ID de aplicaciones, se determinó:

- ✓ Los encargados de acceder a la base de datos tienen una misma contraseña.

8.8. Se verificó que las políticas de seguridad y los procedimientos operativos de identificación y autenticación estén documentados y sean de conocimiento para todas las partes y obtuvo como resultado:

- ✓ La política de seguridad no se encuentra implementada del todo.
- ✓ La política de seguridad no está completa debido a que los usuarios realizan algunas actividades que no se encuentra dentro de la política por ejemplo en el caso de la autentificación de los cajeros y supervisores, este método no está establecido en la política.
- ✓ La política no es conocida por todas las partes afectadas.

Requerimiento 9: Restringir el acceso físico a los datos del titular de la tarjeta.

9.1 Verificar que se utilicen controles de entrada a la empresa para limitar y supervisar el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta.

- ✓ No se mantiene seguridad para las áreas que almacenan los Racks, sistemas de placas o leds en varias oficinas, centros de cómputo, redes, cableados, telecomunicaciones.
- ✓ Los servidores transaccionales pueden ingresar mediante acceso remoto en las consolas de otros sistemas donde se encuentran datos de titular de tarjeta (solo básicos) mediante una contraseña conjunta lo que podría ocasionar riesgo al verse expuestos actos maliciosos.
- ✓ Se verifico que los datos de cámaras de video y otros mecanismos no se almacenan durante al menos tres meses como manda la normativa, estas se eliminan cada 20 días y se regraban los nuevos videos en los mismos dispositivos.
- ✓ No existe una adecuada restricción del acceso físico a los puntos de acceso inalámbricos, Gateway, dispositivos manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones ya que no mantienen cámaras de vigilancia en

donde se ubican estos dispositivos y el ingreso de personas no es absolutamente restringido o con previa autorización documentada.

9.2 Se verificó que se desarrollen procedimientos que permitan distinguir fácilmente a los empleados y a los visitantes.

- ✓ No existe una política documenta que defina como realizar la distinción entre empleados de visitantes.
- ✓ Al no existir la política para visitantes no se puede saber cómo realizan el cambio de requisitos de acceso así como la revocación de identificaciones de empleados cesantes y las identificaciones vencidas de visitantes.
- ✓ El proceso de identificación (asignación de placas de visitantes) no se encuentra definido claramente y limitado solo al personal autorizado.
- ✓ No existe un registro de ingreso y salida de las instalaciones.

9.3 Se observó que se controle el acceso físico de los empleados a las áreas confidenciales mediante, accesos autorizados según el trabajo de cada persona, finalizar el acceso después de terminado el trabajo y desactivar todos los mecanismos de acceso físico como claves, tarjetas de acceso verificar que se devuelvan.

- ✓ No se mantienen formatos de autorización de accesos (formulario) que especifique las responsabilidades de los mismos al tener acceso al entorno de datos de titular de tarjetas (caso de facturación y servidores por el acceso remoto).

9.4 Se verificó que se hayan implementado procedimientos para identificar y autorizar a los visitantes.

- ✓ Los visitantes no siempre van acompañados a las áreas a donde dicen dirigirse.
- ✓ No se maneja una autorización física para las visitas.

- ✓ Los carnets que se otorgan para la diferenciación entre empleados y visitantes no son adecuados, no registran fechas de vencimientos como pide la normativa PCI DSS.
- ✓ No se lleva un registro de los visitantes ni de su ingreso así como de su salida.
- ✓ Al no mantener un registro de visitantes tampoco se estaría cumpliendo con mantener los registros al menos durante 3 meses como manda la normativa.

9.5 Se comprobó y observó que se protejan físicamente todos los medios.

- ✓ Coral hipermercado no almacena datos de titulares de tarjetas y se observó que todos los medios se hayan debidamente resguardados, sin embargo si se pudiese reforzar la seguridad de los Racks.

9.6 Se observó que se lleve un control estricto de la distribución interna o externa de todos los tipos de medios.

- ✓ Este requerimiento no aplica para el cumplimiento de Coral Hipermercado debido a que no almacenan datos de titulares de tarjetas en ningún medio ni físico ni electrónico. Sin embargo se mantienen las bases de datos las mismas que mantienen una falencia en cuanto al monitoreo de las mismas por medio de los accesos remotos, los servidores transaccionales mantienen una contraseña conjunta para brindar soporte.

9.7 Se verificó que se lleve un control estricto del almacenamiento y la accesibilidad de los medios.

- ✓ La política no menciona información alguna sobre el monitoreo periódico de los inventarios de medios, se mantiene un registro de medios pero el personal desconoce del mismo y de sus responsabilidades sobre los equipos asignados.

9.8 Se comprobó que se destruyan los medios cuando ya no sea necesario guardarlos por motivos comerciales o legales.

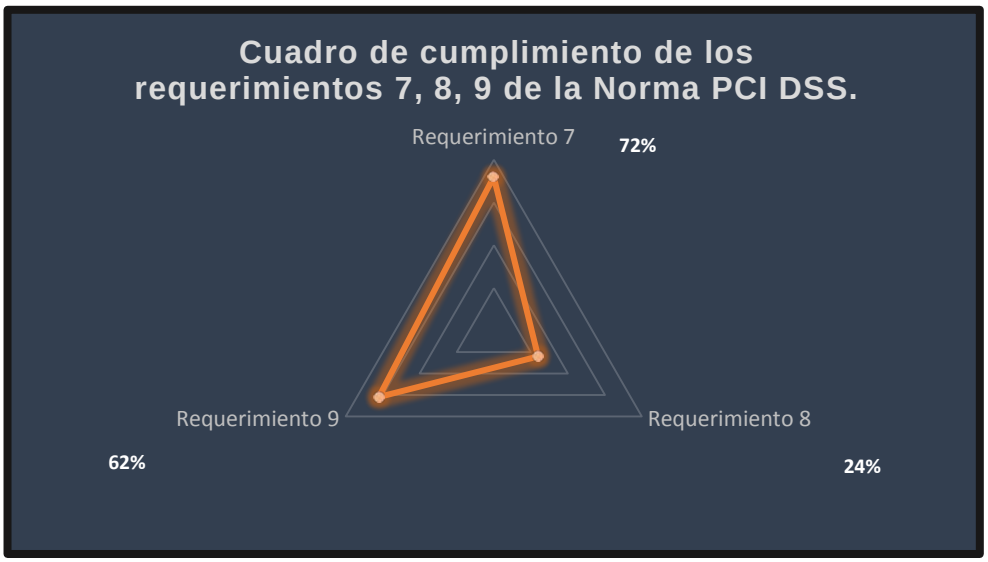
- ✓ Coral Hipermercado cumple con este requerimiento a cabalidad puesto que a más de mantener en la normativa documentados los procesos para destrucción de medios, no se almacenan datos de titulares de tarjetas en ningún dispositivo.

9.9 Se observó que se protejan los dispositivos que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta para proporcionar protección contra alteraciones y sustituciones.

- ✓ No se contempla en la política de seguridad una normativa para los procedimientos de protección de los dispositivos que capturan datos de tarjetas.
- ✓ No se mantiene una lista de los dispositivos, el personal desconoce de estos registros.
- ✓ No se capacita periódicamente al personal sobre la prevención de comportamientos sospechosos, posibles riesgos que existen frente a alteraciones o sustituciones de los dispositivos.
- ✓ Al no existir una lista de los dispositivos no se puede saber con exactitud si esta es actualizada y exacta según como se agreguen o desactiven los dispositivos.
- ✓ Según informo el personal administrativo no se realizan inspecciones de los dispositivos.
- ✓ No se realizan capacitaciones al personal para que estos logren identificar y mantener en cuenta los posibles intentos de alterar los dispositivos.
- ✓ Se entrevistó al personal de puntos de venta y nos informaron que no se han recibido capacitaciones para el manejo adecuado de los dispositivos, simplemente se les enseño lo que deben tener en cuenta para la seguridad de los mismos al ingreso a laborar en la

organización y desde entonces no se les ha actualizado en este tema.

Ilustración 13. Cuadro de cumplimiento de los requerimientos 7, 8, 9 de la Norma de Seguridad de Datos de Titulares de Tarjetas de Pago PCI DSS



Elaborado por: Autoras.

Los resultados obtenidos de la auditoria hecha al cumplimiento de los Requerimientos 7, 8, 9 de la norma PCI DSS a la empresa Coral Hipermercado Racar Plaza con corte a junio 2015, nos permitió evidenciar que se mantiene un nivel de cumplimiento mayor con el 72% en el requerimiento 7. “Restricción al acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa”. Le sigue con un 62% el requerimiento 9 “Restringir el acceso físico a los datos del titular de la tarjeta” y finalmente con un 24% el requerimiento 8 “Identifique y autentifique el acceso a los componentes del sistema”, mediante esta gráfica podríamos afirmar que el requerimiento 8 podría presentar mayor riesgo para la organización.

Conclusión:

Coral Hipermercado de Grupo GO mantiene en su mayoría documentada en la Política de Seguridad que han implementado en la organización,

detallados los procesos a seguir para diversas actividades, sin embargo después de realizar una auditoría a los procedimientos que se deben seguir para lograr el cumplimiento de los Requerimientos de la Normativa PCI DSS se llegó a concluir que la política que mantienen no se encuentra del todo socializada es decir no es de conocimiento de todas las partes afectadas. Se encontró que el sistema de servidores transaccionales no funciona de acordó a las políticas que se mantienen puesto que manejan claves grupales para accesos remotos lo que agrega un riesgo mayor para el monitoreo de actividades realizadas y la determinación de responsabilidades en caso de posibles actos maliciosos. Por otro lado en el Sistema de Facturación los supervisores son los encargados de las anulaciones de Voucher donde intervienen las tarjetas de pago, pero este procedimiento no se encuentra documentado en ninguna parte de la norma de seguridad. Al revisar las identificaciones y autentificaciones logramos observar que estas no son adecuados para los accesos remotos, las contraseñas de servidores transaccionales son compartidas, no existe un bloqueo de claves después de varios intentos, no se cierra sesión automáticamente en las consolas, no se realiza un monitoreo a los accesos remotos, el cambio de contraseñas no tienen establecido un tiempo de vigencia para las mismas. Finalmente la restricción de accesos a los datos de titulares de tarjetas si bien el riesgo se encuentra minimizado a partir de que Coral Hipermercado no almacene datos en ningún dispositivo y a mas a pesar de que no deban mantienen una normativa para la destrucción de medios que almacenen datos confidenciales o datos en general, pero se observó que la seguridad de accesos de visitantes es débil al igual que el manejo de los dispositivos que capturan datos de tarjetas que no mantienen un registro, detalle de responsables ni la ubicación de los mismos, todo lo detallado anteriormente puede originar a que la organización abra brechas para posibles fraudes, robo de datos, hurto o manipulación de terminales lo que se podría prevenir al realizar las respectivas correcciones previo las recomendaciones.

Recomendación:

Previo a las falencias detectadas en la auditoría realizada, hemos visto conveniente recomendar primero la actualización de la política para agregar las especificaciones faltantes como el detalle de accesos según los perfiles de los usuarios, anulación de voucher, registro de visitantes, Seguridad de dispositivos entre otros, la normativa de seguridad de Coral Hipermercado debe ser revisada periódicamente e irse actualizando de igual manera cada vez que surjan cambios para la misma debido a la premura de las circunstancias. Se recomienda también eliminar las claves conjuntas puesto que podría ocasionar indebidos usos de a información, y realizar la socialización de la norma de forma que todo el personal de Grupo GO se mantenga informado para que apoyen al monitoreo de la seguridad de las instalaciones como de la información contenida de sobremanera los datos de los titulares de las tarjetas. Ajustar las políticas de autentificación es imperativo así como las contraseñas del sistema, capacitar más al personal sobre las políticas de autentificación de forma que se mantengan contraseñas seguras. Es vital también que la organización empiece a manejar documentación física de forma que exista evidencia por ejemplo para las autorizaciones de visitas a las instalaciones, llenado de formularios para accesos a los distintos sistemas, considerar el hecho de que las visitas deben ser monitoreadas de una forma más apropiada, el fácil ingreso de terceras personas a la institución da oportunidad a que de igual manera personas mal intencionadas logren el acceso rápido a las instalaciones. En general es necesario mantener procedimientos adecuados para el monitoreo de los cómputos, dispositivos, medios informáticos, y socializar estos procedimientos de forma que se disminuya el riesgo de cometer errores debido al no conocimiento y aplicación de la normativa por parte de los empleados de la organización. Coral Hipermercado debería tomar en consideración las recomendaciones previstas en la brevedad del tiempo

para que se evite verse expuestos a problemas de incumplimientos de la Normativa.

CAPÍTULO 4

4. CONCLUSIONES Y RECOMENDACIONES.

Conclusiones.

Coral Hipermercado de Grupo GO al realizar transacciones con tarjetas de pago se encuentren dentro de la clasificación de Comercios que deben obligatoriamente cumplir con la Normativa PCI DSS. La clasificación establece 4 niveles, Coral Hipermercado según lo establecido por MasterCard se encuentra dentro del Nivel 4, estos deben llenar un Cuestionario de Autoevaluación conocido como SAQ de forma anual, misma que debe ser firmado por el Oficial de la compañía. Por el nivel de transacciones que establece American Express Coral Hipermercado se encuentra como Nivel 2 debiendo además de presentar el Cuestionario de Autoevaluación (SAQ), requerir que un auditor tome la actividad y sea certificado por un Council de PCI o de ser el caso revisada por un (QSA) que es quien realiza la evaluación en el sitio para disminuir el riesgo del negocio. La organización debe cumplir a cabalidad con los Requerimientos de la normativa por lo que se vio viable la realización de la auditoria a los requerimientos 7, 8, 9 en donde se encontraron las siguientes observaciones:

1.- La política no define la anulación de voucher, tarea que lo realiza el supervisor sin ninguna aprobación documentada.

2.- Los encargados del servidor transaccional no tienen manual de funcionamiento, no hay exactitud de que funciones realizan. Tienen acceso a otros componentes del sistema sin previo formulario de autorización y no se detalla en las labores.

3.- Los servidores transaccionales mantienen una clave conjunta para soporte del sistema y accesos remotos.

4.- Los sistemas de control de acceso de los servidores transaccionales no cuentan con la configuración predeterminada de "negar todos", el sistema no se bloquea de forma automática después de varios intentos fallidos.

5.- La política de restricción de accesos a los datos de tarjetas de pago no es socializada a todos los empleados, no se realizan capacitaciones periódicas.

6.- En la política de autentificación no hay parámetros que detallen, un número determinado de intentos y por cuanto tiempo debe permanecer bloqueada la consola en el caso de que se intente ingresar con contraseñas incorrectas.

7.- La política no detalla nada acerca de que se debe inactivar el sistema cuando este sin usarse un lapso de 15 minutos o menos.

8.- No existe monitoreo de las cuentas de acceso remoto.
9.- La empresa no aplica procedimientos para el cambio de credenciales de autenticación. (Los usuarios encargados del servidor transaccional y de los que reguardan los datos de las huellas digitales).

10.- Se utiliza un solo método de autentificación cuando hay acceso remoto, pero según la normativa debería existir dos métodos.

11.- La empresa no usa otros mecanismos de autentificación como tokens, tarjetas inteligentes y certificados que refuercen la seguridad.

12.- No existe debida seguridad para las áreas que almacenan los Racks, sistemas de placas o leds en varias oficinas, centros de cómputo, redes, cableados, telecomunicaciones.

13.- Los datos de cámaras de video y otros mecanismos no se almacenan durante al menos tres meses como manda la normativa, son eliminados cada 20 días y se graban los nuevos videos en los mismos dispositivos.

14.- No existe una política que defina como distinguir empleados de visitantes. 15.- No se mantiene una política para el ingreso de visitantes, se desconoce cómo realizan el cambio de requisitos de acceso y revocación de identificaciones de empleados cesantes e identificaciones vencidas de visitantes.

16.- El proceso de asignación de placas a los visitantes no está definido claramente y limitado solo al personal autorizado. 17.- No existe un registro de ingreso y salida de visitantes.

18.- No existen formatos de autorización que especifiquen las responsabilidades de tener acceso al entorno de datos de titular de tarjetas (servidores transaccionales por el acceso remoto).

19.- No se acompaña a las visitas a las áreas a donde se dirigen.

20.- No se maneja una autorización física para las visitas.

21.- No se realiza monitoreo e inspecciones periódicas de los inventarios de medios, informan que si se mantiene un registro pero el personal desconoce del mismo y de sus responsabilidades sobre los equipos asignados.

22.- No hay normativa de los procedimientos para la protección de los dispositivos que capturan datos de tarjetas.
23.- No se capacita periódicamente al personal sobre el manejo adecuado y la prevención de comportamientos sospechosos, posibles riesgos que existen frente a alteraciones o sustituciones de los dispositivos.

La empresa a pesar de su conocimiento de la normativa PCI DSS con anterioridad no presenta el cumplimiento a cabalidad de los requerimientos, según la auditoría realizada y las observaciones que se lograron encontrar existen falencias en varios procedimientos y política en general. Presentan un 72% de cumplimiento del requerimiento 7, 24% del requerimiento 8, y del requerimiento 9 un 62%, evidenciando la incorrecta implementación de los requerimientos de la normativa. Las

vulnerabilidades encontradas representan riesgo para la organización, desconfianza en de las entidades intermediarias en caso de realizarse una auditoría y percatarse de estas falencias, pudiendo incluso perder el permiso de transaccionar con tarjetas de pago en caso de compromiso de datos haciendo que existan perdidas en el negocio al incurrir en mayores costes.

Recomendaciones

El cumplimiento de los requerimientos de la normativa PCI DSS es de gran aporte para la organización puesto que servirá de apoyo para reforzar la seguridad de la información de datos confidenciales a más de los datos de titulares de tarjetas de pago permitiendo que se corrijan las vulnerabilidades presentadas en la empresa y de esta manera mejorando la toma de decisiones y la gestión de la organización.

En base a lo descrito con anterioridad se recomienda:

1.- Actualizar la política de seguridad de Coral Hipermercado periódicamente de forma que se integren procedimientos faltantes, se detallen actividades a realizar y quien debe realizarlas.

2.- La política debería describir que funciones son atribuidas a los supervisores y servidores transaccionales.

3.- No se debe mantener claves conjuntas ya que involucran un nivel de riesgo alto al verse expuestos a actos mal intencionados, se recomienda asignar una clave única para el control de accesos remotos.

4.- Se debería configurar el sistema de los servidores transaccionales para que mantengan la configuración predeterminada de negar todos de forma que se evite consultas no permitidas o accesos no autorizados.

5.- La normativa de restricción de acceso a los datos de los titulares de tarjetas debe ser socializada a mayor cabalidad de forma que todo el personal comprenda el nivel de riesgo que existe en el manejo no

adecuado de estos datos y también se deberían dar capacitaciones de forma periódica para el conocimiento general de la norma.

6.- Se debe actualizar la política de autenticaciones de la organización de forma que se detalle el número de intentos permitidos así como el establecimiento de tiempo de bloqueo debido a intentos fallidos de contraseñas.

7.- Se debe detallar en la política e implementarse en los sistemas de cómputo la inactivación del sistema luego de que no se use por un lapso de 15 minutos o menos.

8.- Es importante y necesario que se realice un monitoreo de las cuentas de acceso remoto puesto que por su amplitud de ingreso a datos de varias dependencias se encuentran expuestos a mayores riesgos de alteraciones o actos mal intencionados.

9.- Se debe implementar y aplicar procedimientos para el cambio cada cierto tiempo de autenticaciones del personal de forma que se mantenga segura la contraseña al no establecer un parámetro único por tanto tiempo.

10.- Se debería establecer parámetros de configuración de tal manera que el sistema pida dos métodos de autenticación al momento de acceder mediante acceso remoto.

11.- Para reforzar la seguridad y mantener un mayor nivel de confidencialidad, se recomienda mantener otros mecanismos de autenticación o una combinación de ellos.

12.- Se debería prohibir el acceso de personas que no laboren, y no necesiten estrictamente ingresar a áreas donde se encuentran los Racks, sistemas de placas o leds en varias oficinas, centros de cómputo, redes, cableados, telecomunicaciones.

13.- Se deben almacenar los datos de cámaras de video y otros mecanismos durante al menos tres meses como manda la normativa para

mantener un histórico y evidencias de lo ocurrido en caso de necesitarse en posterioridad.

14.- Es necesario que se implemente una política para el ingreso de visitantes a la organización, el sistema que se maneja es muy deficiente, es necesario que se formule un proceso con los requisitos y encargados únicos del ingreso, registro, asignación de placas, y confirmación de salida de personal externo que ingresa a la institución.

15.- Se debe también detallar en la política de visitantes como se realizara la revocación de identificaciones de empleados cesantes e identificaciones vencidas de visitantes.

16.- De igual manera la política debe contener dentro de su documentación quienes serán los encargados exclusivos de asignar las placas de ingreso de los visitantes mismos que correrán con la responsabilidad del ingreso y salida. 17.- Es primordial que se lleve un registro de ingreso y salida de los visitantes de las instalaciones de la organización mediante esto se puede determinar pruebas de auditorías futuras, mantener un control de quienes ingresan a la institución en el día en caso de posibles accidentes en el instante y encontrar a los posibles implicados.

18.- Se debería exigir el llenado de formularios previos antes de otorgarse el acceso al entorno de datos de titular de tarjetas, sobremanera en el caso de los servidores transaccionales.

19.- El acompañamiento a los visitantes a las áreas a donde estos desean dirigirse debería ser primordial según como manda el Requerimiento 9 puesto que ayuda a evitar posibles actos maliciosos de personal ajeno a la institución. 20.- Para el ingreso de visitas a las instalaciones de la organización se recomienda que se exija la previa autorización (formato físico) donde se detalle la firma, y autorizante de la misma.

21.- El monitoreo de los medios así como su inventario debe ser realizado periódicamente para que las responsabilidades sobre los equipos asignados se encuentren claramente definidas.

22.- Se debe incluir en la Política de Seguridad de Coral Hipermercado procedimientos que detallen la protección de los dispositivos que capturan datos de tarjetas, el manejo y responsabilidad de los mismos de forma que se vea minimizado el riesgo de alteraciones a estos dispositivos que mantienen contacto directo con tarjetas de pago.

23.- Es necesario que el personal encargado del manejo de los dispositivos que mantienen contacto con tarjetas de pago (POS) reciban capacitaciones periódicas sobre actualizaciones en temas sobre prevenciones ante comportamientos sospechosos, riesgos de fraudes, alteraciones o sustituciones.

BIBLIOGRAFÍA

Acosta, f. (2009). *diccionario de la real academia española.* honduras: honduras.

BBVA, F. (2013). *Fundeu.es*. Recuperado el 22 de Octubre de 2015, de Experiencia, pericia y experticia, alternativas a expertise: http://www.fundeu.es/recomendacion/experiencia-pericia-y-experticia-alternativas-a-expertise/

Cartaya, M. (2007). *COFAE CID Auditoría de Estado*. Recuperado el 10 de Octubre de 2015, de Riiesgo de Auditoría: http://www.oas.org/juridico/PDFs/mesicic4_ven_ries_aud_2014.pdf

COBIT. (2007). *IT ASSURANCE GUIDE .* Estadis Unidos.

COBIT, F. (2014). *VAL IT.*

Contraloria General del Estado. (s.f.). *Contraloria.gob.ec*. Obtenido de Contraloria.gob.ec: http://www.contraloria.gob.ec/documentos/normatividad/MGAG-Cap-V.pdf

Corporación Gerardo Ortiz. (2010). *Grupo Ortiz*. Obtenido de Grupo Ortiz: http://www.gerardoortiz.com/historia.html

Council, P. S. (2006). *PCI Security Standards Council*. Obtenido de https://es.pcisecuritystandards.org/minisite/en/

Council, P. s. (2012). Ambiente Regulatorio . En P. s. Council, *PCI DSS Education Series* (págs. 2-9). Chicago: Madison Street.

Dalguerre Ordoñez, W. (2013). *Análisis de Riesgo .*

Diccionario, R. A. (2014). *real académia Diccionario.*

Domínguez Torres, M. Á. (2007). PCDI DSS ¿Cómo cumplir? *Estándares* , 93.

Echenique Garcia, J. A. (s.f.). *Auditoria en Informatica.* Mèxico: Mc Graw Hill Interamericana.

griegos, P. d. (Enero de 2012). *Universisdad Autonoma del Estado de Hidalgo.* Obtenido de http://www.uaeh.edu.mx/docencia/P_Presentaciones/prepa3/conceptos_generales_inv.pdf

Informática, D. d. (2015). *Amenazas a la Seguridad de la Información* . Recuperado el 22 de Octubre de 2015, de Seguridadinformatica.unlu.edu.ar: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

ISACA. (2012). *Cobit 5 .*

ISACA. (2014). *Estándar de auditoría y aseguramiento de SI 1401 Reportes.* Recuperado el 20 de Octubre de 2015, de Estándar de auditoría y aseguramiento de SI 1401 Reportes: http://www.isaca.org/Knowledge-Center/Standards/Documents/1401_std_Spanish_1113.pdf

ISACA. (2014). *Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgo en la Planificación.* Recuperado el 15 de Octubre de 2015, de Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgo en la Planificación: http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2202_gui_Spa_0415.pdf

ISACA. (2015). *Auditoría de sistemas de Información Herramientas y Técnicas, Reporte de Auditoría de SI.* Recuperado el 10 de Octubre de 2015, de Auditoría de sistemas de Información Herramientas y Técnicas, Reporte de Auditoría de SI: https://www.isaca.org/Pages/default.aspx?cid=1002083&Appeal=SEM&gclid=COXo0_Kk5sgCFZUWHwodSvIJXQ

ISACA, C. (2007). *Gobermance Institute, IT Assurence Guide.* Chicago.

ISACA, C. (2014). *Definición de Auditoria*. Obtenido de ISACA org.: https://www.isaca.org/Pages/default.aspx?cid=1002083&Appeal=SEM&gclid=CIDTz6W01sYCFUyPHwod0WEMHQ

ISO, 1. (2009). *Información.*

IT Control Objectives ISACA. (2014). *IT Control Objectives for Sarbanes-Oxley.* Obtenido de www.isaca.org/knowledge-center: https://www.isaca.org/Pages/default.aspx?cid=1002083&Appeal=SEM&gclid=CjwKEAiApOq2BRDoo8SVjZHV7TkSJABLe2iDH_1zbGwWYvv0rBBkZW6_O4abtq-Iy-5_OKBxObggGRoC2gXw_wcB

JAVA . (2015). *JAVA*. Obtenido de https://www.java.com/es/about/

Lases, f. M. (2006). *Metodología de la investigación .* México : Hidalgo.

Magdalena, G. d. (2015). *Manual de procesos y Procedimientos.* Recuperado el 16 de Septiembre de 2015, de http://www.magdalena.gov.co/apc-aa-files/61306630636336616166653232336536/manual_de_procesos_y_procedimientos.pdf

Maldonado, M. (2006). Auditoria de Gestión . Quito .

Morales, E. (2012). Estadística y Probabilidad. *Estadística y Probabilidad*. Chile.

Muñoz Razo, C. (2002). Auditoria en Sistemas Computacionales. En C. Muñoz Razo, *Auditoria en Sistemas Computacionales* (págs. 243-269). México: Pearson.

Ochoa Arevalo, P. (05 de marzo de 2014). El Proceso de Auditoria de Sistemas. Cuenca, Azuay, Ecuador.

Ochoa, I. P. (Marzo de 2014). Procesos de Auditoria . Cuenca, Azuay, Ecuador .

ORACLE. (2008). *ORACLEDATABASE*. Obtenido de http://www.oracle.com/lad/corporate/citizenship/index.html

Peña, G. (2013). Riesgo de Auditoria . Cuenca, Azuay , Ecuador .

Peña, I. G. (2014). *Técnicas de Verificación , Universidad del Azuay .* Cuenca.

Quinde, P., & Cedillo, H. (5 de Octubre de 2015). Objetivos de Coral Hipermercado . (B. Patricia, & O. Estefania, Entrevistadores)

Rehage, K., Hunt, S., & Nikitin, F. (2008). Developing The IT Audit Plan . En K. Rehage, S. Hunt, & F. Nikitin, *Developing The IT Audit Plan* (págs. 13-14). The Institute Internal Auditor.

RevistaAvance. (2010). Las huellas perdurables de una mujer emprendora. *Revista Avnace*.

RevistaAvance. (2014). Un gran centro comercial trepado en la loma de Racar . *Revista Avance* , 273.

Rhage, K., Hunt, S., & Nikitin, F. (2008). Developing the IT Audit Plan . En K. Rhage, S. Hunt, & F. Nikitin, *Developing the IT Audit Plan* (pág. 16). The Institute Internal Auditor.

Security Awareness, E. (2013). *PCI DSS EDUCATION SERIES.* Trustwave.

Security Awareness, E. (2013). *PCIDSS EDUCATION SERIES* . Trustwave .

Security Standar, C. (Noviembre 2013). *Norma PCI DSS.*

Security, A. E. (2013). PCCI DS EDUCATION SERIES. En A. E. Security, *PCCI DS EDUCATION SERIES* (pág. 2). Trustwave.

Security, Standar Council. (Octubre de 2010). *Glosario de términos, abreviaturas y acrónimos.* Recuperado el 25 de Octubre de 2015, de Industria de Tarjetas de Pago (PCI) : https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI%20Glossary.pdf

Security, Standards Council. (s.f.). *Qualified Security Assessor Companies*. Recuperado el 25 de Octubre de 2015, de Qualified Security Assessor Companies: https://es.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

Torres, M. Á. (2007). *PCI DSS: ¿Cómo cumplir?* Chicago : SIC.

VISA. (2014). *VISA*. Obtenido de http://www.visa.com.ec/acerca-de-visa/

DISEÑO DEL TRABAJO DE TITULACIÓN

1. SELECCIÓN Y DELIMITACIÓN DEL TEMA

En la actualidad la mayoría de entidades financieras, bancarias y comercios se manejan en sus actividades con tarjetas de pago por lo que es importante para evitar fraudes y mejorar la seguridad de la información de tarjetas, llevar a cabo la implementación y cumplimiento de la norma Payment Card Industry Data Security Standard (PCI DSS) para la seguridad de los datos de titulares de tarjetas de pago". Todos los comercios que participan en el procesamiento de tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirientes, entidades emisoras y proveedores de servicios, como también todas las demás entidades que almacenan, procesan o transmiten CHD (datos del titular de la tarjeta) o SAD (datos de autenticación confidenciales), las mismas que se encuentran obligadas a cumplir con los requerimientos que establece la norma, las entidades de comercio según el nivel en que se encuentre. CORAL HIPERMERCADOS RACAR PLAZA se encuentra en el nivel 2 Y 4 de los comercios que deben aplicar la normativa PCIDSS, por lo que nos centraremos en el requerimiento 7, 8, 9 de la cual aún no

se ha realizado una auditoria de la aplicación de los requerimientos anteriormente nombrados de la normativa.

Por esta razón se ha planteado como tema de investigación, la auditoria de sistemas a los cumplimientos de los requerimientos (7, 8, 9) de la Norma Payment Card Industry Data Security Standard (PCI DSS) con corte a Junio de 2015, haciendo alegación el requerimiento siete a restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa, mientras que el requerimiento ocho nos habla sobre como asignar un ID exclusivo a cada persona que tenga acceso por computadora y finalmente el requerimiento nueve que nos muestra como restringir el acceso físico a los datos del titular de la tarjeta.

Delimitación del tema:

- **Campo de estudio:** Auditoria de sistemas.
- **Área técnica:** Aplicada.
- **Organización:** CORAL HIPERMERCADO, RACAR PLAZA
- **Temporalidad:** Con corte a Junio del 2015.

De esta manera la investigación queda estructurada de la siguiente manera: “Auditoria de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma Payment Card Industry Data Security

Standard (PCI DSS) aplicada a CORAL HIPERMERCADOS, RACAR PLAZA con corte a junio de 2015.”

2. JUSTIFICACIÓN DE LA INVESTIGACIÓN

CORAL HIPERMERCADOS RACAR PLAZA al realizar sus actividades de comercio con tarjetas de pago se encuentra dentro de los establecimientos que deben cumplir lo requerido por la normativa Payment Card Industry Data Security Standard (PCI DSS) establecida por

las marcas, las cuales establecieron niveles de comercio dentro de los cuales CORAL HIPERMERCADO RACAR PLAZA se encuentra ubicado en los comercios a nivel 2 Y 4, mismos que se encuentran regulados por las entidades emisoras de tarjetas de crédito y ambos a su vez obligados a cumplir la Normativa.

Los Comercios deben cumplir con los requerimientos para que a su vez permitan que las entidades emisoras cumplan con lo dispuesto por la Normativa y evitarse incurrir en penas regulatorias y penalidades en caso de evento de compromiso de seguridad, multas de incumplimiento, mayor costo al procesar transacciones con tarjetas de crédito o perder el permiso de transaccional con tarjetas de crédito en caso de un compromiso de datos a más de no fomentar ni mejorar la seguridad de datos de los titulares de tarjetas, los comercios a su vez al no cumplir a cabalidad con la normativa no permitirían que la entidad emisora cumpla con el objetivo de la norma de asegurar la información de los titulares de las tarjetas de pago a más de verse expuesto a que se presenten multas o sanciones, y verse limitado de los procesos de autorización de transacciones para pagos con tarjetas por parte de las Entidades emisoras.

Por tanto las entidades que lleven a cabo procesos con tarjetas de pago al no tener un debido control de la seguridad de las tarjetas de pago por no llevarse a cabo un cumplimiento efectivo de la norma se podrían ver vinculadas a posibles casos de fraude con la información de las tarjetas en caso de fuga de información lo que disminuiría la confianza de los clientes al no contar la organización con el estándar de seguridad ocasionando esto perdida al negocio siendo importante mencionar que las marcas que se encuentran dentro del grupo que respaldan la normativa se verían obligadas a retirar los servicios que están prestan hacia la entidad lo que ocasionaría que las personas que se manejan con tarjetas de crédito para sus pagos que son la mayoría no pudiesen acceder a esta

facilidad viéndose las entidades así como el Comercio propensos a bajos rendimientos.

El cumplimiento de la norma es importante para lograr ejecutar con anticipación los ajustes pertinentes antes de la realización de los cuestionarios anuales de autoevaluación que es un requisito para el cumplimiento de Payment Card Industry Data Security Standard (PCI DSS) usado por los comerciantes y el análisis trimestral de red por un ASV (Proveedor aprobado para el escaneo). Todos los proveedores ASV son requeridos para llevar a cabo los análisis de acuerdo con un conjunto definido de procedimientos. Estos procedimientos dictan que el funcionamiento normal del entorno de cliente no se vea afectado y que el proveedor no debe modificar o entrar en el entorno del cliente. Como resultado, durante el análisis de la red no hay ataques de denegación de servicio y no es requerida ninguna instalación de software o hardware. Las organizaciones al cumplir con todo lo requerido por la Norma lograran minimizar el riesgo al mejorar la seguridad de los datos del titular de las tarjetas de pagos llegando de esta manera a una mejor toma de decisiones.

3. BREVE DESCRIPCIÓN DEL OBJETO DE ESTUDIO

La investigación se realizara en la ciudad de Cuenca en la empresa CORAL HIPERMERCADOS RACAR PLAZA de la corporación Gerardo Ortiz con RUC 0190072002001. El inicio de la corporación Gerardo Ortiz, fue en el año de 1953 con una abacería ubicada en el Mercado Mayorista 10 de Agosto, de la cual se expandió con tiendas mayoristas como lo es Coral Hipermercados, cuenta con cinco locales comerciales en la ciudad de Cuenca.

Coral Hipermercados de la corporación Gerardo Ortiz, es una organización moderna, dedicada a la comercialización de la más alta variedad de productos en líneas tales como calzado, textiles, ferretería,

plásticos y lonas industriales, hogar, maquinaria y equipo, acabados de construcción, hospitalaria, licores, entre otras, cuenta con más de 60 años de experiencia en el mercado ecuatoriano y posee centros de distribución a nivel nacional, donde nos enfocaremos específicamente es en el centro comercial Coral Hipermercado Racar Plaza, se encuentra ubicado en Racar Av. Abelardo J. Andrade, en donde funciona el departamento de Sistemas a cargo del Ing. Humberto Cedillo.

4. FORMULACIÓN DEL PROBLEMA

En el caso que la corporación Coral Hipermercados Racar Plaza no cumpla a cabalidad con la Normativa Payment Card Industry Data Security Standard (PCI DSS) para la seguridad de los datos, puede llegar a verse implicada en multas o sanciones por parte de las entidades emisoras por incumplimiento de lo establecido por estas sobre la seguridad de la información de las tarjetas de pago otorgadas al comercio, posibles fraudes con la fuga de información por lo que disminuirá la confianza de los clientes y las marcas que respaldan la normativa Payment Card Industry Data Security Standard (PCI DSS) podrían restringir los servicios de pagos con tarjetas a las entidades emisoras y estas a su vez al Comercio generando posibles pérdidas en el negocio.

4.1 LISTADO DE PROBLEMAS

- Multas o Sanciones
- No fomenta la seguridad de datos de titulares de las tarjetas.
- Vinculación a posibles fraudes.
- Fuga de información.
- Disminución de la confianza de los clientes.
- Restricción de los servicios de pagos con tarjetas por parte de las marcas que respaldan la normativa Payment Card Industry Data Security Standard (PCI DSS).

- Pérdidas para el negocio.

- **Problema General**

CORAL HIPERMERCADO RACAR PLAZA desconoce el estado actual del nivel de cumplimiento de los requerimientos 7, 8, 9 establecidos por la normativa Payment Card Industry Data Security Standard (PCI DSS) la misma que es obligatoria para los negocios que realicen procesamiento, transmisión o almacenamiento de información de tarjetas de crédito ya sea de forma directa o indirecta mediante algún proveedor de servicios, en el caso que la norma Payment Card Industry Data Security Standard (PCI DSS) no se cumpla a cabalidad, una de las mayores consecuencias seria incurrir en pérdidas lo que afectaría la confianza de los clientes en las transacciones realizadas con tarjetas de pagos, además las marcas que respaldan la normativa restringirían los servicios de pagos con tarjetas a las entidades emisoras y estas a los comercios, quedando la organización vulnerable ante responsabilidades y costes potenciales con lo que incrementaría el riesgos vinculados a los datos de tarjetas de crédito y no se fomentaría una cultura de seguridad en la organización.

5.- DETERMINACIÓN DE LOS OBJETIVOS

5.1 Objetivo General

Verificar el nivel de cumplimiento de la seguridad de los datos de los titulares de las tarjetas de pago por medio de una auditoria de sistemas de manera que permita a la empresa tener información veraz y efectiva, además se logrará el apropiado resguardo de la información de las tarjetas de pago para un correcto desenvolvimiento y toma de decisiones de la empresa.

5.2 Objetivos Específicos

- Comprender el entorno del negocio para lograr identificar medidas efectivas y fortalecer el área de seguridad de datos de las tarjetas de pagos de Coral Hipermercados Racar Plaza.
- Fundamentar el Proceso de la Auditoria de Sistemas, y conocer las implicaciones normativas y sus requerimientos para contrarrestar fraudes y riesgos.
- Evaluar el nivel de cumplimiento de la normativa Payment Card Industry Data Security Standard (PCI DSS) en los requerimientos 7,8, 9 de Coral Hipermercado Racar plaza para poder implementar medidas estratégicas de mejoramiento del negocio.

6.- ELABORACIÓN DEL MARCO TEÓRICO DE REFERENCIA

6.1 MARCO DE ANTECEDENTES

- **Tema:** PCIDSS: ¿cómo cumplir?

  Autor: Miguel Ángel Domínguez Torres.

  Año: Septiembre 2007.

Resumen: Las estadísticas de fraude relacionadas con la industria de tarjetas son numerosas. En respuesta a este incremento de robo de identidad, en 2004 seis de las más grandes marcas de tarjetas, MasterCard, Visa, American Express, Discover y JCB

Internacional colaboraron para crear un conjunto de prácticas seguras para pagos con tarjetas y formaron el Council de PCI Security Standards Council (PCISSC), mediante este estándar buscan reducir el fraude relacionado con las tarjetas de crédito e incrementar la seguridad de los datos, estas marcas obligan a que los comercios reciban requerimientos de cumplimiento PCIDSS por medio de las entidades financieras que a su vez han sido requeridas por las marcas para obligar a los comercios a cumplir PCIDSS es decir que las entidades financieras deben asegurar que todos los comercios y proveedores de servicio a los que representan

cumplen PCIDSS. El punto de partida para muchas organizaciones debe ser preguntarse si deben o no cumplir con PCIDSS, y que tareas deben llevar a cabo para operar bajo estos requerimientos según los niveles propuestos por las marcas de forma que las organizaciones que manejan pagos con tarjetas y cualquier comercio que acepte tarjetas cumplan con las auditorias periódicas, a más de cumplir con el estándar en todo momento evitando que se produzcan posibles repercusiones de no implementar la norma. Por ejemplo CORAL HIPERMERCADOS está obligado a implementar los requerimientos establecidos por el estándar así como otros comercios que manejen datos de tarjetas de pago, los mimos que deberán realizar los cuestionarios, auditorias anuales o trimestrales según sea necesario para su nivel.

- **Tema:** Sistema de pagos basado en el estándar ISO 8583 y normas PCI DSS utilizando lectores de banda magnética desarrollada en Java.

  Autor: Solís Reyes, Carlos Teodoro

  Año: 2013

  Resumen: la siguiente tesis nos da a conocer el desarrollo del Sistema en Java basado en el estándar para transacciones financieras ISO 8583 y en las normas de seguridad de datos PCI DSS, este sistema está orientado al sector comercial y financiero proporcionando un medio seguro para realizar transacciones con tarjetas de crédito utilizando lectores de banda magnética, donde se puede encontrar un módulo de parametrización que permita que la aplicación se adapte a las necesidades del lugar donde se instaló, pudiéndose configurar desde el mensaje que aparece impreso en el voucher hasta las tarjetas de crédito que son aceptadas. Finalmente esta aplicación contribuye el aumento de la disponibilidad para realizar transacciones con tarjetas de crédito

usando fuertes mecanismos de seguridad y algoritmos de encriptación para transmitir la información confidencial.

- **Tema:** Análisis de la implementación del estándar PCI-DSS en la seguridad de la información dentro de una institución financiera. **Autor:** Calle Parrales, Zoila Alexandra

  Año: abr-2015

  Resumen: El presente tema de tesis propone el análisis de la implementación del estándar de seguridad de datos para la industria de tarjetas de pago, conocido por su siglas en inglés PCI-DSS (Payment Card Industry – Data Security Standard), como medida de seguridad para prevenir fraudes en las transacciones que impliquen el uso de tarjetas de crédito y débito, como ayuda al cumplimiento de las exigencias de la Superintendencia de Bancos y Seguros, respecto al procesamiento de las mismas.

  Este estándar exige máxima seguridad en los datos de titular o dueño de la tarjeta, por lo tanto la idea de implementar PCI-DSS se enfoca en proteger y salvaguardar información sensible y confidencial, permitiéndole a la institución financiera (ya sea esta un banco, Cooperativa y otros proveedores de servicios) garantizar la seguridad de los datos de sus clientes. El enfoque del presente documento hace referencia al análisis de la implementación del Estándar PCI-DSS en un banco localizado en la ciudad de Guayaquil.

  El análisis de la implementación del estándar PCI- DSS, abarca desde la definición conceptual, funcionalidad, requerimientos y actores que lo componen hasta la determinación de mejores prácticas de Seguridad que debe aplicar el banco para la implementación de mismo.

En el desarrollo de este proyecto de análisis se toma como estudio los mecanismos de seguridad que posee determinado banco ubicado en la ciudad de Guayaquil, con la finalidad de validar que la propuesta de la implementación del Estándar PCI-DSS es una media que le permitirá a la institución mejorar la seguridad en las transacciones efectuadas con tarjetas de pago, con los resultados de este análisis y la información recolectará se confirmará que estándar ofrece una solución efectiva para incrementar el nivel de seguridad de la información sensible y confidencial de las instituciones Bancarias.

- **Tema:** Diseño de un plan de implementación de controles de seguridad sobre el entorno de tarjetahabiente de la compañía ecuatoriana TEXTILEC S.A

  Autor: Francisco Bolaños, Javier Baquero.

  Año: 2014-09-18

  Resumen: La implementación y gestión de proyectos son de vital importancia para el cumplimiento de las normas de seguridad de la información requeridas por los entes reguladores. Las empresas para poder ofrecer productos o servicios de calidad deben implantarlas. Es por eso que este artículo propone el diseño de implementación de la norma Payment Card Industry Data Security Standard (PCI DSS) a la compañía ecuatoriana TEXTILEC S.A. La propuesta identifica los flujos de datos de tarjetas de pago con base en la normativa PCI DSS, la evaluación del grado de cumplimiento de los requerimientos de la misma y la presentación de un portafolio de proyectos que deben ser emprendidos para el cierre de brechas y el cumplimiento del estándar.

- **Tema:** Plan de proyecto para el proceso de certificación PCI DSS en FISERV costa rica.

  Autor: Leana Romero Arce

Año: Diciembre, 2009

Resumen: el presente tema de investigación está realizado en la empresa Fiserv, Inc. es una empresa dedicada al desarrollo de software para el área financiera, para todas las oficinas de Fiserv se ha establecido como política interna la obtención de la certificación PCI DSS para asegurar la información relacionada con tarjetas de crédito y débito, desde su perspectiva de proveedor de servicios de software en el área financiera.

La certificación PCI DSS es el conjunto de las Normas de Seguridad de la Información de la Industria de Medios de Pago (PCI DSS), creado por las compañías Visa y MasterCard. Esta es aplicada tanto a los bancos, como a comercios y proveedores de servicios relacionados con tarjetas de débito y crédito, para proteger a los dueños de tarjetas y su información confidencial. El objetivo principal de este trabajo, fue desarrollar un Plan de Proyecto para el proceso de Certificación de PCI DSS en Fiserv Costa Rica.

6.2 MARCO TEÓRICO

El presente tema de investigación se sustentará bajo el siguiente marco teórico:

1. Normativa PCIDSS para seguridad de los datos de los titulares de las tarjetas de pago.
2. COBIT 5 (ISO 27005 matrices de riegos de la seguridad de la información) e ISACA (INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION).
3. Proceso de Auditoria Según El Manual de GTAF (GUIA DE AUDITORIA DE TECNOLOGÍA DEL INSTITUTO DE AUDITORES INTERNOS).

6.2.1 NORMATIVA PCIDSS PARA SEGURIDAD DE LOS DATOS DE LOS TITULARES DE LAS TARJETAS DE PAGO.

Según (Council P. s., 2012) El Council de PCI [27]emitió el estándar de seguridad para tarjetas conocido como PCIDSS que es un estándar global para proteger la información de tarjetas y proveer una comprensión sobre los requerimientos que se han diseñado para proteger a todos los tarjeta habientes.

En enero del 2005, el Council de PCI estimo que 234 millones de registros con datos sensibles fueron comprometidos, creando conciencia sobre la necesidad de un estricto conjunto de requerimientos de seguridad. En junio de 2005, el estándar de PCIDSS fue introducido y el Council de PCI impuso fechas para cumplir este estándar en organizaciones de gran tamaño quienes almacenaran, procesara, y/o transmitieran datos de tarjetas. Desde que se introduce PCIDSS nuevas vulnerabilidades de red y aplicaciones ha sido descubierta con regularidad y el estándar ha evolucionado para contrarrestar estas nuevas amenazas. Redes inalámbricas y otro tipo de tecnología emergente han introducido nuevas amenazas y vulnerabilidad, PCIDSS ha cambiado para cumplir con los problemas de seguridad que están adheridos con estas tecnologías. Las mejores prácticas son redefinidas e implementadas cada año. Hoy en día PCIDSS aplica para todos los comercios que acepten o procesen tarjetas de pago sin importar el tamaño, volumen de transacciones o método de procesar pago. PCI DSS aplica para todas las organizaciones que almacenan, procesan y/o transmiten datos de tarjetahabientes[28], por lo que cualquier comercio que acepte o procese pagos con tarjetas debe cumplir con esta norma.

[27] Council de PCI.- Es un foro mundial abierto destinado a la formulación, la mejora, el almacenamiento, la difusión y la aplicación permanentes de las normas de seguridad para la protección de datos de cuentas. (Council P. S., 2006)

[28] Tarjetahabiente: Cliente a quien le ha sido emitida una tarjeta o individual autorizado para utilizar la tarjeta. (Council P. s., 2012)

PCDSSS es un estándar de seguridad que define el conjunto de requerimientos para gestionar la seguridad, definir políticas y procedimientos de seguridad, arquitectura de red, diseño de software y todo tipo de medidas de protección que intervienen en el tratamiento, procesado o almacenamiento de información de tarjetas de crédito e incrementar la seguridad de estos datos. La norma es fruto del esfuerzo de PCI Security Standards Council[29], el comité formado por las principales marcas de tarjetas de crédito Visa, MasterCard American Express, JCB y Discover las mismas que han catalogado a las organizaciones en 3 tipologías. Comercios: (Súper/hipermercados, autopistas, comercio-e, agencias de viajes, etc.) Proveedores de servicios (ISP/ASP, pasarelas de pago, fabricantes de tarjetas, servicios de envío de tarjetas, procesadores de transacciones, etc.). Entidades financieras (bancos, cajas de ahorro, entidades de crédito, etc.). Estas entidades financieras dadas a su trayectoria en gestión de seguridad de la información y por otro lado dadas que cumplen el papel son responsables de asegurar también que todos los comercios y proveedores de servicio a los que representan cumplen PCIDSS.

Por tanto si mi empresa realiza algún tipo de procesamiento, transmisión o almacenamiento de información de tarjetas de crédito, implicando esto el número de la tarjeta o PAN-Primary Account Number[30] ya sea de forma directa o indirecta mediante algún proveedor de servicios, entonces queda afectada por el cumplimiento de los requerimientos. Evitan de esta manera las empresas posibles repercusiones de no implementar PCIDSS como por ejemplo: Estipulado por contrato: multas, rescisiones de contrato, gastos de investigación forense en caso de incidente, etc.

[29] PCI DSS Security Standards Council. - Es un foro mundial abierto destinado a la formulación, la mejora, el almacenamiento, la difusión y la aplicación permanentes de las normas de seguridad para la protección de datos de cuentas. (Council P. S., 2006)

[30] PAN Primary Account Number.- Es el número de cuenta principal exclusivo de una tarjeta de pago, que identifica el emisor y las cuentas específicas del titular de la tarjeta. Generalmente de 16 dígitos. (Council P. s., 2012)

Pérdida de reputación y daños a la imagen corporativa pérdida de clientes; etc.

6.2.1.1 ANÁLISIS PRELIMINAR DEL ESTADO DE CUMPLIMIENTO

Según (Torres, 2007) Define el ámbito al que aplica el estándar (entorno de cumplimiento).

- Identifico como fluye la información de tarjetas a través de los diferentes sistemas, aplicaciones y redes de la organización.
- Cuáles son los departamentos o personas afectadas.
- Grado de madurez de la empresa respecto al cumplimiento de los requerimientos establecidos.
    - Sesión de familiarización con PCIDSS, poniendo en conocimiento de todos los departamentos y empleados afectados, que es PCIDSS.

6.2.1.2 PROGRAMA DE CUMPLIMIENTO PCIDSS

Según (Torres, 2007) Análisis preliminar mediante identificación de relaciones con proveedores de servicio que controlan parte o en algunos casos todo el proceso de negocio. Conocido donde vamos a aplicar el estándar y en qué estado de cumplimiento se encuentra debemos evaluar los riegos sobre los activos que definen el entorno de cumplimiento y definir cómo se van a alcanzar los objetivos marcados por los requerimientos PCIDSS a través del Programa de Cumplimiento PCIDSS.

El programa nos dará a conocer la estrategia para cumplir con los requerimientos establecidos por la norma y concretaremos la planificación de acciones o proyectos que facilitaran la información necesaria para decidir qué acciones abordar así como la justificación en base al riesgo que disminuyen.

6.2.1.3 REQUERIMIENTOS A EVALUAR

- **REQUERIMIENTO 7. "**RESTRINJA EL ACCESO A LOS DATOS DEL TITULAR DE LA TARJETA SEGÚN LA NECESIDAD DE SABER QUE TENGA LA EMPRESA". Mediante este requerimiento se asegurara que el personal autorizado sea el único que pueda acceder a los datos importantes, mediante la implementación de sistemas y procesos que limiten el acceso conforme a la necesidad de conocer y según la responsabilidad del cargo. (Council P. s., 2012)
- **REQUERIMIENTO 8. "**ASIGNAR UN ID[31] EXCLUSIVA A CADA PERSONA QUE TENGA ACCESO POR COMPUTADORA". Garantiza que cada persona que tenga un ID única sea responsable de sus actos. (Torres, 2007)
- **REQUERIMIENTO 9. "**RESTRINJA EL ACCESO FÍSICO A LOS DATOS DEL TITULAR DE

  LA TARJETA". Esto se llevara a cabo mediante la restricción correcta del acceso a datos o sistemas que alojen datos de titulares de tarjetas. (Torres, 2007)

Según Miguel Ángel Domínguez Torres, hace referencia en su enunciado de estándares para PCIDSS, que una buena práctica para las empresas es utilizar como base para la elección de controles de seguridad e implementar una norma de ámbito internacional como es la ISO 27002 de manera que la empresa pueda alinear los requerimientos PCIDSS con las buenas prácticas de seguridad de la información que define ISO 177799 y que hoy en día es estándar adoptado por la mayoría de empresas para definir y gestionar su seguridad de la información. (Torres, 2007)

6.2.2 COBIT 5 (ISO 27005 matrices de riegos de la seguridad de la información) e ISACA (Information System Audit and Control Association).

[31] ID. - Es la identificación única de cada persona para tener acceso al sistema predeterminado por lo que deberán hacerse responsables de sus actos. (Council P. s., 2012)

Según (ISACA C. , Definición de Auditoria, 2014) ISACA es un líder global proveedor de conocimiento, certificaciones, comunidad, promoción y educación sobre aseguramiento y seguridad de sistemas de información (SSII), gobierno empresarial y gestión de TI y riesgo relacionado con TI y cumplimiento. ISACA lanza por primera vez un marco de negocio para el gobierno y la gestión de las TI de la empresa (COBIT) en el año 1996, ISACA actualiza continuamente el COBIT, el cual ayuda a los profesionales de TI y líderes de las organizaciones a llevar a cabo sus responsabilidades en la gestión y gobierno de TI proporcionando un valor al negocio, actualmente ISCA se encuentra orientada al gobierno corporativo de TI.

COBIT es el marco de trabajo para gobierno y gestión de tecnología de información el cual tiene un enfoque en el negocio con orientación a procesos, siendo un estándar aprobado y globalmente aceptado contribuyendo a que las organizaciones cumplan con los requerimientos regulatorios, es decir COBIT es un framework de Gobierno de TI y un conjunto de herramientas de soporte para el gobierno de TI que les permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio.

COBIT se alinea con los principales marcos de referencia usados como:

- Coso ERM, ISO 9000, ISO 31000, ITIL, ISO 27000, CMMI, y ahora PCIDSS.

PROCESO DE MEDIDAS DE CONTROL DE ACCESO	
PCIDSS REQUERIMIENTO 3.0	**PROCESOS COBIT 5**
RESTRINJA EL ACCESO A LOS DATOS DEL TITULAR **DE LA TARJETA SEGÚN LA NECESIDAD DE SABER QUE TENGA LA EMPRESA.**	DSS05.04 Administrar la seguridad del usuario y el acceso lógico.

ASIGNAR UN ID EXCLUSIVA A CADA PERSONA QUE TENGA ACCESO POR COMPUTADORA.	APO03.02 Gestionar la Arquitectura Empresarial: La cartera de servicios de la arquitectura de empresa soporta el cambio empresarial ágil.
	APO07.01 Gestionar los Recursos Humanos: La estructura organización y las relaciones de TI son flexibles y dan respuesta ágil.
RESTRINJA EL ACCESO FÍSICO A LOS DATOS DEL TITULAR DE LA TARJETA.	APO01.06 Definir la información (datos) y la propiedad del sistema.
	DSS05.04 Administrar la seguridad del usuario y el acceso lógico.
	DSS05.05 Administrar el acceso físico a los activos de TI.

Fuente: Cobit Focus, volumen 1, enero 2014.
Elaborado por: Autoras.

6.2.3 PROCESO DE AUDITORIA DE SISTEMAS

Según (ISACA C. , Definición de Auditoria, 2014) Nos dice que, si bien la auditoria puede definirse como un proceso sistemático por el cual un equipo o una persona competente e independiente obtiene y evalúa objetivamente la evidencia respecto a las afirmaciones acerca de un procesos con el fin de formarse una opinión sobre el particular e informar

el grado de cumplimento de dicha afirmación, ahora bien la auditoria de sistemas puede definirse como cualquier auditoria que abarca la revisión y evaluación parcial o total de los sistemas automatizados de procesamiento de información, procesos relacionados no automatizados y las interfaces entre ellos.

6.2.3.1 FASES DE AUDITORIA DE SISTEMAS

Según (ISACA C., Gobermance Institute, IT Assurence Guide, 2007) las fases de auditoría son:

1. **PLANIFICACIÓN**

La creación del universo aseguramiento de TI[32] para la asignación de aseguramiento sirve como el comienzo de todas las iniciativas de aseguramiento. A crear un plan integral, las necesidades profesionales de aseguramiento de combinar una comprensión del universo aseguramiento de TI y la selección de un marco de control de TI apropiado, como COBIT[33]. La agregación de estos dos permite una planificación basada en el riesgo de la iniciativa de aseguramiento. Para establecer los objetivos de garantía de correcta, primero una evaluación de alto nivel necesita ser realizado. El entregable final de esta etapa es el plan de aseguramiento de TI, generalmente anual. (ISACA C., Gobermance Institute, IT Assurence Guide, 2007)

2. **ALCANCE**

El proceso de alcance se puede realizar de tres formas diferentes:

[32] TI.- Tecnología de la información. (Ochoa, 2014)
[33] Cobit.- Marco de negocio para el gobierno y la gestión de las tecnologías de información de la empresa. (ISACA, 2012) [8] ITGI.- Instituto de Gobierno de tecnología de la información. (ISACA, 2012)

- El enfoque más detallado de alcance se inicia desde la definición de los objetivos de negocio y de TI para el medio ambiente bajo estudio y la identificación de un conjunto de los procesos de TI y los recursos (es decir, la garantía de universo) necesarios para apoyar esas metas. Los objetivos que están sujetos a la TI iniciativa se puede asegurar con ámbito a una granularidad inferior (es decir, los objetivos clave de control a medida para la organización).

- Un enfoque de alcance de alto nivel puede comenzar desde la evaluación comparativa de la investigación ejecutada por ITGI[8], proporcionando directrices genéricas sobre la relación de los objetivos de negocio, objetivos de TI y procesos de TI, como se describe en COBIT. Esta cascada genérica de objetivos y procesos puede ser utilizado como una base para la determinación del alcance más detallada, como se requiere para el medio ambiente específico que está siendo evaluada.

- Un enfoque de alcance híbrido combina los métodos detallados y de alto nivel. Este enfoque comienza a partir de la cascada genérica de objetivos y los procesos, pero se adaptaron y modificaron para el entorno específico antes de continuar el alcance a los niveles más detallados.

Los entregables finales de esta etapa son el alcance y los objetivos de las diferentes iniciativas de aseguramiento de TI. (ISACA C., Gobermance Institute, IT Assurence Guide, 2007)

3. EJECUCIÓN

Una de las etapas de aseguramiento de TI es la ejecución, la cual comprende de:

1. Redefinir la comprensión de la TI y el alcance:
    - Identificar y confirmar los procesos críticos de TI.
    - Auto-evaluar la madurez del proceso.

2. Prueba de la eficacia del diseño de control de los objetivos de control clave:

- Probar y evaluar los controles.
- Actualizar y evaluar la madurez del proceso.

3. Pruebe el resultado de los objetivos de control clave:

- Auto-evaluar los controles.
- Prueba y evaluar los controles.

4. Documentar el impacto de control y debilidades:

- Diagnosticar el riesgo operativo.
- Fundamentar riesgo. (ISACA C. , Gobermance Institute, IT Assurence Guide, 2007)

4. REPORTE

1. Conclusión emitido por el profesional de aseguramiento de TI.
2. Exponer los hallazgos y conclusión.

5. SEGUIMIENTO

1. Verificar el cumplimiento de compromisos**.**

2.1 MARCO CONCEPTUAL

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS).- Normas de seguridad de datos de la industria de tarjetas de pago se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial, proporcionan una referencia de requisitos técnicos y operativos para proteger los datos de los titulares de las tarjetas, aplicadas a todas las entidades que participan en el procesamiento de tarjetas de pago. Según (Council P. S., 2006)

COBIT: COBIT es el marco de gestión y de negocio global para el gobierno y la gestión de las TI de la empresa. Siendo un marco de gobierno de las tecnologías de información que proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio. COBIT ayuda a las Organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos. Según documento (Ochoa, 2014)

RIESGO.- el potencial que una amenaza determinada pueda explotar las vulnerabilidades de un activo o grupo de activos causando pérdida o daño a los activos. La combinación de la probabilidad y consecuencia de un evento. (ISACA, 2012)

INFORMACIÓN.- La información es un activo que, como otros activos importantes del negocio, tiene valor para una organización y, por lo tanto, necesita ser protegido adecuadamente. (ISO, 2009)

TECNOLOGÍAS DE LA INFORMACIÓN (TI).- son aquellas que transforman los recursos de datos en una variedad de productos de información. (Ochoa, 2014)

Val IT.- Es un marco de referencia de gobierno que incluye principios rectores generalmente aceptados y procesos de soporte relativos a la evaluación y selección de inversiones de negocios de TI. (COBIT, 2014)

Risk IT.- Es un marco de referencia normativo basado en un conjunto de principios rectores para una gestión efectiva de riesgos de TI. (COBIT, 2014)

BMIS.- (Business Model for Information Security) una aproximación holística[34] y orientada al negocio para la administración de la seguridad informática. (COBIT, 2014)

ITAF.- (IT Assurance Framework) un marco para el diseño, la ejecución y reporte de auditorías de TI y de tareas de evaluación de cumplimiento. (COBIT, 2014)

ISACA.- Es el acrónimo[35] de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información. Fue fundada en el año 1967 cuando un grupo de auditores en sistemas informáticos percibieron la necesidad de centralizar la fuente de información y metodología para el área de operación. Fue en 1969 que el grupo se formalizó a asociación, originalmente incorporada como EDP Auditors Association. En 1976 el nombre pasó a ser ISACA, por el que es actualmente conocida, y se estableció la primera certificación profesional de auditoría de sistemas de información, o CISA. ISACA adicionalmente promueve el avance y certificación de habilidades y conocimientos críticos para el negocio, a través de las certificaciones globalmente respetadas: Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) y Certified in Risk and Information Systems Control™ (CRISC™). (ISACA, 2012)

[34] Holística.- Analiza los eventos desde el punto de vista de las múltiples interacciones que los caracterizan. El holismo supone que todas las propiedades de un sistema no pueden ser determinadas o explicadas como la suma de sus componentes. En otras palabras, el holismo considera que el sistema completo se comporta de un modo distinto que la suma de sus partes. (Diccionario, 2014)

[35] Acrónimo.- Un acrónimo es una clase de sigla cuya pronunciación se realiza del mismo modo que una palabra. Las siglas, por otra parte, son los términos que se componen con las primeras letras de los conceptos que forman una expresión. (Diccionario, 2014)

TERCERIZAR: la tercerización o subcontratación es una práctica llevada a cabo por una empresa cuando contrata a otra firma para que preste un servicio que, en un principio, debería ser brindado por la primera. Este proceso suele llevarse a cabo con el objetivo de reducir los costos**.** (Diccionario, 2014)

ESTANDARIZACIÓN: Ajustar o adaptar las cosas para que se asemejen a un tipo, modelo o norma común. Se define así al proceso de unificación de características en un producto, servicio o procedimiento. (Diccionario, 2014)

RESTRINGIR: Disminuir o reducir a límites menores. (Diccionario, 2014)

ALINEAR: Colocar en línea recta varias personas o cosas: alinear las fichas de dominó; el Sol se alineaba con las estrellas. **2** Incluir a un jugador en el equipo que ha de participar en un partido o en una competición: el entrenador no alineará al jugador ruso en el partido preparatorio. **3** Vincular o asociar a una persona a una tendencia ideológica, política o de otro tipo: los países productores de petróleo se alinearon con Arabia Saudí. (Diccionario, 2014)

SOFTWARE: Se pronuncia aproximadamente 'sófgüer'] *s. m.* Conjunto de programas, lenguajes de programación y datos que controlan que el ordenador funcione y realice determinadas tareas: he comprado un programa de tratamiento de textos para el software de mi ordenador. (Diccionario, 2014)

HARDWARE: [se pronuncia aproximadamente 'járguar'] *s. m.* Conjunto de elementos físicos del sistema de un ordenador, como el teclado o el monitor. Software. *m.* INFORM. Conjunto de unidades físicas, circuitos y dispositivos que componen un sistema informático. (Diccionario, 2014)

BASES DE DATOS.- Los datos son la materia prima de los S.I, es por esta razón que los datos se los considera como un recurso (recurso de

datos) que deben manejarse de forma efectiva para beneficio de todos los usuarios finales. (Ochoa, 2014)

PRELIMINAR: Que sirve de introducción para tratar un tema o una materia: comentario preliminar. *adj./s. m.* Que se hace con anterioridad a una cosa y sirve como preparación: estudios preliminares. (Diccionario, 2014)

REPERCUSIÓN: Influencia de determinada cosa en un asunto o efecto que causa en él.

Resonancia pública que consigue algo o alguien. Consecuencia indirecta de un hecho o decisión. Comentario que suscita un hecho o decisión. (Diccionario, 2014)

DESCRIPTIVA: Que expresa, por medio del lenguaje, las características de una persona o cosa: un texto descriptivo. (Diccionario, 2014)

CUANTITATIVO: *adj.* Relativo a la cantidad. (Diccionario, 2014)

CUALITATIVO: *adj.* Relativo a la cualidad. Que es propio de la forma de ser de una persona o cosa evaluación cualitativa. (Diccionario, 2014)

SISTEMA.- Un sistema es un grupo de componentes interrelacionados que trabajan en conjunto hacia una meta común mediante la aceptación de entradas y generando salidas en un proceso de trasformación organizado. (Ochoa, 2014)

SISTEMA DE INFORMACIÓN (SI).- Es una combinación organizada de personas hardware, software, redes de comunicaciones y recursos de datos que reúne, transforma y disemina información en una organización. (Ochoa, 2014)

AUDITORIA DE SISTEMAS.- Puede definirse como cualquier auditoria que abarca la revisión y evaluación (parcial o total) de los sistemas automatizados de procesamiento de información, procesos relacionados no automatizados y las interfaces entre ellos. (Ochoa, 2014)

GOBIERNO DE TI.- Es parte integral del gobierno de la empresa y está constituido por las estructuras de liderazgo y organizaciones y los procesos que aseguran que la ti de la organización sostiene y extiende la estrategia y los objetivos de la organización. (Ochoa, 2014)

PROCESO.- La noción de proceso halla su raíz en el término de origen latino processus. Según informa el diccionario de la Real Academia Española (RAE), este concepto describe la acción de avanzar o ir para adelante, al paso del tiempo y al conjunto de etapas sucesivas advertidas en un fenómeno natural o necesario para concretar una operación artificial. (Diccionario, 2014)

Un proceso se puede definir como una serie de actividades, acciones o eventos organizados interrelacionados, orientadas a obtener un resultado específico y predeterminado, como consecuencia del valor agregado que aporta cada una de las fases que se llevan a cabo en las diferentes etapas por los responsables que desarrollan las funciones de acuerdo con su estructura orgánica. (Magdalena, 2015)

POLÍTICA.- Se define como la orientación, marco de referencia o directriz que rige las actuaciones en un asunto determinado. (Magdalena, 2015)

NORMA.- Disposición de carácter obligatorio, específico y preciso que persigue un fin determinado enmarcado dentro de una política. (Magdalena, 2015)

SISTEMA AUTOMATIZADO.- La automatización es un sistema donde se trasfieren tareas de producción, realizadas habitualmente por operadores humanos a un conjunto de elementos tecnológicos. Un sistema automatizado consta de dos partes principales: La Parte Operativa es la parte que actúa directamente sobre la máquina. Son los elementos que hacen que la máquina se mueva y realice la operación deseada. La Parte de Mando suele ser un autómata programable (tecnología programada),

aunque hasta hace bien poco se utilizaban relés electromagnéticos, tarjetas electrónicas o módulos lógicos neumáticos (tecnología cableada). En un sistema de fabricación automatizado el autómata programable está en el centro del sistema. Este debe ser capaz de comunicarse con todos los constituyentes de sistema automatizado. (ISACA, 2012)

INTERFACE.- Un interface es una colección de declaraciones de métodos (sin definirlos) y también puede incluir constantes. El papel del interface es el de describir algunas de las características de una clase. Por ejemplo, el hecho de que una persona sea un futbolista no define su personalidad completa, pero hace que tenga ciertas características que las distinguen de otras. (ISACA, 2012)

REQUERIMIENTO.- En ingeniería del software y el desarrollo de sistemas, un requerimiento es una necesidad documentada sobre el contenido, forma o funcionalidad de un producto o servicio. Los requerimientos son declaraciones que identifican atributos, capacidades, características y/o cualidades que necesita cumplir un sistema (o un sistema de software) para que tenga valor y utilidad para el usuario. En otras palabras, los requerimientos muestran qué elementos y funciones son necesarias para un proyecto. (ISACA, 2012)

7.- PREGUNTAS DE INVESTIGACIÓN

1. ¿Cuál es el estado actual de cumplimiento de la normativa PCIDSS en CORAL HIPERMERCADO RACAR PLAZA en el periodo 2015 en la ciudad de Cuenca, provincia del Azuay?

8.- CONSTRUCCIÓN DE VARIABLES E INDICADORES

ESQUEMA TENTATIVA	VARIABLES
Capítulo1. Antecedentes generales de la empresa.	Organización

Capítulo 2. Fundamentación del Proceso de la Auditoria de Sistemas, y conocimiento de las implicaciones normativas y sus requerimientos. **2.1 Concepto de auditoría de sistemas** **2.2 Importancia de la auditoria** **2.3 Tipos de auditoria** **2.4 Tipos de riesgo de auditorias** **2.5 Tipos de controles de auditoria** **2.6 Proceso de la Auditoria de Sistemas** • Planificación • Ejecución • Reporte	Conceptos Auditoria Planificación Normas Programas PCIDSS COBIT Riesgo Control
• Seguimiento **2.7 Normativa PCIDSS para seguridad de os datos de los titulares de las tarjetas de pago.** • Análisis Preliminar del Estado de Cumplimiento • Programa de Cumplimiento PCIDSS, Requerimientos 7, 8, 9.	

Capítulo 3. Evaluación del nivel de cumplimiento de la normativa en los requerimientos 7, 8, 9 de Coral Hipermercado Racar plaza. **proceso de la auditoria de sistemas** 3.1 Planificación 3.2 Ejecución 3.3 Reporte 3.4 Seguimiento	Auditoria Planificación
Capítulo 4. Conclusiones y recomendaciones.	

9.- DISEÑO METODOLÓGICO[36]

a) Tipo de investigación

El tipo de investigación a aplicarse es la Investigación Descriptiva y analítica debido a que nos enfocaremos en el hallazgo de conclusiones mediante la auditoria de la implementación de la norma PCIDSS en CORAL HIPERMERCADO RACAR PLAZA porque en la empresa no se ha llevado a cabo antes una auditoria a los requerimientos 7,8,9 y al no estar seguros de que se está cumpliendo a cabalidad con esta regulación obligatoria establecida por las marcas de tarjetas de pago (Visa, MasterCard, American Express, Diners club y JCB Internacional) no se llegaría a corregir las vulnerabilidades en caso de existir en el almacenamiento de datos de los titulares de las tarjetas, no se cumplirían y enviarían los registros de validación requerida (en caso de aplicar) y no se enviarían los reportes a tiempo de cumplimiento de los bancos

[36] Metodológico.- Proviene de los vocablos griegos método y logos que significan: Estudio o tratado de los métodos. "Rama de la lógica que se encarga del estudio de los diferentes métodos para llegar al conocimiento crítico y reflexivo que permita la fundamentación de la ciencia". (griegos, 2012)

adquirientes y marcas con las que se realicen negocios por lo que el comercio se podría ver implicado en fraudes, multas de incumplimiento, penas regulatorias y penalidades en caso de evento de compromiso de seguridad, mayores costes al procesar transacciones con tarjetas de crédito o hasta llegar a perder el permiso de transaccionar con tarjetas de crédito en caso de un compromiso con los datos es por ello que para lograr una protección confiable y mayoritariamente segura de los datos de los titulares de tarjetas es necesario llevar a cabo una investigación sobre el cumplimiento de los estándares de seguridad establecidas por las marcas las mimas que se encargan de que se estén llevando a cabo las mejores prácticas de seguridad al cumplir con el conjunto de requisitos de PCI. (Council P. s., 2012)

b) Método de la investigación

El método que se utilizara es el Mixto (Cuantitativo y Cualitativo) ya que se busca obtener resultados a través de la auditoria de sistemas a los datos de titulares de tarjetas, obtener estadísticos e indicadores de desempeño que permitan la consideración de nuevas alternativas, mediante el análisis de los manuales que se manejan para la implementación de los requerimientos con la aplicación de técnicas de recolección de datos, métodos de razonamiento inductivo [37]y deductivo [38]logrando así llegar a establecer los resultados de la investigación.

Para el trabajo de titulación a elaborar se llevaran a cabo las siguientes técnicas de investigación para la auditoria a los requerimientos 7, 8, 9 de la normativa PCI DSS aplicado a CORAL HIPERMERCADO RACAR PLAZA. (Ochoa, 2014)**,** (Peña, 2014)

- **Según Método Cuantitativo:**

[37] Razonamiento inductivo.- s aquel que parte de los datos particulares para llegar a conclusiones generales. (Lases, 2006)
[38] Razonamiento deductivo.- es aquel que parte de datos generales aceptados como válidos para llegar a una conclusión de tipo particular. (Lases, 2006)

Documental.-

- Computación: Corrección matemática de cálculos.
- Comprobación: Determinar si los documentos que amparan un acto demuestran: autoridad, legalidad, propiedad y certidumbre.

Encuesta

- Aplicar preguntar con respuesta cerrada.

Rastreo.-

- Seguimiento de una actividad.

Escrita.-

- Análisis: Descomponer el todo en sus elementos.
- Conciliación: Igualar dos conjuntos de datos.
- Confirmación: Obtener información escrita de terceras personas.

- **Según Método Cualitativo:**

Entrevista.-

Método tradicional, entrevistar a las personas adecuadas, prepara las preguntas con antelación, utilizar diagramas, modelos, etc. (Ochoa, 2014). Sirve para obtener información de variada naturaleza sobre aspectos de interés para el auditor. Participan entrevistados y entrevistadores y constituye la más utilizada e importante en la auditoria operativa, en su desarrollo se siguen dos etapas: una planificación y una ejecución. (Peña, 2014)

Observación y análisis de tareas

- Estudia a los futuros usuarios en su entorno de trabajo, a veces se utiliza el video. Anota todo aquello que es susceptible de mejora. Posteriormente genera una serie de requisitos tentativos.

Comparación

- Relacionar dos o más objetos, hechos o magnitudes.

Revisión selectiva

- Separar mentalmente los asuntos que no son típicos o comunes.

Verbal

- Indagación: diálogo no planificado.

Física

- Inspección: existencia de bienes, dinero y documentos.

Brainstorming

- Seleccionar un grupo variado de participantes. Eliminar críticas, juicios y evaluaciones mientras los participantes sugiere idas. Producir muchas ideas recogerlas todas por escrito.

  Otro día en otra sesión se evalúan las ideas (se puntúan).

Otras

- Declaración: rendir testimonio ante autoridad competente.
- Conferencia: proceso en el que el auditor da a conocer los resultados preliminares de su examen.
- Intuición: sexto sentido.

10.- ESQUEMA TENTATIVO DE LA INVESTIGACIÓN

OBJETIVO ESPECÍFICO	CAPÍTULO
Comprender el entorno del negocio para lograr un entendimiento adecuado del área auditada.	**Capítulo 1. Antecedentes generales de la empresa** 1.1 Historia de la empresa 1.2 Misión 1.3 Visión 1.4 Objetivos 1.5 Actividades 1.6 Estructura administrativa 1.7 Estrategias 1.8 Planes y programas 1.9 Políticas y manuales. 1.10 Conocimiento del área auditada 1.11 Tecnología implementada 1.12 Seguridad implementada en el negocio
Fundamentar el Proceso de la Auditoria de Sistemas, y conocer las implicaciones normativas y sus requerimientos.	**Capítulo 2. Fundamentación del Proceso de la Auditoria de Sistemas, y conocimiento de las implicaciones normativas y sus requerimientos**. **2.1 Definición de auditoria** 2.6.1 Concepto de auditoria de sistemas 2.6.2 Importancia de la auditoria 2.6.3 Tipos de auditoria

	2.7 Riesgo de auditoria 2.7.1 Tipos de riesgo de auditorias **2.8 Control de auditoria** 2.31 tipos de controles de auditoria
	2.9 Proceso de la auditoria de sistemas **2.9.1 Planificación** 2.9.1.1 **Entendimiento del negocio** 2.9.1.1.1 Ambiente operativo 2.9.1.1.2 **Factores ambientales de ti** 2.9.1.1.2.1 Nivel de centralización 2.9.1.1.2.2 tecnología desplegada 2.9.1.1.2.3 Grado de personalización 2.9.1.1.2.4 Grado de formalización 2.9.1.1.2.5 Grado de entorno regulatorio o cumplimiento 2.9.1.1.2.6 Grado y método de tercerización 2.9.1.1.2.7 Grado de estandarización de las operaciones 2.9.1.1.2.8 Grado de dependencia tecnológica **2.4.2 Ejecución** 2.4.2.1 Redefinir la comprensión de la TI y el alcance. 2.4.2.2 Prueba de la eficacia del diseño de control de los objetivos de control clave. 2.4.2.3 Pruebe el resultado de los objetivos de

	control clave. 2.4.2.4 Documentar el impacto de control y debilidades. **2.4.3 Reporte** **2.4.4 Seguimiento** **2.5 Norma PCIDSS** 2.5.1 Verificación de los requerimientos 7, 8,9.
Evaluar el nivel de cumplimiento de la normativa en los requerimientos 7,8, 9 de Coral Hipermercado Racar plaza.	**Capítulo 3. Evaluación del nivel de cumplimiento de la normativa en los requerimientos 7, 8, 9 de Coral Hipermercado Racar plaza.** **3.1 Entendimiento del negocio de Coral Hipermercado Racar plaza.**

	3.1.1 Plan estratégico 3.1.2 Visión 3.1.3 Misión 3.1.4 Objetivos 3.1.5 Estrategias 3.1.6 Plan operativo 3.1.7 Estructura organizacional **3.2 Factores ambientales de ti de Coral Hipermercado Racar plaza.** 3.2.1 Nivel de centralización 3.2.2 Tecnología desplegada 3.2.3 Grado de personalización 3.2.4 Grado de formalización 3.2.5 Grado de entorno regulatorio o cumplimiento 3.2.6 Grado y método de tercerización 3.2.7 Grado de estandarización de las operaciones 3.2.8 Grado de dependencia tecnológica **3.3 Redefinir la comprensión de la TI de Coral Hipermercado Racar plaza con su alcance..** **3.4 Prueba de la eficacia del diseño de control de los objetivos de control clave de Coral Hipermercado Racar plaza.** **3.5 Probar el resultado de los objetivos de control clave de Coral Hipermercado Racar plaza.** **3.6 Documentar el impacto de control y debilidades de Coral Hipermercado Racar plaza.**
	Capítulo 4. Conclusiones y recomendaciones.

11.- CRONOGRAMA DE ACTIVIDADES

ACTIVIDADES	MES I				MES II				MES III				MES IV				MES V			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1. Selección y delimitación del tema de investigación																				
2.- Justificación de la investigación																				
3.- Breve descripción del objeto de estudio.																				
4.- Formulación del problema																				
5.- Determinación de los objetivos																				
6.- Elaboración del marco teórico de referencia																				
7.- Preguntas de investigación																				
8.-Construcción de Variables e Indicadores																				
9.- Diseño Metodológico																				
10.- Esquema tentativo de la investigación																				
11.- Cronograma de actividades																				
12.- Presupuesto referencial																				

13.- Bibliografía																				
CAPITULO I. Conocimiento del Negocio																				
CAPITULO II. Fundamentación del Proceso de la Auditoria de Sistemas, y conocimiento de las implicaciones normativas y sus requerimientos																				
CAPITULO III. Evaluación del nivel de cumplimiento de la normativa.																				
4.3 Anexos																				
4.4 Bibliografía																				

12.- PRESUPUESTO REFERENCIAL

Detalle de gastos	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Valor Total
Empastado					$60,00	$60,00
Copias blanco y negro	$40,00	$60,00	$60,00	$50,00	$50,00	$260,00
Elaboración de Encuestas	$00,00	$90,00	$90.00			$180,00
Procesamiento de encuestas	$00,00	$60,00	$60,00			$120,00
Copias a color	$10,00	$10,00	$10,00	$30,00	$30,00	$90,00
Impresión de los capítulos	$20,00	$40,00	$45.00	$45.00	$25,00	$175,00
Internet	$20,00	$20,00	$20,00	$20,00	$20,00	$100,00
Transporte y movilización para el levantamiento de información	$50,00	$50,00	$70,00	$70,00	$80,00	$320,00
TOTAL ESTIMADO						**$1305,00**

13.- BIBLIOGRAFÍA

- COBIT, F. (2014). *VAL IT.*
- Council, P. s. (2012). Ambiente Regulatorio. En P. s. Council, *PCI DSS Education Series* (págs. 2-9). Chicago: Madison Street.
- Council, P. S. (2006). *PCI Security Standards Council*. Obtenido de https://es.pcisecuritystandards.org/minisite/en/
- Diccionario, R. A. (2014). *real academia Diccionario.*
- Griegos, P. d. (Enero de 2012). *Universisdad Autonoma del Estado de Hidalgo.*
- Obtenido de http://www.uaeh.edu.mx/docencia/P_Presentaciones/prepa3/conceptos_genera les_inv.pdf
- Isaca.org, (2015). *Acerca de Nuestro Capítulo*. [online] Available at: http://www.isaca.org/chapters10/Santiago/Acerca/Pages/Default.aspx [Accessed 16 Sep. 2015].
- ISACA, C. (2014). *Definición de Auditoria*. Obtenido de ISACA org.: https://www.isaca.org/Pages/default.aspx?cid=1002083&Appeal=SEM&gclid=C IDTz6W01sYCFUyPHwod0WEMHQ
- ISACA, C. (2007). *Gobermance Institute, IT Assurence Guide.* Chicago.
- Cotecna.com.ec, (2015). [online] Available at: http://www.cotecna.com.ec/~/media/Countries/Ecuador/Documents/Brochureiso-27001-cotecna-ecuador-FINAL.ashx?la=es-ES [Accessed 16 Sep. 2015].

- Lases, f. M. (2006). *Metodología de la investigación.* México: Hidalgo.
- Magdalena, G. d. (2015). *Manual de procesos y Procedimientos.* Recuperado el 16 de Septiembre de 2015, de http://www.magdalena.gov.co/apc-aafiles/61306630636336616166653232336536/manual_de_procesos_y_procedi mientos.pdf
- Ochoa, I. P. (Marzo de 2014). Procesos de Auditoria. Cuenca, Azuay, Ecuador
- Peña, I. G. (2014). Técnicas de Verificación, Universidad del Azuay Cuenca.
- Torres, M. Á. (2007). PCI DSS: ¿Cómo cumplir? Chicago: SIC.

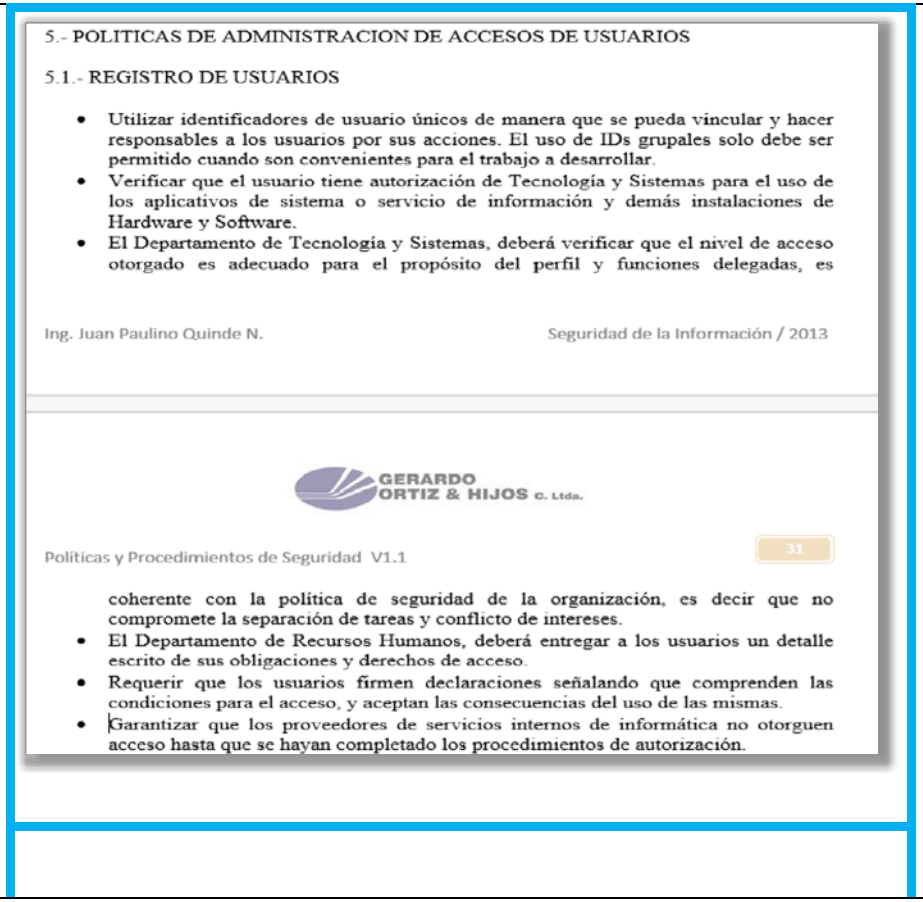
ANEXOS

PAPELES DE TRABAJO

ANEXO 1: PAPELES DE TRABAJO DEL REQUERIMIENTO 7. Restricción al acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. (7.1)

Papeles de Trabajo					
Cumplimiento Normativa PCI DSS					
Empresa auditada:	Coral Hipermercados Racar Plaza GO.			**Ref:** req. 7.1	
Periodo a examinar:	Periodo 2015 con corte a Junio.				
Supervisa:	Patricia Benenaula	**Responsable:**	Estefanía Ortega		
Tema:	Cumplimiento de la Norma PCI DSS requerimiento 7. Restringir el acceso a los datos del titular de la tarjeta según las necesidades de saber que tenga la empresa.			**Código:**	PT001
Objetivo:	Observar las limitaciones del acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso.				
Alcance:	7.1. Solicitar y revisar las políticas escritas para el control de acceso y verificar que estas contengan:				
Procedimiento:					
*Definidas las necesidades de acceso y asignación de privilegios de cada función. * Restricciones de acceso de usuarios con IDs privilegiadas a la menor cantidad de privilegios. *Aprobación documentada de las partes autorizadas que estén incluidas la lista de los privilegios.					
Revisión del procedimiento:					
Coral Hipermercado (GO), presenta la políticas de seguridad GO V 1.1, donde se encuentra incorporada la política de administración de acceso de usuarios la cual se puede observar a continuación:					

Políticas de administración de accesos de Coral Hipermercado (GO)



5.- POLITICAS DE ADMINISTRACION DE ACCESOS DE USUARIOS

5.1.- REGISTRO DE USUARIOS

- Utilizar identificadores de usuario únicos de manera que se pueda vincular y hacer responsables a los usuarios por sus acciones. El uso de IDs grupales solo debe ser permitido cuando son convenientes para el trabajo a desarrollar.
- Verificar que el usuario tiene autorización de Tecnología y Sistemas para el uso de los aplicativos de sistema o servicio de información y demás instalaciones de Hardware y Software.
- El Departamento de Tecnología y Sistemas, deberá verificar que el nivel de acceso otorgado es adecuado para el propósito del perfil y funciones delegadas, es

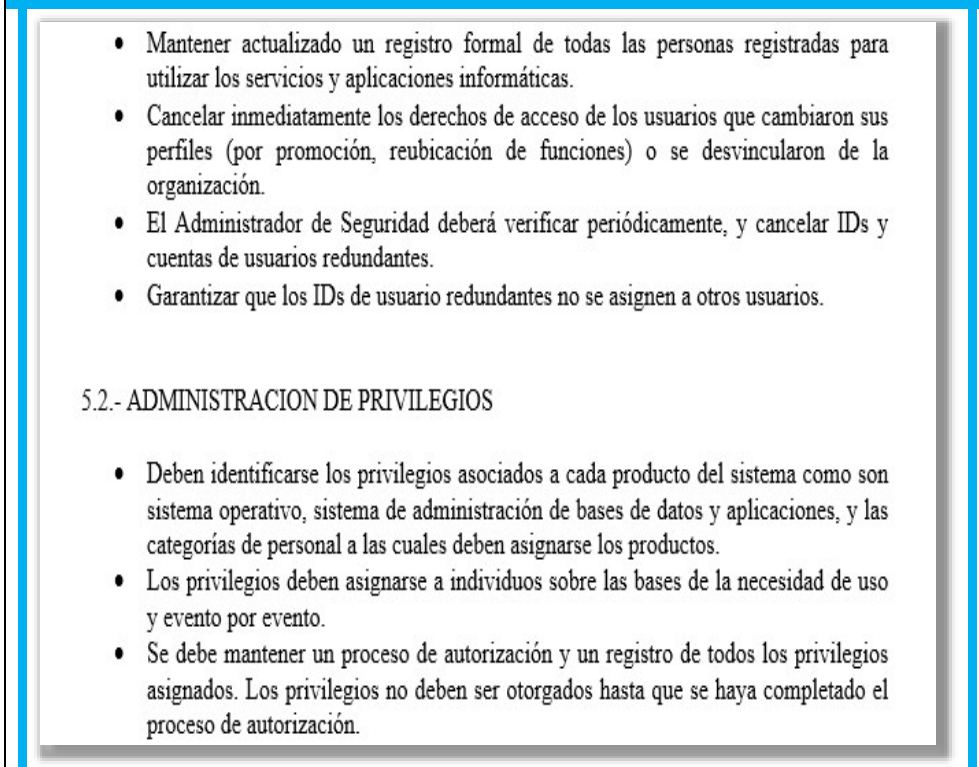
Ing. Juan Paulino Quinde N. Seguridad de la Información / 2013

GERARDO ORTIZ & HIJOS C. Ltda.

Políticas y Procedimientos de Seguridad V1.1 31

coherente con la política de seguridad de la organización, es decir que no compromete la separación de tareas y conflicto de intereses.

- El Departamento de Recursos Humanos, deberá entregar a los usuarios un detalle escrito de sus obligaciones y derechos de acceso.
- Requerir que los usuarios firmen declaraciones señalando que comprenden las condiciones para el acceso, y aceptan las consecuencias del uso de las mismas.
- Garantizar que los proveedores de servicios internos de informática no otorguen acceso hasta que se hayan completado los procedimientos de autorización.



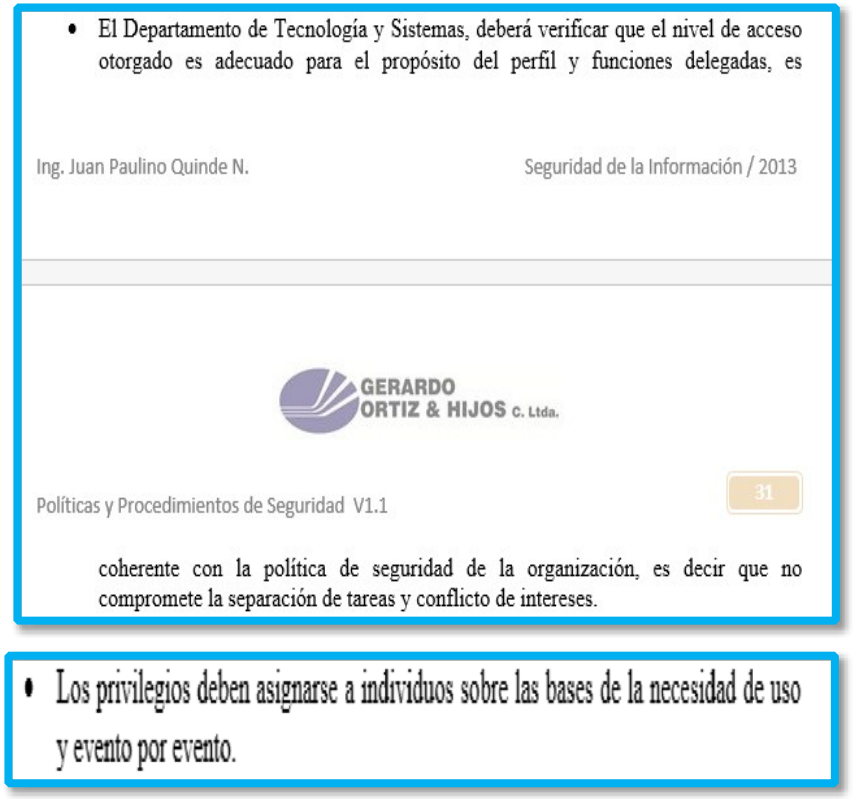
- Mantener actualizado un registro formal de todas las personas registradas para utilizar los servicios y aplicaciones informáticas.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus perfiles (por promoción, reubicación de funciones) o se desvincularon de la organización.
- El Administrador de Seguridad deberá verificar periódicamente, y cancelar IDs y cuentas de usuarios redundantes.
- Garantizar que los IDs de usuario redundantes no se asignen a otros usuarios.

5.2.- ADMINISTRACION DE PRIVILEGIOS

- Deben identificarse los privilegios asociados a cada producto del sistema como son sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- Los privilegios deben asignarse a individuos sobre las bases de la necesidad de uso y evento por evento.
- Se debe mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso de autorización.

Fuente: Coral Hipermercado Racar Plaza (GO).

Comparación de la norma PCI DSS con la política de Coral Hipermercado (GO).



- El Departamento de Tecnología y Sistemas, deberá verificar que el nivel de acceso otorgado es adecuado para el propósito del perfil y funciones delegadas, es

Ing. Juan Paulino Quinde N. Seguridad de la Información / 2013

GERARDO ORTIZ & HIJOS C. Ltda.

Políticas y Procedimientos de Seguridad V1.1 31

coherente con la política de seguridad de la organización, es decir que no compromete la separación de tareas y conflicto de intereses.

- Los privilegios deben asignarse a individuos sobre las bases de la necesidad de uso y evento por evento.

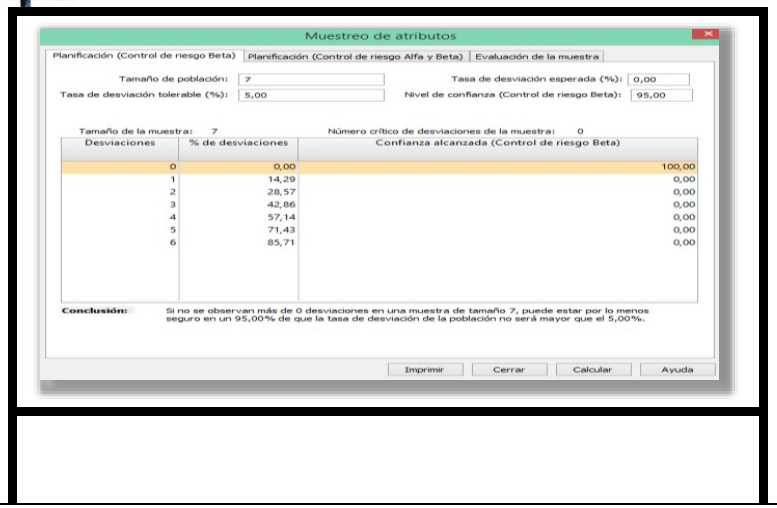
La empresa Coral Hipermercado (GO) según su política de administración de acceso, si tiene definida las necesidades y asignación de privilegios de cada función porque nos indica que el departamento de tecnología y sistemas son los encargados de asignar y verificar que el nivel de acceso sea suficiente para cumplir con las funciones de cada perfil, además la política de la empresa indica que los privilegios si son asignados sobre la base de la necesidad de uso, por lo que cumple con este requerimiento de la norma PCI DSS**.**

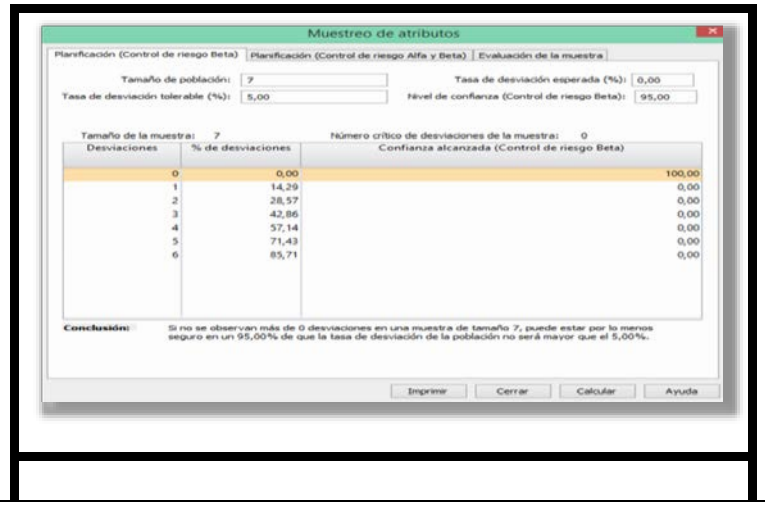
√

Fuente: Coral Hipermercado Racar Plaza (GO)

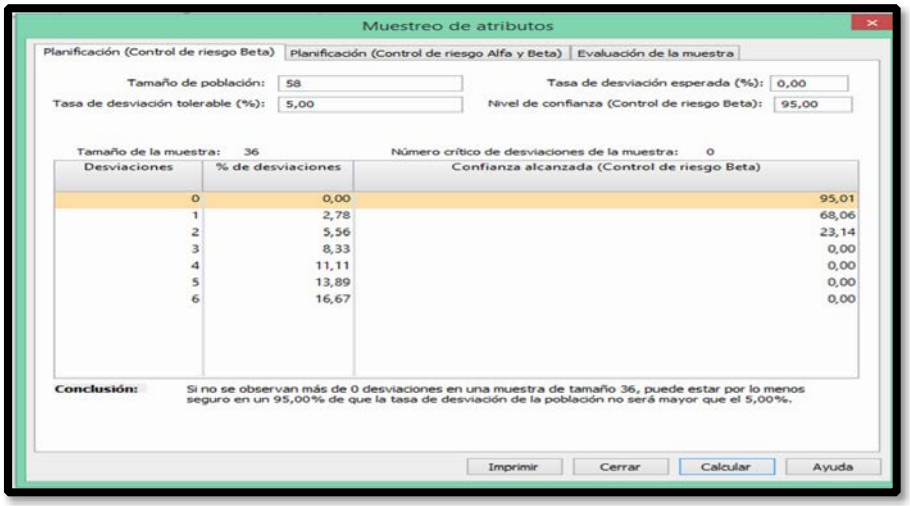
Fragmentos de la Política de administración de acceso de Coral Hipermercado (GO) • Utilizar identificadores de usuario únicos de manera que se pueda vincular y hacer responsables a los usuarios por sus acciones. **Fuente: Coral Hipermercado Racar Plaza (GO)**	La empresa según la política de administración de acceso, si asigna una ID privilegiada a cada uno de sus usuarios con la menor cantidad de privilegios, en el fragmento de la política de administración de accesos se puede observar que se utilizan identificadores de usuarios únicos para que puedan ser responsables de sus acciones, además como se observó en el punto anterior, los usuarios tienen los privilegios necesarios para llevar acabo sus responsabilidades, por lo que es otro requerimiento que la empresa cumple. √
Fragmentos de la Política de administración de acceso de Coral Hipermercado (GO) • El Departamento de Recursos Humanos, deberá entregar a los usuarios un detalle escrito de sus obligaciones y derechos de acceso.	Otro requerimiento de la norma PCI DSS que Coral Hipermercado si cumple es la aprobación documentada, como se puede observar en el fragmento de la política de administración, personal al momento de ingresar a la empresa por primera vez, se les entrega un detalle por escrito de las obligaciones y derechos, además que los

• Se debe mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso de autorización.	privilegios asignados se deben mantener en un procesos de autorización y no se entregaran hasta que se haya finalizado el proceso. √
Para poder verificar que la Política de administración de acceso de Coral Hipermercado (GO) cumple con las parámetros plasmados en la misma, se procederá a realizar las siguientes actividades:	
7.1.1.	**Seleccionar una muestra de las funciones para verificar que las necesidades de acceso de cada función estén definidas e incluyan:** *** Componentes del sistema y recursos de datos que necesitan para realizar su trabajo.** *** Se Identifique los privilegios necesarios para que puedan desempeñar sus funciones.**
La muestra calculada en el programa IDEA tomada de una población de 72 usuarios que trabajan en Coral Hipermercado Racar Plaza, cumpliendo las funciones de supervisores, cajeros y encargados del servidor transaccional, dan como resultado 50 usuarios por analizar.	
Captura de pantalla del cálculo de la muestra de los encargados del servidor transaccional.	**Captura de pantalla del cálculo de la muestra de los supervisores.**
Fuente: Programa Idea.	**Fuente: Programa Idea.**



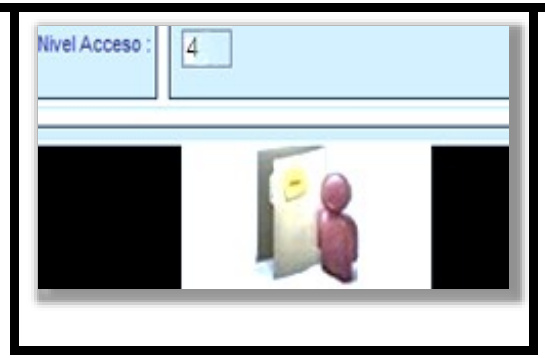


Captura de pantalla del cálculo de la muestra de los cajeros.



Fuente: Programa Idea.

El resultado de la muestra selecciona del programa IDEA fue: 36 Cajeros, 7 supervisores y 7 encargados del servidor transaccional.
De la muestra seccionada se pudo constatar que todos los usuarios tienen las mismas características, por lo que seleccionamos como ejemplo a un usuario de cada función (supervisores, cajeros y servidores transaccionales) para poder realizar el respectivo análisis.
Después de haber seleccionado una muestra de la funciones de Coral Hipermercado Racar Plaza, determinamos que los componentes del sistema y recursos de datos que necesita cada función para acceder a fin de realizar su trabajo son los siguiente:

Captura de pantalla de los componentes del sistema. (cajeros)	**Captura de pantalla de los componentes del sistema. (Encargados del Switch Transaccional)**	**Captura de pantalla de los componentes del sistema. (Supervisores).**
		

Fuente: Coral Hipermercado Racar Plaza (GO)	**Fuente: Coral Hipermercado Racar Plaza (GO)**	**Fuente: Coral Hipermercado Racar Plaza (GO)**

1. Como se puede observar, Los usuarios en una terminal de facturación constan con un nivel de acceso según las funciones que desempeñan, en el caso de los cajeros tienen un nivel de acceso número 2, cuando son supervisores su nivel de acceso es nivel 4, los servidores transaccionales constan como Stwich transaccional porque son usuarios encargados de mantener en correctas condiciones el swtich transaccional para una transacción segura. Los usuarios pueden levantar la sesión en cualquier terminal (una sola sesión por terminal) debido a que se trata del servicio Active Directory (es un servicio de Microsotf establecido en uno o varios servidores en donde se crean usuarios, equipos o grupos, con la finalidad de administrar los inicios de sesión en los equipos conectados a la red), en el caso de cajeros no pueden variar de terminal en el mismo día tienen primero que cuadrar.

Los cajeros, supervisores y encargados del servidor transaccional no son usuarios de base de datos, son usuarios de aplicación, internamente se maneja una base de datos transparente para el usuario administrador, de esa manera se evita que cuando exista pérdida de un usuario con la contraseña, se atente con la seguridad de la base de datos en el momento de que escalan más privilegios.

Por todo lo dicho anteriormente podemos constatar de que la empresa Coral Hipermercado si cumple con este requerimiento de la norma PCI DSS, debido a que en una terminal de facturación los usuarios tienen componentes del sistema y recursos de datos necesarios para realizar su trabajo.

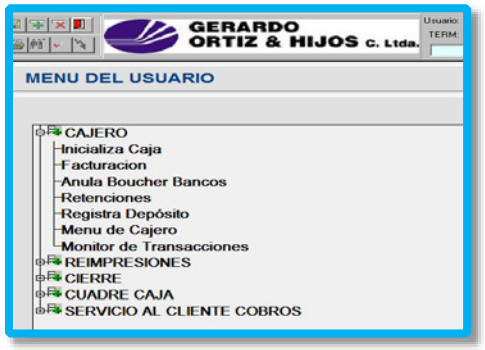
√

2. Identificar los privilegios necesarios de cada función para que puedan desempeñar sus funciones.

En las siguientes ilustraciones se encuentra las funciones con los privilegios necesarios que le permiten al cajero, supervisor y encargado del servidor transaccional realizar su trabajo, para poder verificar que cumpla con la norma se debe comparar con las funciones que fueron otorgadas por recursos

humanos.

Captura de pantalla de los Las funciones que desempeñan los cajeros según el manual de funcionamiento usuarios cajeros. proporcionado por Recursos Humanos son:



Fuente: Coral Hipermercado Racar Plaza

1. Atención al cliente.

2. Generar los reportes para cuadres de caja.

3. Solicitar al supervisor la confirmación de precios de artículos que deben ser verificados.

4. Realizar el depósito del dinero recolectado en caja antes de las 4 pm.

(GO) 5. Revisar que los artículos registrados no estén averiados, en mal estado o incompleto.

6. Reportar al Jefe inmediato errores de marcación detectados.
7. Solicitar al supervisor en presencia del cliente la anulación de registro y autorización de retorno de mercadería.
8. Dar aviso al supervisor cuando los clientes paguen con cheque o pagos con tarjetas de crédito.
9. Vigilar que no ocurran perdidas de mercadería por clientes deshonestos o empleados del almacén.
10. Recibir al inicio del día la base para comenzar la operación.
11. Revisar el stock de productos en las perchas de caja.
12. Solicitar la presencia del supervisor cuando el cliente tenga algún reclamo sobre el registro de mercadería en la factura.
13. Reportar los daños que se presenten en el sistema informático de cajas.
14. Realizar las promociones de ofertas y eventos especiales.

Privilegios otorgados a cajeros

1. Atender al cliente siguiendo los lineamientos del protocolo y registrar los artículos que el cliente ha seleccionado.

2. Generar los reportes para cuadras de cajas.

3. Solicitar al supervisor confirmación de precios de artículos que deben ser verificados.

4. Realizar el depósito del dinero recolectado en caja hasta antes de las 4 pm.

Fuente: Coral Hipermercado Racar Plaza (GO)

Se comparó el manual de funcionamiento de los cajeros con los privilegios otorgados en el sistema y como resultado tenemos:

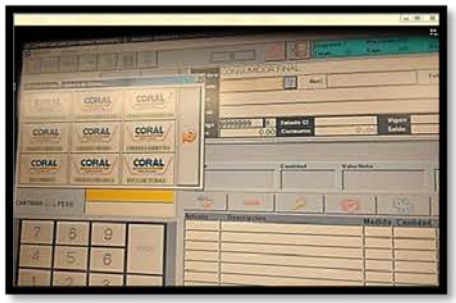
Capturas de pantalla de iniciación de caja.

Una de las funciones de los cajeros según el manual, es la de recibir al inicio del día la base de facturación para comenzar la operación, por esa razón para verificar que cumplan con lo escrito en el manual, se observó a los cajeros seleccionados en la muestra y se llegó a la conclusión de que si tienen que realizar la iniciación de caja dentro del sistema para poder empezar a facturar.

√

Fuente: Coral Hipermercado Racar Plaza (GO)

Captura de pantalla de facturación, selección del producto mediante código de barras y huella del supervisor para anulación de productos no deseados por el cliente.



Además los cajeros son los encargados de atención al cliente por lo que tienen que facturar los productos que el consumidor quiera adquirir, siempre en vigilancia del supervisor cuando exista anulación de productos que se desee devolver y

asegurándose de usar los parámetros y lineamientos otorgados por la empresa para poder realizar una venta segura. En la muestra tomada se llegó a la conclusión de que los cajeros tienen acceso a la facturación dentro del sistema y no pueden realizar anulación de productos sin que el supervisor lo autorice ya que se necesita la huella digital del mismo.

√

Fuente: Coral Hipermercado Racar Plaza.

En el manual de funcionamiento indica que a los cajeros se les proporciona lineamientos para realizar la atención al cliente y la venta del producto, en ocasiones no todas las ventas son en efectivo por lo tanto la empresa otorga, mediante el departamento de créditos, a los cajeros un manual para realizar una venta segura a crédito ya sea con tarjeta o crédito directo de la empresa.

Según las entrevistas realizadas al personal seleccionado, la empresa otorga el manual a los cajeros en el momento de la capacitación cuando ingresan a la empresa, además se realizó capturas de pantalla de los acceso al sistema para poder realizar una venta con tarjeta de pago y se confirmó lo expuesto por el personal.

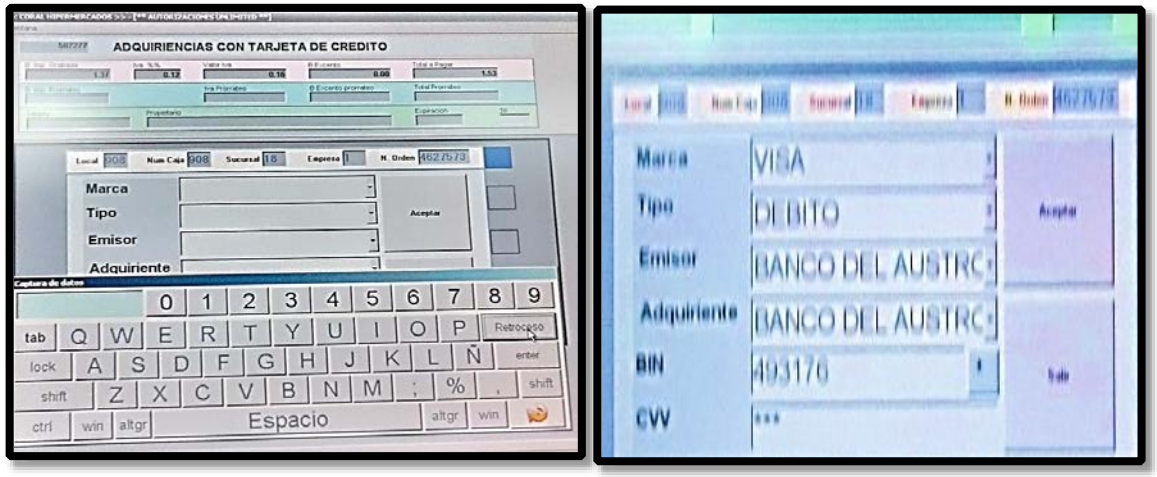
A continuación detallaremos lo expuesto en el párrafo anterior.

El manual otorgado por el departamento de crédito de la empresa indica que existen dos opciones para cobrar con tarjeta estas son:

1. El P.O.S: los cuales están compuesto por Medianet, Datafast y el P.O.S del Banco del Austro, estos los cajeros utilizan cuando el Switch transaccional, que fue creado por la empresa, no funciona, está en mantenimiento o se paga con tarjeta Cuatafácil.

2. El Switch transaccional: Es creado por el departamento de tecnología y sistemas de la empresa, se puede usar con cualquier tarjeta afiliada al establecimiento y cuando se utiliza, el cajero tiene acceso a lo expuesto en las siguientes ilustraciones:

Captura de pantalla para colocar los datos de la tarjeta.

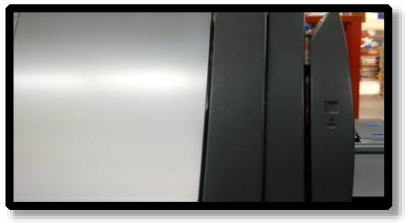


El cajero debe colocar el BIN de la tarjeta para que salgan los datos correspondientes de la misma, después debe colocar el código de validación para que se les otorgue la autorización del banco emisor.

√

Fuente: Coral Hipermercado Racar Plaza (GO)

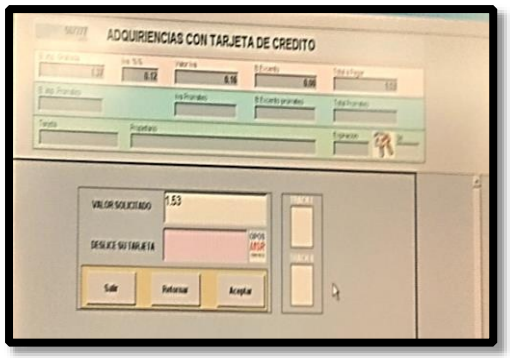
Switch transaccional.



Después se debe deslizar la tarjeta por el Switch transaccional.

√

Captura de pantalla para seleccionar el monto y si es diferido o corriente.



Se debe colocar el monto de la transacción para elegir si es que se quiere a diferido o corriente.

√

Fuente: Coral Hipermercado Racar Plaza (GO)

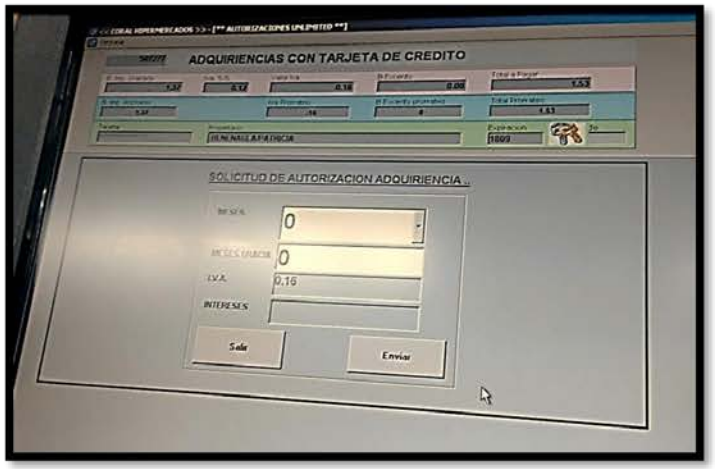
Captura de pantalla cuando es diferido.

Si es diferido seleccionar a cuantos meses.

√

Fuente: Coral Hipermercado Racar Plaza (GO)

Captura de pantalla para aceptar la transacción y que se envíe al Banco emisor.



Y finalmente se selecciona aceptar para que se envíe la información al Banco emisor y así poder realizar la transacción.

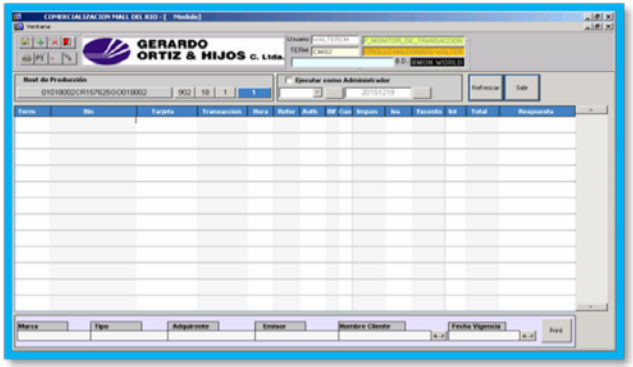
√

Fuente: Coral Hipermercado Racar Plaza (GO)

Todo esto debe ser realizado en presencia del tarjetahabiente (cliente dueño de la tarjeta).

Cuando se realiza la transacción mediante el Switch transaccional, los datos del valor y la factura se registra directamente en la contabilidad, pero cuando se realiza por los P.O.S los cajeros se encargan de registrar en el monitor de transacciones. Este monitor le permite verificar todas las transacciones que se han realizado, especialmente las de tarjeta de crédito.

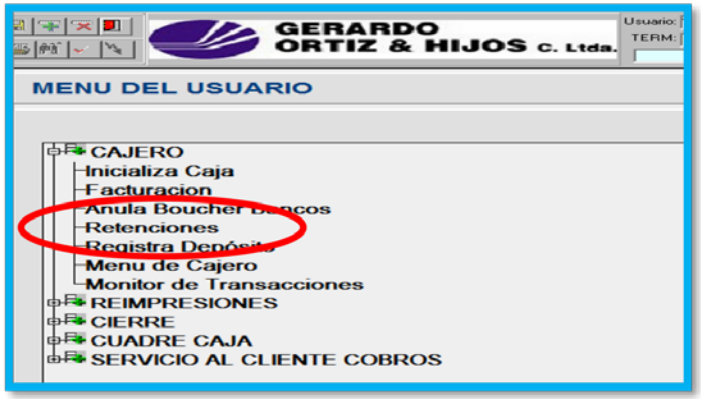
Monitor de transacciones.



Fuente: Coral Hipermercado Racar Plaza (GO)

√

Captura de pantalla de las funciones de los cajeros.

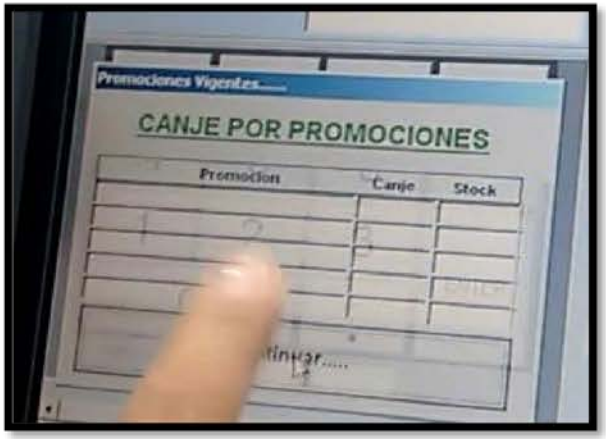


Fuente: Coral Hipermercado Racar Plaza (GO)

El cajero tiene acceso a las retenciones dentro del sistema, pero en el manual de funcionamiento no hace mención de que el cajero pueda realizar algún tipo de retenciones, por lo que el cajero acceso a una función en cual no está autorizado según el manual.

4

Captura de pantalla para activar promociones.



Fuente: Coral Hipermercado Racar Plaza (GO)

Otra de las funciones según el manual es la de realizar promociones de ofertas y eventos especiales. El cajero si tiene acceso a realizar descuentos por promociones y eventos especiales como indica el manual de funcionamiento.

√

Captura de pantalla cuadre de caja.

Fuente: Coral Hipermercado Racar Plaza (GO)

Según el manual de funcionamiento el cajero debe realizar el cuadre de caja al finalizar el día, así como los depósitos del dinero en efectivo a las 4 pm, en el sistema se puede visualizar que los cajeros tienen acceso a la

opción de cuadre de caja y deposito pero no hay ningún parámetro que indique que se cierra la opción de depósito a partir de las 4 de la tarde.

√

Observación: La anulación de voucher no lo puede hacer sin presencia del supervisor porque necesitan la huella del mismo, en el manual de funciones de los cajeros no específica este punto por lo que no se encuentra documentado. **Obs.**

A otros usuarios que debemos analizar son los supervisores, los cuales cuentan con las siguientes funciones en el manual de la empresa y accesos dentro del sistema.

Funciones que desempeñan los supervisores de caja según el manual de funcionamiento proporcionado por Recursos Humanos.

1. Elabora informes de cuadres de caja realizados en el día para contabilidad.
2. Elabora reportes de depósitos de efectivo recolectados en las transacciones de los cajeros.
3. Controla que el personal de cajas este ubicado en cada puesto de trabajo.
4. Reporta las cajas que no operan por fallas técnicas o electrónicas.
5. Facilita la clave para anulación de productos no deseados por los clientes.
6. Verifica que se registre en el escáner todos los productos adquiridos por el cliente.
7. Revisa que el personal de caja no tenga en su poder dinero, comida y celulares.

8. Contar dineros en efectivo, revisar voucher y cheques recolectados durante la transacción del día al momento de realizar cuadre de caja.

9. Controlar que los cajeros cumplan con el protocolo de atención al cliente.

11. Validar que la información entregada en los cuadres de caja por los cajeros coincidan con el dinero entregado.

12. Solicitar la autorización del administrador del local para realizar ventas mayoristas a crédito.

13. Solicitar la autorización con tarjetas de crédito cuando no hay sistema.

14. Realizar la activación del menú del sistema de cuadres de caja.

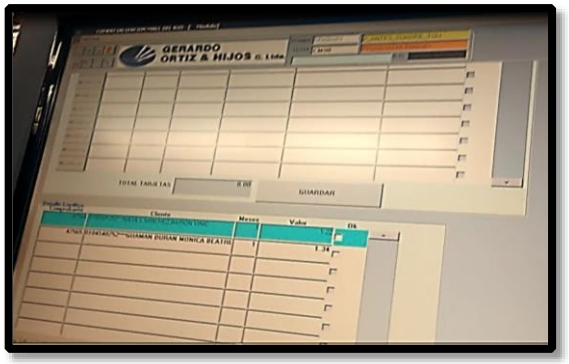
15. Entrenar constantemente al personal de cajas.

16. Asignar y grabar en el sistema las claves de acceso, de los cajeros y retirarlos por ausencia definitiva o temporal.

17. Conocer técnicamente del funcionamiento de las cajas.

Fuente: Coral Hipermercado Racar Plaza (GO)

Captura de pantalla de la revisión de los voucher.



El supervisor se encarga de revisar los voucher al finalizar el día para verificar que conste en el cuadre de caja tanto físicamente como en el sistema, en el caso de que el voucher no se encuentre

se tomará como un faltante de caja, se llegó a la conclusión de que si tienen

√

Fuente: Coral Hipermercado Racar Plaza. acceso a esta opción en el sistema.

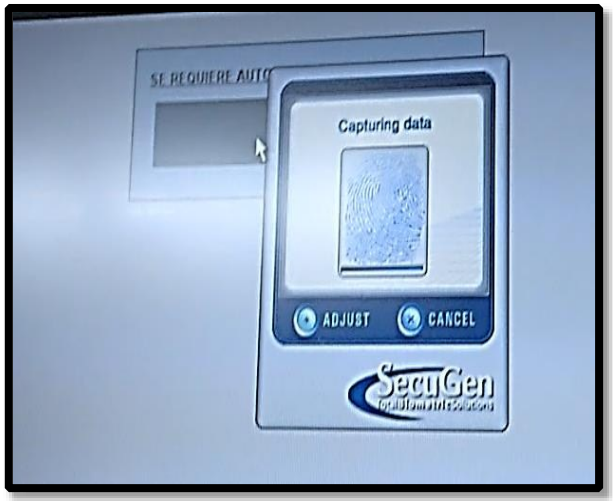
El supervisor tiene que realizar los informes para contabilidad, por lo que se entrevistó al personal y se llegó a la conclusión de que los supervisores entregan este informe a contabilidad incluyendo los respectivos voucher revisados y cotejados.

Otra de los componentes del sistema que ocupan los supervisores es la anulación de voucher, aunque no especifique dentro del manual de funcionamiento de los supervisores, ellos se encargan de este trabajo ya que sin su clave (huella digital) no pueden acceder a realizar dicha labor.

Obs.

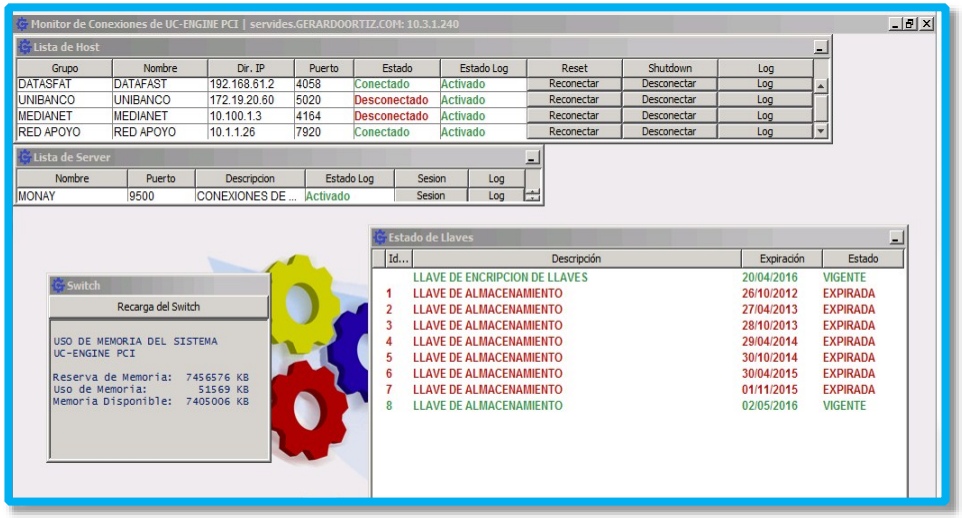
Anulación de voucher.

Captura de pantalla autorización de anulación de voucher.



Fuente: Coral Hipermercado Racar Plaza (GO) Fuente: Coral Hipermercado Racar Plaza (GO)
La empresa no nos proporcionó un manual de funcionamiento para los encargados del servidor transaccional, pero según entrevistas realizadas ellos están encargados de: 1. Velar por la caducidad de las licencias. 2. Controlar las alertas que pueden darse. 3. Procurar su funcionamiento. 4. Verificar la conexión permanente con los entes bancarios. **Fuente: Coral Hipermercado Racar Plaza (GO)**
Podemos observar al Servidor transaccional y los accesos que tiene el personal encargado del mismo, donde podemos comprobar que si cumple con lo dicho en la entrevista, ya que se puede visualizar los P.O.S que tienen fallas con la palabra desconectado, además vigilan si aún la licencia que se utiliza en ese momento está vigente y verifican que todas las máquinas de los P.O.S estén funcionando para que exista una correcta conexión con los

entes bancarios.



√

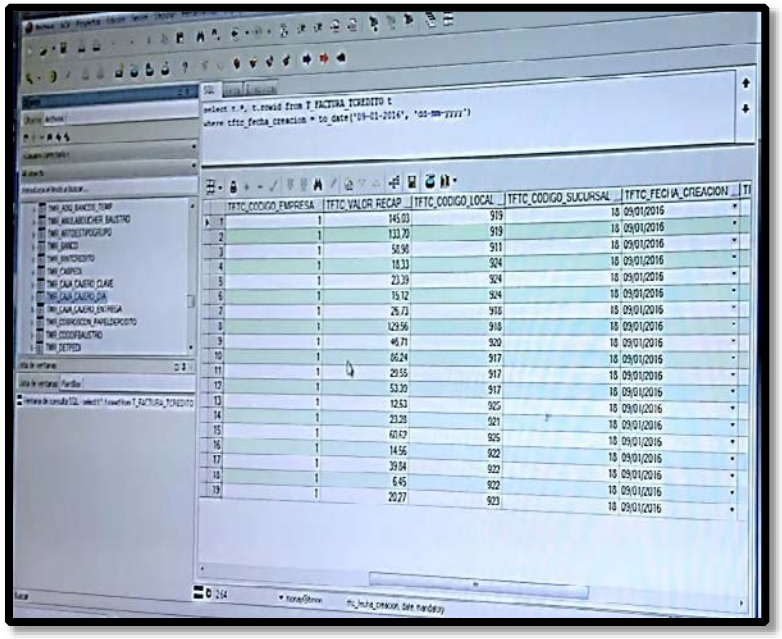
Fuente: Coral Hipermercado Racar Plaza (GO)

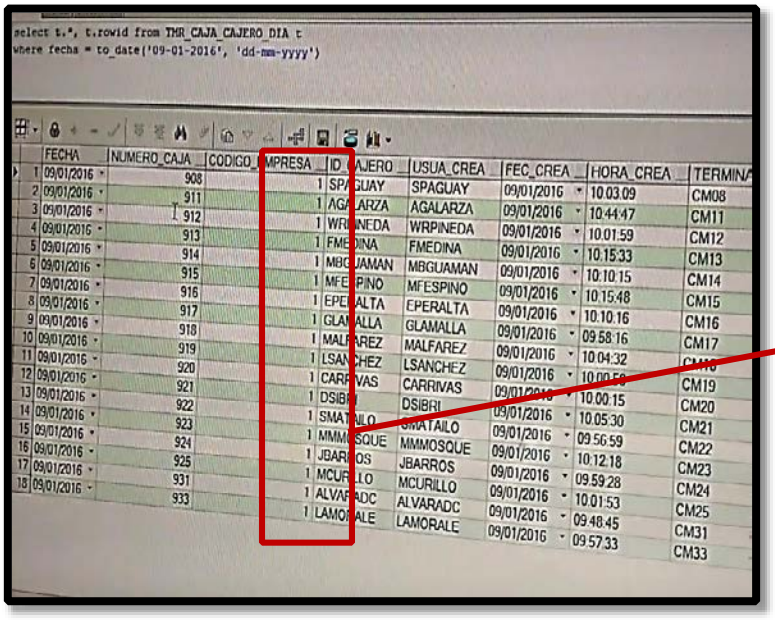
Pero según observaciones realizadas los encargados del servidor transaccional también tiene acceso a :

La base de datos para verificar la transacción que se realizó en caja y si esta se hizo mediante efectivo, crédito de la empr esa o tarjeta de pago, por lo que no tienen bien definidas sus funciones.

Verifican que cajas estén activas en ese momento, cuales están funcionando correctamente y cuales necesitan mantenimiento.

Ilustración…. Captura de pantalla de los Cajeros que se encuentra activos en ese momento en el sistema





Usuarios Activos se indica con el número 1

Fuente: Coral Hipermercado Racar Plaza (GO)

Fuente: Coral Hipermercado Racar Plaza (GO)

7.1.2a: Entrevistar al personal encargado de la asignación de los accesos para verificar que el acceso de usuarios con ID pri vilegiadas cumplan con:

* Asignación solamente a las funciones que específicamente necesitan acceso privilegiado.

*Que esté restringido a la menor cantidad de privilegios que sean necesarios para llevar a cabo las responsabilidades del trabajo.

7.1.2b: Seleccionar una muestra de las ID de usuarios privilegiados y entrevistar al personal de administración encargado con la finalidad de verificar que los privilegios asignados respete: Ser necesarios para el trabajo del usuario.

Estén restringidas a la menor cantidad de privilegios que sean necesarios para llevar a cabo las responsabilidades del trabajo.

La entrevista que se realizó al Ingeniero Walter Criollo, al Ingeniero Huberto Cedillo y al Ingeniero Paulino Quinde, 3 de los encargados de asignar los accesos, nos dio como resultado:

Entrevista a los encargados de asignar el acceso.

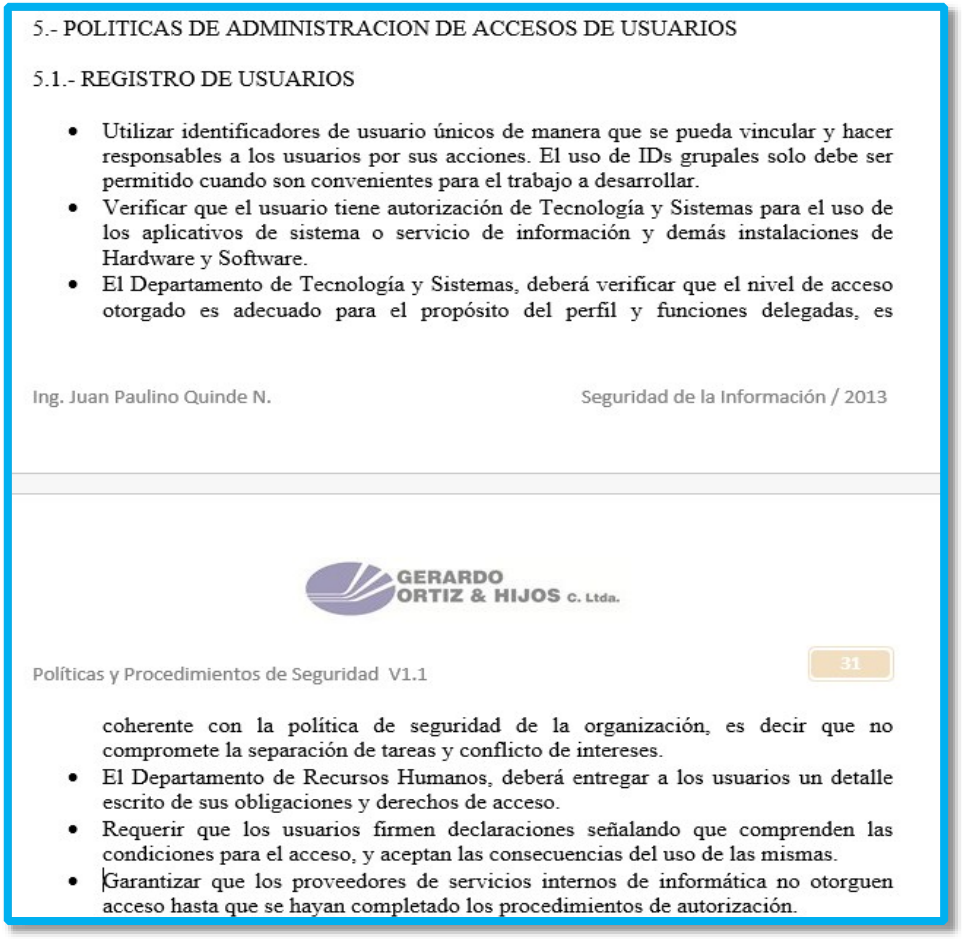
DETALLE	SI	NO	N/A	OBSERVACIONES
¿El acceso de usuarios con ID privilegiadas se asignan solamente a las funciones que necesitan acceso privilegiado? y ¿por qué?	/			En el caso de los cajeros, supervisores y encargados del servidor transaccional la empresa Coral Hipermercado, asigna en las ID de cada usuario las funciones necesarias para realizar el trabajo.

¿Se restringe a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo?	/			Los cajeros son los únicos que pueden realizar la facturación, los supervisores son aquellos que pueden anular voucher, mientras que los encargados del servidor transaccional son los únicos que tienen acceso al Switch para realizar algún mantenimiento o reparación.

Elaborado por : Autoras

7.1.3: Seleccionar una muestra de las ID de usuarios y comparar con la aprobación documentada para verificar que exista una aprobación documentada, además que las partes autorizadas aprobaron el documento y Los privilegios especificados en la documentación coinciden con los roles asignado a la persona.

Políticas de administración de accesos de Coral Hipermercado (GO). **Manual de funcionamiento de Coral Hipermercado.**



5.- POLITICAS DE ADMINISTRACION DE ACCESOS DE USUARIOS

5.1.- REGISTRO DE USUARIOS

- Utilizar identificadores de usuario únicos de manera que se pueda vincular y hacer responsables a los usuarios por sus acciones. El uso de IDs grupales solo debe ser permitido cuando son convenientes para el trabajo a desarrollar.
- Verificar que el usuario tiene autorización de Tecnología y Sistemas para el uso de los aplicativos de sistema o servicio de información y demás instalaciones de Hardware y Software.
- El Departamento de Tecnología y Sistemas, deberá verificar que el nivel de acceso otorgado es adecuado para el propósito del perfil y funciones delegadas, es

Ing. Juan Paulino Quinde N. Seguridad de la Información / 2013

GERARDO ORTIZ & HIJOS C. Ltda.

Políticas y Procedimientos de Seguridad V1.1 31

coherente con la política de seguridad de la organización, es decir que no compromete la separación de tareas y conflicto de intereses.

- El Departamento de Recursos Humanos, deberá entregar a los usuarios un detalle escrito de sus obligaciones y derechos de acceso.
- Requerir que los usuarios firmen declaraciones señalando que comprenden las condiciones para el acceso, y aceptan las consecuencias del uso de las mismas.
- Garantizar que los proveedores de servicios internos de informática no otorguen acceso hasta que se hayan completado los procedimientos de autorización.

Fuente: Coral Hipermercado Racar Plaza (GO)

Fuente: Coral Hipermercado Racar Plaza (GO)

En las imágenes otorgadas por Coral Hipermercado (visualizadas en la sección anterior) se comprueba que existe aprobación documentada y autorizada, también podemos observar el manual de funcionamiento autorizado de la empresa Coral Hipermercado, además podemos visualizar las políticas de administración de control de acceso.

Los privilegios de acceso si coinciden con lo expuesto en los manuales, como se pudo observar en el punto 7.1.1, excepto cuando se trata de anulación de un voucher, a pesar de que no se encuentre entra las funciones del supervisor, ellos también se encargan de esto.

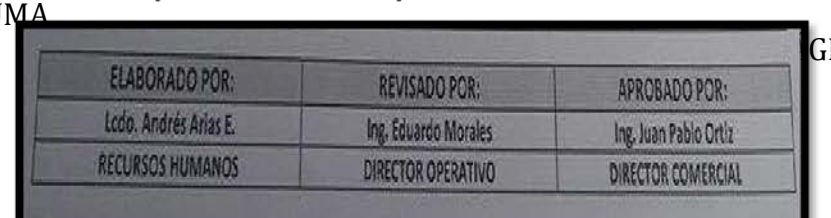
En el caso de los encargados del servidor transaccional, no pudimos obtener aprobación documentada pero con las entrevista realizadas y las observaciones hechas, llagamos a la conclusión que tienen acceso a otras funciones a aparte de lo expuesto en las entrevistas, ya que pueden acceder a la base de datos de facturación.

Obs.

Conclusiones y recomendaciones:

Las políticas de administración de control de acceso de Coral Hipermercado cumple en un gran mayoría con la norma PCI DSS, ya que abarca casi todos puntos del requerimiento descrito en el papel de trabajo 001, además la empresa aplica la política en la práctica diaria, pero cuando se trata de

Aprobación de las partes.



ELABORADO POR:	REVISADO POR:	APROBADO POR:
Lcdo. Andrés Arias E.	Ing. Eduardo Morales	Ing. Juan Pablo Ortiz
RECURSOS HUMANOS	DIRECTOR OPERATIVO	DIRECTOR COMERCIAL

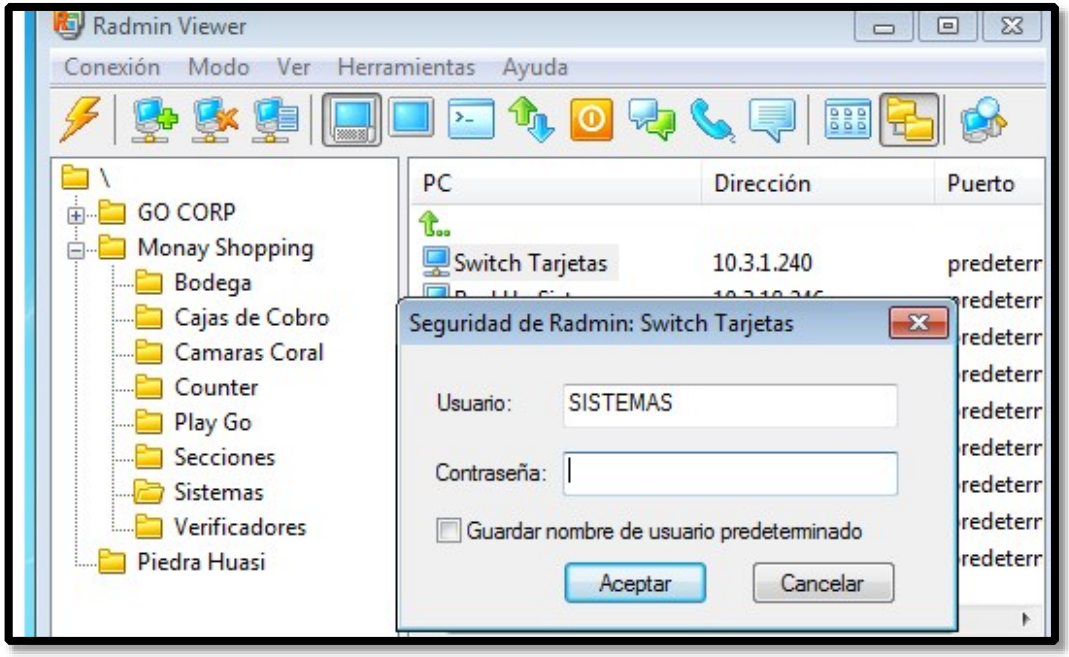
aprobación documentada no cumplen con todo lo necesario, debido a que en la anulación de Voucher de la tarjeta de pago, en el manual no se especifica quien debería realizar esta función, el supervisor lo hace directamente sin que se encuentre dentro del manual de funcionamiento de los supervisores, además no hay un manual de funcionamiento para los encargados del servidor transaccional por lo que no se sabe con exactitud que funciones debe cumplir, pero según las entrevistas y observaciones realizadas ellos tienen acceso a componentes del sistema y recursos de datos fuera de lo expuesto por la empresa. Todo lo mencionado podría ser perjudicial debido a que el personal debe conocer y respetar siempre las políticas y los procedimientos operativos para asegurarse de que el acceso este controlado y de esta manera se limita según las funciones de la necesidad de saber del usuario y de la menor cantidad de privilegios, además se recomienda actualizar los manuales de funcionamiento de la empresa, colocando las funciones del supervisor según el trabajo que realiza y elaborar un manual de funcionamiento para el encargado del servidor transaccional y de esa manera se defina bien cuáles son con exactitud las funciones necesarias que tienen para que puedan realizar su trabajo.
Elaborado por: Autoras

ANEXO 2: PAPELES DE TRABAJO DEL REQUERIMIENTO 7. Restricción al acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. (7.2).

Papeles de Trabajo

Cumplimiento Normativa PCI DSS					
Empresa auditada:	Coral Hipermercado Racar Plaza GO.			**Ref:** Req. 7.2	
Periodo a examinar:	Periodo 2015 con corte a Junio.				
Supervisa:	Estefanía Ortega	**Responsable:**	Patricia Benenaula		
Tema:	Cumplimiento de la Normativa PCI DSS requerimiento 7. Restringir el acceso a los datos del titular de la tarjeta según las necesidades de saber que tenga la empresa.			**Código:**	PT002
Objetivo:	Verificar que se estableció un sistema de control de acceso para los componentes del sistema de manera que restrinja el acceso según la necesidad del usuario de conocer y que se configure para "negar todo".				
Alcance:	7.2 Observar y evaluar los parámetros del sistema y la documentación para verificar que el sistema de control de acceso se implemente de la siguiente forma:				
Procedimiento:					
*Confirmar que los sistemas de control de acceso se implementen en todos los componentes del sistema.					
*Confirmar que los sistemas de control de acceso estén configurados de manera que los privilegios asignados a una persona se realicen según la clasificación del trabajo y la función.					
*Confirma que los sistemas de control de acceso cuenten con la configuración predominada de "negar todos".					
Revisión del procedimiento:					
7.2.1 Confirmar que los sistemas de control de acceso se implementen en todos los componentes del sistema					
Entrevista al personal administrativo grupo (GO) Acceso Remoto req.7.2.1				**Obs.**	

Hemos podido confirmar que los parámetros del sistema para servidores transaccionales permiten el acceso mediante el uso de una contraseña, sin embargo la parte administrativa nos informa que existe una sola contraseña para el monitoreo de 7 personas que sirve incluso para accesos remotos al sistema de facturación.



Fuente: Coral Hipermercado Racar Plaza (GO).

Entrevista al personal administrativo grupo (GO) Acceso Remoto req.7.2.1	√

Por otro lado el sistema de facturación y supervisión se encuentra debidamente implementados los sistemas de control de accesos en todos sus componentes.

Fuente: Coral Hipermercado Racar Plaza (GO).

Entrevista al personal administrativo grupo (GO) req.7.2.2

7.2.2. Confirmar que los sistemas de control de acceso estén configurados de manera que los privilegios asignados a una persona se realicen según la clasificación del trabajo y la función.

√

Los sistemas de control de acceso de usuarios según los privilegios si se cumplen según lo observado puesto que tanto para el sistema de facturación, supervisión, soporte y administración se desarrollan privilegios según las funciones de las personas, por ejemplo en facturación se les asigna un sistema de huella para ingresar al sistema de facturación, y dentro del programa solo se manejan funciones estrictamente

	necesarias para el control de las ventas.

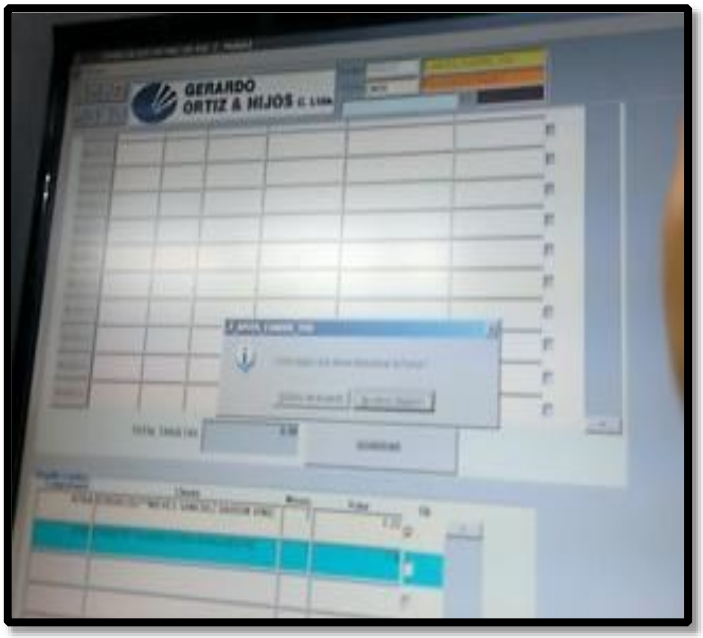
Fuente: Coral Hipermercado Racar Plaza (GO).

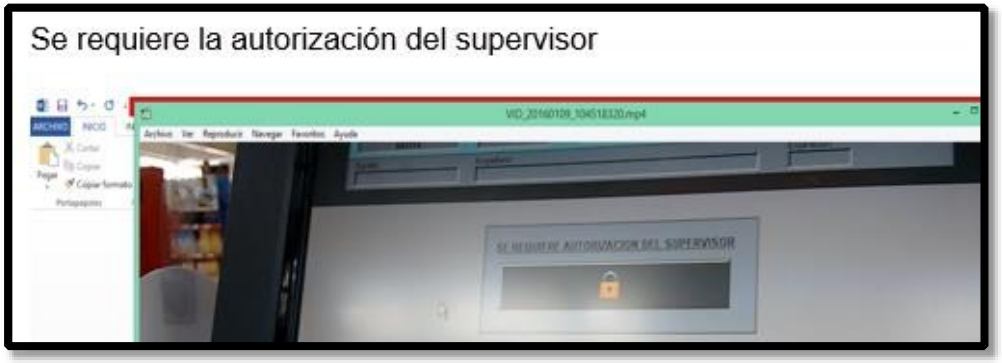
Entrevista al personal administrativo grupo (GO)	
Se logró observar que también los servidores transaccionales mantienen privilegios asignados según la clasificación de su trabajo sin embargo más adelante podremos observar que existe una falencia en la documentación ya que no se encuentran bien definidas las funciones que deben realizar.	√

Fuente: Coral Hipermercado Racar Plaza (GO).

7.2.3 Confirma que los sistemas de control de acceso cuenten con la configuración predominada de "negar todos".

Entrevista al personal administrativo configuraciones negar accesos (GO) req. 7.2.3

	Obs
 	La normativa nos pide confirmar que los sistemas de control de acceso cuenten con la configuración de negar todos para accesos no permitidos según los privilegios, se pudo evidenciar que para funciones que no les pertenecen a un cajero solo a supervisores (por ej. anulación de vouchers) el sistema nos rechaza inmediatamente la acción, también con el sistema de huellas que

	maneja facturación este riesgo quedaría minimizado, sin embargo como se explicó anteriormente de los servidores transaccionales no es igual puesto que no se bloquea el sistema y se comparte la clave.

Fuente: Coral Hipermercado Racar Plaza (GO).

Conclusiones y recomendaciones:

Los sistemas de control de acceso que ha implementado Coral Hipermercado para el manejo de los componentes y parámetros del sistema si mantiene un acceso restringido según el usuario, sin embargo presenta falencia para el caso de los servidores transaccionales debido a que se mantiene una clave para el manejo de varias personas en accesos remotos y además no mantiene configuraciones para negar todos en caso de accesos no permitidos.

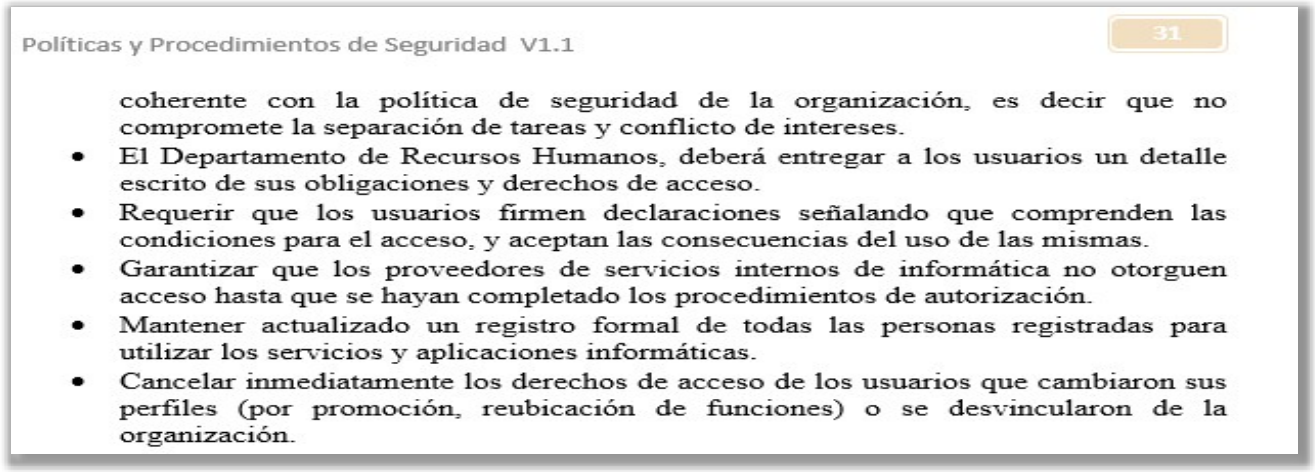
Elaborado por: Autoras

ANEXO 3: PAPELES DE TRABAJO DEL REQUERIMIENTO 7. Restricción al acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. (7.3).

Papeles de Trabajo				
Cumplimiento Normativa PCI DSS				
Empresa auditada:	Coral Hipermercado Racar Plaza GO.		**Ref:** Req. 7.3	
Periodo a examinar:	Periodo 2015 con corte a Junio.			
Supervisa:	Estefanía Ortega	**Responsable:**	Patricia Benenaula	
Tema:	Cumplimiento de la Normativa PCI DSS requerimiento 7. Restringir el acceso a los datos del titular de la tarjeta según las necesidades de saber que tenga la empresa.		**Código:**	PT003
Objetivo:	Verificar y asegurar que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.			
Alcance:	Revisar la documentación, entrevistar al personal y verificar que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de tarjeta cumplan:			
Procedimiento:				
*Verificar que se encuentren documentados.				

* Verificar que estén implementados.
* Verificar que sean de conocimiento para todas las partes afectadas.
Revisión del procedimiento:

Revisar la documentación y verificar que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta se encuentren documentados.	
Políticas de Seguridad, administración de accesos de Coral Hipermercado (GO). 5.- POLITICAS DE ADMINISTRACION DE ACCESOS DE USUARIOS 5.1.- REGISTRO DE USUARIOS	√√



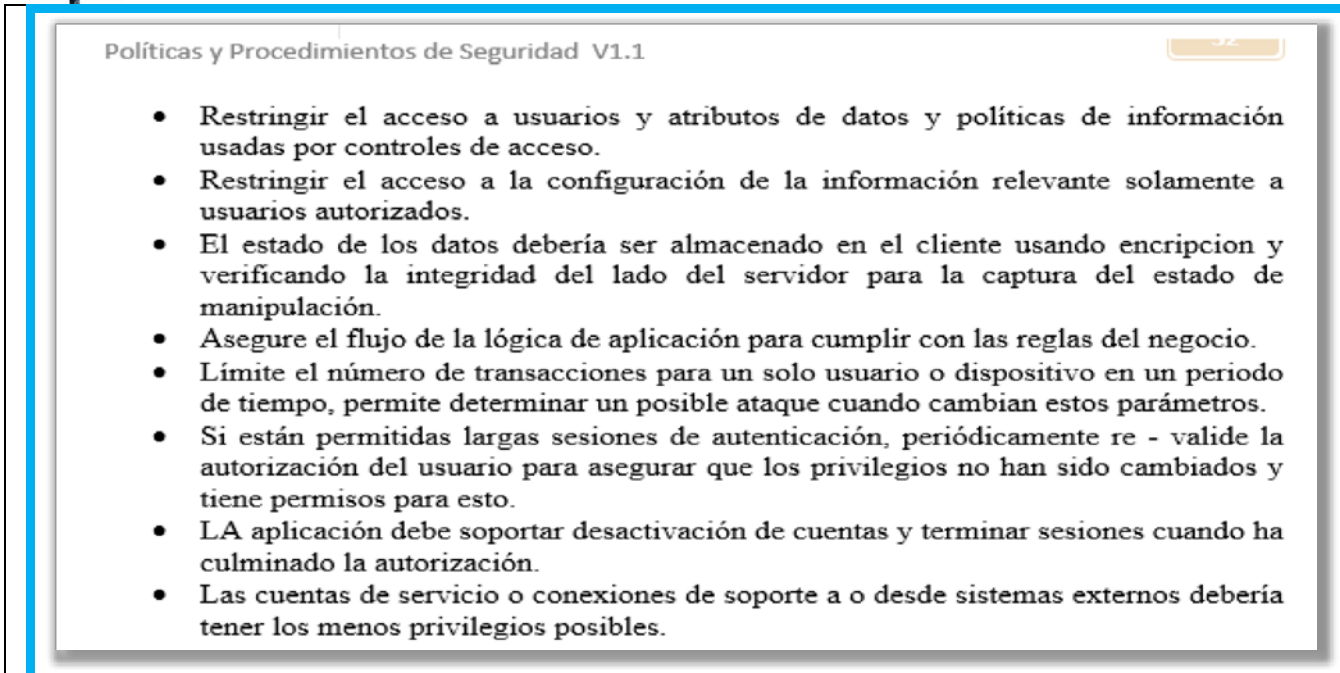
Políticas y Procedimientos de Seguridad V1.1 31

coherente con la política de seguridad de la organización, es decir que no compromete la separación de tareas y conflicto de intereses.

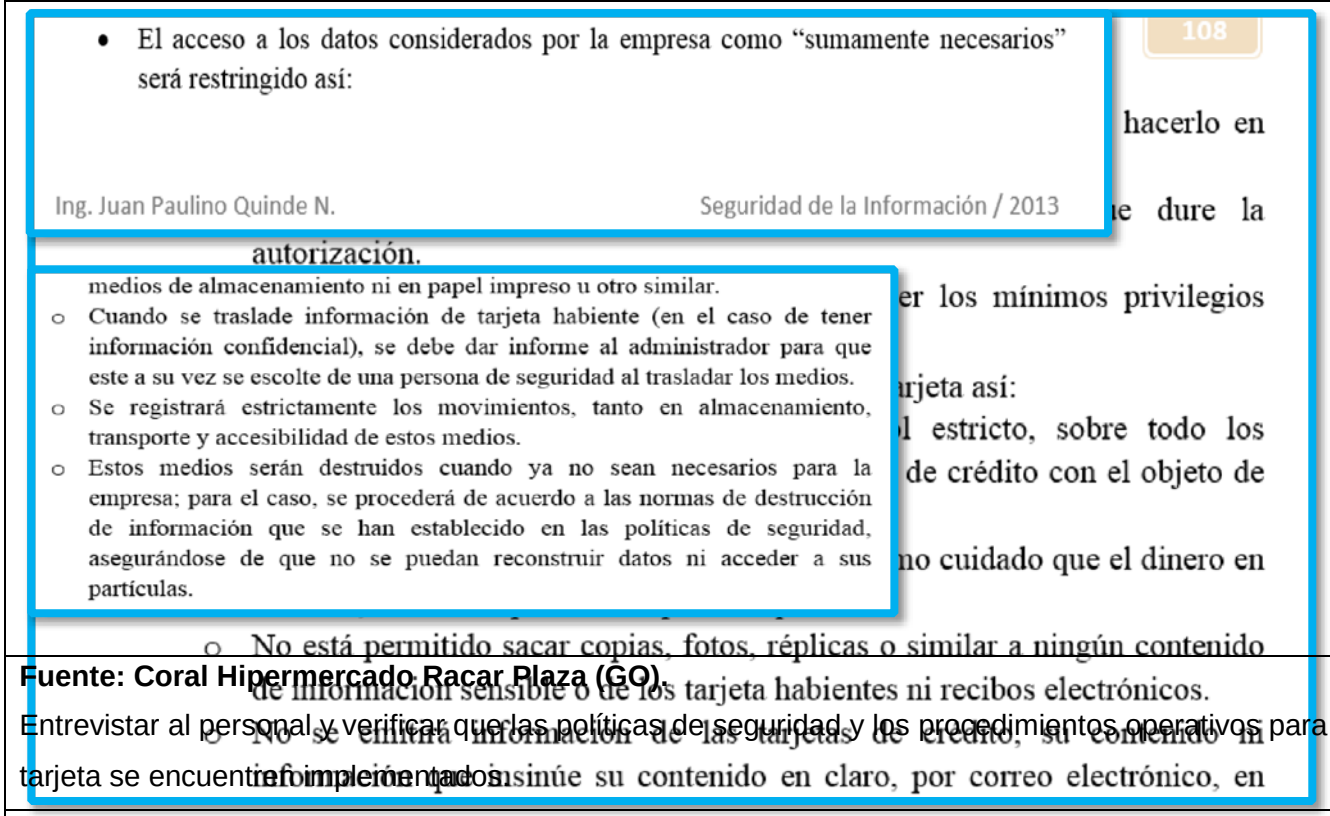
- El Departamento de Recursos Humanos, deberá entregar a los usuarios un detalle escrito de sus obligaciones y derechos de acceso.
- Requerir que los usuarios firmen declaraciones señalando que comprenden las condiciones para el acceso, y aceptan las consecuencias del uso de las mismas.
- Garantizar que los proveedores de servicios internos de informática no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- Mantener actualizado un registro formal de todas las personas registradas para utilizar los servicios y aplicaciones informáticas.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus perfiles (por promoción, reubicación de funciones) o se desvincularon de la organización.

Al revisar la Política de Seguridad de Coral Hipermercado de Grupo GO se verifico que las políticas de seguridad para el acceso a los datos de titulares de tarjetas si se encuentran documentados, registra la política el detalle de la restricción de acceso según las responsabilidades, firma

• El Departamento de Tecnología y Sistemas, deberá verificar que el nivel de acceso otorgado es adecuado para el propósito del perfil y funciones delegadas, es 13.5.- CONTROL DE ACCESO • Los controles de acceso deben ser asegurados. • Denegar el acceso si la solicitud no puede acceder a su información de configuración de seguridad. • Asegure el control de todas las solicitudes, incluyendo scripts generados por el servidor, y solicitudes de los clientes con tecnologías como AJAX y Flash. • Segregar privilegios lógicos desde códigos de otra aplicación. • Restringir acceso a archivos u otro origen, incluyendo las aplicaciones de control directas desde afuera, solo para usuarios autorizados. • Restringir el acceso a URL's protegidas para solo personal autorizado. • Restringir acceso a funciones protegidas solo para usuarios autorizados. • Restringir referencias directas a objetos solamente a usuarios autorizados. • Restringir el acceso a servicios solamente a usuarios autorizados.	de declaraciones señalando las condiciones para el acceso, menciona también la política que no se deberá otorgar acceso hasta que se haya completado el debido procedimiento de autorización para el acceso.



De los procedimientos operativos: La Norma de Seguridad de Coral Hipermercado de Grupo GO también hace referencia el procedimiento acerca del acceso a los datos que deben ser considerados como sumamente necesarios para restringir el acceso a los mismos así como también se menciona la restricción del acceso a los datos del titular de la tarjeta sin embargo solo se hace constar en la norma puesto que como se había indicado este riesgo se encuentra disminuido ya que Coral Hipermercado no almacena datos de titular de tarjetas.	√√



- El acceso a los datos considerados por la empresa como "sumamente necesarios" será restringido así:

Ing. Juan Paulino Quinde N. Seguridad de la Información / 2013

108

hacerlo en

ıe dure la

autorización.

medios de almacenamiento ni en papel impreso u otro similar.

- Cuando se traslade información de tarjeta habiente (en el caso de tener información confidencial), se debe dar informe al administrador para que este a su vez se escolte de una persona de seguridad al trasladar los medios.
- Se registrará estrictamente los movimientos, tanto en almacenamiento, transporte y accesibilidad de estos medios.
- Estos medios serán destruidos cuando ya no sean necesarios para la empresa; para el caso, se procederá de acuerdo a las normas de destrucción de información que se han establecido en las políticas de seguridad, asegurándose de que no se puedan reconstruir datos ni acceder a sus partículas.

er los mínimos privilegios

ırjeta así:

ıl estricto, sobre todo los

de crédito con el objeto de

no cuidado que el dinero en

- No está permitido sacar copias, fotos, réplicas o similar a ningún contenido de información sensible o de los tarjeta habientes ni recibos electrónicos.
- No se elimina información de las tarjetas de crédito, su contenido in

información sinúe su contenido en claro, por correo electrónico, en

Fuente: Coral Hipermercado Racar Plaza (GO).

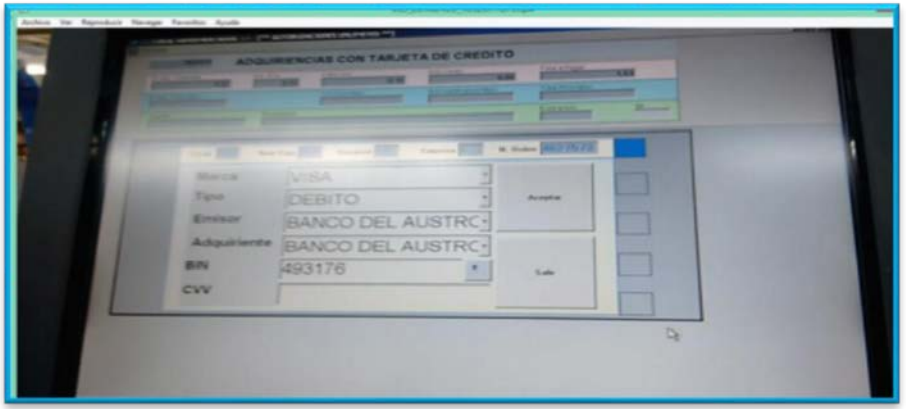
Entrevistar al personal y verificar que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta se encuentren implementados.

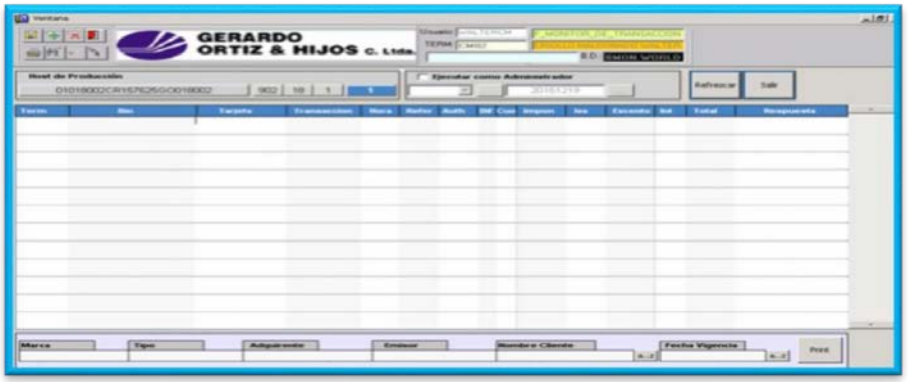
Entrevista al personal administrativo grupo (GO) req.7.2.2

Hemos conversado con el personal administrativo de Coral Hipermercado de Grupo GO sobre la implementación de controles de acceso y procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta y podemos confirmar que como se mencionó con anterioridad primero no se almacenan datos de titulares de tarjetas, como se vio en el Req. 7.2 el acceso a los datos es según las funcion es y labores que

desempeñe cada empleado, en el Sistema de Facturación solo se conservan los datos básicos así como también encriptan los mismos para el registro en la base de datos que se lo vera en lo posterior, adicional a esto los accesos son mediante contraseñas y tockens de seguridad.

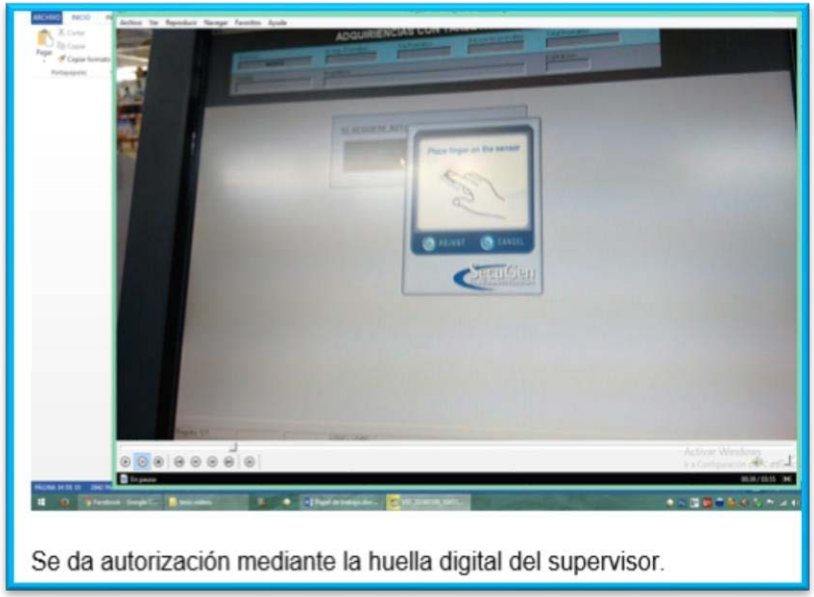
√√



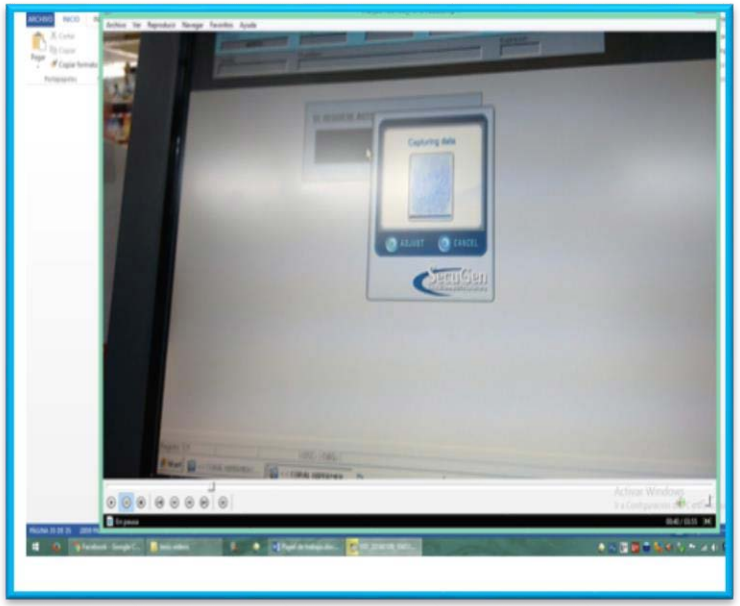


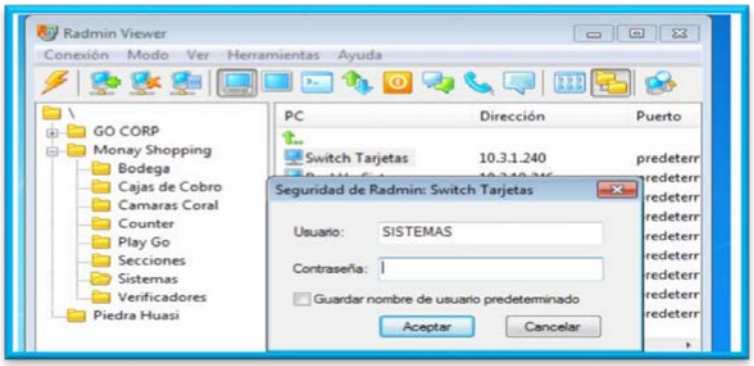
Podemos observar algunos de los controles de acceso que mantienen coral hipermercado Racar plaza de grupo Ortiz para restringir el acceso a los datos del titular de la tarjeta como la huella digital, restricciones en caso de funciones que no pertenezcan al empleado, y también podemos verificar que los datos que se pueden visualizar de los tarjetahabientes en el sistema de facturación solo se registran datos básicos para enviar al banco emisor pero no se almacenan en el sistema.

√√



Se da autorización mediante la huella digital del supervisor.





Fuente: Coral Hipermercado Racar Plaza (GO).

Verificar que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta son de conocimiento para todas las partes afectadas.	
Entrevista al personal administrativo grupo (GO)	
Al conversar con los empleados, facturación, supervisores, y servidor transaccional de Grupo Ortiz de Coral Hipermercado se nos ha dado a conocer que no se tiene conocimiento sobre una política de seguridad, el procedimiento que mantienen es mecánico, el trabajo se les es asignado al ingresar a la entidad pero no se tiene un conocimiento general sobre la documentación y socialización de la normativa. Cabe mencionar que el personal de facturación nos ha indicado que se les realiza una capacitación cada 3 meses por parte del departamento de crédito para el manejo adecuado de pagos con tarjetas de pago pero esto no implica el conocimiento de una normativa ni del proceso de seguridad de accesos a los datos.	**Obs**
Fuente: Coral Hipermercado Racar Plaza (GO).	
Conclusiones y Recomendaciones:	
Al conversar con los empleados, facturación, supervisores, y servidor transaccional de Grupo Ortiz de Coral Hipermercado se nos dio a conocer que no se tiene conocimiento sobre una política de seguridad se encuentra documentada e implementada pero no existe un conocimiento general o una socialización de la normativa. Cabe mencionar que el personal de facturación nos ha indicado que se les realiza una capacitación cada 3 meses por parte del departamento de crédito para el manejo adecuado de pagos con tarjetas de pago pero esto no implica el conocimiento de una normativa ni del proceso de seguridad de accesos a los datos.	
Elaborado por: Auditoras	

ANEXO 4: PAPELES DE TRABAJO DEL REQUERIMIENTO 8. Identifique y autentifique el acceso a los componentes del sistema. (8.1).

Papeles de Trabajo				
Cumplimiento Normativa PCI DSS				
Empresa auditada:	Coral Hipermercados Racar Plaza GO.		**Ref:** req.8.1.	
Periodo a examinar:	Periodo 2015 con corte a Junio.			
Supervisa:	Patricia Benenaula	**Responsable:**	Estefanía Ortega	
Tema:	Cumplimiento de la Norma PCI DSS requerimiento 8. Identifique y autentifique el acceso a los componentes del sistema.		**Código:**	PT001
Objetivo:	Verificar que se haya definido e implementado las políticas y procedimientos para garantizar la correcta administración de la identificación de todos usuarios, en los componentes del sistema.			
Alcance:	8.1: Solicitar, revisar los procedimientos y confirmar que estos definan los procesos para los siguientes puntos:			
Procedimiento:				
Todos los usuarios tengan asignada una ID exclusiva para tener accesos a los componentes del sistema o los datos del titular de la tarjeta. Que todas las ID de usuarios se hayan implementado solamente con los privilegios especificados en la aprobación documentada. Las ID, tarjetas inteligentes, tokens, etc., de los usuarios cesantes se hayan desactivado o eliminado de las listas de acceso. Además que los usuarios inactivos se eliminen o inhabiliten en el caso de que tengan más 90 días inactivos. Monitorear las cuentas de acceso remoto de los encargados del mantenimiento del sistema cuando este utilice.				

Los parámetros de autentificación se encuentren configurados de manera que se bloquee la cuenta de todos usuarios después de realizar, como máximo seis intentos de inicio de sesión no válidos.

También que los parámetros de las contraseñas se encuentren configurados de manera que al bloquear la cuenta de un usuario, esta permanezca bloqueada un minimo de 30 minutos o hasta que el administrador del sistema la restablezca.

Y que se inactive el sistema en el caso que pase sin ser usado un lapso de 15 minutos o menos.

Revisión del procedimiento:

Procedimiento para creación de usuarios bajo el lineamiento establecido.

OBJETIVO Crear usuarios bajo el lineamiento tanto de seguridad como la convergencia con el requerimiento que su puesto demanda.
ALCANCE Usuarios, Seguridad de la información, DBA, jefes de departamento, Jefes de TI.
FRECUENCIA Según la necesidad de nuevos usuarios del sistema.

DESCRIPCION DEL PROCEDIMIENTO

Numero	Actividad	Responsable
1	El Jefe de departamento solicita la creación de un nuevo usuario en el sistema (RRHH lo hace muchas de las veces)	Jefe del Departamento del área a la que pertenece el usuario
2	El departamento de seguridad de la información verifica la necesidad del usuario, el perfil necesario y la manera formal de solicitarlo.	Seguridad de la información
3	El área de seguridad realiza la petición de creación de usuarios al DBA, fundamentándose en los principios de seguridad de la empresa.	Seguridad de la información
4	El DBA crea un usuario de aplicaciones el mismo que es ligado al usuario de Base de datos.	DBA
5	El DBA emite comunicado de creación del usuario	Seguridad de la información
6	Seguridad de la información verifica y registra el usuario creado con los perfiles y roles asignado.	Seguridad de la información
7	Seguridad de la información comunica al usuario respecto al ID creado y concientiza respecto al uso que éste involucra.	Seguridad de la Información
8	El usuario ingresa por primera vez al sistema y realiza el cambio de clave.	Usuario

Que estén Implementados con los privilegios específicos de la aprobación documentada

Todos los usuarios tienen asigno un ID exclusiva para tener acceso a los datos.

Fuente: Coral Hipermercado Racar Plaza (GO)

Se comprobó que existe un procedimiento para crear usuarios con ID únicas y con los privilegios necesarios para poder realizar el trabajo establecido.

Además en los procedimientos para creación de usuarios, se puede observar que hay un procedimiento para inhabilitar o eliminar los usuarios inactivos.

√

Procedimiento para los usuarios que se da de baja.

OBJETIVO Dar de baja a usuarios dentro del entorno de seguridad así como la necesidad de registro del área de Recursos humanos.
ALCANCE Usuarios, Seguridad de la información, DBA, jefes de departamento, Jefes de TI.
FRECUENCIA Según la necesidad de bajar usuarios del sistema.

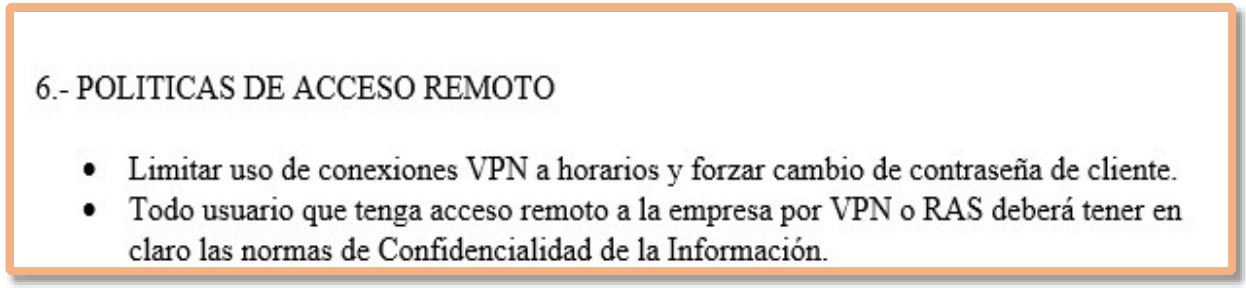
DESCRIPCION DEL PROCEDIMIENTO

Numero	Actividad	Responsable
1	El Jefe de departamento solicita la baja de un usuario en el sistema (RRHH lo hace muchas de las veces)	Jefe del Departamento del área a la que pertenece el usuario
2	El departamento de seguridad de la información verifica la necesidad de la baja y la manera formal de solicitarlo.	Seguridad de la información
3	El área de seguridad realiza la petición de Baja de usuarios al DBA, fundamentándose en los principios de seguridad de la empresa.	Seguridad de la información
4	El DBA da de baja el usuario de aplicaciones el mismo que es ligado al usuario de Base de datos.	DBA
5	El DBA emite comunicado de baja del usuario	Seguridad de la información
6	Seguridad de la información verifica y registra el usuario bajado con los perfiles y roles asignado.	Seguridad de la información
7	Seguridad de la información comunica al usuario respecto al ID bajado.	Seguridad de la Información

La política de seguridad comunica que los usuarios desvinculados de la empresa Coral Hipermercado, se debe de dar de baja inmediatamente de su salida.

Fuente: Coral Hipermercado Racar Plaza (GO)

Políticas de Acceso Remoto.



6.- POLITICAS DE ACCESO REMOTO

- Limitar uso de conexiones VPN a horarios y forzar cambio de contraseña de cliente.
- Todo usuario que tenga acceso remoto a la empresa por VPN o RAS deberá tener en claro las normas de Confidencialidad de la Información.

Existe una política para el acceso remoto pero ningún procedimiento indica cómo debería ser este tipo de acceso.

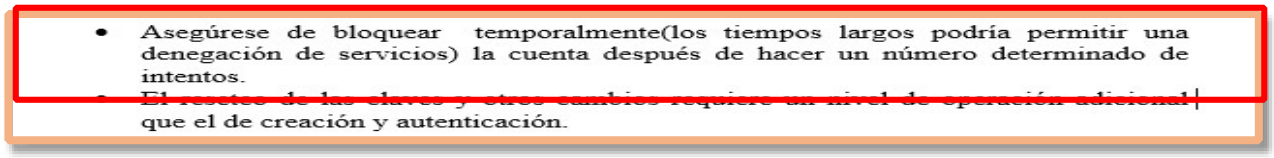
Obs.

Fuente: Coral Hipermercado Racar Plaza (GO)

Las políticas de autentificación de claves nos indican que debe bloquearse el usuario cuando exista un mínimo determinado de intentos para acceder al sistema, pero no hay algún parámetro que indique, cuales es número determinado de intentos y por cuanto tiempo debe permanecer bloqueada.

Obs.

Política de autenticación de claves.



- Asegúrese de bloquear temporalmente(los tiempos largos podría permitir una denegación de servicios) la cuenta después de hacer un número determinado de intentos.
- El reseteo de las claves y otros cambios requiere un nivel de operación adicional que el de creación y autenticación.

Fuente: Coral Hipermercado Racar Plaza (GO)

No existe ninguna política o procedimiento acerca de que se debe inactivar el sistema en el caso de que pase sin ser usado un lapso de 15 minutos o menos. **Obs.**

Par verificar que los procedimientos y las políticas se cumplan se realizará las siguientes actividades: 8.1.1: Entrevistar al personal administrativo para confirmar que todos los usuarios tengan asignada una ID exclusiva para tener accesos a los componentes del sistema o los datos del titular de la tarjeta.

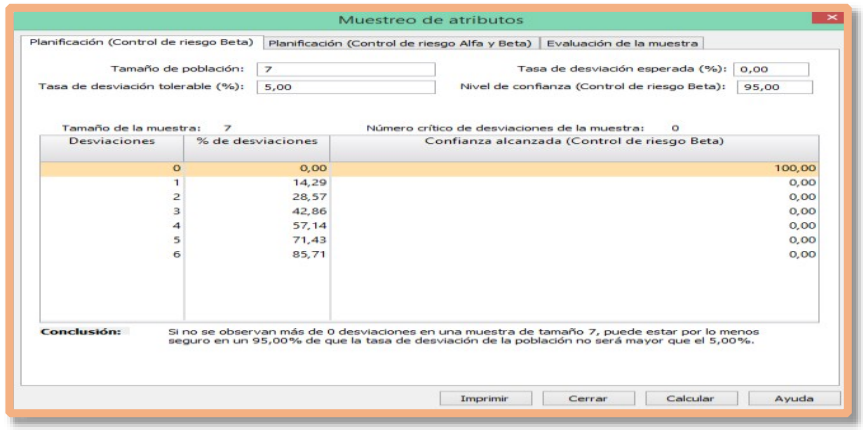
Según la entrevista realizadas al Ingeniero Walter Cedillo, nos dio como resultado que todos los usuarios que tienen accesos a los componentes del sistema o datos del titular de la tarjeta usan su ID exclusiva, excepto los encargados del servidor transaccional que a pesar de que tienen un ID único comparten entre los 7 designados la misma contraseña. **Obs.**

8.1.2: Tomar una muestra de ID de usuarios y evalúe las autorizaciones asociadas y observe los parámetros del sistema a fin de verificar que todas las ID de usuarios se han implementado solamente con los privilegios especificados en la aprobación documentada.

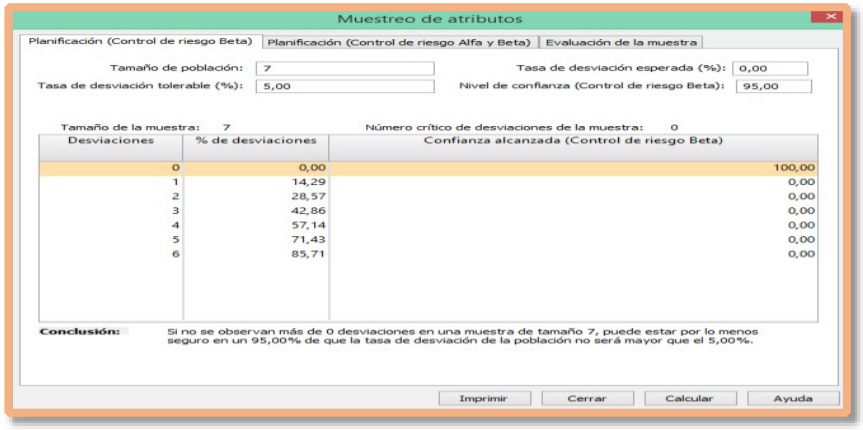
La muestra calculada en el programa IDEA tomada de una población de 72 ID de usuarios que trabajan en Coral Hipermercado Racar Plaza, cumpliendo las funciones de supervisores, cajeros y encargados del servidor transaccional, dan como resultado 50 ID de usuarios por analizar.

Captura de pantalla del cálculo de la muestra de los encargados del servidor transaccional.

Captura de pantalla del cálculo de la muestra de los supervisores.

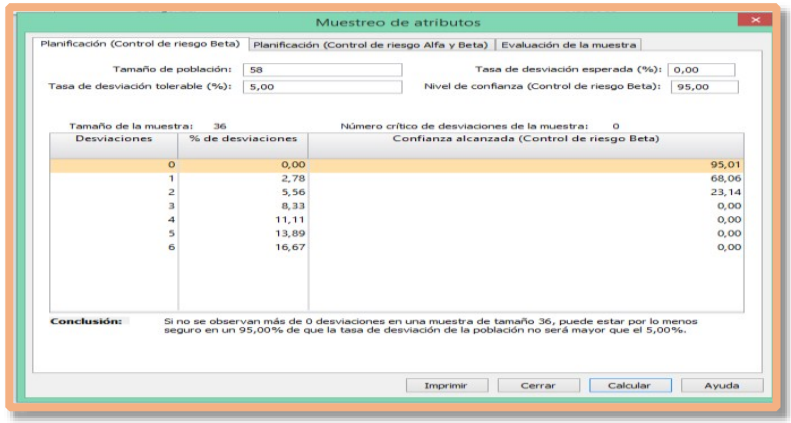


Fuente: Programa Idea



Fuente: Programa Idea

Captura de pantalla del cálculo de la muestra de los cajeros.

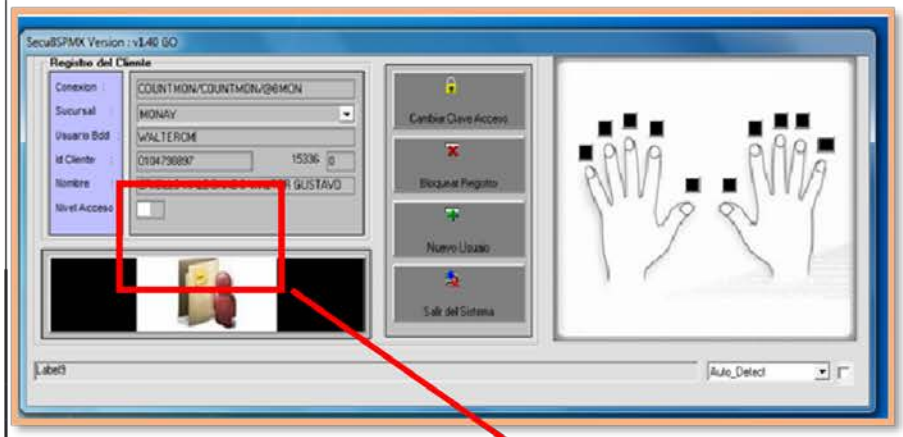


Fuente: Programa Idea Auditoria.

El resultado de la muestra selecciona del programa IDEA fue: 36 ID de Cajeros, 7 ID de supervisores y 7 ID de encargados del servidor transaccional.

De la muestra seccionada se pudo constatar que todos los usuarios tienen las mismas características, por lo que seleccionamos como ejemplo a una ID de caja usuario (supervisores, cajeros y servidores transaccionales) para poder realizar el respectivo análisis.

Parámetros de configuración de las ID (cajeros y supervisores).



Lugar donde se coloca el parámetro de configuración para las ID. Puede ser nivel 2 para cajero y nivel 4 para

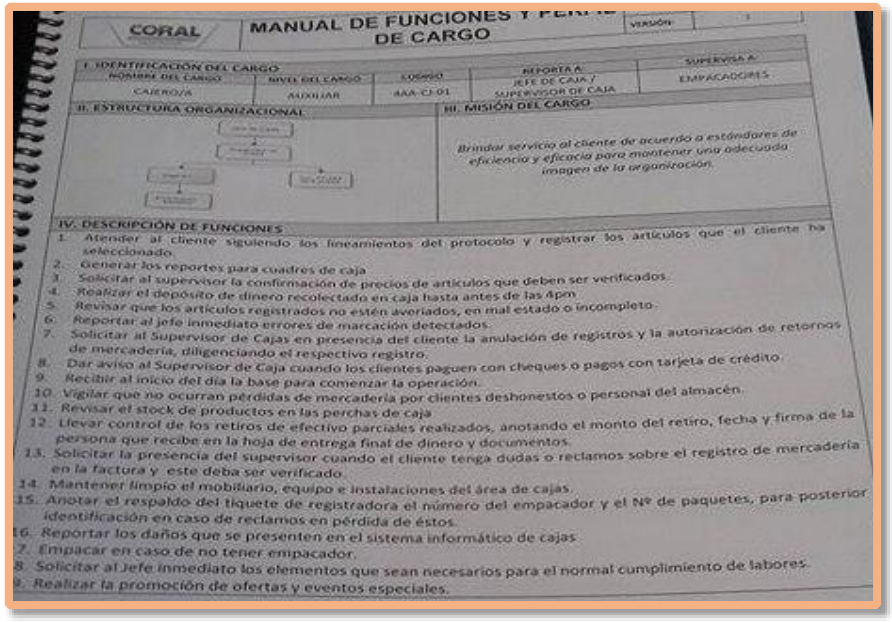
En el caso de las ID de usuarios de cajeros y supervisores podemos observar que sus ID son exclusivas para cada usuario, número de cédula y huella digital, y tiene acceso privilegiado según el parámetro de configuración que se les otorgue al inicio de la creación del usuario.

En el caso de los cajeros el parámetro de configuración es acceso nivel 2.

Para los supervisores el parámetro es el número 4, el cual le otorga acceso a las funciones que presenta el manual de funcionamiento de Coral Hipermercado, pero a pesar de que los supervisores tengan acceso a la anulación de voucher, esta función no se encuentra documentada en el manual. √

Manual de funcionamiento de supervisores. **de los cajeros.**

Captura de pantalla de las funciones



CORAL | MANUAL DE FUNCIONES Y PERFIL DE CARGO

I. IDENTIFICACIÓN DEL CARGO

NOMBRE DEL CARGO	NIVEL DEL CARGO	CÓDIGO	REPORTA A	SUPERVISA A
CAJERO/A	AUXILIAR	4AA-CJ-01	JEFE DE CAJA / SUPERVISOR DE CAJA	EMPACADORES

II. ESTRUCTURA ORGANIZACIONAL

III. MISIÓN DEL CARGO

Brindar servicio al cliente de acuerdo a estándares de eficiencia y eficacia para mantener una adecuada imagen de la organización.

IV. DESCRIPCIÓN DE FUNCIONES

1. Atender al cliente siguiendo los lineamientos del protocolo y registrar los artículos que el cliente ha seleccionado.
2. Generar los reportes para cuadres de caja.
3. Solicitar al supervisor la confirmación de precios de artículos que deben ser verificados.
4. Realizar el depósito de dinero recolectado en caja hasta antes de las 4pm.
5. Revisar que los artículos registrados no estén averiados, en mal estado o incompleto.
6. Reportar al jefe inmediato errores de marcación detectados.
7. Solicitar al Supervisor de Cajas en presencia del cliente la anulación de registros y la autorización de retornos de mercadería, diligenciando el respectivo registro.
8. Dar aviso al Supervisor de Caja cuando los clientes paguen con cheques o pagos con tarjeta de crédito.
9. Recibir al inicio del día la base para comenzar la operación.
10. Vigilar que no ocurran pérdidas de mercadería por clientes deshonestos o personal del almacén.
11. Revisar el stock de productos en las perchas de caja.
12. Llevar control de los retiros de efectivo parciales realizados, anotando el monto del retiro, fecha y firma de la persona que recibe en la hoja de entrega final de dinero y documentos.
13. Solicitar la presencia del supervisor cuando el cliente tenga dudas o reclamos sobre el registro de mercadería en la factura y este deba ser verificado.
14. Mantener limpio el mobiliario, equipo e instalaciones del área de cajas.
15. Anotar el respaldo del tiquete de registradora el número del empacador y el Nº de paquetes, para posterior identificación en caso de reclamos en pérdida de éstos.
16. Reportar los daños que se presenten en el sistema informático de cajas.
17. Empacar en caso de no tener empacador.
18. Solicitar al Jefe inmediato los elementos que sean necesarios para el normal cumplimiento de labores.
19. Realizar la promoción de ofertas y eventos especiales.

Fuente: Coral Hipermercado Racar Plaza (GO)

Fuente: Coral Hipermercado Racar Plaza (GO)

En el caso de los encargados del servidor transaccional según las entrevistas realizadas a las siete personas que trabajan en esta área, llegamos a la conclusión de que las contraseñas y las ID son grupales, debido a que para acceder ellos colocan el mismo usuario y contraseña con la finalidad de que

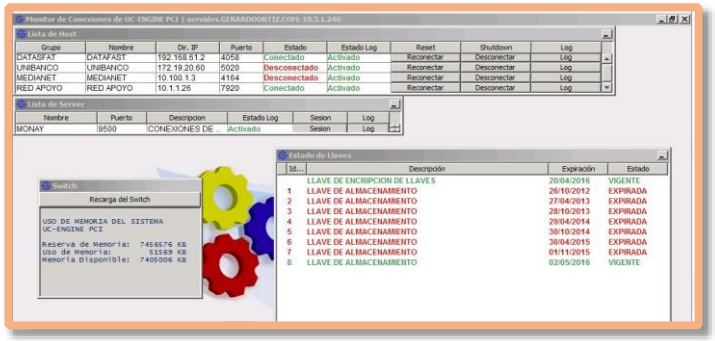
cuando exista mantenimiento pueda hacerlo cualquiera de los siete, pero los privilegios otorgados son los necesarios para realizar el trabajo, no se nos entregó aprobación documentada alguna acerca de las funciones y privilegios, pero según entrevistas realizadas, los encargados del servidor transaccional realizan las siguiente funciones:

1. Velar por la caducidad de las licencias.

2. Controlar las alertas que pueden emanar.
3. Procurar su funcionamiento.
4. Verificar la conexión permanente con los entes bancarios.

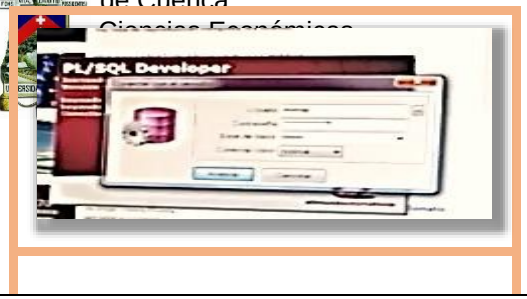
Según observaciones realizadas, también tienen acceso a la base de datos de facturación, la ID y contraseña de la base de datos es la misma para los siete encargados. **obs.**

Switch transaccional.



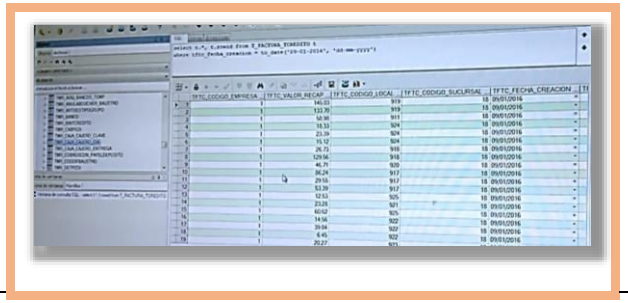
Fuente: Coral Hipermercado Racar Plaza (GO)

Acceso la base de datos.



Fuente: Coral Hipermercado Racar Plaza (GO)

Base de datos de la facturación.



Fuente: Coral Hipermercado Racar Plaza (GO)

8.1.3: Seleccionar una muestra de los usuarios cesantes en los últimos seis meses y revisar las listas de accesos de usuarios actuales tanto para accesos local y remoto, de esa manera se verificará que las ID de dichos usuarios se hayan desactivado o eliminado de las listas de acceso, además se debe verificar que todos los métodos de autentificación físicos (tarjetas inteligentes, tokens) se hayan devuelto o desactivado.

La política de administración de acceso de Coral Hipermercado, nos indica que se debe inhabilitar a los usuarios cesantes, por lo que se tomó una muestra de todos los usuarios que tienen acceso al sistema en los últimos seis meses.

De la lista de usuarios otorgada por Coral Hipermercado Racar Plaza existe once empleados cesantes los cual se encuentran inactivos en el sistema, debido a que los usuarios cesantes se representa con el número nueve dentro del sistema. En el momento que sale de la empresa recursos humanos comunica al departamento de sistemas para que se realice rápidamente la desactivación del usuario. En el caso de los encargados del servidor transaccional se les entrega un carnet que les permite acceder a los datos físicos de la tarjeta de pagos, así como también para acceder a las otras sucursales para el mantenimiento del sistema, estas tarjetas son devueltas a recursos humanos el momento que sale de la empresa.

√

Ilustración……

Lista de usuarios activos e inactivos.

Inactivo

Uni de Cuenca
Fac Ciencias Económicas.
Car Contabilidad y Auditoría.

Inactivo

HUEID	HUENOMBRE	HUEESTADO
102584240	BARRETO CANTOS FELIPE ROLANDO	1
107183683	BARROS BARROS JENNY PAOLA	1
105912885	BRAVO CAYANCELA MARIA JOSE	9
105737142	BUENO ASITIMBAY LISSETH CAROLINA	1
106424302	BUNAY PINDE JENNY ELIZABETH	9
1720347325	CEDILLO VALVERDE SONIA MERCEDES	1
104798897	CRIOLLO MALDONADO WALTER GUSTAVO	1
106516172	CURILLO BUESTAN MARIA PAOLA	1
1803378353	ESCUDERO BONILLA FREDDY NAPOLEON	9
105415376	ESPINOSA GUAZHIMA MARIA FERNANDA	1
105771091	FAICAN MUNOZ DAYSI ANDREA	1
104858766	FAREZ NARVAEZ MERCEDES ALEXANDRA	1
106029911	GALARZA BALAREZO ANA LUCIA	1
924923832	GUAMAN BAZAN DORA DEL ROCIO	1
104540752	GUAMAN DURAN MONICA BEATRIZ	1
1[illegible]	GUERRERO ORELLANA CARLOS JHAN	9
1[illegible]	GUERRERO ORELLANA DANIS JHOSELYN	9
1[illegible]	MORALES SANTACRUZ LUIS ANGEL	1
1[illegible]	MOSQUERA MEDINA MARY JOHANNA	1
1[illegible]	ORELLANA BARZALLO GABRIELA	1
106225741	PARA LOPEZ ALEXANDRA MARIBEL	9
107626004	PEREZ ALEXANDRA	1
705323087	QUELA TARQUI MARIA LUCINDA	1
105261333	ORTIZ MOLINA NELLY MARILU	1
106821044	LLIGUIN GUARTAZACA GLORIA ALEXANDR	1
106940968	PACHECO PACHECO GLADIS PATRICIA	9
105221332	LOZADO MENDIETA MARIA ELIZABETH	9
604676619	PALAGUACHI PAGUAY TRANSITO SENAIDA	1
102424447	PAREDES VALDIVIESO GUILLERMO RAFAE	1
106035181	QUILLE DOMINGUEZ GABRIEL LEONARD	1
706724671	QUIMI ZHININ LISSETH MICHELLE	9
106454648	RIVAS RAMON CARMEN ROCIO	1

Inactivo Inactivo

302581137	ROBLES BERMEO LAURA MAGALY	9
104914742	SANCHEZ PLACENCIA LUIS ALBERTO	1
106981632	SIBRI ZUÑIGA DIANA VICTORIA	1
105831903	TAPIA BRITO ANGEL OSWALDO	1
105247555	TAPIA EDISSON	1
705333821	TOLEDO ZHICAY DIANA CAROLINA	1
706461464	TORRES CRIOLLO ANDREA JULIANA	9

Inactivo

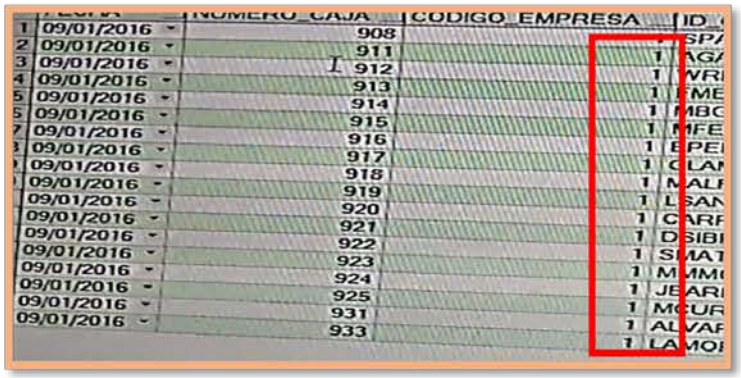
Inactivo

Inactivo

Inactivo
Inactivo

Cuando están activos podemos encontrarlos como en la base de datos con el número 1, así:

Base de datos empleados activos



	FECHA	NUMERO_CAJA	CODIGO_EMPRESA	ID
1	09/01/2016	908		SP/
2	09/01/2016	911	1	AG/
3	09/01/2016	912	1	VR
4	09/01/2016	913	1	ME
5	09/01/2016	914	1	MBC
5	09/01/2016	915	1	MFE
7	09/01/2016	916	1	EPE
8	09/01/2016	917	1	CLA
9	09/01/2016	918	1	MALI
	09/01/2016	919	1	LSAN
	09/01/2016	920	1	CARF
	09/01/2016	921	1	DSIBI
	09/01/2016	922	1	SMAT
	09/01/2016	923	1	MMM
	09/01/2016	924	1	JEAR
	09/01/2016	925	1	MCUR
	09/01/2016	931	1	ALVAF
	09/01/2016	933	1	LAMO

Fuente: Coral Hipermercado Racar Plaza (GO)

8.1.4: Observar las cuentas de usuarios inactivos y verifique que se eliminen o inhabiliten las que lleven más de 90 días inactivas.

Pudimos observar que en Coral Hipermercado Racar Plaza se cancelan inmediatamente los derechos de los usuarios (se inactivan) cuando se desvinculan de la organización, por lo tanto si cumple con este punto de la normativa.

8.1.5: Entrevistar al personal administrativo y observar los procesos de administración de cuentas de acceso remoto para verificar si se monitoreen las cuentas de acceso remoto que se utilizan.

En la entrevista realiza al Ingeniero Walter Criollo y con las observaciones hechas en Coral Hipermercado Racar Plaza, se llegó a la conclusión de que no existe monitoreo al momento de realizar acceso remoto, este acceso solo lo puede realizar los encargados del servidor transaccional para poder desarrollar su trabajo en todas las sucursales, además pueden realizar a la hora que ellos crean necesario. **obs.**

8.1.6: Seleccionar una muestra de los componentes del sistema para inspeccionar los parámetros de configuración del sistema para verificar que los parámetros de autentificación se encuentren configurados de manera que se solicite el bloqueo de la cuenta de usuarios después de realizar como máximo seis intentos de inicio de sesión no válidos. A pesar que la política de seguridad de Coral Hipermercado, habla acerca de bloquear temporalmente la cuenta después de hacer un número determinado de intentos, Según entrevistas realizadas al personal de Coral Hipermercado Racar Plaza y pruebas hechas al sistema, no se bloquea cuando se hace más de seis intentos, por lo que la corporación no cumple con este parámetro de la norma. **obs.**
8.1.7: Seleccionar una muestra para verificar que los parámetros de las contraseñas se encuentren configurados de tal manera que permanezca bloqueada la cuenta de usuario, mínimo 30 minutos o hasta que el administrador del sistema la restablezca.
Ya que el punto anterior no se cumplió, este tampoco tiene acogida dentro de la empresa, por lo tanto es otro parámetro de la norma que no cumple la empresa Coral Hipermercado. **obs.**
8.1.8: Seleccionar una muestra de los componentes del sistema para inspeccionar los parámetros de configuración del sistema para verificar que las funciones de tiempo máximo de inactividad del sistema se encuentren establecidos en 15 minutos o menos. Con las pruebas realizadas en la muestra selecciona de cajeros, supervisores así como los servidores transaccionales y las entrevista hechas, pudimos observar que el sistema no se inactiva cuando se encuentra sin utilizar un lapso máximo de 15 minutos, este no se cierra mientras no se lo haga manualmente, la empresa no cumple con el requerimiento establecido en la norma PCI DSS. **obs.**
conclusiones y recomendaciones:
Coral Hipermercado tiene un bajo nivel de cumplimiento de este requerimiento de la norma PCI DSS, porque las políticas y procedimientos de
autenticación no se encuentran del todo completas, en el caso del acceso remoto la empresa no especifica en ninguna norma o procedimiento como debe ser un el acceso remoto. Además la empresa no menciona que debe ocurrir en el caso de que el sistema esté inactivo en un lapso de 15 minutos, también otra de las debilidades es que los encargados del servidor transaccional usan una misma contraseña para los siete designados, al tener una contraseña compartida puede existir inconvenientes en el hecho de que no se mantiene una responsabilidad individual, si es que suceda algún inconveniente no se sabría de quien es la responsabilidad. La empresa al no monitorear el acceso remoto se puede tener dificultades ya que se accedería en el momento que se desee y sin vigilancia de que se pueda hacer algún acto que exponga los datos del titular de la tarjeta o de la tarjeta. La empresa no tiene bloqueo de

cuenta en el caso de que se haga varios intentos de inicio de sesión no válidos, al no tener implementado este requerimiento corre el riesgo de que algún individuo con intensiones maliciosas intente adivinar la clave. Como se mencionó anteriormente Coral Hipermercado no tiene parámetros que le permita inactivar el sistema en el caso de que pase un lapso de 15 minutos sin utilizar, esto puede causar que algún individuo se lleve datos del titular de la tarjeta en el momento de que el usuario se aleje del computador. Se recomienda a la empresa Coral Hipermercado, que se realice un ajuste en la política de autenticación así como también un ajuste en la configuración del sistema en la parte de las contraseñas y de esa manera corregir las falencias mencionadas para un mejor funcionamiento de la seguridad de los datos del titular de la tarjeta y de la tarjeta mismo.
Elaborado por: Autoras.

ANEXO 5: PAPELES DE TRABAJO DEL REQUERIMIENTO 8. Identifique y autentifique el acceso a los componentes del sistema. (8.2).

Papeles de Trabajo		
Cumplimiento Normativa PCI DSS		
Empresa auditada:	Coral Hipermercados Racar Plaza GO.	**Ref:** req.8.2
Periodo a examinar:	Periodo 2015 con corte a Junio.	

Supervisa:	Patricia Benenaula.	**Responsable:**	Estefanía Ortega.		
Tema:	Cumplimiento de la Norma PCI DSS requerimiento 8. Identifique y autentifique el acceso a los componentes del sistema.			**Código:**	PT002
Objetivo:	Verificar que exista una correcta administración de autenticación de todos los usuarios en los componentes del sistema y que se usa al menos algo que el usuario sepa (contraseña, o frase de seguridad), algo que el usuario tenga (dispositivo token, tarjeta inteligente) y algo que el usuario sea (rasgo biométrico).				
Alcance:	8.2: Solicitar documentos que describa métodos de autentificación para revisarlos, comprar con los componentes del sistema y verificar que estos funcionen de manera coherente.				
Procedimiento:					
Solicitar documentos que describa métodos de autentificación para revisarlos, comprar con los componentes del sistema y verificar que estos funcionen de manera coherente.					
Revisión del procedimiento:					
Políticas de administración de autentificación y claves (GO).					

13.3.- ADMINISTRAR AUTENTICACION Y CLAVES

- Requerir autenticación de todas las páginas y recursos, excepto los destinados específicamente a ser público.
- Todos los controles de autenticación debe ser aplicada en un ambiente que cree confianza
- Establezca y utilice estándares , pruebas de autenticación de servicios siempre que sea posible
- ¿Use una implementación centralizada para todos los controles de autenticación, incluyendo librerías para llamadas externas de autenticación de servicios
- Separar la lógica de autenticación del recurso que se solicita y usar la redirección desde y hacia el control de autenticación centralizada.
- Todo control de autenticación no debería violar la seguridad.
- Todas las funciones de gestión administrativa y de cuenta debe tener por lo menos un mecanismo de autenticación primaria.

Ing. Juan Paulino Quinde N. Seguridad de la Información / 2013

GERARDO ORTIZ & HIJOS C. Ltda.

Políticas y Procedimientos de Seguridad V1.1 50

- Si dispone de un almacén de datos asegúrese de usar criptografía. La tabla que almacena las contraseñas es capaz de escribir solo por aplicación, no use DM5 si es que es posible evitar.

- Se debe implementar hashing de contraseñas.
- Validar la autenticación de datos solamente al término de todos los datos de entrada específicamente para implementación de autenticación secuencial.
- Las respuestas de autenticación fallida no debería indicar que parte de los datos de autenticación fueron las incorrectas. Debe salir "usuario Y/O clave incorrectos".
- Use autenticación para conexiones hacia sistemas externos que involucre información o funciones sensibles.
- Credenciales de autenticación para acceso de servicios externos a las aplicaciones deben ser encriptados y guardar en un lugar protegido y validado (servidor), el código fuente no es un lugar seguro.
- Use solamente solicitudes HTTP POST para transmitir credenciales de autenticación.
- Envíe solamente contraseñas no temporales a través de una conexión encriptado o datos cifrados.
- Asegure el requerimiento de una clave compleja, establezca la política de regulación (números, letras, símbolos, etc).
- Regule la longitud de la clave (16 es mejor que 8).
- La clave no debería mostrarse en la pantalla, peor aún poder copiarse.
- Asegúrese de bloquear temporalmente(los tiempos largos podría permitir una denegación de servicios) la cuenta después de hacer un número determinado de intentos.
- El reseteo de las claves y otros cambios requiere un nivel de operación adicional que el de creación y autenticación.
- El reseteo de claves debe soportar preguntas randómicas (libro favorito, cuantas tarjetas, etc.) y entre ellas una pregunta de la que solo el cliente sabe que no es verdad no estaría mal.
- No envíe correos a una dirección registrada con el vínculo temporal y contraseña
- Las claves y links temporales deberían tener tiempos de expiración cortas.
- Refuerce el cambio de claves temporales para el próximo uso.
- Desactivar la funcionalidad "Recordarme" en los campos de claves.
- El último uso (logrado o no) debe ser reportados a este la próxima vez que ingrese a su cuenta.
- Volver autenticar los usuarios antes de hacer operaciones críticas.
- Use multi factores de autenticación para reforzar transacciones sensibles o de alto valor.

Fuente: Coral Hipermercado Racar Plaza (GO).

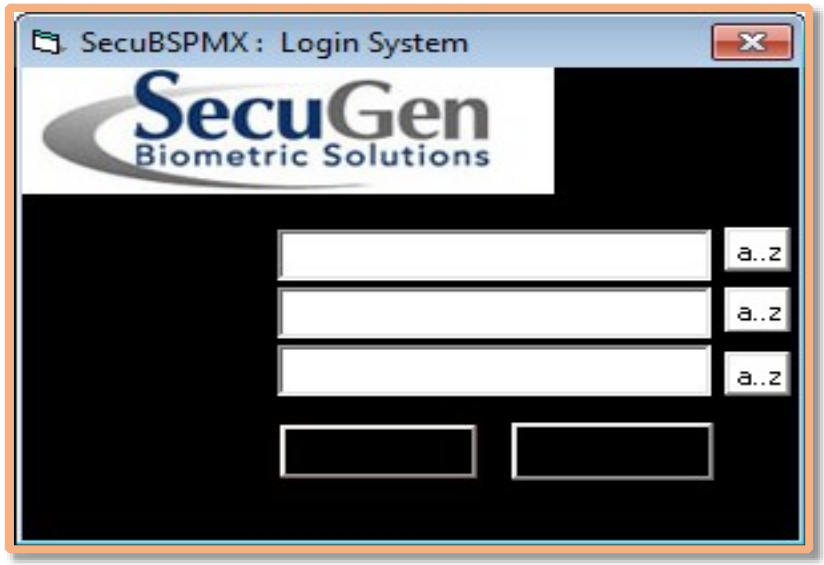
La empresa Coral Hipermercado, dentro de sus políticas de autenticación no describe la forma de autenticación de los cajeros y supervisores, por lo que no constan dentro de las políticas todas las formas de autenticación. **Obs.**
8.2.1: Solicitar y evaluar parámetros de configuración para verificar que las contraseñas se protejan durante la transmisión y el almacenamiento mediante una criptografía sólida.
Los parámetros de configuración de las contraseñas para los usuarios (cajeros, supervisores y personas encargadas del servidor transaccional) de Coral Hipermercado según las entrevistas realizadas al Ingeniero Paulino Quinde encargado del área de sistemas de Racar Plaza, nos indica que: 1. Las contraseñas no se debe almacenar ya que Oracle tiene su propio manejo de contraseñas. 2. Se debe usar una implementación centralizada para todos los controles de autentificación. 3. Todas las funciones de gestión administrativa y de cuenta debe tener un mecanismo de autentificación primario. 4. Si se dispone de algún almacén de datos se debe usar criptografía 5. Use solamente solicitudes HTTP POST para transmitir credenciales de autentificación. 6. Envían solo contraseñas no temporales a través de una conexión encriptados o datos cifrados. 7. La clave no debe ser visualizada en la pantalla. 8. La clave no puede ser copiada. 9. El reseteo de las claves y otros cambios requiere un nivel de operación adicional que el de creación y autentificación.
10. Desactivar la funcionalidad "recordarme " en los campos e claves. **Fuente: Coral Hipermercado Racar Plaza (GO).**

En las pruebas realizadas a Coral Hipermercado Racar Plaza se verificó como se realiza la creación, transmisión y almacenamiento de las contraseñas de cajeros, supervisores y servidores transaccionales.

El programa de Login Sytem para la creación de contraseñas de cajeros y supervisores solo puede ingresar el encargo de sistemas de cada Coral.

En el caso de los cajeros y supervisores el usuario y contraseña que utilizan es el número de cédula y la huella digital de esta manera Coral Hipermercado busca una forma más segura de resguardar los datos, pero se procederá analizar también la manera de como almacenan las datos de las huellas digitales.

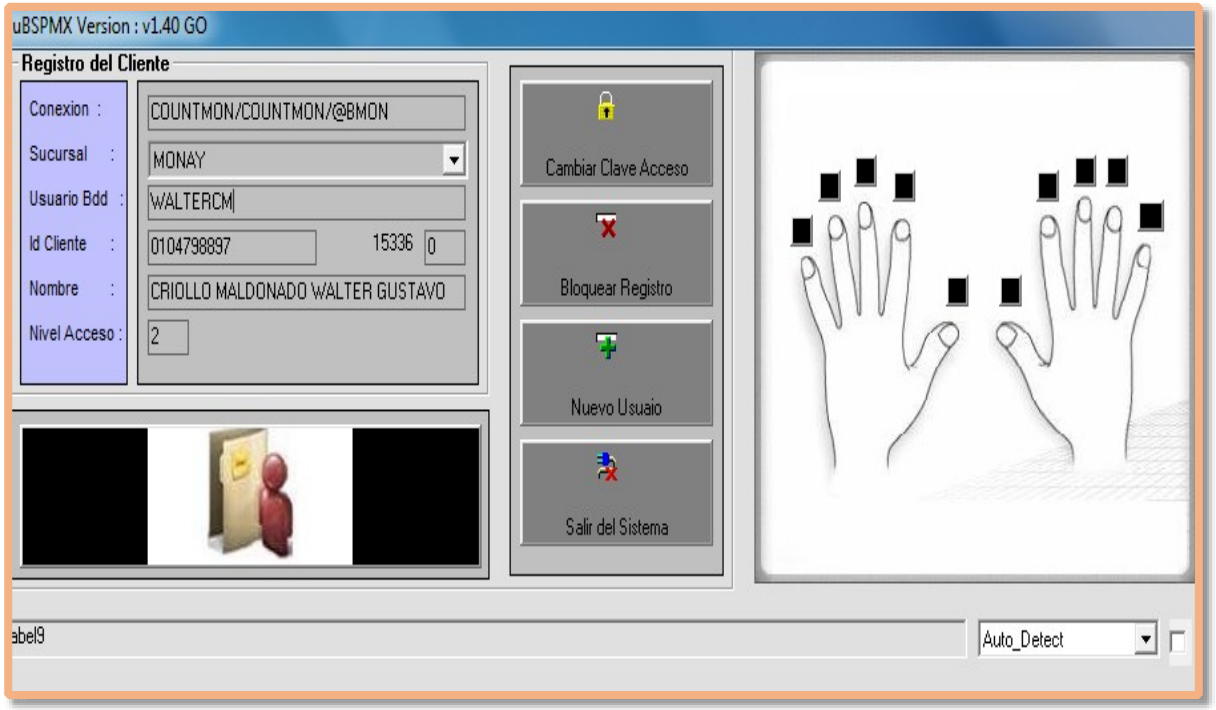
Ingreso para crear contraseñas de cajeros y supervisores.



Fuente: Coral Hipermercado Racar Plaza (GO). √

Se registra la huella digital del usuario después de haber recibido los datos de recursos humanos acerca de la función que va desempeñar

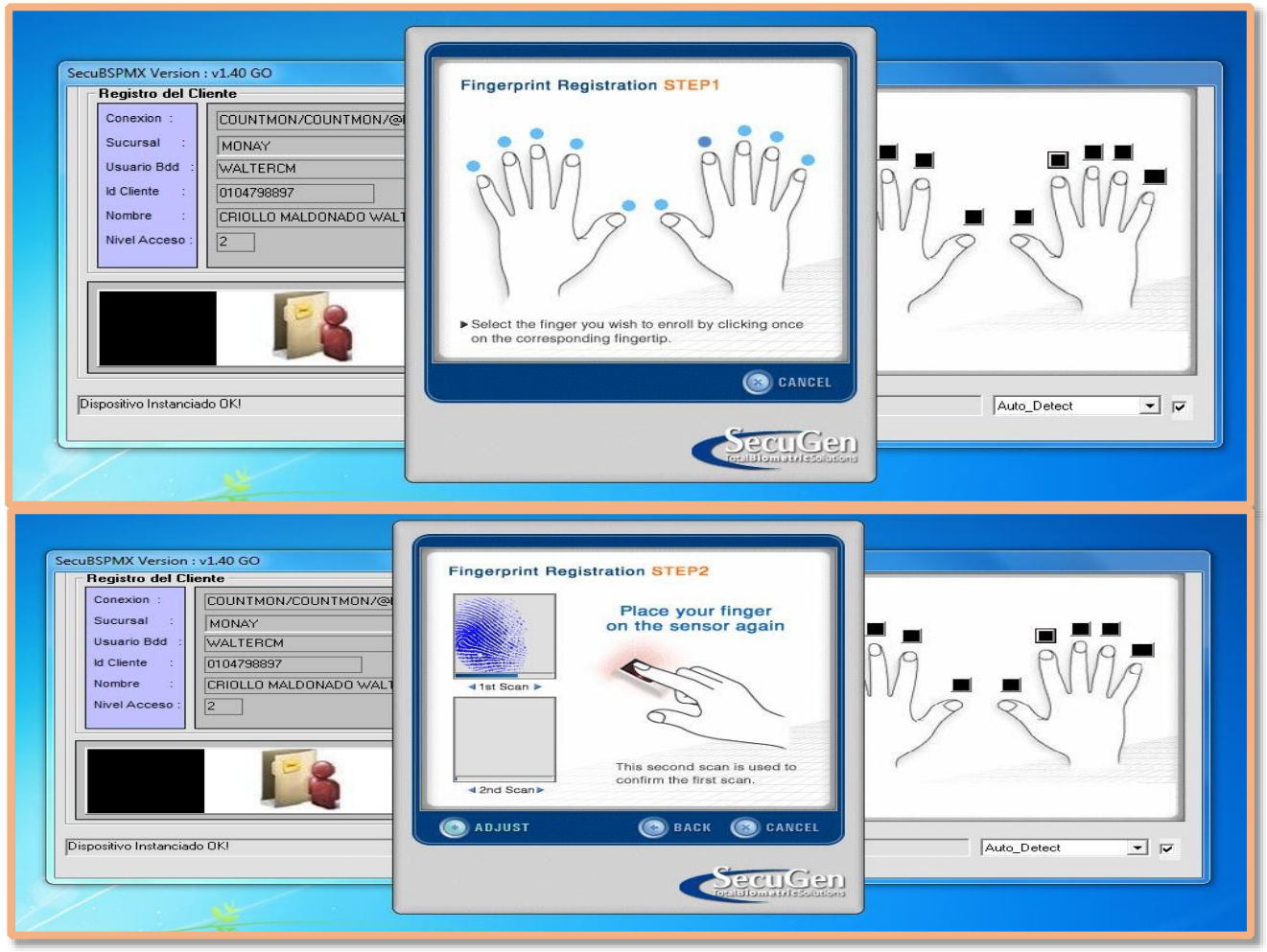
Registro de las Huellas digitales.



Fuente: Coral Hipermercado Racar Plaza (GO).

El dedo índice es registrado como la contraseña de entrada al sistema.

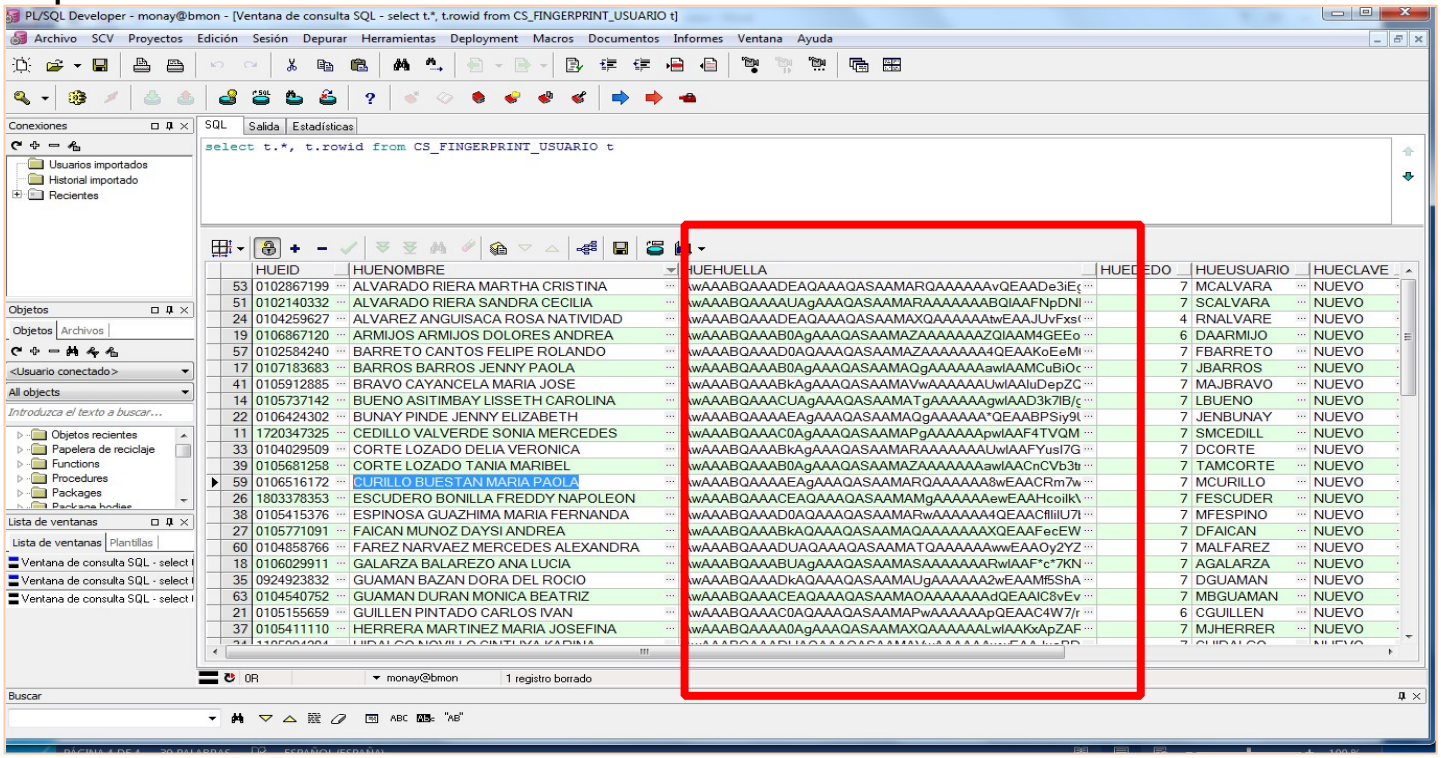
Registro del dedo índice para contraseña en el sistema.



Fuente: Coral Hipermercado Racar Plaza (GO).

Se guarda la huella digital de manera encriptada y no se puede hacer copia del código de la huella digital encriptada.

Base de datos de las huellas digitales de manera encriptada.



Fuente: Coral Hipermercado Racar Plaza (GO).

Coral Hipermercado si protege las contraseñas de los cajeros y supervisores durante la transmisión, pero a pesar de que las contraseñas se almacena mediante una criptografía sólida, las ID y contraseña para el ingreso de la base de datos de las huellas digitales de los cajeros y supervisores, son compartidas entre los encargados de cada Coral, por lo que no cumple con cabalidad este requerimiento de la norma. **Obs.**
En el caso del servidor transaccional según las entrevistas hechas al Ingeniero Paulino Quinde encargado de sistemas de Coral Hipermercado Racar Plaza llegamos a la conclusión de que las contraseñas deben tener: 1. La longitud de las contraseñas no debería ser inferiores a ocho caracteres. 2. Elaborar las contraseñas con una mezcla de caracteres alfabéticos (combinando mayúsculas y minúsculas), dígitos y caracteres especiales (@, ¡, +, &). 3. No usar las mismas contraseñas tanto para una base de datos, para un sistema operativo o para un equipo de comunicaciones. 4. Cambiar las contraseñas regularmente. (Puede ser de acuerdo a la criticidad o cuando se sospeche su descifrado).
8.2.2: Revisar los procedimientos de autenticación que sirven para modificar las credenciales de autenticación y observar al personal de seguridad que revise la identicación del usuario antes de modificar la credencial ya sea por teléfono, correo electrónico, internet u otro método no personal. La empresa Coral Hipermercado no tiene implementado ningún procedimiento acerca de la modificación de la autentificación del usuario, por lo tanto no aplican este requerimiento dentro de la empresa. **Obs.**
8.2.3: Seleccionar una muestra de los componentes del sistema de usuarios inspeccionar los parámetros de configuración del sistema para

verificar que los parámetros de la contraseña del usuario se encuentren configurados de una longitud mínima de siete caracteres y una combinación de caracteres numéricos y alfabéticos.

Dentro de la política de autentificación de Coral Hipermercado, indica que las contraseñas deben ser una clave que esté compuesto por números, letras y símbolos, además la longitud de la clave debe ser por lo menos de 16 caracteres.

Al momento de verificar si es que la política se implementa pudimos observar que en el caso de los cajeros y supervisores pueden ingresar por medio del número de cédula y la huella digital haciendo que sea más complejo el ingreso, pero este modo de autentificación no se encuentra registrado en ninguna política de Coral Hipermercado.

En el caso de los encargados del servidor transaccional se pudo observar que las contraseñas constan de 16 dígitos y según las entrevistas realizadas al Ingeniero Walter Criollo, están compuestas por números y letras.

Obs.

8.2.4: Tomar una muestra de los usuarios para poder inspeccionar los parámetros de configuración de las contraseñas y verificar que estos se encuentren configurados de manera que se le solicite al usuario cambiar su contraseña al menos cada 90 días.

Con las pruebas realizadas se llegó a la conclusión de que el personal nunca realiza cambios a las contraseñas desde el momento del ingreso a la empresa, ya que en el caso de los cajeros por ser su número de cédula y su huella digital no necesitan cambiar porque es un rasgo biométrico único. La empresa debe resguardar los datos que quedan de la huella digital de manera encriptada, se realizó las respectivas observaciones y se pudo observar que si resguardan esta información con criptografía sólida y sin posibilidad de realizar una copia de la huella digital hacia el usuario del cajero o supervisor, pero los encargados de entrar a la base de datos donde se encuentran esta información no cuentan con una contraseña segura ya que según las entrevistas realizadas tienen la misma contraseña desde hace un año.

En el caso de los encargados del servidor transaccional, tienen el mismo inconveniente dicho en el párrafo anterior, ellos tienen la misma contraseña desde hace un año, por lo que no tienen una contraseña segura. **Obs.**

8.2.5: Seleccionar una muestra de los componentes del sistema de usuarios para verificar que los parámetros de configuración de las contraseñas se encuentren configuradas de tal manera que no se puedan repetir con las cuatro últimas contraseñas.

Como se observó en el punto anterior las contraseñas nunca se cambian desde el momento de sus ingreso a la empresa, en el caso de los cajeros y supervisores, y cuando los encargados del servidor transaccional no realizan cambios desde hace un año, eso quiere decir que este requerimiento es otro de los que no aplican dentro de la empresa.

Obs.

8.2.6: Solicitar una muestra de los parámetros de configuración de las contraseñas de nuevos usuarios y contraseñas restablecidas para usuarios existentes con el fin de que el personal de seguridad verifique que se configuren en un valor único para cada usuario y se cambie después del primer uso.

Este requerimiento tampoco se aplica dentro de la empresa Coral Hipermercado porque se utiliza la misma clave que se les dio al ingresar a la empresa.

Obs.

Conclusiones y recomendaciones:

Las contraseñas utilizadas en Coral Hipermercado para los usuarios cajeros y supervisores son a través de la huella digital y el número de cédula, es una forma más segura de resguardar los datos porque es un rasgo biométrico único. Estas información es almacenada de manera encriptada y no se puede realizar copia a otro usuario, haciendo más segura la información, además los encargados del servidor tienen contraseñas de 16 dígitos combinadas con números y letras como lo indica la norma pero la empresa tiene inconvenientes que pueden costar los datos del titular de la tarjeta y de la tarjeta mismo, como: Los métodos de autenticación de los cajeros y supervisores no se encuentran registrados en la política de autenticación, además no aplican los procedimientos de autenticación para el cambio de credenciales de autentificación ya que no se ha hecho ningún cambio de la contraseña desde que

ingresaron a la organización, esto hace que una persona malintencionada se le proporcione más tiempo para descubrir la contraseña. Se recomienda implementar procedimientos de cambios de autenticación siguiendo los estándares de la norma, además que se debe reformar los parámetros de configuración de las contraseñas para que pida cambio de la misma al menos cada 90 días como indica la norma.
Elaborado por: Autoras.

ANEXO 6: PAPELES DE TRABAJO DEL REQUERIMIENTO 8. Identifique y autentifique el acceso a los componentes del sistema. (8.3).

Papeles de Trabajo		
Cumplimiento Normativa PCI DSS		
Empresa auditada:	Coral Hipermercados Racar Plaza GO.	**Ref:** req.8.3
Periodo a examinar:	Periodo 2015 con corte a Junio.	

Supervisa:	Patricia Benenaula.	**Responsable:**	Estefanía Ortega.		
Tema:	Cumplimiento de la Norma PCI DSS requerimiento 8. Identifique y autentifique el acceso a los componentes del sistema.			**Código:**	PT003
Objetivo:	Observar que se incorpore la autenticación de dos factores para el acceso remoto a la red desde fuera de la misma por parte del personal.				
Alcance:	Revisar la configuración del sistema para los servidores y sistema de acceso remoto y verificar que se exija la autentificación de dos factores (tokens, contraseñas, etc.)				

Procedimiento:

Revisar la configuración del sistema para los servidores y sistema de acceso remoto (acceder desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar, a través de una red local o externa) y verificar que se exija la autentificación de dos factores (tokens, contraseñas, etc.)

Observar a un grupo de empleados que se conecte de manera remota a la red para verificar que se use al menos dos formas de autenticación

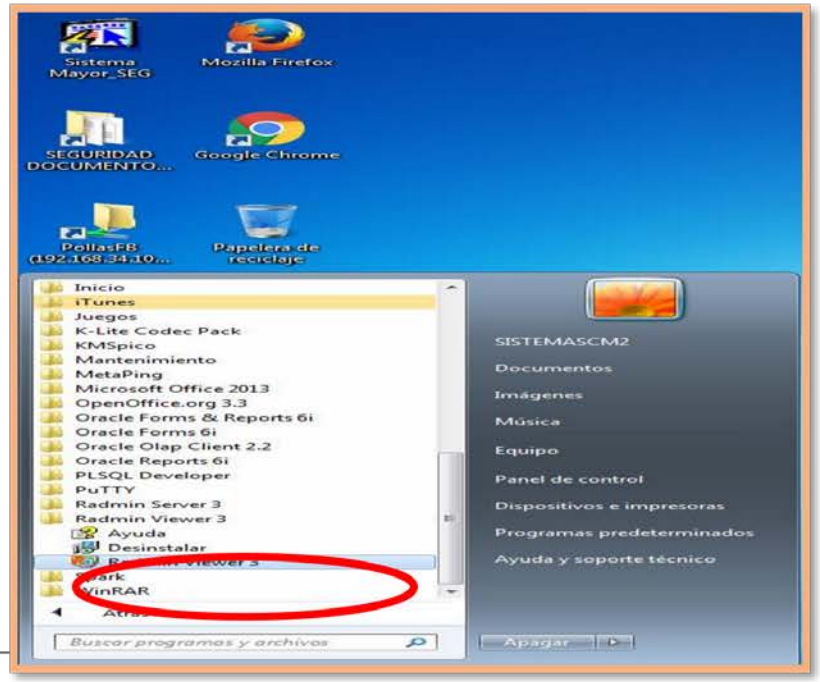
Revisión del procedimiento:

Las políticas de acceso remoto de la empresa Coral Hipermercado nos indica que existe una conexión VPN (Es una red segura para conexiones locales

sobre una red pública como Internet).

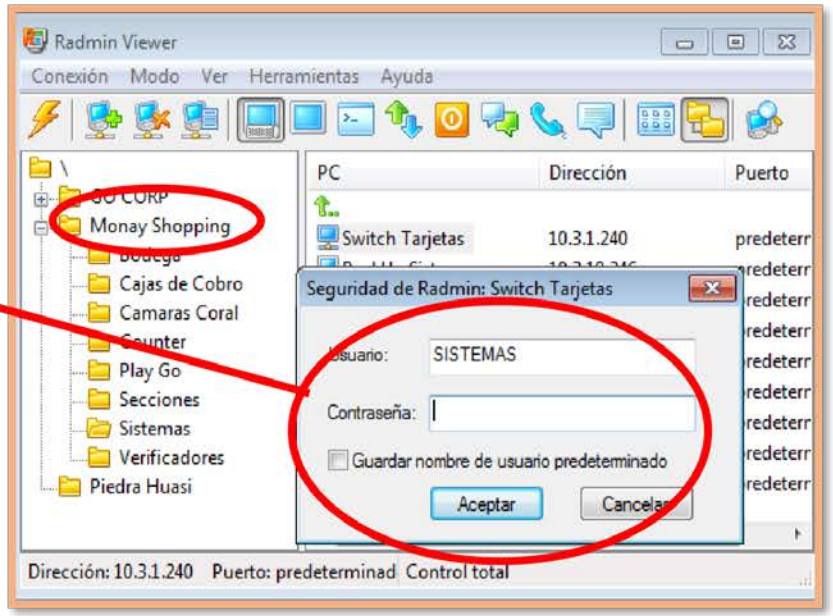
Los únicos usuarios del universo auditable que pueden tener acceso remoto son los encargados del servidor transaccional, es por eso que se realizó las respectivas pruebas, haciendo un acceso remoto hacia Coral Hipermercado Monay y el resultado fue que para poder entrar al Switch transaccional solo se necesita de un método de autenticación, al existir un solo método de autenticación para el acceso remoto se llegó a la conclusión de que la empresa no cumple con el requerimiento de la norma. **Obs.**

Primer paso para ingresar al Switch Transaccional.

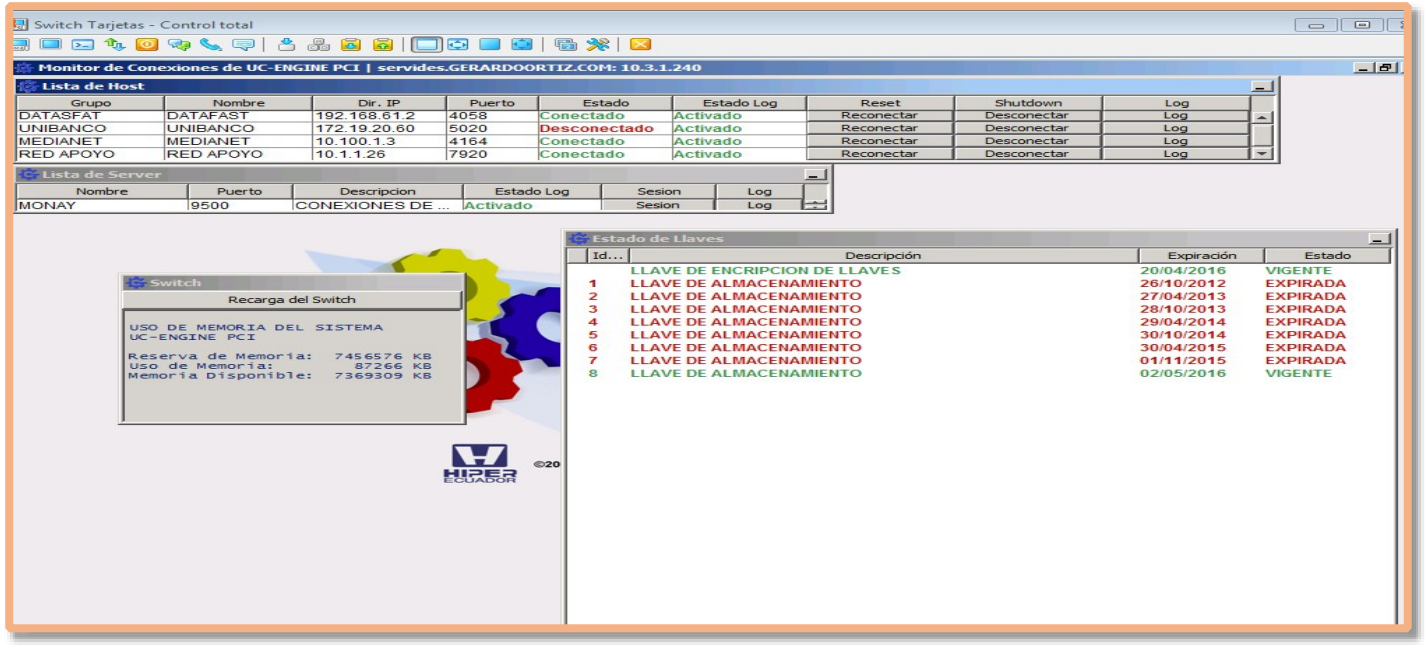


Un solo método de autentificación

Ingreso al Switch Transaccional.



Monitor PCI transaccional de tarjetas.



Fuente: Coral Hipermercado Racar Plaza (GO).

Conclusiones y recomendaciones:

Existe un solo método de autenticación para el acceso remoto, solo se ingresa la contraseña y el usuario que está en un computador fuera de la red puede realizar el acceso, esto podría exponer los datos del titular de la tarjeta porque es más fácil el ingreso al computador con un método que con dos métodos e autenticación.

Se recomienda cambiar la configuración del acceso remoto para que pida dos métodos de autentificación en el caso de que se quiera acceder, además se debe implementar procesos para el acceso remoto y se debe tener un control cuando se realice el mismo.

ANEXO 7: PAPELES DE TRABAJO DEL REQUERIMIENTO 8. Identifique y autentifique el acceso a los componentes del sistema. (8.4).

Papeles de Trabajo					
Cumplimiento Normativa PCI DSS					
Empresa auditada:	Coral Hipermercados Racar Plaza GO.			**Ref:** req.8.4.	
Periodo a examinar:	Periodo 2015 con corte a Junio.				
Supervisa:	Patricia Benenaula.	**Responsable:**	Est efanía Ortega		
Tema:	Cumplimiento de la Norma PCI DSS requerimiento 8. Identifique y autentifique el acceso a los componentes del sistema.			**Código:**	PT004
Objetivo:	Verificar que se documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios y que esta incluya lineamientos para seleccionar una credencial de autenticación sólida, además de como los usuarios deben proteger las credenciales, instrucciones para no seleccionar contraseñas utilizadas anteriormente e instrucciones para cambiar la contraseña si es necesario.				
Alcance:	Revisar los procedimientos de autentificación y entrevistar al personal para verificar que los procedimientos y las políticas de autentificación se distribuyen a todos los usuarios.				
Procedimiento:					

Verificar que estas los procedimientos de autenticación incluyan: Lineamientos sobre cómo seleccionar credenciales de autenticación sólidas. (Para ayudar al personal a colocar una contraseña que sea difícil de adivinar.) Lineamiento de como los usuarios deben proteger las credenciales de autenticación. Instrucciones a los usuarios para que no utilicen contraseñas que ya estaban anteriormente. Instrucciones para cambiar las contraseñas en el caso de que se corra riesgo.

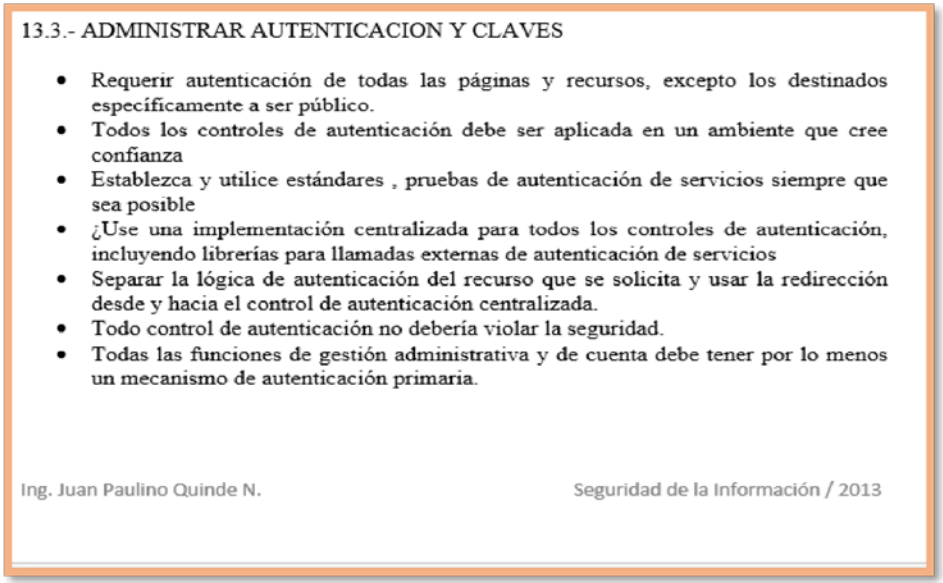
Entrevistar a un grupo de usuarios para verificar que conozca los procedimientos y políticas de autenticación.

Revisión del procedimiento:

A pesar de que Coral Hipermercado cuenta con una política de administración de autentificación y claves, esta no es distribuida a los empleados, según entrevistas realizadas, los cajeros y los supervisores no tienen conocimiento de la política de autentificación y claves en cambio los encargados del servidor transaccional conocen de la política pero no se les ha distribuido como tal.

La empresa no tiene ningún tipo de procedimiento o instrucciones para cambiar las contraseñas, así como tampoco consta dentro de sus políticas sobre no utilizar contraseñas anteriores en el caso de cambio.

Políticas de administración de autentificación y claves (GO). **Obs.**



13.3.- ADMINISTRAR AUTENTICACION Y CLAVES

- Requerir autenticación de todas las páginas y recursos, excepto los destinados específicamente a ser público.
- Todos los controles de autenticación debe ser aplicada en un ambiente que cree confianza
- Establezca y utilice estándares , pruebas de autenticación de servicios siempre que sea posible
- ¿Use una implementación centralizada para todos los controles de autenticación, incluyendo librerías para llamadas externas de autenticación de servicios
- Separar la lógica de autenticación del recurso que se solicita y usar la redirección desde y hacia el control de autenticación centralizada.
- Todo control de autenticación no debería violar la seguridad.
- Todas las funciones de gestión administrativa y de cuenta debe tener por lo menos un mecanismo de autenticación primaria.

Ing. Juan Paulino Quinde N. Seguridad de la Información / 2013

GERARDO ORTIZ & HIJOS C. Ltda.

Políticas y Procedimientos de Seguridad V1.1 50

- Si dispone de un almacén de datos asegúrese de usar criptografía. La tabla que almacena las contraseñas es capaz de escribir solo por aplicación, no use DM5 si es que es posible evitar.

- Se debe implementar hashing de contraseñas.
- Validar la autenticación de datos solamente al término de todos los datos de entrada específicamente para implementación de autenticación secuencial.
- Las respuestas de autenticación fallida no debería indicar que parte de los datos de autenticación fueron las incorrectas. Debe salir "usuario Y/O clave incorrectos".
- Use autenticación para conexiones hacia sistemas externos que involucre información o funciones sensibles.
- Credenciales de autenticación para acceso de servicios externos a las aplicaciones deben ser encriptados y guardar en un lugar protegido y validado (servidor), el código fuente no es un lugar seguro.
- Use solamente solicitudes HTTP POST para transmitir credenciales de autenticación.
- Envíe solamente contraseñas no temporales a través de una conexión encriptado o datos cifrados.
- Asegure el requerimiento de una clave compleja, establezca la política de regulación (números, letras, símbolos, etc).
- Regule la longitud de la clave (16 es mejor que 8).
- La clave no debería mostrarse en la pantalla, peor aún poder copiarse.
- Asegúrese de bloquear temporalmente(los tiempos largos podría permitir una denegación de servicios) la cuenta después de hacer un número determinado de intentos.
- El reseteo de las claves y otros cambios requiere un nivel de operación adicional que el de creación y autenticación.
- El reseteo de claves debe soportar preguntas randómicas (libro favorito, cuantas tarjetas, etc.) y entre ellas una pregunta de la que solo el cliente sabe que no es verdad no estaría mal.
- No envíe correos a una dirección registrada con el vínculo temporal y contraseña
- Las claves y links temporales deberían tener tiempos de expiración cortas.
- Refuerce el cambio de claves temporales para el próximo uso.
- Desactivar la funcionalidad "Recordarme" en los campos de claves.
- El último uso (logrado o no) debe ser reportados a este la próxima vez que ingrese a su cuenta.
- Volver autenticar los usuarios antes de hacer operaciones críticas.
- Use multi factores de autenticación para reforzar transacciones sensibles o de alto valor.

Coral Hipermercado si tiene lineamientos dentro de su política para que los usuarios protejan las credenciales de autentificación.

Coral Hipermercado También consta de lineamientos para seleccionar credenciales de autentificación segura de esa manera ayuda al personal a que tengan contraseñas

que sean de difícil adivinar.
Fuente: Coral Hipermercado Racar Plaza (GO).
Conclusiones y recomendaciones:
Coral hipermercado cuenta con una política de autenticación y claves que está compuesta por lineamientos que ayudan a proteger las credenciales de autenticación y tener contraseñas seguras difíciles de adivinar. La empresa no reparte la política de autenticación a los usuarios, además no tiene ningún lineamiento que ayude al cambio de contraseñas para no usar las a anteriores, esto afecta a la empresa debido a que el personal no tiene conocimiento de la política que le ayudará a entender y cumplir de manera correcta la misma, la empresa tampoco tiene definida un lineamiento que ayude al cambio de contraseñas, puede existir la posibilidad de que esta deje de ser segura y no podrá prevenir que usuarios mal intencionados utilicen una contraseña legítima para obtener acceso no autorizado. Se recomienda una actualización de la política donde se incluya los lineamientos de cambio de contraseña, además que se capacite al personal para que tengan conocimientos de la política y que se les reparta la misma.
Elaborado por: Autoras.

ANEXO 8: PAPELES DE TRABAJO DEL REQUERIMIENTO 8. Identifique y autentifique el acceso a los componentes del sistema. (8.5).

Papeles de Trabajo					
Cumplimiento Normativa PCI DSS					
Empresa auditada:	Coral Hipermercados Racar Plaza GO.			**Ref:** req.8.5.	
Periodo a examinar:	Periodo 2015 con corte a Junio.				
Supervisa:	Patricia Benenaula.	**Responsable:**	Estefanía Ortega		
Tema:	Cumplimiento de la Norma PCI DSS requerimiento 8. Identifique y autentifique el acceso a los componentes del sistema.			**Código:**	PT005
Objetivo:	Verificar que se haya definido e implementado las políticas y procedimientos para garantizar la correcta administración de la identificación de todos usuarios, en los componentes del sistema.				
Alcance:	Seleccionar una muestra de los componentes del sistema, y revisar las listas de ID de usuarios y verificar que:				

Procedimiento: .Las ID de usuarios genéricas sean desactivadas o eliminadas. .Además se debe revisar que no exista ID de usuarios compartidas para realizar actividades de administración del sistema y demás funciones críticas. .Las ID de usuarios compartidas y genéricas no se deben utilizar para administrar componentes del sistema. Solicitar y revisar las políticas y procedimientos de autentificación para verificar que las contraseñas y las ID de grupo y compartidas u otro método de autenticación parecidos, estén prohibidos. Se debe entrevistar a los administradores del sistema para verificar que las contraseñas de grupo y compartidas no se distribuyan, incluso en el caso que se solicite.
Revisión del procedimiento:

ID de usuarios.

MSICHIQ	204		EXPIRED
MZHINGRI	205		OPEN
NAGUA	206		OPEN
NAGUILAR	207		OPEN
NESCUDE	208		OPEN
NRAMIREZ	209		OPEN
PCAB01	210		OPEN
SPARRA	232		OPEN
PPENA	212		OPEN
QUEJAS	213		OPEN
RCHILLO	214		OPEN
REPROCES	215		OPEN
RPESANT	216		OPEN
RPRIETO	217		OPEN
RSARMIE	218		OPEN
SEGUNDO	219		OPEN
SIGU	220		OPEN
TOVAR	221		OPEN
USER02	222		OPEN
USER2	223		OPEN
USER3	224		OPEN
VCAIVINA	225		OPEN
VCAVIED	226		OPEN
VFREIRE	227		OPEN
WCRIOLLO	228		OPEN
XCUESTA	229		OPEN
XGARCIA	230		OPEN
JPUCHI	231		OPEN
KARMIJOS	253		OPEN
ETAPIA	233		OPEN
EGUZMAN	234		OPEN
JSALAZAR	235		OPEN
FREYES	236		OPEN
ASANCHO	237		OPEN
NCHANG	238		OPEN
MCHANG	239		OPEN

Todos los usuarios tienen una ID exclusiva.

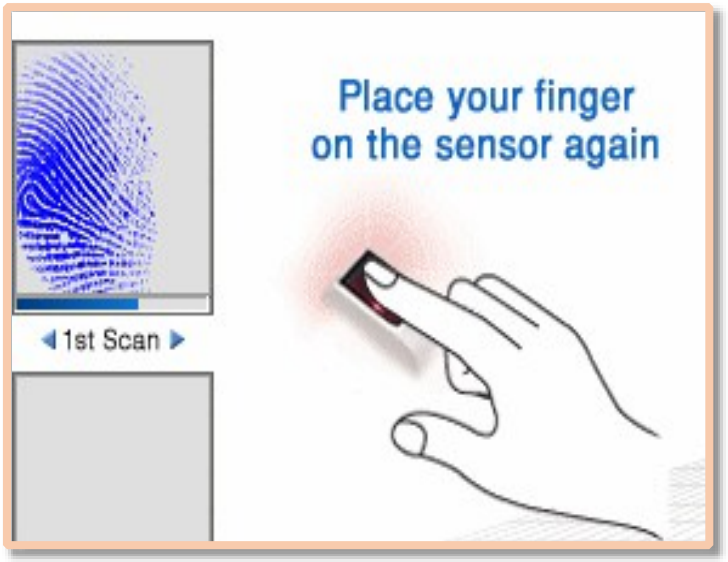
Fuente: Coral Hipermercado Racar Plaza (GO). √

Los cajeros y supervisores ingresan al sistema por medio la cédula de identidad y la huella digital.

Lugar donde se digita el número de cédula.

Fuente: Coral Hipermercado Racar Plaza (GO).

Registro de la huella digital.



Fuente: Coral Hipermercado Racar Plaza (GO).

La información otorgada por la empresa Coral Hipermercado nos muestra que existe una ID exclusiva para cada usuario, sin embargo al momento de realizar las respectivas pruebas, los usuarios cajeros y supervisores si tienen una ID y contraseña exclusiva, pero en el caso de los encargados del

servidor transaccional las ID y contraseñas son compartidas entre ellos según entrevistas realizadas y observaciones hechas.

Además las contraseñas son las mismas otorgadas al momento de su ingreso a la empresa.

Obs.

Conclusiones y recomendaciones:

Según los dato otorgados todos los usuarios tiene ID exclusivas, pero al momento de realizar entrevista y observaciones los usuarios encargados del servidor transaccional tienen ID y contraseñas compartidas, además las contraseñas que son las mismas que se les otorgó cuando ingresaron a la empresa, esto hace que la empresa se responsabilice por las acciones de una persona ya que cualquier persona del grupo puede haber realizado la acción, por lo tanto no se sabría sobre quién debe caer la responsabilidad. Se recomienda realizar una reforma en las ID y contraseñas de los encargados del servidor transaccional, de tal manera que no se les permita usar una grupal sino que cada uno tenga exclusividad, además se debe realizar una configuración de los parámetros de contraseñas, pidiendo al usuario que debe cambiar obligatoriamente pasado los 30 días.

Elaborado Por: Autoras.

ANEXO 9: PAPELES DE TRABAJO DEL REQUERIMIENTO 8. Identifique y autentifique el acceso a los componentes del sistema. (8.6).

Papeles de Trabajo
Cumplimiento Normativa PCI DSS

Empresa auditada:	Coral Hipermercados Racar Plaza GO.		**Ref:** req.8.6.	
Periodo a examinar:	Periodo 2015 con corte a Junio.			
Supervisa:	Patricia Benenaula.	**Responsable:**	Estefanía Ortega	
Tema:	Cumplimiento de la Norma PCI DSS requerimiento 8. Identifique y autentifique el acceso a los componentes del sistema.		**Código:**	PT006
Objetivo:	Verificar que en el caso de que se use otros mecanismos de autenticación estos se asignen a una sola cuenta y no compartirlos entre varias, además verificar que se implementen controles físicos y lógicos para garantizar que solo la cuenta deseada usa esos mecanismos para acceder.			
Alcance:	Revisar las políticas y procedimientos de autentificación para verificar que los procedimientos que usan mecanismos de autentificación (tokens de seguridad, tarjetas inteligentes y certificados) estén definidas dentro de la política y procedimientos, además estos mecanismos deben ser asignados a una solo persona y no ser compartida y con los controles físicos y lógicos garantizan que la cuenta deseada es la única que usa ese mecanismo para acceder.			

Procedimiento:

Se debe entrevistar al personal de seguridad y se debe examinar los parámetros de configuración del sistema y los controles físicos para verificar que se implementen controles a fin de garantizar que solo la cuenta deseada usa esos mecanismos para acceder.

Revisión del procedimiento:

La empresa Coral hipermercado no consta de mecanismos de autentificación como tokens de seguridad, tarjetas inteligentes y certificadas por lo que no aplica este requerimiento.

Conclusiones y recomendaciones:
La empresa Coral Hipermercado no usa tokens, tarjetas inteligentes y certificados, esto hace que no se identifiquen usuarios no autorizados, haciendo que puedan acceder usando mecanismos de autentificación compartidos y con total libertad. Se recomienda implementar mecanismos de autenticación más seguros, además que se debe reformar la política de autenticación para resguardar los datos relacionados con las tarjetas de pago y así evitar actos maliciosos.
Elaborado por. Autoras.

ANEXO 10: PAPELES DE TRABAJO DEL REQUERIMIENTO 8. Identifique y autentifique el acceso a los componentes del sistema. (8.7).

Papeles de Trabajo

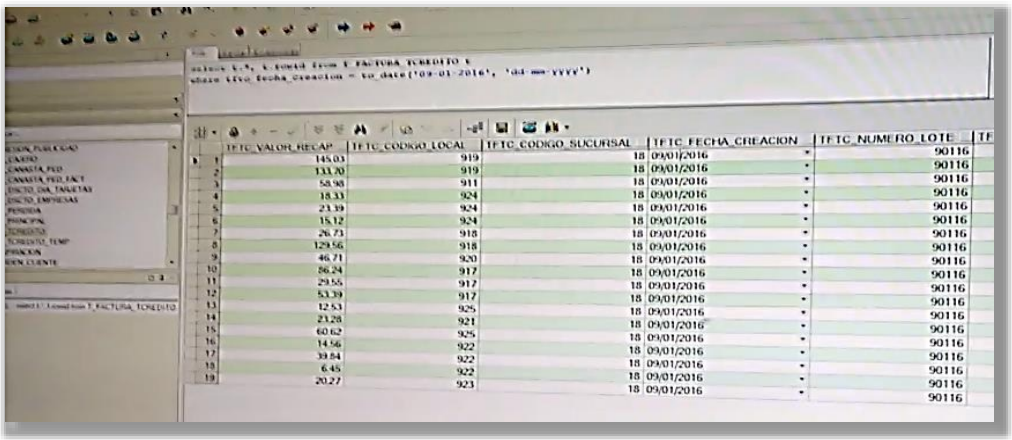
Cumplimiento Normativa PCI DSS					
Empresa auditada:	Coral Hipermercados Racar Plaza GO.			**Ref:** req.8.7.	
Periodo a examinar:	Periodo 2015 con corte a Junio.				
Supervisa:	Patricia Benenaula.	**Responsable:**	Estefanía Ortega		
Tema:	Cumplimiento de la Norma PCI DSS requerimiento 8. Identifique y autentifique el acceso a los componentes del sistema.			**Código:**	PT007
Objetivo:	Observar que se restrinjan todos los accesos a cualquier base de datos que tengan datos del titular de la tarjeta por lo que cualquier consulta y acción se realicen mediante métodos programáticos, solo los administradores de la base de datos puedan acceder, solo las aplicaciones pueden usar las ID de aplicaciones.				
Alcance:					
Revisar los parámetros de configuración de la aplicación y de la base de datos para verificar que todos los usuarios estén autentificados antes de acceder. Revisar los parámetros de configuración de la base de datos y de la aplicación para verificar que el acceso de todos los usuarios, consultas del usuario y acciones del usuario en la base de datos se realicen únicamente mediante métodos programáticos. Evaluar los parámetros de control de acceso de la base de datos y los parámetros de configuración de la aplicación de la base de datos y verifique que el acceso directo del usuario a la base de datos, o las consultas a esta, esté limitado a los administradores de la base de datos. Revisar los parámetros de control de accesos de la base de datos, los parámetros de configuración de la aplicación de la base de datos y las ID de aplicaciones relacionadas para verificar que solo las aplicaciones pueden usar las ID de la aplicación.					

Revisión del procedimiento:

Los usuarios de la base de datos son los siete encargados del servidor transaccional ellos comparten contraseñas para el ingreso, aquí solo se almacena el nombre del titular de la tarjeta, valor de la compra, número de factura, número de voucher y lote.

En el caso de la aplicación los cajeros y los supervisores pueden acceder a los datos del titular de la tarjeta, ellos tienen una ID única al igual que la contraseña, ingresan por medio del número de cédula y huella digital como se mencionó anteriormente; los datos del titular de la tarjeta se pueden observar a través del monitor de transacciones, al igual que el servidor transaccional pueden acceder a datos como: nombre del titular de la tarjeta, valor de la compra, número de factura, número de voucher y lote**.** **Obs.**

Acceso a la base de datos. **Base de datos de las transacciones realizadas en caja durante el día.**

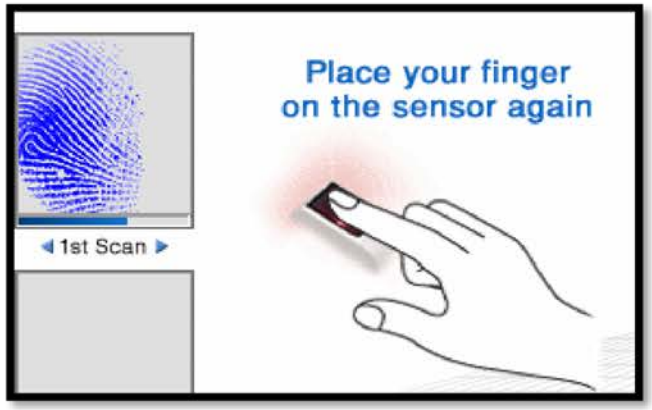


Fuente: Coral Hipermercado Racar Plaza (GO) **Fuente: Coral Hipermercado Racar Plaza (GO)**

Lugar donde se digita el número de cédula.

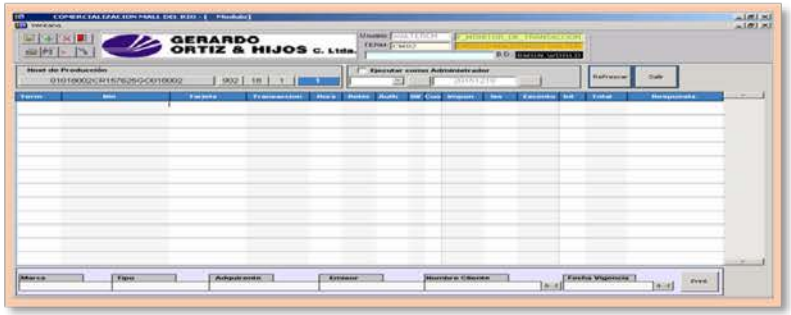
Fuente: Coral Hipermercado Racar Plaza (GO).

Registro de la huella digital.



Fuente: Coral Hipermercado Racar Plaza (GO).

Ilustración……. Monitor de transacciones.



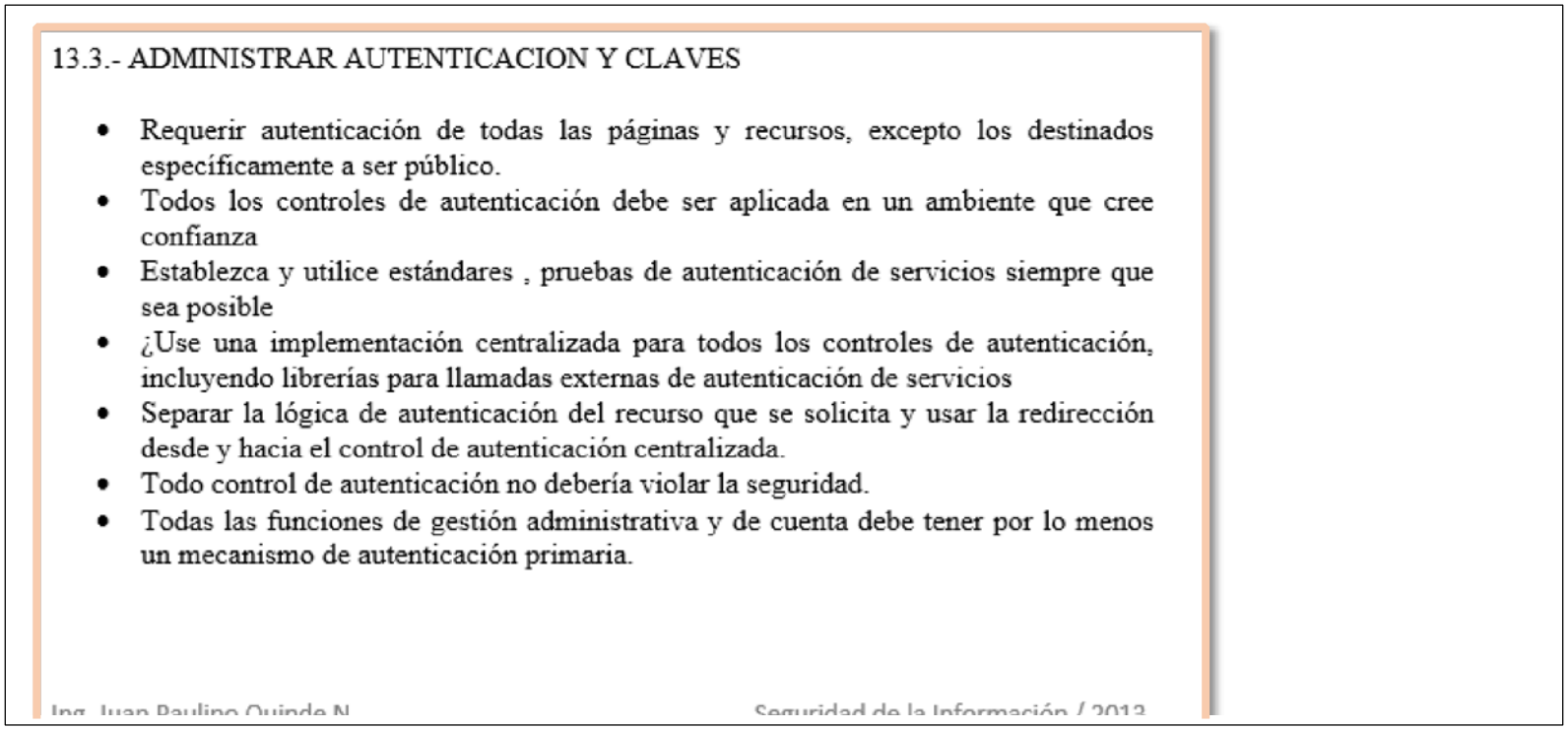
Fuente: Coral Hipermercado Racar Plaza (GO)

Conclusiones y recomendaciones:
Los cajeros y los supervisores tienen una ID y contraseña única, además solo pueden acceder a información básica del titular de la tarjeta (Nombre, número de factura, valor adquirido, número de Boucher y número de lote). Los siete encargados de acceder a la base de datos solo pueden acceder a información básica del titular de la tarjeta (Nombre, número de factura, valor adquirido, número de Boucher y número de lote) así como lo específica la norma, pero los Siete tienen la misma contraseña para acceder, esto hace que se incremente el riesgo de que puedan realizar actos maliosos con los datos del titular de la tarjeta. Se recomienda reformar los métodos de autenticación y los parámetros de autenticación dentro del sistema, además que se debe asignar una contraseña individual, de esa manera la responsabilidad será individual.
Elaborado por: Autoras.

ANEXO 11: PAPELES DE TRABAJO DEL REQUERIMIENTO 8. Identifique y autentifique el acceso a los componentes del sistema. (8.8).

Papeles de Trabajo					
Cumplimiento Normativa PCI DSS					
Empresa auditada:	Coral Hipermercados Racar Plaza GO.			**Ref:** req.8.8.	
Periodo a examinar:	Periodo 2015 con corte a Junio.				
Supervisa:	Patricia Benenaula.	**Responsable:**	Estefanía Ortega		
Tema:	Identifique y autentifique el acceso a los componentes del sistema.			**Código:**	PT008
Objetivo:	Verificar que las políticas de seguridad y los procedimientos operativos de identificación y autenticación estén documentados y sean de conocimiento para todas las partes.				
Alcance:	Revisar la documentación y entrevistar al personal para verificar que las políticas de seguridad y los procedimientos estén documentados, implementados y sean conocidos para todas las partes afectadas.				
Actividades:					
Revisar la documentación y entrevistar al personal para verificar que las políticas de seguridad y los procedimientos estén documentados, implementados y sean conocidos para todas las partes afectadas.					
Revisión del procedimiento:					

La empresa si tiene política de seguridad documentada al igual que procedimientos, pero esta no se encuentra implementada del todo además que no está completa debido a que los usuarios realizan algunas actividades que no se encuentra dentro de la política por ejemplo en el caso de la autentificación de los cajeros y supervisores, este método no está establecido en la política de autentificación y claves, además que la política
no es conocida por todas las partes afectadas.
Obs. **Políticas de administración de autentificación y claves (GO).**



13.3.- ADMINISTRAR AUTENTICACION Y CLAVES

- Requerir autenticación de todas las páginas y recursos, excepto los destinados específicamente a ser público.
- Todos los controles de autenticación debe ser aplicada en un ambiente que cree confianza
- Establezca y utilice estándares , pruebas de autenticación de servicios siempre que sea posible
- ¿Use una implementación centralizada para todos los controles de autenticación, incluyendo librerías para llamadas externas de autenticación de servicios
- Separar la lógica de autenticación del recurso que se solicita y usar la redirección desde y hacia el control de autenticación centralizada.
- Todo control de autenticación no debería violar la seguridad.
- Todas las funciones de gestión administrativa y de cuenta debe tener por lo menos un mecanismo de autenticación primaria.

Ing. Juan Paulino Quinde N. Seguridad de la Información / 2013

- Se debe implementar hashing de contraseñas.
- Validar la autenticación de datos solamente al término de todos los datos de entrada específicamente para implementación de autenticación secuencial.
- Las respuestas de autenticación fallida no debería indicar que parte de los datos de autenticación fueron las incorrectas. Debe salir "usuario Y/O clave incorrectos".
- Use autenticación para conexiones hacia sistemas externos que involucre información o funciones sensibles.
- Credenciales de autenticación para acceso de servicios externos a las aplicaciones deben ser encriptados y guardar en un lugar protegido y validado (servidor), el código fuente no es un lugar seguro.
- Use solamente solicitudes HTTP POST para transmitir credenciales de autenticación.
- Envíe solamente contraseñas no temporales a través de una conexión encriptado o datos cifrados.
- Asegure el requerimiento de una clave compleja, establezca la política de regulación (números, letras, símbolos, etc).
- Regule la longitud de la clave (16 es mejor que 8).
- La clave no debería mostrarse en la pantalla, peor aún poder copiarse.
- Asegúrese de bloquear temporalmente(los tiempos largos podría permitir una denegación de servicios) la cuenta después de hacer un número determinado de intentos.
- El reseteo de las claves y otros cambios requiere un nivel de operación adicional que el de creación y autenticación.
- El reseteo de claves debe soportar preguntas randómicas (libro favorito, cuantas tarjetas, etc.) y entre ellas una pregunta de la que solo el cliente sabe que no es

Fuente: Coral Hipermercado Racar Plaza (GO).

Conclusiones y recomendaciones:

La empresa si tiene política de seguridad documentada al igual que procedimientos, pero no se encuentra implementada del todo además que no está completa debido a que los usuarios realizan algunas actividades que no se encuentra dentro de la política por ejemplo en el caso de la autenticación de los cajeros y supervisores, este método no está establecido en la política de autenticación y claves, además que no es conocida por todas las partes afectadas, el personal debe conocer y respetar siempre las políticas y procedimientos operativos para que pueda administrar la identificación y la autorización.

Se recomienda realizar una reforma total de la política, después de eso se debe realizar capacitaciones al personal para que se distribuya y se conozca de la misma.

Elaborado por: Autoras.

Universidad de Cuenca
Facultad de Ciencias Económicas.
Carrera de Contabilidad y Auditoría.

PATRICIA MARÍA BENENAULA LITUMA.
PÁGINA 329 ESTEFANÍA LISETH ORTEGA LÓPEZ.

Universidad de Cuenca
Facultad de Ciencias Económicas.
Carrera de Contabilidad y Auditoría.

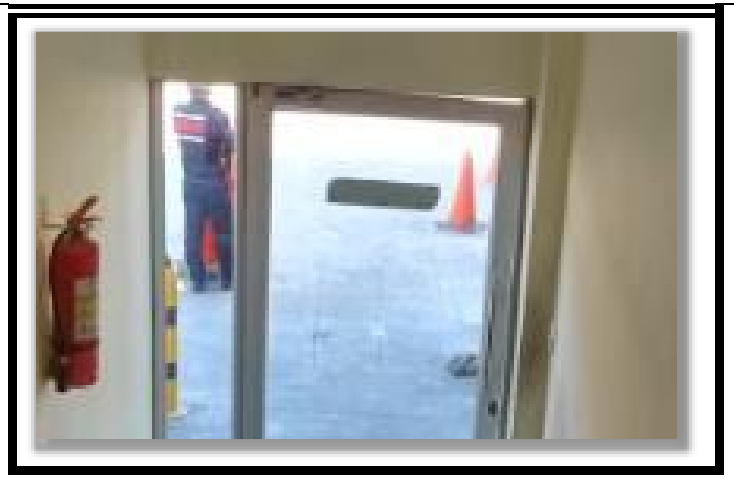
PATRICIA MARÍA BENENAULA LITUMA.
PÁGINA 330 ESTEFANÍA LISETH ORTEGA LÓPEZ.

ANEXO 12: PAPELES DE TRABAJO DEL REQUERIMIENTO 9. Restringir el acceso físico a los datos del titular de la tarjeta.

(9.1)

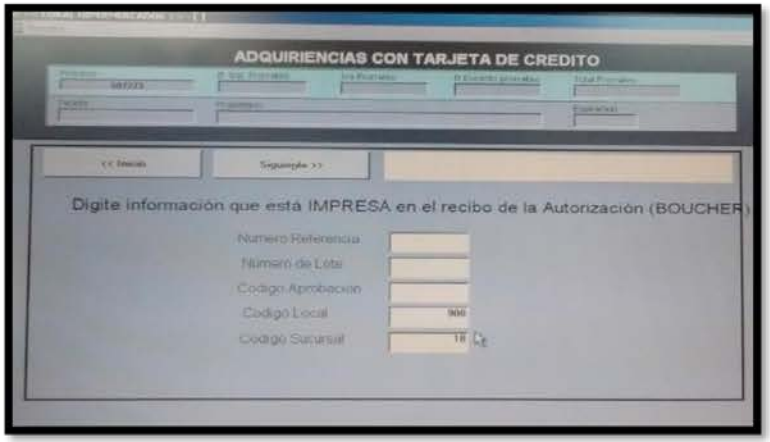
Papeles de Trabajo				
Cumplimiento Normativa PCI DSS				
Empresa auditada:	Coral Hipermercado Racar Plaza (GO).		**Ref:** Req. 9.1	
Periodo a examinar:	Periodo 2015 con corte a Junio.			
Supervisa:	Estefanía Ortega	**Responsable:**	Patricia Benenaula	
Tema:	Cumplimiento de la Normativa PCI DSS Requerimiento 9. Restringir el acceso físico a los datos del titular de la tarjeta.		**Código:**	PT001
Objetivo:	Verificar que se utilicen controles de entrada a la empresa apropiados para limitar y supervisar el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta.			
Alcance:	Verificar la existencia de controles de seguridad física para cada sala de informática, centro de datos y otras áreas físicas con sistemas en el entorno de datos del titular de la tarjeta.			
Procedimiento:				
Revisión de la política de seguridad				
Política de seguridad de Coral Hipermercado (GO).				

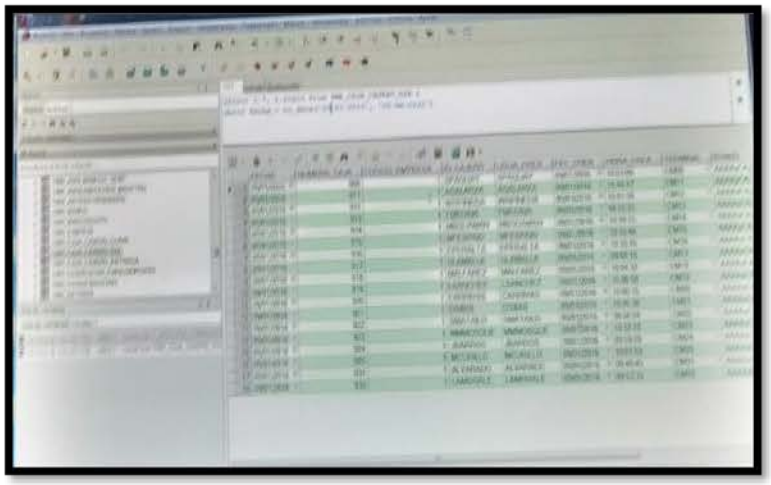
• Se impedirá el acceso físico a los datos del titular de la tarjeta así: o Los medios en papel que tendrán un control estricto, sobre todo los documentos que se generen a partir de la tarjeta de crédito con el objeto de mantener su confidencialidad. o Se distribuirán en la caja registradora con el mismo cuidado que el dinero en efectivo, en un compartimento previsto para ello. o No está permitido sacar copias, fotos, réplicas o similar a ningún contenido de información sensible o de los tarjeta habientes ni recibos electrónicos. o No se emitirá información de las tarjetas de crédito, su contenido ni información que insinúe su contenido en claro, por correo electrónico, en medios de almacenamiento ni en papel impreso u otro similar. o Cuando se traslade información de tarjeta habiente (en el caso de tener información confidencial), se debe dar informe al administrador para que este a su vez se escolte de una persona de seguridad al trasladar los medios. o Se registrará estrictamente los movimientos, tanto en almacenamiento, transporte y accesibilidad de estos medios. o Estos medios serán destruidos cuando ya no sean necesarios para la empresa; para el caso, se procederá de acuerdo a las normas de destrucción de información que se han establecido en las políticas de seguridad	√√ Hemos querido revisar la norma para saber si se contiene alguna información sobre el acceso físico a los datos y lo que se puede visualizar es lo que se detalla.
Fuente: Coral Hipermercado Racar Plaza (GO).	
Observación de las instalaciones de seguridad de Coral Hipermercado de grupo (GO)	
*Verificar que se controle el acceso con lectores de placas de identificación u otros dispositivos, incluidas placas autorizada s y llave y candado.	
	√



Se logró observar que se mantiene un cuidado acorde a la política para el acceso a las instalaciones, para el departamento de sistemas el control se realiza mediante llave y candado pero no se mantiene la señalización necesaria (por ej. permiso solo personal autorizado), se ha podido observar también que de ser el caso se podría acceder a las instalaciones de computo, redes e informática con algo de facilidad comparado con los departamentos como crédito, tarjetas de

		crédito entre otros el ingresos es más seguro.
Fuente: Coral Hipermercado Racar Plaza (GO).		
*Observar un intento de algún administrador del sistema para iniciar sesión en las consolas de sistemas seleccionados de forma aleatoria en un entorno de titulares de tarjetas y verificar que estén "aseguradas" y se impida el uso no autorizado.		
Entrevista al personal administrativo grupo (GO)	Cabe recordar que Coral Hipermercado no almacena datos de Titulares de tarjetas por lo que la información del sistema de facturación es tal como se muestra en la imagen de la	**Obs**





ilustración, y como se informó anteriormente los usuarios del sistema de facturación (cajeros) mantienen un sistema de control de acceso mediante huella digital por lo que este riesgo se vería minimizado.	
En el sistema de soporte y servidores transaccionales se puede ingresar mediante acceso remoto tanto a bases de datos donde se encuentran datos de titular de tarjeta (solo básicos) así como a las consolas de los cajeros para realizar monitoreo lo que podría ocasionar riesgo al verse expuestos actos maliciosos y sobretodo	Al conocer que el sistema de administradores (personal de soporte técnico) a través de accesos remotos pueden ingresar a las consolas de sistemas como facturación para la realización de monitoreo lo que presenta un riesgo para la organización, a más de que los empleados pueden iniciar sección indistintamente del computador pero con su clave e ID exclusiva,

	cabe mencionar que las claves para el ingreso a las bases de datos mantiene una clave conjunta con una ID exclusiva pero con sola una clave para todos los empleados que realicen soporte mediante accesos remotos.	excepto los cajeros que en donde inician sección terminan hasta el cuadre de caja del final del día.

Fuente: Coral Hipermercado Racar Plaza (GO).

Req. 9.1.1 Verificar que se utilicen cámaras de video y otros mecanismos de control de acceso para supervisar el acceso físico de personas a áreas confidencial

* Verificar que las cámaras de video y otros mecanismos de control de acceso se usen para supervisar los puntos de entrada y salida de áreas confidenciales.

Observación de las instalaciones de Coral Hipermercado de Grupo (GO)

	√

Se observó que Coral hipermercado Racar Plaza mantiene instaladas cámaras de seguridad en todos sus locales tanto en entradas como salidas, son de uso para control de todo el almacén de cada una de las áreas, ingreso y salida de todos los clientes, y áreas confidenciales así como oficinas departamentales.

Fuente: Coral Hipermercado Racar Plaza (GO).

***Verificar que las cámaras de video y otros mecanismos de control de acceso estén protegidos contra alteraciones o desactivaciones.**
Se observó que el departamento de tecnología y soporte cuenta con el debido control de acceso de terceras personas a las cámaras de seguridad de respaldo de los departamentos y el local en general.
*** Verificar que se controlen las cámaras de video y otros mecanismos, y que los datos de dichas cámaras o mecanismos se almacenen, al menos, durante tres meses.**
Se conversó con el encargado de las cámaras de seguridad y videos y según la información que nos ha dado se ha comprobado que los videos se van eliminando automáticamente cada 20 días y se vuelven a grabar en los mismos dispositivos. A más que no se mantiene la debida seguridad para el departamento de monitorio de videos de las cámaras de seguridad ya que se encuentra presto al ingreso de personal no autorizado, porque la seguridad en puertas es apropiada pero no hay concientización de llevarla a cabo y no existe una señalización debida.
Req. 9.1.2 Verificar que se implementen controles físicos o lógicos para restringir el acceso a conexiones de red de acceso público.
*Entrevistar al personal responsable y observar las ubicaciones de las conexiones de red de acceso público para verificar que se implementen controles físicos o lógicos a fin de restringir el acceso a las conexiones de red de acceso público.
Entrevista al personal administrativo grupo (GO)

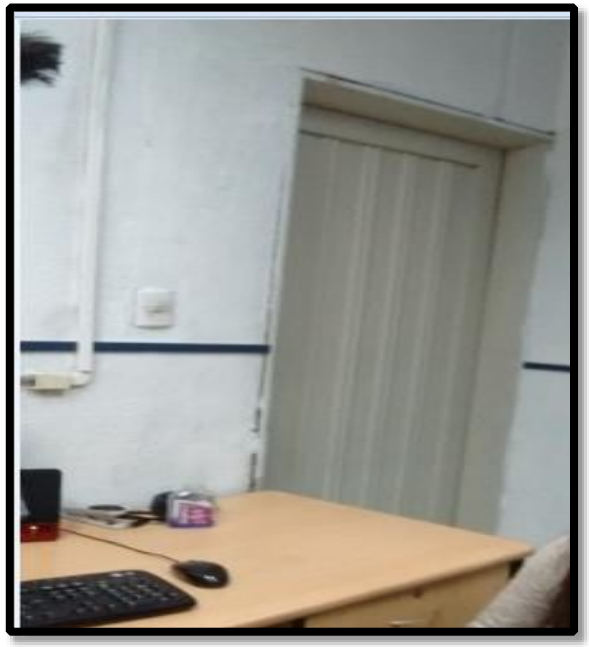
	Obs

Coral Hipermercado no mantiene una red de acceso público, no existen redes wifi ya que se utiliza fibra óptica, sin embargo se mantiene un Rack para la conexión de redes de telecomunicaciones, este no mantiene una debida seguridad como podemos observar la puerta de ingreso no se encuentra asegurada y se comprobó que el acceso no es restringido para personal

	absolutamente necesario según sus funciones.

Fuente: Coral Hipermercado Racar Plaza (GO).

Req. 9.1.3 Verificar que se limite el acceso físico a los puntos de acceso inalámbricos, Gateways, dispositivos man uales, hardware de redes o comunicaciones y líneas de telecomunicación.

Instalaciones de departamento de cámaras de Coral Hipermercado (GO).	**Obs**
 	Se observó que el acceso físico a puntos de acceso de redes, comunicaciones y líneas de telecomunicación de las instalaciones y oficinas de coral hipermercados de grupo Ortiz no se encuentran debidamente resguardadas puesto que no se tiene un nivel adecuado de seguridad para limitar el acceso, las

	puertas se encuentran sin seguros, el entorno de las mismas podría ser de riesgo para el ingreso de cualquier persona ajena a la entidad, a su vez no hay cámaras que vigilen los RACKS

Fuente: Coral Hipermercado Racar Plaza (GO).

Conclusiones y recomendaciones:

Hemos concluido que no se mantiene un adecuado sistema de seguridad estricto para los entornos de sistemas de redes, dispositivos manuales, comunicaciones y líneas de telecomunicaciones puesto que se encuentran al acceso fácil de personas ajenas a la entidad, no están debidamente señalizados mediante letreros que prohíban el ingreso y no mantienen cámaras de seguridad de acceso a centros confidenciales como el monitoreo de las cámaras de seguridad y los RACKs.

Elaborado por: Autoras.

ANEXO 13: PAPELES DE TRABAJO DEL REQUERIMIENTO 9. Restringir el acceso físico a los datos del titular de la tarjeta. (9.2)

Papeles de Trabajo				
Cumplimiento Normativa PCI DSS				
Empresa auditada:	Coral Hipermercados Racar Plaza GO.		**Ref:** Req. 9.2	
Periodo a examinar:	Periodo 2015 con corte a Junio.			
Supervisa:	Estefanía Ortega	**Responsable:**	Patricia Benenaula	
Tema:	Cumplimiento de la Normativa PCI DSS Requerimiento 9. Restringir el acceso físico a los datos del titular de la tarjeta.		**Código:**	PT002
Objetivo:	Verificar que se desarrollen procedimientos que permitan distinguir fácilmente a los empleados y a los visitantes.			
Alcance:	Verificar y revisar los procesos documentados para verificar que los procedimientos se definan de manera tal que se pueda realizar una identificación y distinción entre empleados y visitantes.			
Procedimiento:				
Req. 9.2a Verificar y revisar los procesos documentados para verificar que los procedimientos se definan de manera tal que se pueda realizar una identificación y distinción entre empleados y visitantes.				
Política de seguridad de Coral Hipermercado (GO).			**Obs.**	

PROCEDIMIENTO PARA INGRESO, PROMOCION Y SALIDA DE PERSONAL

El proceso en el que se enmarca el reclutamiento, asensos o cambios de cargos (aquí se incluye la desliga temporal) se ha tomado desde los que dispone el área de recursos humanos y delineándolo de la siguiente forma en 3 diferentes etapas:

- El proceso de reclutamiento y selección de personal empieza con la definición del perfil del postulante, y continúa con la búsqueda, reclutamiento o convocatoria de postulantes,

- Dar de baja un empleado.- Cuando un trabajador renuncia a sus labores o es despedido se procederá de la siguiente manera:
  - Se recibe por escrito la renuncia o el visto del mismo si es el caso.
  - Se le pide que entregue su trabajo a la persona que se hará cargo de sus labores. La ley no obliga a hacer días de labor adicional si éste no desea hacerlo.
  - Se solicita al área informática que se le disminuyan privilegios cuando pudiere constatarse que se trata de un empleado descontento.
  - El empleado tendrá que dejar por escrito todas las tareas que realizaba, usuarios que utilizaba, documentos que manejaba y cualesquier dato adicional respecto a sus labores. Esto es en el acta de entrega-recepción.
  - Cuando el empleado se retira se bloquean los accesos de esta persona, se obtiene una copia del equipo en el que trabajaba, el mismo que se almacenará en un lugar seguro y finalmente se procede a limpiar la máquina y prepararla para el futuro usuario.

. Juan Paulino Quinde N. Seguridad de la Información / 2013

En la normativa de seguridad de Coral Hipermercado de grupo GO se contempla un procedimiento para el personal en su ingreso a la institución así como su desvinculación sin embargo no se encuentra un procedimiento establecido para la diferenciación de los visitantes y cómo será su tratamiento para las visitas a las instalaciones de la organización.

La normativa hace una referencia breve acerca de que se debe apoyar a un control físico de seguridad sin mención de visitantes o terceras personas.

Fuente: Coral Hipermercado Racar Plaza (GO).

***Verificar que estos procesos incluyan:**
- Identificación de empleados o visitantes nuevos (por ej. Mediante la asignación de placas).
Placas de identificación de Coral Hipermercado (GO).

√

Se observó en la visita realizada a las instalaciones de las oficinas de Coral Hipermercado de Grupo GO que si se entregan carnets para visitantes a las instalaciones, los mismos que contienen una descripción de la planta o área a la que se dirige el visitante.

Fuente: Coral Hipermercado Racar Plaza (GO).

- Cambiar los requisitos de acceso:

Dentro de los requisitos de acceso según la entrevista realizada al personal administrativo de Coral Hipermercado de Grupo GO se nos informó que para el ingreso a las instalaciones de la empresa es necesario entregar la cedula como un documento de identificación y previo a la entrega de este documento se le entrega al visitante un carnet de identificación, sin embargo no se mantiene una política ni documentada ni implementada de los requisitos específicos y no se sabe cuál es la frecuencia con que se cambian los mismos	**Obs**

- Revocar las identificaciones de empleados cesantes y las identificaciones vencidas de visitantes (por ej. Placas de identificación).	
Se consultó con el personal administrativo de Coral Hipermercado de grupo GO y no nos proporcionaron información sobre si las identificaciones de los empleados cesantes así como de los visitantes que se encuentren vencidas sean revocadas ni tampoco existe conocimiento de que exista una política.	**Obs**
Req. 9.2b Observar los procesos para identificar y distinguir entre empleados y visitantes y verificar que los visitante s están claramente identificados, y que es fácil distinguir entre empleados y visitantes.	
Se pudo revisar la política de seguridad y se evidencio que no se mantienen procesos de identificación para la distinción de empleados y visitantes, sin embargo a pesar de no existir una normativa documentada, este proceses existe de forma verbal y de conocimiento general para la parte de seguridad de la empresa ya que se nos dio a conocer que para los empleados se tiene ubicado un uniforme, para el ingreso a las instalaciones se les asigna un clave para la marcación de entradas y salidas, mientras que para los visitantes se mantienen carnets de identificación y se les pide la cedula hasta su devolución en la salida de las instalaciones, sin embargo no se nos mencionó que lleven a cabo un procedimiento más riguroso, o que se basen en una normativa.	**Obs**
Fuente: Coral Hipermercado Racar Plaza (GO).	
Req. 9.2c Verificar que el acceso al proceso de identificación (como el sistema de placas) este limitado solo al perso nal autorizado.	
Al entrevistar al personal de seguridad de Coral Hipermercado nos informaron que solo ellos (Guardias de Seguridad) son los encargados de entregar las autorizaciones para los visitantes o empleados nuevos, sin embargo se observó que no se existe responsabilidad sobre el proceso puesto que no se mantiene un registro de autorización mediante algún oficio o documento de respaldo, no existe un registro de las visitas, y esto puede dar lugar a que tampoco se	**Obs**

tenga certeza de que personas llegan a las instalaciones como visitantes realmente y no sean infiltrados con intenciones no acordes a la institución.	
Req. 9.2d Revisar los métodos de identificación implementados (como placas de identificación) para verificar qu e identifiquen, claramente a los visitantes, también verificar que sea fácil realizar una distinción entre empleados y visitantes.	
Como se puede observar en la foto a continuación el departamento de seguridad se encarga del ingreso de visitantes mediante la entrega de carnets en donde no se registra el nombre de las persona pero si se indica a donde se dirige y que es un visitante, por lo que sí existe una identificación fácil de empleados y visitantes pero de forma visual ya que no se mantiene una normativa, políticas o procedimientos establecidos que se renueven requisitos o monitoreo del ingreso de personas externas a la organización, se debería tener en cuenta para reforzar los procesos de identificación y distinción.	√
Departamento administrativo Coral Hipermercado (GO).	

Fuente: Coral Hipermercado Racar Plaza (GO).

Conclusiones y recomendaciones:

Se concluyó en que primero no existen procesos documentados que permitan socializar la distinción entre empleados y visitantes, por lo que no se puede saber si los requerimientos que se solicitan para el ingreso a las instalaciones son los más adecuados, si se revocan o no las identificaciones cesantes o quien realiza el manejo de los carnets que se entregan y que existan o no las autorizaciones debidas ya que según lo que se nos ha informado en las entrevistas realizadas al personal administrativo todo el procedimiento que se sigue para visitas en verbal, existe una autorización verbal, y se sigue las actividades que se han venido haciendo desde tiempo atrás. Se podría mejorar la seguridad para las instalaciones. Solicitar una autorización u oficio previo para el ingreso sería de gran ayuda, mantener un registro de visitas, y sobretodo asignar un acompañante para los visitantes hasta verificar que lleguen al lugar que han indicado dirigirse y con la persona que solicitan.

Elaborado por: Autoras.

ANEXO 14: PAPELES DE TRABAJO DEL REQUERIMIENTO 9. Restringir el acceso físico a los datos del titular de la tarjeta.

(9.3)

Papeles de Trabajo				
Cumplimiento Normativa PCI DSS				
Empresa auditada:	Coral Hipermercado Racar Plaza GO.		**Ref:** Req. 9.3	
Periodo a examinar:	Periodo 2015 con corte a Junio.			
Supervisa:	Estefanía Ortega	**Responsable:**	Patricia Benenaula	
Tema:	Cumplimiento de la Normativa PCI DSS Requerimiento 9. Restringir el acceso físico a los datos del titular de la tarjeta.		**Codigo:**	PT003
Objetivo:	Observar que se controle el acceso físico de los empleados a las áreas confidenciales.			
Alcance:	En el caso de un grupo de empleados con acceso físico al CDE (entorno de datos del titular de la tarjeta), entrevistar al personal responsable y observar las listas de control de acceso para verificar que:			
Procedimiento:				
***Se autorice el acceso al CDE (entorno de datos del titular de la tarjeta)**				
***La persona necesita acceder para realizar su trabajo.**				
Al realizar la entrevista al personal encargado de las Bases de Datos de Coral Hipermercado se pudo conocer que primero no existe un CDE (Entorno de datos del titular de la tarjeta) puesto que como se comentó con anterioridad Coral Hipermercado no almacena datos de titulares de tarjetas, sin embargo existe un registro de información básica de las tarjetas (mencionadas en anteriores requisitos) las mismas que se registran en la Base de Datos manejada por los servidores transaccionales quienes a mas dan soporte para los sistemas de facturación mediante acceso remoto.				

Se nos informó que no existe un listado de control de acceso en este caso a la base de datos en este caso de información básica de la tarjeta ya que esta es una función necesaria diariamente en el caso de sistema de facturación para realizar las transacciones con tarjetas de pago en caso de necesitarse soporte pero estos realizan el ingreso cuando es exclusivamente necesario según se nos informa para la realización de sus labores.	√

No se nos ha pedido una revisión de la política sin embargo se revisó y se puede visualizar en las siguientes imágenes que la política de seguridad de Coral Hipermercado si mantiene un detalle de procedimientos para el uso adecuado de Datos Confidenciales de Tarjetas de Crédito a pesar de que la organización no almacene los datos de titulares de tarjetas como se mencionó ya anteriormente.

Política de seguridad de Coral Hipermercado (GO) Procedimientos para uso adecuado de datos de Tarjetas.

Coral hipermercado Racar plaza mantiene un procedimiento de manejo adecuado de datos confidenciales de tarjetas de crédito, mismo que según lo observado en las entrevistas realizadas al personal administrativo si se lleva a cabo. √√

PROCEDIMIENTOS PARA USO ADECUANDO DE DATOS CONFIDENCIALES DE TARJETAS DE CREDITO

Considerando el pago vía tarjetas de crédito, es indispensable fomentar la seguridad de los datos de un titular de una tarjeta y optar por medidas de seguridad consistentes y reconocidas a nivel mundial.

Comenzando por aplicar los principales principios ya definidos en las políticas de seguridad tales como:

- Desarrollar y mantener una red segura,
- Mantener un programa de administración de vulnerabilidades
- Implementar medidas sólidas de control de acceso.
- Mantener una política de seguridad en la información.
- Supervisar y evaluar las redes con regularidad

En estos casos se determina el siguiente procedimiento o política con el objeto de que lo hagan uso las entidades que se relacionen con su manejo, sean estos desarrolladores, implementadores, cajeros, administradores, etc.

Estarán regidos por las siguientes cláusulas

- Solamente se accederá a la información *necesaria* de la tarjeta.
- Bajo ninguna circunstancia se almacenará el contenido de los tracks de las tarjetas aun considerando que estas puedan almacenarse encriptadas.
- En el caso de transmitir datos temporales de tarjetas por la red, hacerlo mediante técnicas de encriptación de datos.
- Únicamente se deben recibir los datos confidenciales, procesarlos para la autorización y luego borrarlos, incluso si son cifrados.
- Bajo ninguna circunstancia se almacenará el código o valor de verificación de la tarjeta (número de 3 o 4 dígitos impresos en el anverso o reverso del plástico)
- Tampoco almacenar el número de identificación persona (PIN).
- Enmascarar tanto el PIN como el PAN en la pantalla y en cualesquier documento impreso o en el peor de los casos poner a la vista únicamente los primeros 6 y los últimos 4 dígitos.

Es necesario **proteger los datos del titular de la tarjeta** sin considerar si éstos fueron almacenado o no. Si se reciben y/o borran datos de autenticación confidenciales es imprescindible que se ponga en práctica procesos de eliminación de datos, a fin de controlar que los datos sean irrecuperables.

El principio al que se pretende alcanzar es NO almacenar datos de autenticación confidenciales después de la autorización financiera, incluso si estos se los pretende mantener de forma encriptada.

Para el caso de procesar tarjetas de crédito de cualesquier entidad financiera es posible que sea necesario retener elementos de la banda magnética por un tiempo mínimo determinado (hasta realizar la autorización), tales como:

- El nombre del titular de la tarjeta
- El número de cuenta principal (PAN)
- Fecha de Vencimiento
- Código de servicio.

- Estos medios serán destruidos cuando ya no sean necesarios para la empresa; para el caso, se procederá de acuerdo a las normas de destrucción de información que se han establecido en las políticas de seguridad, asegurándose de que no se puedan reconstruir datos ni acceder a sus partículas.

Fuente: Coral Hipermercado Racar Plaza (GO).

Req. 9.3b Observar el acceso del personal al CDE (entorno de datos del titular de la tarjeta) para verificar que todo el personal tenga autorización antes de que accedan.

Si bien cada empleado según sus funciones mantienen acceso al entorno de datos del titular de la tarjeta (Datos básicos en Cajas y Base de Datos) pero no se realiza la firma de un formulario al empleado en donde se especifique que es una autorización para el respaldo de la responsabilidad que mantiene el empleado al acceder al entorno de los datos.	**Obs**

Req. 9.3c Seleccionar un grupo de empleados que hayan dejado de trabajar recientemente y revisar las listas de co ntrol de acceso para verificar que no tenga acceso físico al CDE (entorno de datos del titular de la tarjeta).

Se observó las listas que se manejan en las bases de datos de los empleados que se encuentran activos así como de los cesantes (De un registro de 16 empleados por día se seleccionó 9 aleatoriamente) se observó que lo empleados que se desvinculan de la organización no son eliminados del sistema sino mantenidos como inactivos para tener un histórico como se especifica en la normativa de seguridad de Coral Hipermercado, sin embargo nos informó el personal encargado del control de la base de datos que una vez que un empleado se desvincula de la organización	√

el departamento de recursos humanos se encarga de realizar la eliminación del acceso a todos los sistemas, con lo que el riesgo de este requerimiento se minimizaría.	
Fuente: Coral Hipermercado Racar Plaza (GO).	
Conclusiones y Recomendaciones:	
Coral Hipermercado de Grupo GO no almacena datos de Titulares de tarjetas sin embargo los datos básicos que se almacenan por control de registro de transacciones de los titulares de las tarjetas mantiene un procedimiento documentado, sin embargo se recomendaría que el mismo sea monitoreado, actualizado y verificar que sea de conocimiento de todo el personal, puesto que varios accesos no cuentan con las debidas autorizaciones solo se realiza por un medio informativo oral pero no se realiza el llenado de un formato de autorización previamente firmado y que sirva como respaldo.	
Elaborado por: Autoras.	

ANEXO 15: PAPELES DE TRABAJO DEL REQUERIMIENTO 9. Restringir el acceso físico a los datos del titular de la tarjeta. (9.4)

Papeles de Trabajo
Cumplimiento Normativa PCI DSS

Empresa auditada:	Coral Hipermercados Racar Plaza GO.		**Ref:** Req. 9.4	
Periodo a examinar:	Periodo 2015 con corte a Junio.			
Supervisa:	Estefanía Ortega	**Responsable:**	Patricia Benenaula	
Tema:	Cumplimiento de la Normativa PCI DSS Requerimiento 9. Restringir el acceso físico a los datos del titular de la tarjeta.		**Código:**	**PT004**
Objetivo:	Verificar que se hayan implementado procedimientos para identificar y autorizar a los visitantes.			
Alcance:	Verificar que los controles de acceso y las autorizaciones de los visitantes se implementen de la siguiente manera:			
Procedimiento:				
*Observar los procedimientos y entrevistar al personal para verificar que los visitantes reciben autorización antes de acceder a áreas de procesamiento o almacenamiento de los datos del titular de la tarjeta y que estén siempre acompañados.				
Política de seguridad de Coral Hipermercado (GO).				
La política de seguridad no detalla un procedimiento exclusivo para la administración del ingreso de visitantes, sin embargo se menciona que para el ingreso se entregaran placas, y que está prohibido el acceso a personal no autorizado, solicitando la cedula de identidad pero no se menciona nada sobre el acompañamiento, requisitos, autorizaciones entre otros parámetros por lo que la normativa no se encuentra completa para la garantía de seguridad contra posibles agentes externos con intenciones maliciosas.			**Obs**	

3.- POLITICAS DE SEGURIDAD AMBIENTAL

- Definir claramente el perímetro de seguridad.
- Totalmente prohibido el acceso de personal no autorizado al centro de cómputo principal y alterno.
- Todas las puertas de incendio de un perímetro de seguridad deben tener alarma y cerrarse automáticamente.
- El acceso a los pisos superiores del edificio deberá ser controlado por el personal de seguridad, solicitando a la persona su cédula de ciudadanía / identidad o pasaporte.
- Deberá ser entregado un carné de visitante en el cual se detallará el piso al que tiene acceso.
- Si se encuentra a una persona en un piso diferente al indicado en el carné, es responsabilidad de todos los empleados notificar inmediatamente a seguridad.
- El acceso de los empleados a cada piso será controlado por una tarjeta magnética.
- El acceso al centro de cómputo será controlado por una tarjeta magnética. Esta será exclusiva de personal autorizado de la división de Tecnología y Sistemas.

En la entrevista realizada al personal se nos informó que las autorizaciones para previas visitas no se realizan mediante formularios o formatos documentados sino que en su mayoría son solamente autorizadas mediante llamadas telefónicas que realizan los altos mandos por lo que no se está cumplimiento con la norma persistiendo un

Entrevista al personal administrativo grupo (GO) Carnet de Visitante

riesgo para la organización.

- Deben planificarse continuamente escenarios de evacuación del edificio para casos de incendio, amenazas de bombas, entre otros.
- Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.
- Deberán implementarse procedimientos para recuperarse después de situaciones adversas tal como son:
  - ❖ Incendios
  - ❖ Robos
  - ❖ Inundaciones
  - ❖ Manifestaciones
  - ❖ Terremotos
  - ❖ Humo
  - ❖ Polvo
  - ❖ Vibraciones
  - ❖ Efectos Químicos
  - ❖ Radiación Electromagnética
  - ❖ Explosiones

Ing. Juan Paulino Quinde N. Seguridad de la Información / 2013

Políticas y Procedimientos de Seguridad V1.1

- ❖ Fallas Eléctricas
- ❖ Amenazas de bomba
- ❖ Virus Informático
- ❖ Negación de Servicios Informáticos

- Los edificios deben ser discretos y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores, que identifiquen la presencia de actividades de procesamiento de información
- Las funciones y el equipamiento de soporte, por ejemplo: fotocopiadoras, máquinas de fax, deben estar ubicados adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
- Las puertas y ventanas deben estar bloqueadas cuando no hay vigilancia y debe considerarse la posibilidad de agregar protección externa a las ventanas, en particular las que se encuentran al nivel del suelo.
- Se deberán implementar adecuados sistemas de detección de intrusos. Los mismos deben ser instalados según estándares profesionales y probados periódicamente.
- Estos sistemas comprenderán todas las puertas exteriores y ventanas accesibles. Las áreas vacías deben tener alarmas activadas en todo momento. También deben protegerse otras áreas, como la sala de cómputos o las salas de comunicaciones

Hemos observado el procedimiento de visita de una persona externa a las instalaciones de Coral Hipermercado Racar plaza y se ha evidenciado que se mantiene un control de ingreso mediante asignación de carnets de identificación mediante la entrega de la cedula de identidad por parte del visitante pero no se realiza una verificación de previa autorización por parte de las autoridades administrativas, no se firma ningún formulario solamente se da aviso mediante vía oral (telefónica).

Obs

Fuente: Coral Hipermercado Racar Plaza (GO).

***Observar el uso de las placas para visitantes u otro tipo de identificación a fin de verificar que las placas de identificación física no permitan el acceso sin acompañantes a áreas físicas donde se procesan o conservan datos del titular de la tarjeta.**

El departamento de seguridad de coral hipermercado Racar plaza mantiene carnets de identificación para visitantes, sin embargo si se permite el acceso a áreas físicas sin acompañantes pero también cabe recordar que Coral Hipermercado

no almacena datos de titular de tarjeta puesto que se minimizaría este riesgo, por otro lado seria riesgoso para los departamentos de crédito en donde se manejan en parte los vouchers y demás documentación pero para el ingreso o visita se necesita una autorización previa de gerencia sin embargo no se maneja formatos solo se realiza la autorización mediante comunicación oral.	**Obs**
Req. 9.4.2 a. Observar las personas dentro de las instalaciones para verificar que se usen placas para visitantes u otro tipo de identificación y que los visitantes se puedan distinguir fácilmente de los empleados que trabajan en la empresa.	
El departamento de seguridad como método de identificación de visitantes de empleados usan carnets de identificación para visitantes y los empleados se encuentran registrados los mismos que realizan sus marcaciones tanto para entrada como salida de sus labores, a más de tener sus respectivos uniformes, por lo que sí existe una distinción sin embargo el riesgo no se minimizaría del todo puesto que no se realiza una gestión de seguridad para el otorgamiento de los carnets de visitantes.	√
Req. 9.4.2 b Verificar que las placas para visitantes y otro tipo de identificación tengan vencimiento.	
Se revisaron los carnets y se pudo observar que no mantienen una seguridad adecuada puesto que no conllevan identificación del visitante y no tiene fecha de caducidad solo sirve como un identificativo visual como se pudo observar anteriormente en la imagen del carnet que se otorga para las visitas.	**Obs**
Req. 9.4.3 Verificar y observar la salida de los visitantes de las instalaciones para verificar que se solicita la entrega de su placa o de otro tipo de identificación al partir o al momento del vencimiento.	
Se observó la salida de los visitantes de las instalaciones de Coral Hipermercado, si bien al momento de su salida se	

comprobó que se realiza la entrega del carnet de identificación como visitante al personal de seguridad de la entidad para que de igual manera le sea devuelto al visitante su documento de identificación que le fue retenido para su ingreso a las oficinas.	√
Req. 9.4.4 Verificar y comprobar que se implemente un registro de visitantes para registrar el acceso físico a la s instalaciones, así como también a las salas de informática y a los centros de datos donde se almacenan o transmiten los datos del titular de la tarjeta.	
Como habíamos mencionado Coral Hipermercado no almacena datos de titular de tarjeta sin embargo tampoco se lleva un registro de visitantes a las instalaciones de las oficinas departamentales solo se pide la cedula de los mismos en su ingreso y se les es devuelta a la salida sin realizar ningún registro.	**Obs**
Fuente: Coral Hipermercado Racar Plaza (GO).	
9.4.4 b Verificar que el registro incluya: 1. nombre del visitante, 2. empresa representada, 3. empleado que autoriz a el acceso físico.	
El departamento de seguridad (guardias encargados del ingreso de visitantes) nos han informado que no se lleva un registro de visitantes ni de su ingreso ni salida de las instalaciones, solo se verifica mediante la entrega y devolución de la cedula como ya se mencionó anteriormente.	**Obs**
9.4.4 c Verificar que el registro se conserve durante tres meses como mínimo a menos que la ley estipule lo contr ario.	
No se llevan a cabo registros de visitantes, no se cumple con este requerimiento.	**Obs**
Fuente: Coral Hipermercado Racar Plaza (GO).	
Conclusiones y recomendaciones:	
Coral Hipermercado de Grupo Ortiz no mantiene un adecuado control de ingreso de los visitantes existen varias falencias como la falta de registros de ingresos y personal que autoriza las visitas (formularios debidamente firmados y autorizados por un superior), placas de identificación con fecha	

de vencimiento y que permitan la adecuada diferenciación de visitantes así como el proceso de administración al permitir que el visitante ingrese sin la compañía en todo momento de un empleado.
Elaborado por: Autoras.

ANEXO 16: PAPELES DE TRABAJO DEL REQUERIMIENTO 9. Restringir el acceso físico a los datos del titular de la tarjeta. (9.5)

Papeles de Trabajo			
Cumplimiento Normativa PCI DSS			
Empresa auditada:	Coral Hipermercados Racar Plaza GO.		**Ref:** Req. 9.5
Periodo a examinar:	Periodo 2015 con corte a Junio.		
Supervisa:	Estefanía Ortega	**Responsable:**	Patricia Benenaula L.

Tema:	Cumplimiento de la Normativa PCI DSS Requerimiento 9. Restringir el acceso físico a los datos del titular de la tarjeta.	**Código:**	PT005
Objetivo:	Verificar que se protejan físicamente todos los medios.		
Alcance:	Verificar que los procedimientos para proteger los datos del titular de la tarjeta incluyan controles para el resguardo seguro de todos los medios (entre otros, computadoras, dispositivos electrónicos extraíbles, recibos e informes en papel y faces).		
Procedimiento:			
Req. 9.5 Verificar que los procedimientos para proteger los datos del titular de la tarjeta incluyan controles para el resguardo seguro de todos los medios (entre otros, computadoras, dispositivos electrónicos extraíbles, recibos e informes en papel y faxes).			
Política de seguridad de Coral Hipermercado (GO).			

16.- POLITICAS DE REVISION DEL PERIMETRO DE SEGURIDAD

Con el objeto de proteger los datos (propietarios, confidenciales o de cualquier otro tipo), se considerará mantener ciertos servicios en marcha tales como servidor de correo, servidor www, etc.), el ámbito de protección contempla daños tanto el hardware, daños malintencionados, borrados, etc. Actualmente las probabilidades de que ocurra un "mal" suceso es muy amplio, pruebas de red, intrusiones físicas, ingeniería social y muchas otras ocurren a diario y no estamos exentos de entre tantas empresas que han sido víctimas de pérdida de información sensible.

Es necesario listar todos aquellos recursos (servidores, servicios, datos y otros componentes) que contengan datos, den servicios y formen parte de nuestra infraestructura. A continuación detallamos una pequeña lista de acuerdo a lo que hemos considerado puede afectar al grupo:

- Recursos a proteger
  - Servidores físicos
  - Servidores de correo y servicios
  - Servidores de DNS y servicios
  - Servidores de WWW y servicios
  - Servidores de ficheros y servicios
  - Datos internos de la compañía, como registros contables.
  - Infraestructura de la red (cables, hubs, switches, routers, etc.)
  - Sistema telefónico (PBX, buzones de voz, etc.)
- Que vamos a proteger de estos recursos.
  - Daños físicos (humo, agua, comida, etc.)
  - Borrado / modificación de datos (registros contables, deterioro de tu sitio web, etc.)
  - Exposición de datos (registros contables, etc.)
  - Continuidad de servicios (mantenimiento activo de los servidores de correo/www/ficheros).

√√

Dentro de la política de seguridad de Coral Hipermercado existe un procedimiento de seguridad para la protección de los medios con el objetivo de proteger los datos confidenciales, dando a conocer que tipo de recursos se protegerán, de que circunstancias se deben resguardar y a mas explica las vulnerabilidades a las que estaríamos expuestos en caso de no llevar a cabo este sistema de protección. Se realizó una visita a las instalaciones y se pudo observar que el resguardo de los

medios es seguro, existe seguridad física, cámaras de seguridad,

señalización contra incendios y el ingreso a las instalaciones depende de quien lo autorice informando al personal de seguridad previamente pero de forma verbal.

- Evitar que otros hagan uso ilegal/impropio de tus servicios (envíos masivos de correos, etc.)

- A que estamos expuestos.
  - Escaneos de red
  - Ingeniería social – varía, normalmente suelen ser objetivo la gente más vulnerable
  - Intrusión física. Es bastante rara, pero un empleado hostil con un par de alicates podría causar mucho daño en un armario de telecomunicaciones.
  - Empleados que venden datos a la competencia – ocurre
  - La competencia, que alquile a gente especializada para penetrar activamente en tu red nadie suele hablar de esto, pero también ocurre.

Ahora, definido la lista de los recursos a asegurar y con el objeto de atenuar la seguridad de datos de la institución, el personal técnico y el que se relaciona directamente con hardware y software deben realizar su hardening respectivo, el mismo que será verificado y observado por el departamento de seguridad antes de que este sea puesto en producción, aquí se tomará en cuenta lo siguiente:

Es imprescindible el upgrade del firmware , contraseñas complejas, configuración de la Bios, deshabilitar inicios de sistemas por cualesquier unidad para evitar cualesquier entrada de malware, tanto como considerar por lo menos 2 particiones primarias (una de OS y otra de archivos importantes) considerando como mínima seguridad en la información, evitando de esa manera cualesquier componente innecesario.

Req. 9.5.1 Almacenar los medios de copias de seguridad en un lugar seguro, preferentemente, en un lugar externo a la empresa como un centro alternativo o para copias de seguridad o en un centro de almacenamiento comercial. Revise la seguridad de dicho lugar una vez al año como mínimo.
*** Observar la seguridad física del lugar de almacenamiento para confirmar que el almacenamiento del medio de la copia de seguridad este protegido**
Se conversó con el personal administrativo de Coral Hipermercado y se nos indicó que en cada base de datos remota existe una réplica en Stanby que se usa como contingente en caso de pérdida de la base de datos.
Instalaciones de Coral Hipermercado (GO).

√

Como se mencionó en el requerimiento anterior (Req. 9,4) Coral Hipermercado de Grupo GO no almacena los datos de titulares de tarjetas por lo que este riesgo se minimizaría sin embargo, los

		medios como computadores, Medianet, Switch transaccionales, sistema de redes se encuentran respaldados por los guardias de seguridad de la planta (existe una seguridad específica para el departamento por los guardias que se encargan de la seguridad de todo el almacén). Sin embargo se mantiene el servidor de red que si se encuentra en un lugar externo a las instalaciones del local.
Fuente: Coral Hipermercado Racar Plaza (GO).		
***Verificar que la seguridad del lugar de almacenamiento se revise, al menos una vez por año.**		
La seguridad de los lugares donde se mantienen los equipos, dispositivos, telecomunicaciones, Switch entre otros medios si se mantienen en constante revisión y supervisión a cargo del departamento de seguridad y de los empleados que están asignados para sus labores.		√
Conclusiones y recomendaciones:		
Coral Hipermercado no mantiene dispositivos o medios de almacenamiento de datos de los titulares de tarjetas, se maneja, los computadores del		

sistema de facturación, Switch o Medianet por donde se realiza el pago con tarjetas de pago, y demás sistemas de red por donde se realiza toda la transaccionalidad del negocio, según lo observado se ha podido comprobar que se mantiene una seguridad contra posibles vulneraciones de personas externas a la organización mal intencionados.
Elaborado por: Autoras.

ANEXO 17: PAPELES DE TRABAJO DEL REQUERIMIENTO 9. Restringir el acceso físico a los datos del titular de la tarjeta. (9.6)

Papeles de Trabajo		
Cumplimiento Normativa PCI DSS		
Empresa auditada:	Coral Hipermercados Racar Plaza GO.	**Ref:** Req. 9.6

Periodo a examinar:	Periodo 2015 con corte a Junio.			
Supervisa:	Estefanía Ortega	**Responsable:**	Patricia Benenaula	
Tema:	Cumplimiento de la Normativa PCI DSS Requerimiento 9. Restringir el acceso físico a los datos del titular de la tarjeta.		**Código:**	PT006
Objetivo:	Verificar que se lleve un control estricto de la distribución interna o externa de todos los tipos de medios.			
Alcance:	Verificar que exista una política para controlar la distribución de medios y que dicha política abarque todos los medios distribuidos, incluso los que se distribuyen a personas.			

Procedimiento:

Req. 9.6 Verificar que exista una política para controlar la distribución de medios y que dicha política abarque todos los medios distribuidos, incluso los que se distribuyen a personas.

No se nos otorgó información de cómo se realiza la distribución de medios físicos ni documentación que registran Coral Hipermercado, sin embargo según lo informado por el personal del departamento de tarjetas de crédito nos indican que los voucher se almacenan (documentación) por clasificaciones y se mantiene un histórico (no se elimina). De las bases de datos no se informó cómo se realiza el acceso ni el respaldo de las mismas.

Política de seguridad de Coral Hipermercado (GO).

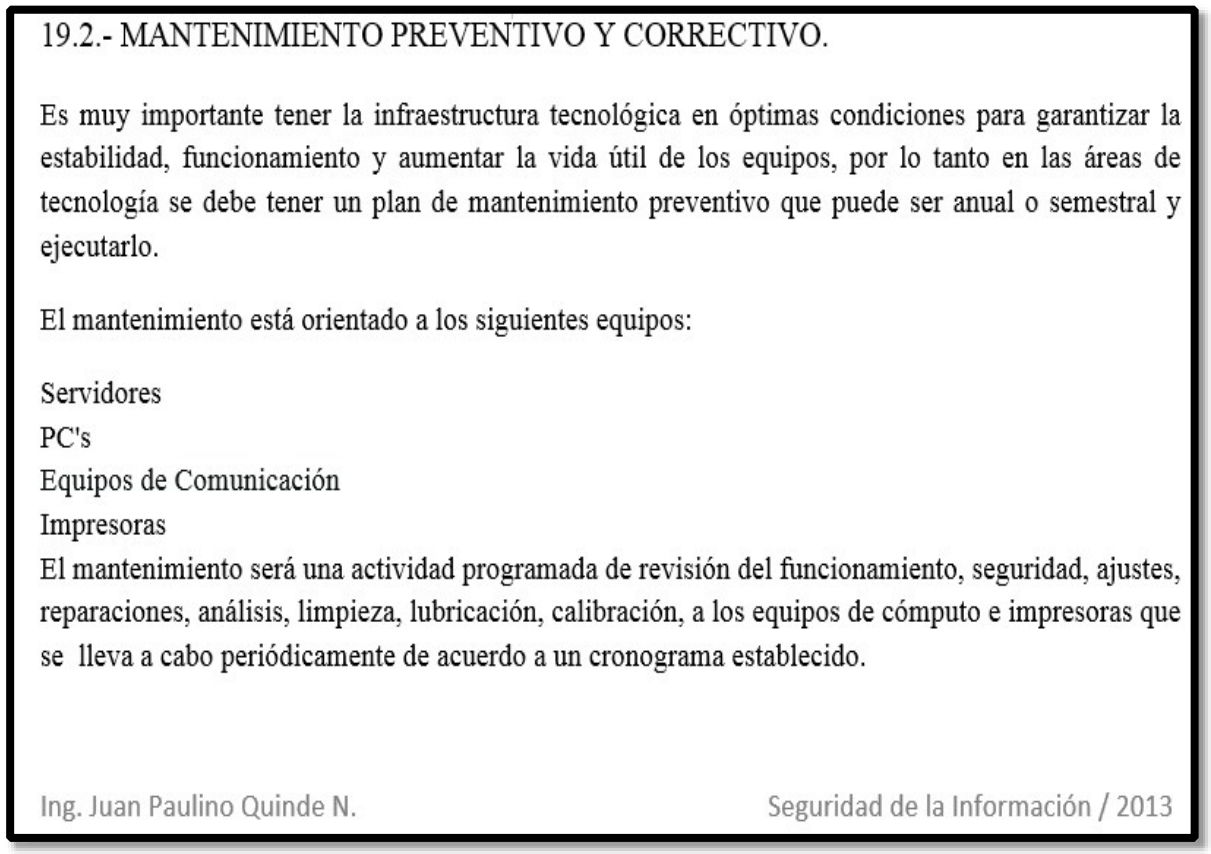
13.9.- SEGURIDAD EN LA BASE DE DATOS • De ser posible no use consultas con parámetros. • Utilizar la validación de la entrada y la codificación de salida. Si estos fallan, no ejecute el comando de base de datos	**marca** ∅

	Dentro de la política de seguridad de Coral Hipermercado contempla la seguridad en la base de datos, lo que se puede entender es el procedimiento que mantienen para la protección de estos datos mismos que podrían ser distribuidos en medios sin embargo esto no nos ha quedado claro puesto que es información que no se detalló al consultar en la Empresa.
Req. 9.6.1 Verificar que todos los medios se hayan clasificado para poder determinar la confidencialidad de los datos.	
Este requerimiento no se realizaría puesto que coral hipermercados Racar plaza no almacenan datos de titulares de tarjetas.	
Req. 9.6.2a Entrevistar al personal y revisar los registros para verificar que todos los medios enviados fuera de la empresa esten registrados y se envien por correo seguro u otro método de envió que se pueda rastrear.	
No se logró obtener esta información, sin embargo Coral Hipermercado no almacena datos del titular de la tarjeta que deban ser enviados por medios por lo que este riesgo se minimizaría.	
Req. 9.6.2b Seleccionar una muestra actual de varios días de registros de seguimiento externos de todos los medios y verificar que se documenten los detalles de seguimiento.	
Este requerimiento no aplicaría puesto que Coral Hipermercado no almacena datos de titulares de tarjetas.	
Req. 9.6.3 Asegurarse de que la gerencia apruebe todos y cada uno de los medios que se trasladen desde un área seguro (incluso cuando se	

distribuyen los medios a personas).
***Seleccionar una muestra actual de varios días de registros de seguimiento externos de todos los medios, mediante la evaluación de los registros y las entrevistas al personal responsable, verificar que se cuente con la debida autorización de la gerencia cuando sea necesario trasladar los medios desde un área segura (incluso: cuando los medios se distribuyen a personas).**
Este requerimiento no aplicaría puesto que Coral Hipermercado no almacena datos de titulares de tarjetas.
Fuente: Coral Hipermercado Racar Plaza (GO).
Conclusiones y recomendaciones:
Coral Hipermercado no almacena datos de titular de tarjetas por lo tanto no existe el riesgo de almacenamiento de este tipo de información en medios o dispositivos, sin embargo para otro tipo de información que se respalden en medios, como por ejemplo las bases de datos como se puede evidenciar en el fragmento de la política se mantienen las precauciones de ser el caso para su manejo y según lo informado por el personal administrativo para la distribución se utiliza la conexión mediante acceso remoto.
Elaborado por: Autoras.

ANEXO 18: PAPELES DE TRABAJO DEL REQUERIMIENTO 9. Restringir el acceso físico a los datos del titular de la tarjeta. (9.7)

Papeles de Trabajo				
Cumplimiento Normativa PCI DSS				
Empresa auditada:	Coral Hipermercados Racar Plaza GO.		**Ref:** req. 9.7	
Periodo a examinar:	Periodo 2015 con corte a Junio.			
Supervisa:	Estefanía Ortega	**Responsable:**	P atricia Benenaula	
Tema:	Cumplimiento de la Normativa PCI DSS Requerimiento 9. Restringir el acceso físico a los datos del titular de la tarjeta.		**Código:**	PT007
Objetivo:	Verificar que se lleve un control estricto del almacenamiento y la accesibilidad de los medios.			
Alcance:	Obtener y revisar la política para controlar el almacenamiento y el mantenimiento de todos los medios y verificar que la política requiera inventarios periódicos de medios.			
Actividades:				
Req. 9.7 Obtener y revisar la política para controlar el almacenamiento y el mantenimiento de todos los medios y verificar que la política requiera inventarios periódicos de medios.				
Política de seguridad de Coral Hipermercado (GO).				



19.2.- MANTENIMIENTO PREVENTIVO Y CORRECTIVO.

Es muy importante tener la infraestructura tecnológica en óptimas condiciones para garantizar la estabilidad, funcionamiento y aumentar la vida útil de los equipos, por lo tanto en las áreas de tecnología se debe tener un plan de mantenimiento preventivo que puede ser anual o semestral y ejecutarlo.

El mantenimiento está orientado a los siguientes equipos:

Servidores
PC's
Equipos de Comunicación
Impresoras

El mantenimiento será una actividad programada de revisión del funcionamiento, seguridad, ajustes, reparaciones, análisis, limpieza, lubricación, calibración, a los equipos de cómputo e impresoras que se lleva a cabo periódicamente de acuerdo a un cronograma establecido.

Ing. Juan Paulino Quinde N. Seguridad de la Información / 2013

√√

Al observar la política de seguridad de Coral

Hipermercado se comprobó que se hace referencia sobre lo importante que es tener en óptimas condiciones la infraestructura informática, siendo necesario mantener un plan preventivo de mantenimiento para lograr una mayor estabilidad, funcionamiento de los mismos, donde se revisara la seguridad y funcionamiento periódico según lo establecido.

*La política menciona además

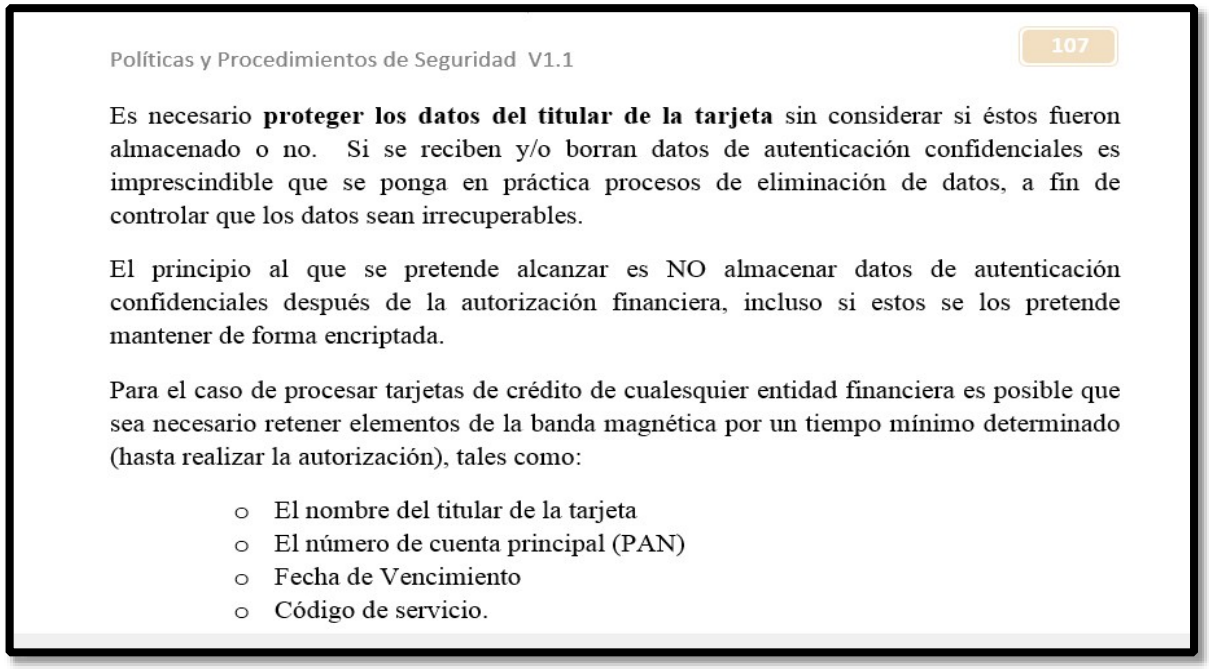
19.3.- PREPARACION DE HARDWARE Y SOFTWARE. El departamento de TI mediante su respectivo personal realizará la entrega de los equipos de cómputo y demás equipos instalados y debidamente configurados en la ubicación o sitio que nos indique el requerimiento o el usuario y listos para entrar en operación, dentro de las actividades que se realiza se encuentran las siguientes: • Instalación del sistema operativo que el usuario necesite • Instalación de antivirus • Inventariados y etiquetados • Instalación de herramientas ofimáticas • Aplicación de parches y actualizaciones a las aplicaciones • Instalación de las aplicaciones de gestión del negocio • Actas de entrega de equipo a los usuarios.	que una vez entregado los equipos a los respectivos usuarios se realizara un inventario de los mismos pero no se menciona nada acerca de la revisión periódica de los mismos y a mas según lo observado en las visitas se nos informó que el personal desconoce de un registro de los medios con su numeración a quien pertenece entre otros datos sin embargo esto es cuestión de aplicación de la normativa puesto que esta si contempla el inventario y asignación de los medios.
Fuente: Coral Hipermercado Racar Plaza (GO).	
req. 9.7.1 Revisar los registros de inventarios de medios para verificar que se conserven los registros y que se lleven a cabo inventarios de medios, al menos una vez al año.	
Se consultó con la administración de seguridad y se nos informó que si realizan inventarios de los dispositivos y medios pero que no se nos podría mostrar el registro.	∅

Conclusiones y recomendaciones:
Se concluyó que si se mantienen políticas para el mantenimiento de los medios, pero no se nos permitió observar el registro de inventariado de los medios del almacenamiento y accesibilidad de los mismos pero según nos informó personal administrativo no se les han realizado un monitorio o inventario periódico de los medios que se encuentran a cargo de los empleados y estos desconocen de que existan registros de estos medios.
Fuente: Coral Hipermercado Racar Plaza (GO).
Elaborado por: Autoras.

ANEXO 19: PAPELES DE TRABAJO DEL REQUERIMIENTO 9. Restringir el acceso físico a los datos del titular de la tarjeta. (9.8)

Papeles de Trabajo

Cumplimiento Normativa PCI DSS				
Empresa auditada:	Coral Hipermercados Racar Plaza GO.		**Ref:** req. 9.8	
Periodo a examinar:	Periodo 2015 con corte a Junio.			
Supervisa:	Estefanía Ortega	**Responsable:**	Patricia Benenaula	
Tema:	Cumplimiento de la Normativa PCI DSS Requerimiento 9. Restringir el acceso físico a los datos del titular de la tarjeta.		**Código:**	PT008
Objetivo:	Verificar que se destruyan los medios cuando ya no sea necesario guardarlos por motivos comerciales o legales.			
Alcance:	Revisar periódicamente la política de destrucción de medios y verificar que abarque todos los medios y que defina requisitos para:			
Procedimiento:				
*Los materiales de copias en papel se deben cortar en tiras, incinerarse o convertirse en pulpa para tener la certeza de que no podrán reconstruirse. *Los contenedores de almacenamiento que se usan para los materiales que se destruirán deben estar protegidos. *Los datos del titular de la tarjeta guardados en medios electrónicos deben permanecer irrecuperables medianet un programa con la función de borrado seguro de acuerdo con las normas aceptadas en la industria para lograr una eliminación segura o mediante la destrucción física de los medios.				
Observación. Si bien como se ha mencionado con anterioridad en otros requerimientos de la norma, Coral Hipermercado no almacena datos de titulares de tarjetas por lo que no aplicaría el cumplimiento de este requerimiento para la entidad sin embargo en la política de seguridad si se hace constar el procedimiento para destrucción de medios y se describe a continuación.				

Política de seguridad de Coral Hipermercado (GO). Protección datos del Titular	√√
	Esto es lo que especifica la política de seguridad de Coral Hipermercado acerca del almacenamiento y protección de datos del titular de la tarjeta.
Política de seguridad de Coral Hipermercado (GO). Destrucción de Medios	√√

PROCEDIMIENTO DE MANEJO, DISTRIBUCION Y DESTRUCCION DE INFORMACION.

La firma Gerardo Ortiz & Hijos ha considerado implantar políticas explícitas en cuanto al ciclo de vida de la información y tres etapas: generación, conservación y destrucción.

El objetivo principal es NO dejar brecha especialmente en la última fase de este proceso, en concreto la destrucción de datos confidenciales.

PCI-DSS establece que para que la información sea susceptible de protección esta debe de cumplir las siguientes características:

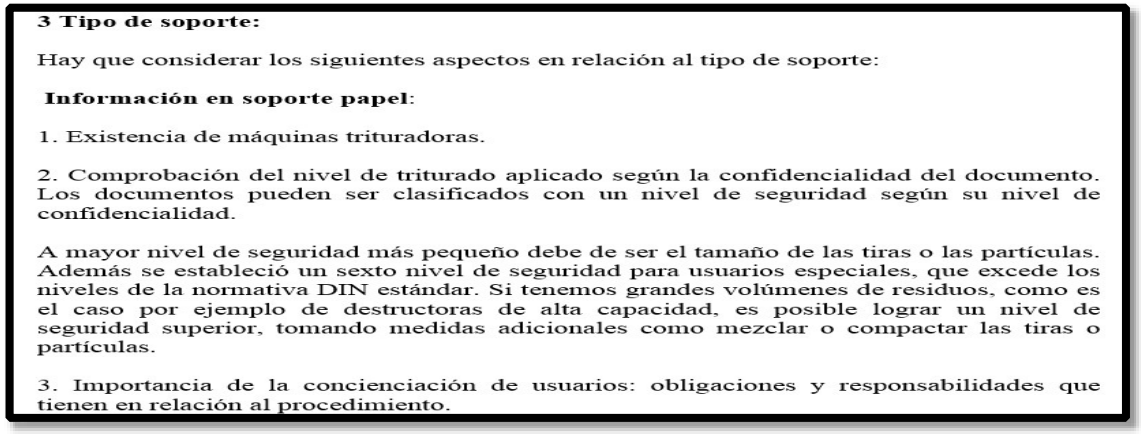
- Ser secreta, es decir que no sea generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza ese tipo de información.
- Tener un valor comercial por ser secreta.
- Haber sido objeto de medidas razonables para mantenerla secreta, tomadas por su titular.

Esto es lo que especifica la norma de seguridad de Coral Hipermercado en cuanto al procedimiento de destrucción de medios. Como podemos observar la normativa es muy específica en cuanto al detalle de las fases de destrucción de medios, procedimientos a seguir, el tipo de medios que se deben considerar, entre otros parámetros por lo que Coral Hipermercado si cumple con mantener dentro de sus políticas la revisión de medios.

La normativa, sobre protección de datos es muy estricta al respecto, exigiendo altos niveles de seguridad en la destrucción de documentos no sólo con soporte en papel, también se debe eliminar la información de plásticos, microfichas, formatos de almacenamiento ópticos (CD, CD-RW, HD DVD, VMD y Blue Ray) cintas de video, películas de triacetato y cualquier otro medio de almacenamiento, unidades flash USB, discos externos e internos, teléfonos móviles, PDA's, Tabletas, contendores multimedia, etc…

Ing. Juan Paulino Quinde N. Seguridad de la Información / 2013

Fuente: Coral Hipermercado Racar Plaza (GO).	
Req. 9.8.1a Entrevistar al personal y revisar los procedimientos para verificar que los materiales de copias en papel se corten en tiras, se incineren o se conviertan en pulpa para tener la certeza de que no podrán reconstruirse.	
Se observó en la entrevista realizada al personal de tarjetas de crédito, que para los vouchers se mantiene un archivo histórico y no se elimina los mismos de hecho se mantienen desde sus inicios en cartones en la misma área del departamento.	**Obs**
Req. 9.8.1b Revisar los contenedores de almacenamiento utilizados para los materiales que se destruyan y verificar que dichos contenedores estén asegurados.	
Coral Hipermercados de Grupo GO no almacenan datos del titular de la tarjeta, por lo que este requerimiento no aplica.	√
Req. 9.8.2 Verificar que los datos del titular de la tarjeta guardados en dispositivos electrónicos sean irrecuperables mediante un programa con la función de borrado seguro de acuerdo con las normas aceptadas por la industria para lograr una eliminación segura, o bien destruir los medios físicamente.	
Coral Hipermercado de Grupo GO no almacena datos del titular de la tarjeta, este requerimiento no aplica, Sin embargo la política de Coral Hipermercado en cuanto a lo mencionado sobre lo que manifiesta el requerimiento 7 si contempla dentro del documento de Política de Seguridad, detallamos a continuación:	√
Política de seguridad de Coral Hipermercado (GO) Destrucción de Medios	√



3 Tipo de soporte:

Hay que considerar los siguientes aspectos en relación al tipo de soporte:

Información en soporte papel:

1. Existencia de máquinas trituradoras.

2. Comprobación del nivel de triturado aplicado según la confidencialidad del documento. Los documentos pueden ser clasificados con un nivel de seguridad según su nivel de confidencialidad.

A mayor nivel de seguridad más pequeño debe de ser el tamaño de las tiras o las partículas. Además se estableció un sexto nivel de seguridad para usuarios especiales, que excede los niveles de la normativa DIN estándar. Si tenemos grandes volúmenes de residuos, como es el caso por ejemplo de destructoras de alta capacidad, es posible lograr un nivel de seguridad superior, tomando medidas adicionales como mezclar o compactar las tiras o partículas.

3. Importancia de la concienciación de usuarios: obligaciones y responsabilidades que tienen en relación al procedimiento.

La normativa detalla lo siguiente en cuanto al procedimiento de destrucción de medios en papel, discos duros y removibles, teléfonos celulares, tabletas, e imágenes y videos.

Fuente: Coral Hipermercado Racar Plaza (GO).

Conclusiones y recomendaciones:

Coral Hipermercado como se había mencionado con anterioridad no almacena datos del titular de la tarjeta lo que minimiza prácticamente todo el riesgo que contempla este requerimiento y además la empresa a pesar de no requerir el cumplimiento de este requerimiento si contemplan como un refuerzo procedimientos para la destrucción de medios e información confidencial para empresa.

Elaborado por: Autoras.

ANEXO 20: PAPELES DE TRABAJO DEL REQUERIMIENTO 9. Restringir el acceso físico a los datos del titular de la tarjeta. (9.9)

Papeles de Trabajo

Cumplimiento Normativa PCI DSS

Empresa auditada:	Coral Hipermercados Racar Plaza GO.		**Ref:** Req. 9.9
Periodo a examinar:	Periodo 2015 con corte a Junio.		
Supervisa:	Estefanía Ortega	**Responsable:**	Patricia Benenaula L.
Tema:	Cumplimiento de la Normativa PCI DSS Requerimiento 9. Restringir el acceso físico a los datos del titular de la tarjeta.	**Código:**	PT009
Objetivo:	Verificar que se protejan los dispositivos que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta para proporcionar protección contra alteraciones y sustituciones.		
Alcance:	Revisar las políticas y los procedimientos documentados para verificar que se realice lo siguiente:		
Procedimiento:			
***Conservar una lista de los dispositivos.**			
*** Inspeccionar los dispositivos periódicamente para buscar intentos de alteración o sustitución.**			
*** Capacitar al personal para que detecten comportamientos sospechosos e informen la alteración o sustitución de dispositivos.**			
Se conversó con el personal administrativo de cajas y se nos ha informado que no tienen conocimiento de la lista de dispositivos (POS) así como también no han observado que se les realice inspecciones periódicas de búsqueda de intentos de alteración o sustitución, nos indicaron que si se les realiza capacitaciones periódicas (cada 3 meses			

aproximadamente) pero sobre el uso de las tarjetas de crédito de los clientes, mas no se realiza una capacitación para que mantengan conocimientos sobre posibles eventos de alteración en los dispositivos. Adicional a esto la normativa de Seguridad de Coral Hipermercado no contempla procedimientos ni pollitas para el manejo y seguridad de los dispositivos que capturan datos de tarjetas de pago.	**Obs**
Req. 9.9.1 Revisar la lista de los dispositivos y verificar que incluya: *** Marca y modelo del dispositivo.** *** Ubicación del dispositivo (por ejemplo, la dirección de la empresa o de la instalación donde se encuentra el dispositivo).** *** Número de serie delo dispositivo u otro método de identificación única.**	
El personal administrativo de Coral Hipermercado nos informa que se les ha informado que si existe un listado de los dispositivos que manejan datos de tarjetas de pago pero que ellos desconocen de la lista ya que no se les ha permitido el acceso a esta o no se les ha socializado sobre su existencia.	**Obs**
Req. 9.9.1 b Seleccionar una muestra de dispositivos de la lista y observar la ubicación del dispositivo para verificar que la lista sea exacta y este actualizada.	
No existe esta información ya que los empleados desconocen de la ubicación y existencia de los supuestos listados que se les ha informado que si se manejan pero no ha habido ninguna socialización para el conocimiento de las mismas.	**Obs**
Req. 9.9.1c Entrevistar al personal para verificar que la lista de dispositivos se actualice cuando se agreguen, reubiquen, desactiven, etc., dispositivos.	
Como se comentó anteriormente el personal de Coral Hipermercado desconoce de la existencia de un registro de dispositivos, de igual manera nos indican que desde que comienzan a laborar se les asigna los dispositivos con los	

que laboraran (cabe mencionar que los cajeros rotan según los turnos y según esto se ubican a laborar en cajas diferentes) pero no se les ha realizado una inspección de estos ni se conoce de la asignación o responsabilidad personal de cada uno.	**Obs**
Req. 9.9.2a Revisar los procedimientos documentados para verificar que estén definidos para incluir:	
*** Procedimientos para inspeccionar los dispositivos.**	
*** Frecuencia de las inspecciones.**	
Coral Hipermercado de Grupo Ortiz no mantiene dentro de sus políticas detallados procedimientos sobre la inspección de dispositivos y por lo tanto la frecuencia de inspección de los mismos, es importante mencionar el riesgo que abarca el hecho de tener socializado la responsabilidad que implica el manejo de los mismos y la asignación de estos a un determinado empleado mediante un registro formal.	**Obs**
Req. 9.9.2b Entrevistar al personal responsable y observar los procesos de inspección para verificar lo siguiente:	
*** El personal conoce los procedimientos para inspeccionar los dispositivos.**	
*** Todos los dispositivos se inspeccionan periódicamente para buscar indicios de alteraciones y sustitución.**	
Como se menciona anteriormente en las entrevistar realizadas al personal de Coral Hipermercados sobre todo a los supervisores, nos informan que desconocen de procedimientos aplicados para la inspección de los dispositivos, solamente saben que al final de las labores se mantienen los equipos que fueron asignada a cada Cajero en este	

caso quien es responsable de dar a conocer cualquier indicio sospechoso, sin embargo esto no le exime del riesgo a la empresa ya que no se mantiene documentada en la normativa de seguridad el procedimiento como tal y tampoco existen capacitaciones acerca de cómo manejar estos dispositivos ante alteraciones o prevenir ante posibles sustituciones de actos maliciosos.	**Obs**
Req. 9.9.3 Verificar que se capacite al personal para que detecten indicios de alteración o sustitución en los dispositivos.	
*Comprobar que el personal verifique la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de otorgarles autorización para acceder y modificar un dispositivo o soluci onar algún problema. *Observar que el personal no permita instalar, cambiar ni devolver di spositivos sin verificación. *Verificar que el personal se encuentre atento a comportamientos sospechosos cerca del dispositivo (por ejemplo, p ersonas desconocidas que intentan desconectar o abrir el dispositivo. *Verificar que informen al personal correspondiente sobre comportamientos sospechoso e indicios de alteració n o sustitución de dispositivos (por ejemplo, a un gerente o encargado de seguridad).	

Al entrevistar al personal responsable de los dispositivos (Cajeros) nos dieron a conocer que si bien no existe un procedimiento documentado o capacitaciones periódicas pero el personal a medida que va obteniendo experiencia en las labores diarias conoce sobre la identidad de personas que son del personal técnico y quienes no se encuentran autorizados en caso de no tener la experiencia necesaria siempre cualquier situación que se les presenten la tienen que notificar al supervisor y este a su vez al jefe inmediato. Al inicio de la integración de personal nuevo a la institución se les capacita de forma verbal sobre lo que no se debe realizar, no permitir que personas externas, accedan, instalen o cambien los dispositivos sin previo aviso de su superior. El personal de los puntos de venta nos indicó que solo ellos manejan el dispositivo es decir no permiten que nadie se acerque a estos.	
Req. 9.9.3b Entrevistar a un grupo del personal del punto de venta para verificar que hayan recibido capacitación y que conozcan los procedimientos para realizar:	
*** Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de otorgarles autorización para acceder y modificar un dispositivo o solucionar algún problema.**	
*** No instalar, cambiar ni devolver dispositivos sin verificación.**	
*** Estar atentos a comportamientos sospechosos cerca del dispositivo (por ejemplo, personas desconocidas que intentan desconectar o abrir el dispositivo).**	
*** Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ejemplo, a un gerente o encargado de seguridad).**	
Se conversó con un grupo del personal de punto de venta y nos informaron que solamente se les capacito al ingresar a laborar a la empresa sobre no dejar que terceras personas accedan o modifiquen los dispositivos sin previa	

autorización de un inmediato superior, que deben informar cualquier situación adversa que se presente al encargado de la seguridad o de ser el caso al Gerente de la Sucursal, sin embargo estas capacitaciones no son periódicas el conocimiento que se obtiene es debido a la experiencia según el tiempo de sus labores en la organización de todas formas si existe un conocimiento de lo que se debe realizar.	√

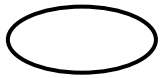
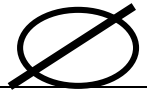
Fuente: Coral Hipermercado Racar Plaza (GO).

Conclusiones y recomendaciones:

Coral Hipermercado no mantiene un procedimiento de seguridad documentado para los dispositivos sin embargo si hay un conocimiento general por parte de los empleados debido a capacitaciones recibidas en sus inicios de labores de ingreso a laborar en la organización pero estas deberían ser según lo requiere el cumplimiento de la normativa, así como también no se mantiene un registro de dispositivos, el personal desconoce de listado de dispositivos y su responsabilidad ante la seguridad de estos. El personal debido a la experiencia que van adquiriendo mantiene seguridad ante los dispositivos pero esto no es suficiente para minimizar el riesgo que implican los dispositivos que si bien mantienen contacto directo con las tarjetas de pago.

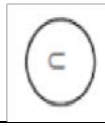
Elaborado por: Autoras.

ANEXO 21: Marcas de Auditoria.

Marca	Significado
√	**Cotejado, comprobado.**
√√	**Verificada la documentación.**
	**Cifra que no debe ser considerada. Es decir, no incluirse en tabulación, sumatorias, inventarios, etc.**
	**Documentado o punto pendiente por aclarar, revisar o localizar.**

⊗	**Documento o punto pendiente que fue aclarado, verificado o comprobado.**

↳	**Confrontado contra registro.**
T	**Total**
≥	**Verificado con reporte de**
√	**Verificado físicamente.**
↳	**Confortado contra documentación comprobatoria en original.**

e √	**Expediente revisado.**
d √	**Documento integrado en expediente.**
dc √	**Documentación comprobatoria revisada.**
	**Confrontado contra evidencia física.**
	**Pedido, contrato o dato por confirmar mediante compulsa.**

Obs.	Referencia de alguna irregularidad en el papel de trabajo, que posteriormente se describirá en una cédula de observación.
✓	Muestra seleccionada para revisión.

Elaborado por: Autoras.