RESUMEN

En una organización la gestión y administración de la seguridad puede tornarse compleja y difícil de realizar, esto no por razones técnicas, más bien por razones culturales de las organizaciones, coordinar la administración de los recursos institucionales en busca de asegurar y salvaguardar el entorno tecnológico, sin un adecuado marco de control técnico-administrativo que integre el conocimiento y el esfuerzo proporcionado por los mecanismos automatizados, tomará en la mayoría de los casos un ambiente inimaginablemente hostil, para lo cual es de suma importancia emplear un conjunto de mecanismos reguladores de las funciones y actividades desarrolladas por cada uno de los miembros de la institución.

El presente trabajo muestra como los procedimientos y políticas de seguridad, integra estos esfuerzos de una manera conjunta. Éste documento pretende, ser el medio de comunicación en el cual se establezcan las reglas, normas, controles y procedimientos que regulen la forma en que la EMUCE, prevenga, proteja y maneje los riesgos de seguridad informática en diversas circunstancias.

PALABRAS CLAVES: tecnología, seguridad lógica, análisis de riesgo, gestión de riesgo, seguridad informática, técnico-administrativo

ABSTRACT

In an organization the management and administration of the security can become complex and difficult to make, this not for technical reasons, more well for cultural reasons of the organizations, to coordinate the administration of the institutional resources in search of assuring and safeguard the technological surroundings, without an adapted frame of engineering and management control that integrates the knowledge and the effort provided by the automated mechanisms, will take in most of the cases an unimaginably hostile atmosphere, for which it is of extreme importance of using a set of regulating mechanisms of the functions and activities developed by each one of the members of the institution.

The present work shows like the procedures and policies of security, Integra these efforts of a joint way. This one document tries, to be the mass media in which the rules, norms, controls and procedures settle down that regulate the form in which the EMUCE, prevents, protects and handles the risks of computer science security in diverse circumstances.

TABLA DE CONTENIDO

UNIVERSIDAD DE CUENCA
FACULTAD DE INGENIERÍA
MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

“Diseño del Proceso Administrativo de la Seguridad Informática en la “Empresa Municipal de Servicios de Cementerios, Salas de Velación y Exequias”, EMUCE – Cuenca”

Tesis previa a la obtención del título de Magister en Gerencia de Sistemas de Información

AUTOR: ING. JUAN F. VICUÑA P.

TUTOR: ING. CLAUDIO CRESPO, MSC

Cuenca, Junio de 2009

DEDICATORIA

A mis hijos adorados María Verónica, Juan Andrés y Diego Fernando. Nunca es tarde para seguir aprendiendo. Si se puede.

AGRADECIMIENTO

La larga lista de personas que intervinieron en el desarrollo de este trabajo impide que se las mencionen aquí, para todas ellas mi aprecio y cariño.

El contenido del presente documento es de exclusiva responsabilidad de su autor.

Ing. Juan F. Vicuña P.

CAPITULO I

MARCO TEORICO

1.1 Introducción

En una organización la gestión y administración de la seguridad puede tornarse compleja y difícil de realizar, esto no por razones técnicas, más bien por razones culturales de las organizaciones, coordinar la administración de los recursos institucionales en busca de asegurar y salvaguardar el entorno tecnológico, sin un adecuado marco de control técnico-administrativo que integre el conocimiento y el esfuerzo proporcionado por los mecanismos automatizados, tomará en la mayoría de los casos un ambiente inimaginablemente hostil, para lo cual es de suma importancia emplear un conjunto de mecanismos reguladores de las funciones y actividades desarrolladas por cada uno de los miembros de la institución.

La EMUCE al ser una empresa municipal, su única política es el servicio a la ciudadanía, ofreciendo atención oportuna, solidaria, humana y sobre todo con costos accesibles.

La misión de la EMUCE: Somos una Empresa Municipal dedicada a la prestación de Servicios Funerarios con calidad, que buscan atender solidariamente a quienes pasan por momentos difíciles.

La visión de la EMUCE: Ser una empresa que cumpla los requerimientos de la ciudadanía en cuanto a soluciones exequiales integrales de manera innovadora, creativa y eficiente.

Objetivos de la EMUCE: Mejorar la cobertura de los servicios exequiales nivel de la ciudad con mucha calidad humana, rapidez y sobre todo con solidaridad.

La EMUCE se encuentra estructurada de la siguiente manera:

FUNCION DIRECTIVA

Se encuentra integrada por el Alcalde de Cuenca, como Presidente del Directorio, un Concejal como Vicepresidente, un representante de la Dirección Provincial de Salud, un representante de la ciudadanía, y el Director Administrativo de la I Municipalidad.

FUNCION EJECUTIVA

Representada por el Gerente de la empresa, quien es nombrado por el Ilustre Consejo Cantonal.

FUNCION ADMINISTRATIVA

Integrada por las siguientes dependencias: Jefatura Administrativa - Financiera, Departamento de Contabilidad, Recaudación, Bodega y Servicios Varios.

FUNCION OPERATIVA

Integrada por el Administrador del Cementerio, el Inspector de Cementerio y el personal de servicio.

El presente trabajo muestra como los procedimientos y políticas de seguridad, integra estos esfuerzos de una manera conjunta. Éste documento pretende, ser el medio de comunicación en el cual se establezcan las reglas, normas, controles y procedimientos que regulen la forma en que la EMUCE, prevenga, proteja y maneje los riesgos de seguridad informática en diversas circunstancias.

En términos generales la presente tesis pretende definir políticas de seguridad informática, englobando los procedimientos y políticas más adecuadas, tomando como base principal cuatro razones, las mismas que se describen a continuación:

1.1.1 Seguridad Organizacional

Dentro de este, se establece el marco formal de seguridad que debe sustentar la EMUCE, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

1.1.2 Seguridad Lógica

Establece e integra los mecanismos y guías técnicas-administrativas, que permitan monitorear y conocer el acceso a los activos de información, que incluye los procedimientos para la administración de los usuarios, definición de las responsabilidades de los diferentes actores en el sistema, definición de los perfiles de seguridad de los usuarios, control de acceso a los sistema (aplicaciones) y documentación sobre programas que se ejecutan en la empresa, que van desde el control de cambios en la configuración de los equipos y sistemas, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

1.1.3 Seguridad Física

Determina los requerimientos mínimos que se deben satisfacer en cuanto a seguridad perimetral, de forma que se puedan determinar controles en el manejo del hardware, cambios en la información y control de los ingreso a las distintas áreas con base en la importancia de los activos.

1.1.4 Seguridad Legal

Integra los requerimientos de seguridad que deben cumplir todos los empleados, socios y usuarios de la red institucional bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos de la EMUCE en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como cuestiones relacionadas con la legislación del país y contrataciones externas. Cada uno de los criterios anteriores, sustenta un entorno de

administración de suma importancia, para la seguridad de la información dentro de la red institucional de la EMUCE.

El presente documento pretende ser una orientación hacia los temas tratados en el desarrollo del trabajo de fin de maestría.

Para iniciar el desarrollo del tema, en primer lugar se converso con el Gerente de la EMUCE con la finalidad de obtener su aceptación sobre la aplicación del trabajo en la empresa.

En segundo lugar se han mantenido una serie de reuniones informales con los Directivos de la Maestría en Gerencia de Sistemas de Información con la finalidad de definir la viabilidad del tema así como el alcance que se dará al mismo. Con ésta aceptación se procede a realizar los trámites pertinentes para la legalización del tema de tesis.

1.1.5 Descripción del problema.

El trabajo final del fin de maestría será una aplicación práctica sobre la diseño del proceso administrativo de la seguridad informática en la EMUCE – Cuenca.

El compromiso que se asumirá con la Empresa Municipal será el definir el proceso administrativo de la seguridad informática así como la elaboración y entrega del Manual de Políticas de Seguridad, Manual de Procedimiento de Seguridad y Un Plan de Contingencia para los activos informáticos que posee la empresa.

El desarrollo de estos documentos conlleva el levantamiento de información y elaboración de los documentos finales entregables tanto para la EMUCE como para la MGSI, el mismo que se desarrollara durante los últimos tres trimestres del presente y el primer trimestre del año 2009.

1.1.6 Justificación.

La implementación de medidas de seguridad, es un proceso técnico-administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Las medidas de seguridad informática implementadas en una institución deben convertirse en las políticas de seguridad informática, las que conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas e instalaciones informáticas. En razón de lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos. Las Políticas de Seguridad Informática constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por tanto, deben constituir un proceso continuo y retroalimentado que observe la concientización, los métodos de acceso a la información, el monitoreo de cumplimiento y la renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

Todo lo anteriormente con la finalidad de ayudar a garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos.

En términos generales, la seguridad informática puede entenderse como aquellas reglas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible a robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

En este sentido, es la información juntamente con los equipos que la soportan el elemento principal a proteger, reguardar y recuperar dentro de la Empresa.

La falta de seguridad informática, se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y por que no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas contra la seguridad, integridad y confidencialidad de los datos e información así como de los activos informáticos.

Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita un eficiente administración del riesgo.

Para ello, resulta importante establecer políticas de seguridad, las cuales van desde la evaluación, el diseño de procedimientos de operación y control para establecer los niveles de protección de los recursos.

Este tipo de políticas permitirá desplegar una arquitectura de seguridad basada en soluciones tecnológicas, así como el desarrollo como el desarrollo de un plan de acción para el manejo de incidentes y recuperación para disminuir el impacto, ya que previamente habremos identificado y definido los activos (datos, software, hardware, instalaciones, recursos humanos, etc.) a proteger.

Es importante tener en consideración, que las amenazas no disminuirán y las vulnerabilidades no desaparecerán en su totalidad, por lo que los niveles de inversión en el área de seguridad en cualquier empresa, deberán ir acorde a la importancia de la información en riesgo.

Así mismo, cada dispositivo que conforma la red empresarial necesita un nivel de seguridad apropiado y la administración del riesgo implica una protección multidimensional y no únicamente tecnológica.

En consecuencia “un esquema de seguridad empresarial contempla la seguridad física y lógica de una compañía”.

1.1.7 Objetivos.

1.1.7.1 Objetivo General.

Diseñar el proceso administrativo de la seguridad informática en la EMUCE – Cuenca.

1.1.7.2 Objetivos Específicos.

- Definir la planificación de la seguridad informática al interior de la EMUCE.
- Determinar los procedimientos de control de la seguridad informática.
- Establecer los activos relacionados con la tecnología de información y comunicación que posee la EMUCE.
- Relacionar los activos y determinar la cascada de falla.
- Detectar las principales amenazas por cada tipo de archivo.
- Fijar Salvaguardas para los activos seleccionados.
- Elaborar un Plan de Contingencias y Recuperación a nivel informático.
- Definir Políticas de Seguridad.
- Elaborar un Manual de Procedimientos de Seguridad.

1.1.8 Alcance.

El alcance del trabajo de Tesis de fin de Maestría comprenderá la definición de la planificación, administración y control de la seguridad para los planes de seguridad informática en la EMUCE – Cuenca.

El levantamiento de información de los activos relacionados con la tecnología de información y comunicación que posee la EMUCE y elaboración de sus respectivas fichas de activos y relación de los mismos.

Formará parte también de este trabajo el desarrollo de un Manual de Políticas de Seguridad aplicado a la EMUCE.

Se incluirá un Manual de Procedimiento aplicable a la empresa y un Plan de Contingencias para la misma.

No formarán parte del presente trabajo todos los activos no relacionados con el ámbito de los sistemas de información y comunicación así como la definición de mecanismos de seguridad de las redes de transmisión de datos de la organización.

1.2 Administración de la Seguridad

> "*Para muchas empresas, la información y la tecnología que las soportan representan sus más valiosos activos, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI*"[1].

[1] COBIT, Resumen ejecutivo, página 6

Ésta dependencia que en la actualidad tienen las organizaciones en cuanto a las tecnologías de información y comunicación son las que deben propiciar una gestión de la seguridad informática en las instituciones sobre todo en aquellas que tienen misión críticas en sus operaciones cotidianas.

La administración de la seguridad informática se basa en un sistema de gestión que comprende la estructura de la organización, las políticas institucionales, los procedimientos de seguridad y control, los procesos y los recursos necesarios para implementar la Administración de la Seguridad de la Información (SGSI).

Un sistema de gestión de la seguridad se implanta de acuerdo a estándares internacionales de seguridad como la ISO 27001 basada en el código de buenas prácticas y objetivos de control de la ISO 17799, el cual se centra en la preservación de las características de confidencialidad, integridad y disponibilidad.

1.3 Importancia de los Manuales de Normas y Políticas

Como parte integral de un Sistema de Gestión de Seguridad de la Información (SGSI), un manual de normas y políticas de seguridad, trata de definir; ¿Qué?, ¿Por qué?, ¿De qué? y ¿Cómo? se debe proteger la información. Estos tienen una serie de objetivos en los cuales se establecen los mecanismos que son necesarios para implementar un nivel de seguridad adecuado a las necesidades Institucionales. Estos documentos tratan a su vez de ser un instrumento de interpretación de la seguridad para toda la organización.

1.4 Definición de Normas y Políticas de Seguridad

1.4.1 ¿Qué son las Normas de Seguridad?

Las normas de seguridad son un conjunto de reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de

responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo y tecnológico de la institución.

Las normas y políticas de seguridad están basadas en estándares internacionales que garantizan las mejores prácticas. Las principales son las siguientes:

ISO 27000, vocabulario y definiciones (terminología para el resto de estándares de la serie).

ISO 27001, especificación del sistema de gestión de la seguridad de la información (SGSI). Esta norma será certificable bajo los esquemas nacionales de cada país.

ISO 27002, actualmente la **ISO 17799**, que describe el Código de buenas prácticas para la gestión de la seguridad de la información.

ISO 27003, que contendrá una guía de implementación.

ISO 27004, estándar relacionado con las métricas y medidas en materia de seguridad para evaluar la efectividad del sistema de gestión de la seguridad de la información.

ISO 27005, que proporcionará el estándar base para la gestión del riesgo de la seguridad en sistemas de información.

BS 7799 es una norma que presenta los requisitos para un Sistema Administrativo de Seguridad de la Información (**SASI**). **BS 7799** es adoptado como norma ISO y denominada **ISO/IEC 17799**.

1.4.2 ¿Qué son las Políticas de Seguridad?

Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y

servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.

Una política de seguridad informática (PSI) es una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger y el por qué de ello.

Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

1.5 Políticas de Seguridad

1.5.1 Elementos de una Política de Seguridad Informática

Como mencionábamos en el apartado anterior, una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.

- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud qué pasara o cuándo algo sucederá; no es una sentencia obligatoria de la ley.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la

infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.

1.5.2 Algunos Parámetros para Establecer Políticas de Seguridad

Si bien las características de la PSI que hemos mencionado hasta el momento, nos muestran una perspectiva de las implicaciones en la formulación de estas directrices, revisaremos a continuación, algunos aspectos generales recomendados para la formulación de las mismas.

- Efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.

- Involucrar a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.

- Comunicar a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Recordar que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar los activos críticos de la funcionalidad de su área u organización.

- Desarrollar un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.

1.5.3 ¿Por qué las Políticas de Seguridad Informática Generalmente no Consiguen Implementarse?

Muchas veces, las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, con relativo éxito. Según algunos estudios, resulta una labor ardua convencer a los altos ejecutivos de la necesidad de buenas políticas y prácticas de seguridad informática.

Muchos de los inconvenientes se inician por los tecnicismos informáticos y por la falta de una estrategia de mercadeo de los especialistas en seguridad que, llevan a los altos directivos a pensamientos como: "más dinero para los juguetes de los ingenieros".

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad que, en muchos de los casos, lleva a comprometer su información sensible y por ende su imagen corporativa.

Ante esta encrucijada, los encargados de la seguridad deben asegurarse de que las personas relevantes entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos. En particular, la gente debe conocer las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir. Una intrusión o una travesura pueden convertir a las personas que no entendieron, en blanco de las políticas o en señuelos de los verdaderos vándalos. Luego, para que las PSI logren abrirse espacio en el interior de una organización deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

De igual forma, las PSI deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en su hacer diario,

donde se identifiquen las necesidades y acciones que materializan las políticas. En este contexto, entender la organización, sus elementos culturales y comportamientos nos debe llevar a reconocer las pautas de seguridad necesarias y suficientes que aseguren confiabilidad en las operaciones y funcionalidad de la compañía.

A continuación, mencionamos algunas recomendaciones para concientizar sobre la seguridad informática:

- Desarrollar ejemplos organizacionales relacionados con fallas de seguridad que capten la atención de sus interlocutores.
- Asociar el punto anterior a las estrategias de la organización y a la imagen que se tiene de la organización en el desarrollo de sus actividades.
- Articular las estrategias de seguridad informática con el proceso de toma de decisiones y los principios de integridad, confidencialidad y disponibilidad de la información.
- Mostrar una valoración costo-beneficio, ante una falla de seguridad.
- Justificar la importancia de la seguridad informática en función de hechos y preguntas concretas, que muestren el impacto, limitaciones y beneficios sobre los activos claves de la organización.

1.5.4 Las Políticas de Seguridad Informática como base de la Administración de la Seguridad Integral

Las políticas de seguridad informática conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas. En razón de lo anterior, son parte del engranaje del sistema

de seguridad que la organización posee para salvaguardar sus activos. Las PSI constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por tanto, deben constituir un proceso continuo y retroalimentado que observe la concientización, los métodos de acceso a la información, el monitoreo de cumplimiento y la renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

Las políticas por sí mismas no constituyen una garantía para la seguridad de la organización. Ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y a reconocer en los mecanismos de seguridad informática factores que facilitan la normalización y materialización de los compromisos adquiridos con la organización.

La seguridad tiene varios estratos:

- El marco jurídico adecuado.
- Medidas técnico-administrativas, como la existencia de políticas y procedimientos o la creación de funciones, como administración de la seguridad o auditoría de sistemas de información interna.

Ambas funciones han de ser independientes y nunca una misma persona podrá realizar las dos ni existir dependencia jerárquica de una función respecto de otra.

En cuanto a la administración de seguridad pueden existir, además, coordinadores en las diferentes áreas funcionales y geográficas de cada entidad, especialmente si la dispersión, la complejidad organizativa o el volumen de la entidad así lo demandan.

En todo caso, debe existir una definición de funciones y una separación suficiente de tareas. No tiene sentido que una misma persona autorice una transacción, la introduzca, y revise después los resultados (un diario de operaciones, por ejemplo), porque podría planificar un fraude o encubrir cualquier anomalía; por ello deben intervenir funciones / personas diferentes y existir controles suficientes. La seguridad física, como la ubicación de los centros de procesos, las protecciones físicas, el control físico de accesos, los vigilantes, las medidas contra el fuego y el agua, y otras similares.

La llamada seguridad lógica, como el control de accesos a la información exige la identificación y autenticación del usuario, o el cifrado de soportes magnéticos intercambiados entre entidades o de respaldo interno, o de información transmitida por línea. Puede haber cifrado de la información por dispositivos físicos o a través de programas, y en casos más críticos existen los dos niveles.

1.6 Control de la Seguridad

Cada vez más, la alta dirección se está dando cuenta del impacto significativo que la información puede tener en el éxito de una empresa. La dirección espera un alto entendimiento de la manera en que la tecnología de información y comunicación es operada y de la posibilidad de que sea aprovechada con éxito para tener una ventaja competitiva. En particular, la alta dirección necesita saber si con la información administrada en la empresa es posible que:

- Garantice el logro de sus objetivos.
- Tenga suficiente flexibilidad para aprender y adaptarse.
- Cuente con un manejo juicioso de los riesgos que enfrenta.
- Reconozca de forma apropiada las oportunidades y actúe de acuerdo a ellas.

Para garantizar los puntos antes indicados, es necesaria la implementación de procesos de control dentro del gobierno de tecnologías de información y comunicación por lo tanto:

"Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos. Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular"[2].

Por lo tanto, el sistema empresarial de controles internos impacta en la tecnología de información y comunicación en tres niveles:

- Al nivel de dirección ejecutiva, se fijan los objetivos de negocio, se establecen políticas y se toman decisiones de cómo aplicar y administrar los recursos empresariales para ejecutar la estrategia de la compañía. El enfoque genérico hacia el gobierno y el control se establece por parte de la alta dirección y se comunica a todo lo largo de la empresa. El ambiente de control de TI es guiado por este conjunto de objetivos y políticas de alto nivel.

- Al nivel de procesos de negocio, se aplican controles para actividades específicas del negocio. La mayoría de los procesos de negocio están automatizados e integrados con los sistemas aplicativos de TI, dando como resultado que muchos de los controles a este nivel estén automatizados. Estos se conocen como controles de las aplicaciones. Sin embargo, algunos controles dentro del proceso de negocios permanecen como procedimientos manuales, como la autorización de transacciones,

[2] COBIT 4, página 18

la separación de funciones y las conciliaciones manuales. Los controles al nivel de procesos de negocio son, por lo tanto, una combinación de controles manuales operados por el negocio, controles de negocio y controles de aplicación automatizados. Ambos son responsabilidad del negocio en cuanto a su definición y administración aunque los controles de aplicación requieren que la función de TI dé soporte a su diseño y desarrollo.

- Para soportar los procesos de negocio, TI proporciona servicios, por lo general de forma compartida, por varios procesos de negocio, así como procesos operacionales y de desarrollo de TI que se proporcionan a toda la empresa, y mucha de la infraestructura de TI provee un servicio común (es decir, redes, bases de datos, sistemas operativos y almacenamiento). Los controles aplicados a todas las actividades de servicio de TI se conocen como controles generales de TI. La operación formal de estos controles generales es necesaria para que dé confiabilidad a los controles en aplicación. Por ejemplo, una deficiente administración de cambios podría poner en riesgo (por accidente o de forma deliberada) la confiabilidad de los chequeos automáticos de integridad.

1.7 Metodología de análisis y gestión de riesgos de los sistemas de información

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)[3] surge como respuesta a la percepción de que la Administración (y en general toda la sociedad) depende de forma creciente de las tecnologías de la información para la consecución de sus objetivos de servicio. La razón de ser de MAGERIT está directamente relacionada con la

[3] MINISTERIO DE ADMINISTRACIONES PUBLICAS, Madrid, junio de 2006

generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.

En el periodo transcurrido desde la publicación de la primera versión de MAGERIT (1997) hasta la fecha, el análisis de riesgos se ha venido consolidando como paso necesario para la gestión de la seguridad.

Esta metodología interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan. Si dicha información o los servicios que se prestan gracias a ella son valiosos, esta metodología les permitirá saber cuánto de este valor está en juego y les ayudará a protegerlo.

Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos y por ello han aparecido multitud de guías informales, aproximaciones metódicas y herramientas de soporte todas las cuales buscan objetivar el análisis para saber cuán seguros (o inseguros) están y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Pese a que se ha puesto en manos de los sistemas de información graves responsabilidades para cumplir los objetivos de las organizaciones, no deja de ser un tema recurrente la inquietud por su seguridad. Los afectados, que frecuentemente no son técnicos, se preguntan si estos sistemas merecen su confianza, confianza que se ve mermada por cada fallo y, sobre todo, cuando la inversión en defensa de los medios de trabajo no se traduce en la ausencia de fallos. Lo ideal es que los sistemas no fallen. Pero lo cierto que se

acepta convivir con sistemas que fallan. El asunto no es tanto la ausencia de incidentes como la confianza en que están bajo control: se sabe qué puede pasar y se sabe qué hacer cuando pasa. El temor a lo desconocido es el principal origen de la desconfianza y, en consecuencia, aquí se busca conocer para confiar: conocer los riesgos para poder afrontarlos y controlarlos.

1.7.1 Objetivos de MAGERIT

MAGERIT persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de detenerlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.
- También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de un proyecto de análisis y gestión de riesgos:

  Modelo de valor: Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

Mapa de riesgos: Relación de las amenazas a que están expuestos los activos.

Evaluación de salvaguardas: Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

Estado de riesgo: Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

Informe de insuficiencias: Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema.

Plan de seguridad: Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos

1.7.2 Realización del análisis y de la gestión

Esta sección expone de forma conceptual en qué consiste el análisis de riesgos y como realizar su gestión, qué se busca en cada momento y qué conclusiones se derivan.

Hay dos grandes tareas a realizar:

1.7.2.1 Análisis de riesgos

Que permite determinar qué tiene la Organización y estimar lo que podría pasar.

Elementos:

- Activos, que no son sino los elementos del sistema de información (o estrechamente relacionados con este) que aportan valor a la Organización

- Amenazas, que no son sino cosas que les pueden pasar a los activos causando un perjuicio a la Organización

- Salvaguardas (o contra medidas), que no son sino elementos de defensa desplegados para que aquellas amenazas no causen [tanto] daño.

Con estos elementos se puede estimar:

- El impacto: lo que podría pasar

- El riesgo: lo que probablemente pase

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento.

1.7.2.1 Gestión de riesgos

Que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para contener las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la organización asume.

Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

1.7.3 Análisis de riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos:

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.

- Determinar a qué amenazas están expuestos aquellos activos.
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

1.7.3.1 Paso 1. Activos

Se denominan activos los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

El activo esencial es la información que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes:

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.

- Las instalaciones que acogen equipos informáticos y de comunicaciones.

- Las personas que explotan u operan todos los elementos anteriormente citados.

1.7.3.2 Paso 2. Amenazas

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

Hay accidentes naturales (terremotos, inundaciones,...) y desastres industriales (contaminación, fallos eléctricos,...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos. Hay amenazas causadas por las personas, bien errores, bien ataques intencionados.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

1.7.3.4 Paso 3. Determinación del impacto

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen materializarse en los medios.

1.7.3.3 Paso 4. Salvaguardas

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjugan simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridades físicas y, por último, está la política de personal.

Las salvaguardas entran en el cálculo del riesgo de dos formas:

- Reduciendo la frecuencia de las amenazas. Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

- Limitando el daño causado. Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz, lo que implica que:

- Es teóricamente idónea.

- Está perfectamente desplegada, configurada y mantenida.
- Se emplea siempre.
- Existen procedimientos claros de uso normal y en caso de incidencias los usuarios están formados y concienciados.
- Existen controles que avisan de posibles fallos.

Entre una eficacia del 0% para aquellas que están de adorno y el 100% para aquellas que son perfectas, se estimará un grado de eficacia real en cada caso concreto.

1.7.3.5 Paso 5. Determinación del riesgo

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia.

El riesgo crece con el impacto y con la frecuencia.

1.7.4 Impacto residual

Si se han hecho todos los deberes a la perfección, el impacto residual debe ser despreciable.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un impacto residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

1.7.5 Riesgo Residual

Si se han hecho todos los deberes a la perfección, el riesgo residual debe ser despreciable.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un riesgo residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la frecuencia de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la nueva tasa de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.

La magnitud de la frecuencia tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

CAPITULO II

DESARROLLO DE LA METODOLOGÍA

2.1 Antecedentes

La Empresa Municipal de Servicios de Cementerio, Salas de Velaciones y Exequias, EMUCE – Cuenca; es una empresa con un nivel de manejo informático incipiente, no cuenta con un centro informático de una manera formal, el manejo de los recursos de información y comunicación no cuenta con procesos definidos de una manera formal ni informal.

El “Centro de Computo”, es un área adscrita a la Jefatura Administrativa de la EMUCE, no cuenta con una oficina para su funcionamiento; no existe una persona que tenga la responsabilidad del manejo de los recursos de tecnología de información y comunicación, la persona encargada, que funge con las responsabilidades de Coordinador del Centro de Computo, tiene un nivel de formación de Tecnólogo, además de desempeñar otras funciones no afines con el área de tecnología de información como son las de bodeguero de la Empresa.

2.2 Análisis General

Los antecedentes arriba descritos, dan una breve idea del funcionamiento del Centro de Computo de la Empresa Municipal de Cementerios y presenta un panorama de los inconvenientes encontrados en el desarrollo del presente trabajo, ya que debido a la cultura informática que tiene la organización, muchas de las recomendaciones realizadas en la selección de las políticas informáticas son el fruto de estudio y experiencia del autor del presente trabajo.

Con estos antecedentes se cree que es necesario definir un conjunto de políticas que ayuden a “controlar” el uso y manejo de los recursos informáticos de la institución; las políticas son las siguientes:

- Política de excepción de responsabilidades.
- Política de responsabilidad sobre los activos.
- Política de clasificación de la información.
- Política de seguridad ligada al personal.
- Política de capacitación de usuarios
- Política de control de accesos
- Política de licenciamiento de software

Es necesario indicar en la EMUCE, no existe desarrollo de sistemas de información, únicamente utilizan servicios de información proporcionados por un manejador de archivos realizado en FoxPro, software que fue realizado por una tercera persona ajena a la EMUCE, la Coordinadora del Centro de Computo realiza el mantenimiento de las aplicaciones siempre y cuando estos mantenimientos no exijan demasiada modificación al código fuente. Es discrecionalidad de la Coordinadora del Centro de Computo el llamar o no a la persona externa para realizar modificaciones a los sistema de la EMUCE.

Este antecedente permite realizar la recomendación de unas políticas que son:

- Política de responsabilidad y procedimientos operativos.
- Política de planificación y aceptación de sistemas.
- Política de mantenimiento.
- Política de de seguridad de accesos de terceros

La Empresa Municipal de Cementerios y Salas de Velaciones cuenta con un servicio de acceso a Internet y servicio de correo electrónico para todos

los empleados de la empresa, por lo tanto es necesario control el uso y acceso de los recursos, lo que lleva a recomendar la siguiente política:

- Política de uso de correo electrónico.

El funcionamiento de los sistemas de la Empresa se basa en conexiones de red contra un servidor en el cual se encuentran centralizadas las aplicaciones institucionales, sin embargo, a pesar de contar con un control de acceso a la red empresarial, es necesario recomendar las siguientes políticas a ser aplicadas para mejorar el control:

- Política de control de acceso a la red.
- Política de control de acceso al sistema operativo.
- Política de control de acceso a las aplicaciones.
- Política de monitoreo del acceso y uso del sistema
- Política de responsabilidades del usuario.
- Política de administración de acceso de usuarios

Con la finalidad de crear una cultura de seguridad, se recomienda la creación de una política de:

- Política de respuesta a incidentes o anomalías de seguridad.

Es necesario también la definición de un conjunto de metodología que ayuden a normar y definir el uso de los recursos informáticos así como la definición de políticas que nos ayuden a controlar el desarrollo y mantenimiento de las políticas de seguridad que deberán ser implementadas en la EMUCE; por lo tanto, se definen un conjunto de políticas de propósito general con la finalidad de solventar este criterio.

Las políticas son las siguientes:

- Política de políticas de seguridad.
- Política de protección contra software malicioso.
- Política de manejo de seguridad y medios de almacenamiento.
- Política de seguridad de los equipos.
- Política de controles generales.
- Política de revisión de políticas de seguridad y cumplimiento técnico.
- Política de consideración sobre auditorias de sistemas.

2.3 Desarrollo de la Metodología.

La metodología de MAGERIT plantea el análisis de riesgos en cinco pasos fundamentales que son los siguientes:

- Determinación de activos.
- Determinación de amenazas.
- Determinación del impacto.
- Determinación de salvaguardas.
- Determinación del riesgo.

2.3.1 Determinación de activos.

Para el proceso de determinación de los activos relacionados con el área de tecnología de información y comunicación de la EMUCE, el principal problema que su tuvo que enfrentar fue la falta de un inventario formal tanto de hardware con de software de la institución.

La EMUCE no cuenta con un inventario de recursos informáticos, únicamente cuenta con un listado de los equipos que utilizan cada una de las personas en la institución. Este listado no cuenta con las definiciones de las características técnicas de cada uno de los componentes informáticos ni con el software que se ejecuta en cada uno de los equipos.

Es también necesario indicar que, el nivel de licenciamiento de software en la institución es muy bajo, se llega a esta conclusión ya que no se me pudo demostrar la existencia de las licencias de software aunque estas fueron solicitadas en algunas ocasiones a la Señora Eulalia Machuca que entre sus funciones está la de Coordinador del Centro de Cómputo.

Para solucionar este problema, se procedió a realizar un listado de los activos informáticos a los cuales se tuvo acceso, sin embargo, obtener las características técnicas no fue posible por la gran cantidad de tiempo que esta actividad demanda.

A pesar de ser importante las características técnicas de los activos, no son indispensables para el desarrollo de la metodología; para el presente trabajo se utilizó únicamente el listado de los activos que es el requisito de la metodología.

La falta de ésta información no afecta el resultado de los procedimientos y políticas de seguridad ya que las amenazas y la degradación sobre un activo están en función del tipo de activo más que en función de las características técnicas del mismo.

La metodología MAGERIT no hace referencia a la obsolescencia tecnológica de los activos, sino más bien, al nivel de protección de los mismos (ya sean de última tecnología o no) y el grado de confiabilidad que puedan tener estas salvaguardas para cada uno de ellos; ya que la obsolescencia tecnológica debe ser analizada por expertos en cada una de las área de tecnología de información y comunicación, lo que está más allá del alcance del

presente trabajo; lo cual no implica recomendar a la EMUCE un adecuado control de sus activos informáticos.

El listado final de los activos informáticos con los que se realiza el presente trabajo se encuentra detallado en el anexo II del presente trabajo.

La siguiente actividad en desarrollar, luego de terminada la fase de determinación de activos consistió en realizar la relación entre los activos institucionales, actividad realizada por el autor del presente trabajo y revisada por la Coordinadora del Centro de Computo de la EMUCE.

Los modelos de fichas realizadas para relacionar los activos se presentan en el anexo III y la totalidad de las fichas llenas se las presenta en el anexo IV. A continuación se muestra una ficha llena de uno de los activos con el propósito de demostrar su utilización.

[SW] Aplicaciones (software)	
Código: APL-005	**Nombre: Subsistema de acceso a aplicaciones**
Descripción: Permite el control de acceso a las aplicaciones. Otorga permisos de acceso	
Propietario: EMUCE	
Responsable: Econ. Gustavo Gavilanes	

Tipo (marque todos los adjetivos que procedan):
( ) [prp] desarrollo propio (in house)
(X) [sub] desarrollo a medida (subcontratado)
( ) [std] estándar (off the shelf)
( ) [browser] navegador web
( ) [www] servidor de presentación
( ) [email_client] cliente de correo electrónico
( ) [app] servidor de aplicaciones
( ) [file] servidor de ficheros
(X) [dbms] sistema de gestión de bases de datos
( ) [tm] monitor transaccional
( ) [office] ofimática
( ) [av] anti virus
( ) [backup] sistema de backup
( ) [os] sistema operativo

Dependencia de activos inferiores	
Activo: APL-001	**Grado: Alto**
¿Por qué? Si no funciona el subsistema de control de acceso, no es posible acceder a los sistemas	
Activo: APL-002	**Grado: Alto**
¿Por qué? Si no funciona el subsistema de control de acceso, no es posible acceder a los sistemas	
Activo: APL-003	**Grado: Alto**
¿Por qué? Si no funciona el subsistema de control de acceso, no es posible acceder a los sistemas	
Activo: APL-004	**Grado: Alto**
¿Por qué? Si no funciona el subsistema de control de acceso, no es posible acceder a los sistemas	
Activo: APL-006	**Grado: Alto**
¿Por qué? Si no funciona el subsistema de control de acceso, no es posible acceder a los sistemas	

Una vez llenadas todas las fichas, se pudo obtener la dependencia funcional de los activos informáticos de la EMUCE.

2.3.2 Determinación de Amenaza.

Para el proceso de determinación de amenazas, basado en la lista de se determino las posibles amenazas que podrían afectar a cada uno de los activos. El proceso se lo realizó mediante una reunión con la Coordinadora del Centro de Cómputo.

La técnica utilizada para ésta reunión es la entrevista personal, ya que es una técnica basada en sesiones de trabajo con el objetivo de obtener información de una forma individual, en la cual únicamente intervienen los perfiles del entrevistado y entrevistador.

Las interrogantes utilizadas en la entrevista son de tipo cerrado, circunscritas a las respuestas obtenidas en la tabla que se encuentra expuesta en los siguientes párrafos.

Para el proceso de la definición de las amenazas, se procedió a realizar un cuadro basado en una escala de valoración cuantitativa basada en el grado de incertidumbre de la posibilidad de que la misma se presente. La escala utilizada se presenta a continuación:

- Posibilidad alta
- Posibilidad media
- Posibilidad baja

La decisión de utilizar una escala de esta naturaleza radico principalmente en la dificultad para conseguir información científicamente sustentable en el medio sobre el grado de incertidumbre de la presencia de fenómenos naturales, fallas de software, índices de delincuencia, etc.

En base a esto, la encuesta utilizada durante el proceso de la entrevista se centro en:

- ¿Cuál es la posibilidad de que se presente un daño en el software que utiliza la institución?

  La posibilidad de que el software sufra algún daño (intencionado o no) es pequeña ya que el mantenimiento del mismo se lo realiza

mediante contrato con terceras personas; en la EMUCE se hace únicamente administración del software.

- ¿Cuál es la posibilidad de que se presente una pérdida de software de la institución?

Al servidor en el cual se encuentra instalado el software de aplicaciones de la EMUCE solo tiene acceso la persona encargada del Centro de Cómputo.

Nota: se pudo corroborar que las restricciones de acceso son únicamente lógicas, el servidor se encuentra en un lugar de acceso público para los empleados de la EMUCE.

- ¿Cuál es la probabilidad de que se presente un sabotaje al software de la institución?

Mínima.

Nota: a pesar que las personas que laboran en la EMUCE, no cuentan con perfil informático; el acceso físico al servidor puede ser un factor importante a considerar.

- ¿Cuál es la posibilidad de que sea sustraído los equipos informáticos de la institución?

Los equipos que pueden ser sustraídos son los de atención al público.

Nota: La EMUCE cuenta con sistema de alarma y vigilancia las 24 horas.

- ¿Cuál es la posibilidad de una falla de energía?

Baja. La EMUCE cuenta con ups para el servidor.

- ¿Cuál es la posibilidad de un incendio?

  Baja. Por el tipo de negocio, sobre todo por la Sala de Velaciones, se ha tratado de no tener material inflamable.

  Nota: en las salas de velaciones existen cortinas que se podrían contaminar con las velas. En las oficinas existe alfombra y muchos documentos.

- ¿Cuál es la posibilidad de una inundación?

  Por la ubicación geográfica, no existe una posibilidad muy baja de inundación.

  Nota: Hay que tomar en consideración las llaves de los baños que no son de cierre automático.

Las “notas” son consideraciones del autor del presente trabajo en base a las observaciones realizadas de las instalaciones de la institución.

Las amenazas de los activos institucionales se presentan en los cuadros que se muestran unos párrafos más adelante.

El objetivo de estas entrevistas fue obtener información de los riesgos a los cuales están sometidos los activos, tratando de que la información no quede oculta de forma voluntaria o involuntaria y tratando de no caer en un nivel de detalle que impida separar lo esencial de lo accesorio.

Para la definición de las amenazas, se tomo como referencia la metodología MAGERIT[4] – Catálogo de Elementos, en el cual se detallan las amenazas que pueden afectar a los diferentes tipos de activos. En base a las amenazas que presenta ésta sección, se seleccionaron aquellas que se

[4] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

consideraron con una mayor probabilidad de que se presenten de acuerdo a la ubicación geográfica del edificio de la EMUCE[5].

Las amenazas determinadas fueron las siguientes:

A nivel de software.

- Falla del software.
- Pérdida del software.
- Sabotaje.

A nivel de hardware.

- Daño del hardware.
- Robo.
- Falla de energía.
- Incendio.
- Terremoto.
- Inundación.

En base a las amenazas determinadas se crea el siguiente cuando en el cual se muestran la amenazas para cada uno de los activos informáticos de la EMUCE.

[5] Empresa Municipal de Cementerios, Salas de Velaciones y Exequias

Amenazas del Software

Código	Descripción	Amenaza		
		Falla del Software	Pérdida del software	Sabotaje
APL-001	Subsistema de contabilidad	x	x	x
APL-002	Subsistema de inventarios	x	x	x
APL-003	Subsistema de recaudaciones	x	x	x
APL-004	Subsistema de servicios	x	x	x
APL-005	Subsistema de administración de accesos a aplicaciones	x	x	x
APL-006	Subsistema de nómina	x	x	x

Cuadro 1. Amenazar definidas para el software.

Amenazas del Hardware

Código	Descripción	Amenaza					
		Daño del hardware	Robo	Falla de energía	Incendio	Terremoto	Inundación
EQU-001	Equipo de Gerencia	x	x	x	x	x	x
EQU-002	Equipo de Jefatura Financiera	x	x	x	x	x	x
EQU-003	Equipo de Jefatura Administrativa	x	x	x	x	x	x
EQU-004	Equipo de Contabilidad	x	x	x	x	x	x
EQU-005	Equipo de Bodega	x	x	x	x	x	x
EQU-006	Equipo de Recaudación	x	x	x	x	x	x
EQU-007	Equipo de Compras	x	x	x	x	x	x
EQU-008	Equipo del Departamento Técnico	x	x	x	x	x	x
EQU-009	Equipo de Ventas	x	x	x	x	x	x
EQU-010	Equipo de Secretaría	x	x	x	x	x	x
EQU-011	Equipo de Funeraria	x	x	x	x	x	x
EQU-012	Equipo de la Casa de Velaciones	x	x	x	x	x	x

EQU-013	Equipo de Servicios	x	x	x	x	x	x
EQU-014	Equipo de Servicios	x	x	x	x	x	x
EQU-015	Impresora de Secretaría	x	x	x	x	x	x
EQU-016	Impresora de Recaudación	x	x	x	x	x	x
EQU-017	Impresora de la Jefatura Financiera	x	x	x	x	x	x
EQU-018	Impresora de Contabilidad	x	x	x	x	x	x
EQU-019	Impresora de la Jefatura Administrativa	x	x	x	x	x	x
EQU-020	Impresora de Compras	x	x	x	x	x	x
EQU-021	Impresora de Funeraria	x	x	x	x	x	x
EQU-022	Modem de conexión a Internet	x	x	x	x	x	x
EQU-023	Switch de conectividad LAN	x	x	x	x	x	x
EQU-024	Centralilla telefónica	x	x	x	x	x	x
EQU-025	Servidor	x	x	x	x	x	x
SOP-001	Disco externo de respaldos	x	x	x	x	x	x
RED-	Red telefónica	x	x		x	x	x

001							
RED-002	Red de datos	x	x		x	x	x
RED-003	Red punto a punto	x	x		x	x	x
AUX-001	Ups del servidor	x	x	x	x	x	x
AUX-002	Ups de Compras	x	x	x	x	x	x
AUX-003	Ups de Ventas	x	x	x	x	x	x
INS-001	Edificio de la EMUCE				x	x	x

Cuadro 2: Amenazas definidas para el hardware.

Para este caso concreto, en la EMUCE no existen más salvaguardas que la implementación de un UPS para el equipo que funge servidor y un sistema inicial de respaldos en un disco externo.

Una vez determinadas las amenazas sobre cada uno de los activos institucionales, se procede con la valoración de los mismos, la valoración de la basa en los siguientes criterios, los mismos que son parte de la metodología MAGERIT[6] en el análisis de la dimensión de los riesgos.

- Disponibilidad.
- Integridad de los datos.
- Confidencialidad de los datos.
- Autenticidad de los usuarios del servicio.
- Autenticidad del origen de los datos.
- Trazabilidad del servicio.
- Trazabilidad de los datos

Es necesario indicar, que estos criterios de valoración no son aplicables a todos los activos, están más relacionados con los datos que proporcionan los sistemas de información; esto es así puesto que, el hardware es “fácilmente” reemplazable, mientras que la pérdida de datos produce un impacto mucho más grave para las organizaciones.

2.3.3 Determinación del impacto.

En este paso de la metodología, se realiza también una valoración de las amenazas en el sentido del impacto que provocaría la ocurrencia de las

[6] Metodología de Análisis y Gestión de Riesgos, Método, Pagina 19

mismas. La siguiente tabla muestra la valoración del impacto en relación con los activos de la EMUCE.

El proceso de valoración del impacto se lo realiza mediante una reunión con la Coordinadora del Centro de Computo; La técnica utilizada para ésta reunión es la entrevista personal, ya que es una técnica que está basada en sesiones de trabajo con el objetivo de obtener información de una forma individual, en la cual únicamente intervienen los perfiles del entrevistado y entrevistador; las preguntas realizadas a la Coordinadora del Centro de Computo hicieron referencia al impacto que podría tener cada una de las amenazas sobre los activos.

En este punto de la metodología, las respuestas fueron bastante guiadas por parte del entrevistado, puesto que la persona encargado del Centro de Cómputo, no tenía mucho conocimiento respecto de este tema.

La escala de valoración para los impactos de las amenazas en los activos institucionales es la siguiente:

- Alto
- Medio
- Bajo

El banco de preguntas con sus respectivas respuestas y anotaciones se la presenta a continuación las preguntas realizadas para el grupo de activos pertenecientes a la categoría de software y las preguntas realizadas para el grupo de hardware.

¿Cuál podría ser el impacto de una falla del subsistema de…?

¿Cuál podría ser el impacto de una pérdida del subsistema de…?

¿Cuál podría ser el impacto ante un sabotaje en el subsistema de…?

Las preguntas anteriores se repitieron para todas las aplicaciones de software; las que se presentan a continuación para el grupo de activos de hardware.

¿Cuál podría ser el impacto ante un daño del hardware en el…?

¿Cuál podría ser el impacto ante un robo del…?

¿Cuál podría ser el impacto ante una falla de energía del…?

¿Cuál podría ser el impacto ante un incendio en el que se afecte el…?

¿Cuál podría ser el impacto ante un terremoto en el que se afecte el…?

¿Cuál podría ser el impacto de una inundación en el que se afecte el…?

Y finalmente, la preguntas relacionadas con los activos pertenecientes al grupo de los edificios fueron las siguientes:

¿Cuál podría ser el impacto de un incendio sobre el edificio de la EMUCE?

¿Cuál podría ser el impacto de un terremoto sobre el edificio de la EMUCE?

¿Cuál podría ser el impacto de una inundación sobre el edificio de la EMUCE?

Los resultados de la encuesta se presentan en la siguiente tabla:

Impacto por Activo

Código	Descripción	Amenaza	Impacto
APL-001	Subsistema de contabilidad	Falla del software	Alto
		Pérdida del software	Alto
		Sabotaje	Alto
APL-002	Subsistema de inventarios	Falla del software	Alto
		Pérdida del software	Alto
		Sabotaje	Alto
APL-003	Subsistema de recaudaciones	Falla del software	Alto
		Pérdida del software	Alto
		Sabotaje	Alto
APL-004	Subsistema de servicios	Falla del software	Alto
		Pérdida del software	Alto
		Sabotaje	Alto
APL-005	Subsistema de administración de accesos a aplicaciones	Falla del software	Alto
		Pérdida del software	Alto
		Sabotaje	Alto
APL-006	Subsistema de nómina	Falla del software	Alto
		Pérdida del software	Alto
		Sabotaje	Alto
EQU-001	Equipo de Gerencia	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto

		Terremoto	Alto
		Inundación	Bajo
EQU-002	Equipo de Jefatura Financiera	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto
		Inundación	Bajo
EQU-003	Equipo de Jefatura Administrativa	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto
		Inundación	Bajo
EQU-004	Equipo de Contabilidad	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto
		Inundación	Bajo
EQU-005	Equipo de Bodega	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto

		Inundación	Bajo
EQU-006	Equipo de Recaudación	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto
		Inundación	Bajo
EQU-007	Equipo de Compras	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto
		Inundación	Bajo
EQU-008	Equipo del Departamento Técnico	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto
		Inundación	Bajo
EQU-009	Equipo de Ventas	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto
		Inundación	Bajo

EQU-010	Equipo de Secretaría	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto
		Inundación	Bajo
EQU-011	Equipo de Funeraria	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto
		Inundación	Bajo
EQU-012	Equipo de la Casa de Velaciones	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto
		Inundación	Bajo
EQU-013	Equipo de Servicios	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto
		Inundación	Bajo
EQU-014	Equipo de Servicios	Daño del hardware	Medio

		Robo	Medio
		Falla de energía	Bajo
		Incendio	Alto
		Terremoto	Alto
		Inundación	Bajo
EQU-015	Impresora de Secretaría	Daño del hardware	Bajo
		Robo	Bajo
		Falla de energía	Bajo
		Incendio	Bajo
		Terremoto	Bajo
		Inundación	Bajo
EQU-016	Impresora de Recaudación	Daño del hardware	Bajo
		Robo	Bajo
		Falla de energía	Bajo
		Incendio	Bajo
		Terremoto	Bajo
		Inundación	Bajo
EQU-017	Impresora de la Jefatura Financiera	Daño del hardware	Bajo
		Robo	Bajo
		Falla de energía	Bajo
		Incendio	Bajo
		Terremoto	Bajo
		Inundación	Bajo
EQU-018	Impresora de Contabilidad	Daño del hardware	Bajo
		Robo	Bajo

		Falla de energía	Bajo
		Incendio	Bajo
		Terremoto	Bajo
		Inundación	Bajo
EQU-019	Impresora de la Jefatura Administrativa	Daño del hardware	Bajo
		Robo	Bajo
		Falla de energía	Bajo
		Incendio	Bajo
		Terremoto	Bajo
		Inundación	Bajo
EQU-020	Impresora de Compras	Daño del hardware	Bajo
		Robo	Bajo
		Falla de energía	Bajo
		Incendio	Bajo
		Terremoto	Bajo
		Inundación	Bajo
EQU-021	Impresora de Funeraria	Daño del hardware	Bajo
		Robo	Bajo
		Falla de energía	Bajo
		Incendio	Bajo
		Terremoto	Bajo
		Inundación	Bajo
EQU-022	Modem de conexión a Internet	Daño del hardware	Medio
		Robo	Medio
		Falla de energía	Medio

		Incendio	Medio
		Terremoto	Medio
		Inundación	Medio
EQU-023	Switch de conectividad LAN	Daño del hardware	Alto
		Robo	Alto
		Falla de energía	Alto
		Incendio	Alto
		Terremoto	Alto
		Inundación	Alto
EQU-024	Centralilla telefónica	Daño del hardware	Alto
		Robo	Alto
		Falla de energía	Alto
		Incendio	Alto
		Terremoto	Alto
		Inundación	Alto
EQU-025	Servidor	Daño del hardware	Alto
		Robo	Alto
		Falla de energía	Alto
		Incendio	Alto
		Terremoto	Alto
		Inundación	Alto
SOP-001	Disco externo de respaldos	Daño del hardware	Bajo
		Robo	Bajo
		Falla de energía	Bajo
		Incendio	Bajo

		Terremoto	Bajo
		Inundación	Bajo
RED-001	Red telefónica	Daño del hardware	Medio
		Robo	Medio
		Incendio	Medio
		Terremoto	Medio
RED-002	Red de datos	Daño del hardware	Alto
		Incendio	Alto
		Terremoto	Alto
		Inundación	Alto
RED-003	Red punto a punto	Daño del hardware	Bajo
		Robo	Bajo
		Falla de energía	Bajo
		Incendio	Bajo
		Terremoto	Bajo
		Inundación	Bajo
AUX-001	Ups del servidor	Daño del hardware	Bajo
		Robo	Bajo
		Falla de energía	Bajo
		Incendio	Bajo
		Terremoto	Bajo
		Inundación	Bajo
AUX-002	Ups de Compras	Daño del hardware	Bajo
		Robo	Bajo
		Falla de energía	Bajo

		Incendio	Bajo
		Terremoto	Bajo
		Inundación	Bajo
AUX-003	Ups de Ventas	Daño del hardware	Bajo
		Robo	Bajo
		Falla de energía	Bajo
		Incendio	Bajo
		Terremoto	Bajo
		Inundación	Bajo
INS-001	Edificio de la EMUCE	Incendio	Alto
		Terremoto	Alto
		Inundación	Alto

También se analizó la probabilidad de ocurrencia de las amenazas. La probabilidad se la evaluó de acuerdo a la siguiente escala:

- Muy probable
- Probable
- Poco probable

La siguiente tabla muestra la probabilidad de ocurrencia de las amenazas en relación con cada uno de los activos de la EMUCE.

Impacto por Activo

Código	Descripción	Amenaza	Impacto	Ocurrencia
APL-001	Subsistema de contabilidad	Falla del software	Alto	Probable
		Pérdida del software	Alto	Probable
		Sabotaje	Alto	Poco Probable
APL-002	Subsistema de inventarios	Falla del software	Alto	Probable
		Pérdida del software	Alto	Probable
		Sabotaje	Alto	Poco Probable
APL-003	Subsistema de recaudaciones	Falla del software	Alto	Probable
		Pérdida del software	Alto	Probable
		Sabotaje	Alto	Poco Probable
APL-004	Subsistema de servicios	Falla del software	Alto	Probable
		Pérdida del software	Alto	Probable
		Sabotaje	Alto	Poco Probable
APL-005	Subsistema de administración de accesos a aplicaciones	Falla del software	Alto	Poco Probable
		Pérdida del software	Alto	Probable
		Sabotaje	Alto	Probable
APL-006	Subsistema de nómina	Falla del software	Alto	Poco Probable
		Pérdida del software	Alto	Probable
		Sabotaje	Alto	Probable
EQU-001	Equipo de Gerencia	Daño del hardware	Medio	Probable
		Robo	Medio	Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable

		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-002	Equipo de Jefatura Financiera	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-003	Equipo de Jefatura Administrativa	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-004	Equipo de Contabilidad	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-005	Equipo de Bodega	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable

		Inundación	Bajo	Poco Probable
EQU-006	Equipo de Recaudación	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-007	Equipo de Compras	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-008	Equipo del Departamento Técnico	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-009	Equipo de Ventas	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable

EQU-010	Equipo de Secretaría	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-011	Equipo de Funeraria	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-012	Equipo de la Casa de Velaciones	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-013	Equipo de Servicios	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-014	Equipo de Servicios	Daño del hardware	Medio	Probable

		Robo	Medio	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-015	Impresora de Secretaría	Daño del hardware	Bajo	Probable
		Robo	Bajo	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Bajo	Poco Probable
		Terremoto	Bajo	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-016	Impresora de Recaudación	Daño del hardware	Bajo	Probable
		Robo	Bajo	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Bajo	Poco Probable
		Terremoto	Bajo	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-017	Impresora de la Jefatura Financiera	Daño del hardware	Bajo	Probable
		Robo	Bajo	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Bajo	Poco Probable
		Terremoto	Bajo	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-018	Impresora de Contabilidad	Daño del hardware	Bajo	Probable
		Robo	Bajo	Poco Probable

		Falla de energía	Bajo	Poco Probable
		Incendio	Bajo	Poco Probable
		Terremoto	Bajo	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-019	Impresora de la Jefatura Administrativa	Daño del hardware	Bajo	Probable
		Robo	Bajo	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Bajo	Poco Probable
		Terremoto	Bajo	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-020	Impresora de Compras	Daño del hardware	Bajo	Probable
		Robo	Bajo	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Bajo	Poco Probable
		Terremoto	Bajo	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-021	Impresora de Funeraria	Daño del hardware	Bajo	Probable
		Robo	Bajo	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Bajo	Poco Probable
		Terremoto	Bajo	Poco Probable
		Inundación	Bajo	Poco Probable
EQU-022	Modem de conexión a Internet	Daño del hardware	Medio	Probable
		Robo	Medio	Poco Probable
		Falla de energía	Medio	Poco Probable

		Incendio	Medio	Poco Probable
		Terremoto	Medio	Poco Probable
		Inundación	Medio	Poco Probable
EQU-023	Switch de conectividad LAN	Daño del hardware	Alto	Probable
		Robo	Alto	Poco Probable
		Falla de energía	Alto	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Alto	Poco Probable
EQU-024	Centralilla telefónica	Daño del hardware	Alto	Probable
		Robo	Alto	Poco Probable
		Falla de energía	Alto	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Alto	Poco Probable
EQU-025	Servidor	Daño del hardware	Alto	Probable
		Robo	Alto	Poco Probable
		Falla de energía	Alto	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Alto	Poco Probable
SOP-001	Disco externo de respaldos	Daño del hardware	Bajo	Probable
		Robo	Bajo	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Bajo	Poco Probable

		Terremoto	Bajo	Poco Probable
		Inundación	Bajo	Poco Probable
RED-001	Red telefónica	Daño del hardware	Medio	Poco Probable
		Robo	Medio	Poco Probable
		Incendio	Medio	Poco Probable
		Terremoto	Medio	Poco Probable
RED-002	Red de datos	Daño del hardware	Alto	Poco Probable
		Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Alto	Poco Probable
RED-003	Red punto a punto	Daño del hardware	Bajo	Probable
		Robo	Bajo	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Bajo	Poco Probable
		Terremoto	Bajo	Poco Probable
		Inundación	Bajo	Poco Probable
AUX-001	Ups del servidor	Daño del hardware	Bajo	Probable
		Robo	Bajo	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Bajo	Poco Probable
		Terremoto	Bajo	Poco Probable
		Inundación	Bajo	Poco Probable
AUX-002	Ups de Compras	Daño del hardware	Bajo	Probable
		Robo	Bajo	Poco Probable
		Falla de energía	Bajo	Poco Probable

		Incendio	Bajo	Poco Probable
		Terremoto	Bajo	Poco Probable
		Inundación	Bajo	Poco Probable
AUX-003	Ups de Ventas	Daño del hardware	Bajo	Probable
		Robo	Bajo	Poco Probable
		Falla de energía	Bajo	Poco Probable
		Incendio	Bajo	Poco Probable
		Terremoto	Bajo	Poco Probable
		Inundación	Bajo	Poco Probable
INS-001	Edificio de la EMUCE	Incendio	Alto	Poco Probable
		Terremoto	Alto	Poco Probable
		Inundación	Alto	Poco Probable

2.3.4 Determinación de salvaguardas

El proceso de determinación de salvaguardas en el presente trabajo se lo realizó tomando en cuenta tres aspectos que forman parte de la metodología MAGERIT:

- Identificación de las salvaguardas existentes,
- Valoración de las salvaguardas existentes, y
- Definición de salvaguardas.

2.3.4.1 Identificación de las salvaguardas existentes.

En la empresa Municipal de Cementerios, Salas de Velaciones y Exequias, como se menciono anteriormente no existe una cultura de seguridad informática, por lo que, las únicas salvaguardas con la que cuenta la institución son un UPS para el equipo que funge de servidor y un disco externo utilizado para el respaldo de la información de los sistemas institucionales.

Ante estas únicas medidas de contingencia que existen en la institución, el activo principal que es la información, está sujeta a que se pueda perder o deteriorar. De alguna manera, el respaldo del servidor realizado en el disco externo podría ayudar en algo al proceso de recuperación de la información de los sistemas informáticos, sin embargo, no existe una política definida que explique claramente que tan frecuente se tiene que realizar el respaldo de la información.

Otra información que esta expuesta a grave riesgo es la que cada uno de los usuarios mantiene en sus computadores personales, sobre esta información no existe evidencia de que se realice respaldo alguno.

2.3.4.2 Valoración de las salvaguardas existentes.

Las salvaguardas existentes, si bien pueden prestar una respuesta adecuada para su propósito, no son suficientes para proteger todos los activos de la institución puesto que, están dedicadas exclusivamente hacia el servidor descuidando los demás recursos de información que tiene la empresa.

El párrafo anterior se pone en evidencia ya que el hardware está sometido a las siguientes amenazas[7]:

- Desastres naturales.
- De origen industrial.
- Errores y fallos no intencionados.
- Ataques intencionados.

2.3.4.3 Definición de salvaguardas.

Las salvaguardas definidas para cada uno de los activos de la institución se muestran en la siguiente tabla:

[7] Metodología de Análisis y Gestión de Riesgos, Catálogo de Elementos, Página 27

Salvaguardas por Activo

Código	Descripción	Amenaza	Impacto	Ocurrencia	Salvaguarda
APL-001	Subsistema de contabilidad	Falla del software	Alto	Probable	Respaldo de información
		Pérdida del software	Alto	Probable	Respaldo de información
		Sabotaje	Alto	Poco Probable	Control de acceso físico y lógico
APL-002	Subsistema de inventarios	Falla del software	Alto	Probable	Respaldo de información
		Pérdida del software	Alto	Probable	Respaldo de información
		Sabotaje	Alto	Poco Probable	Control de acceso físico y lógico
APL-003	Subsistema de recaudaciones	Falla del software	Alto	Probable	Respaldo de información
		Pérdida del software	Alto	Probable	Respaldo de información
		Sabotaje	Alto	Poco Probable	Control de acceso físico y lógico
APL-004	Subsistema de servicios	Falla del software	Alto	Probable	Respaldo de información
		Pérdida del software	Alto	Probable	Respaldo de información
		Sabotaje	Alto	Poco Probable	Control de acceso físico y lógico
APL-005	Subsistema de administración de accesos a aplicaciones	Falla del software	Alto	Poco Probable	Respaldo de información
		Pérdida del software	Alto	Probable	Respaldo de información
		Sabotaje	Alto	Probable	Control de acceso físico y lógico
APL-006	Subsistema de nómina	Falla del software	Alto	Poco Probable	Respaldo de información
		Pérdida del software	Alto	Probable	Respaldo de información
		Sabotaje	Alto	Probable	Control de acceso físico y lógico
EQU-001	Equipo de Gerencia	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica

		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
EQU-002	Equipo de Jefatura Financiera	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
EQU-003	Equipo de Jefatura Administrativa	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el

					hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
EQU-004	Equipo de Contabilidad	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
EQU-005	Equipo de Bodega	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware

		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
EQU-006	Equipo de Recaudación	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
EQU-007	Equipo de Compras	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el

					hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
EQU-008	Equipo del Departamento Técnico	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
EQU-009	Equipo de Ventas	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware

		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
EQU-010	Equipo de Secretaría	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
EQU-011	Equipo de Funeraria	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el

					hardware
EQU-012	Equipo de la Casa de Velaciones	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
EQU-013	Equipo de Servicios	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware

EQU-014	Equipo de Servicios	Daño del hardware	Medio	Probable	Respaldo de información
		Robo	Medio	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Alto	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
EQU-015	Impresora de Secretaría	Daño del hardware	Bajo	Probable	Seguro para el hardware
		Robo	Bajo	Poco Probable	Seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Bajo	Poco Probable	Seguro para el hardware
		Terremoto	Bajo	Poco Probable	Seguro para el hardware
		Inundación	Bajo	Poco Probable	Seguro para el hardware
EQU-016	Impresora de Recaudación	Daño del hardware	Bajo	Probable	Seguro para el hardware
		Robo	Bajo	Poco Probable	Seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Bajo	Poco Probable	Seguro para el hardware
		Terremoto	Bajo	Poco Probable	Seguro para el hardware
		Inundación	Bajo	Poco Probable	Seguro para el hardware
EQU-	Impresora de la	Daño del hardware	Bajo	Probable	Seguro para el hardware

017	Jefatura Financiera	Robo	Bajo	Poco Probable	Seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Bajo	Poco Probable	Seguro para el hardware
		Terremoto	Bajo	Poco Probable	Seguro para el hardware
		Inundación	Bajo	Poco Probable	Seguro para el hardware
EQU-018	Impresora de Contabilidad	Daño del hardware	Bajo	Probable	Seguro para el hardware
		Robo	Bajo	Poco Probable	Seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Bajo	Poco Probable	Seguro para el hardware
		Terremoto	Bajo	Poco Probable	Seguro para el hardware
		Inundación	Bajo	Poco Probable	Seguro para el hardware
EQU-019	Impresora de la Jefatura Administrativa	Daño del hardware	Bajo	Probable	Seguro para el hardware
		Robo	Bajo	Poco Probable	Seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Bajo	Poco Probable	Seguro para el hardware
		Terremoto	Bajo	Poco Probable	Seguro para el hardware
		Inundación	Bajo	Poco Probable	Seguro para el hardware
EQU-020	Impresora de Compras	Daño del hardware	Bajo	Probable	Seguro para el hardware
		Robo	Bajo	Poco Probable	Seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Bajo	Poco Probable	Seguro para el hardware
		Terremoto	Bajo	Poco Probable	Seguro para el hardware
		Inundación	Bajo	Poco Probable	Seguro para el hardware
EQU-021	Impresora de Funeraria	Daño del hardware	Bajo	Probable	Seguro para el hardware
		Robo	Bajo	Poco Probable	Seguro para el hardware

		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Bajo	Poco Probable	Seguro para el hardware
		Terremoto	Bajo	Poco Probable	Seguro para el hardware
		Inundación	Bajo	Poco Probable	Seguro para el hardware
EQU-022	Modem de conexión a Internet	Daño del hardware	Medio	Probable	Seguro para el hardware
		Robo	Medio	Poco Probable	Seguro para el hardware
		Falla de energía	Medio	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Medio	Poco Probable	Seguro para el hardware
		Terremoto	Medio	Poco Probable	Seguro para el hardware
		Inundación	Medio	Poco Probable	Seguro para el hardware
EQU-023	Switch de conectividad LAN	Daño del hardware	Alto	Probable	Seguro para el hardware
		Robo	Alto	Poco Probable	Seguro para el hardware
		Falla de energía	Alto	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Seguro para el hardware
		Terremoto	Alto	Poco Probable	Seguro para el hardware
		Inundación	Alto	Poco Probable	Seguro para el hardware
EQU-024	Centralilla telefónica	Daño del hardware	Alto	Probable	Seguro para el hardware
		Robo	Alto	Poco Probable	Seguro para el hardware
		Falla de energía	Alto	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Alto	Poco Probable	Seguro para el hardware
		Terremoto	Alto	Poco Probable	Seguro para el hardware
		Inundación	Alto	Poco Probable	Seguro para el hardware
EQU-025	Servidor	Daño del hardware	Alto	Probable	Seguro para el hardware
		Robo	Alto	Poco Probable	Seguro para el hardware
		Falla de energía	Alto	Poco Probable	Fuente alterna de alimentación eléctrica

		Incendio	Alto	Poco Probable	Seguro para el hardware
		Terremoto	Alto	Poco Probable	Seguro para el hardware
		Inundación	Alto	Poco Probable	Seguro para el hardware
SOP-001	Disco externo de respaldos	Daño del hardware	Bajo	Probable	Respaldo de información
		Robo	Bajo	Poco Probable	Respaldo de información y seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Terremoto	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
		Inundación	Bajo	Poco Probable	Respaldo de información, sistema contra incendios, seguro para el hardware
RED-001	Red telefónica	Daño del hardware	Medio	Poco Probable	Seguro para el hardware
		Robo	Medio	Poco Probable	Seguro para el hardware
		Incendio	Medio	Poco Probable	Seguro para el hardware
		Terremoto	Medio	Poco Probable	Seguro para el hardware
RED-002	Red de datos	Daño del hardware	Alto	Poco Probable	Seguro para el hardware
		Incendio	Alto	Poco Probable	Seguro para el hardware
		Terremoto	Alto	Poco Probable	Seguro para el hardware
		Inundación	Alto	Poco Probable	Seguro para el hardware
RED-003	Red punto a punto	Daño del hardware	Bajo	Probable	Seguro para el hardware
		Robo	Bajo	Poco Probable	Seguro para el hardware

		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Bajo	Poco Probable	Seguro para el hardware
		Terremoto	Bajo	Poco Probable	Seguro para el hardware
		Inundación	Bajo	Poco Probable	Seguro para el hardware
AUX-001	Ups del servidor	Daño del hardware	Bajo	Probable	Seguro para el hardware
		Robo	Bajo	Poco Probable	Seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Bajo	Poco Probable	Seguro para el hardware
		Terremoto	Bajo	Poco Probable	Seguro para el hardware
		Inundación	Bajo	Poco Probable	Seguro para el hardware
AUX-002	Ups de Compras	Daño del hardware	Bajo	Probable	Seguro para el hardware
		Robo	Bajo	Poco Probable	Seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Bajo	Poco Probable	Seguro para el hardware
		Terremoto	Bajo	Poco Probable	Seguro para el hardware
		Inundación	Bajo	Poco Probable	Seguro para el hardware
AUX-003	Ups de Ventas	Daño del hardware	Bajo	Probable	Seguro para el hardware
		Robo	Bajo	Poco Probable	Seguro para el hardware
		Falla de energía	Bajo	Poco Probable	Fuente alterna de alimentación eléctrica
		Incendio	Bajo	Poco Probable	Seguro para el hardware
		Terremoto	Bajo	Poco Probable	Seguro para el hardware
		Inundación	Bajo	Poco Probable	Seguro para el hardware
INS-001	Edificio de la EMUCE	Incendio	Alto	Poco Probable	Seguro para el edificio
		Terremoto	Alto	Poco Probable	Seguro para el edificio
		Inundación	Alto	Poco Probable	Seguro para el edificio

2.3.5 Determinación del Riesgo.

Para la realización de esta etapa de la metodología se utilizo el análisis mediante tablas en el cual se combinó en un sistema simple ordenado por importancia con la finalidad de que al incluir muchos detalles se perjudique la visión de conjunto[8].

Los métodos simples han demostrado mucha utilidad en la realización de análisis de esta naturaleza sin que por ello no muestren los resultados esperados[9].

La escala de valoración utilizada en el proceso es la siguiente:

- Alto.
- Medio.
- Bajo.

La tabla siguiente muestra los resultados del análisis de riesgo de los activos.

[8] Metodología de Análisis y Gestión de Riesgos, Guía de Técnicas, Pagina 6

9 ISO/IEC 13335-1:2004 – Information technology – Guidelines for the management of IT security – Part 1: Concepts and models for Information and communications technology security management.

Impacto por Activo

Código	Descripción	Amenaza	Impacto	Riesgo
APL-001	Subsistema de contabilidad	Falla del software	Alto	Medio
		Pérdida del software	Alto	Medio
		Sabotaje	Alto	Bajo
APL-002	Subsistema de inventarios	Falla del software	Alto	Medio
		Pérdida del software	Alto	Medio
		Sabotaje	Alto	Bajo
APL-003	Subsistema de recaudaciones	Falla del software	Alto	Medio
		Pérdida del software	Alto	Medio
		Sabotaje	Alto	Bajo
APL-004	Subsistema de servicios	Falla del software	Alto	Medio
		Pérdida del software	Alto	Medio
		Sabotaje	Alto	Bajo
APL-005	Subsistema de administración de accesos a aplicaciones	Falla del software	Alto	Medio
		Pérdida del software	Alto	Medio
		Sabotaje	Alto	Bajo
APL-006	Subsistema de nómina	Falla del software	Alto	Medio
		Pérdida del software	Alto	Medio
		Sabotaje	Alto	Bajo
EQU-001	Equipo de Gerencia	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo

		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo
EQU-002	Equipo de Jefatura Financiera	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo
EQU-003	Equipo de Jefatura Administrativa	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo
EQU-004	Equipo de Contabilidad	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo
EQU-005	Equipo de Bodega	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo

		Inundación	Bajo	Bajo
EQU-006	Equipo de Recaudación	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo
EQU-007	Equipo de Compras	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo
EQU-008	Equipo del Departamento Técnico	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo
EQU-009	Equipo de Ventas	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo

EQU-010	Equipo de Secretaría	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo
EQU-011	Equipo de Funeraria	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo
EQU-012	Equipo de la Casa de Velaciones	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo
EQU-013	Equipo de Servicios	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo
EQU-014	Equipo de Servicios	Daño del hardware	Medio	Bajo

		Robo	Medio	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Bajo	Bajo
EQU-015	Impresora de Secretaría	Daño del hardware	Bajo	Bajo
		Robo	Bajo	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Bajo	Bajo
		Terremoto	Bajo	Bajo
		Inundación	Bajo	Bajo
EQU-016	Impresora de Recaudación	Daño del hardware	Bajo	Bajo
		Robo	Bajo	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Bajo	Bajo
		Terremoto	Bajo	Bajo
		Inundación	Bajo	Bajo
EQU-017	Impresora de la Jefatura Financiera	Daño del hardware	Bajo	Bajo
		Robo	Bajo	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Bajo	Bajo
		Terremoto	Bajo	Bajo
		Inundación	Bajo	Bajo
EQU-018	Impresora de Contabilidad	Daño del hardware	Bajo	Bajo
		Robo	Bajo	Bajo

		Falla de energía	Bajo	Bajo
		Incendio	Bajo	Bajo
		Terremoto	Bajo	Bajo
		Inundación	Bajo	Bajo
EQU-019	Impresora de la Jefatura Administrativa	Daño del hardware	Bajo	Bajo
		Robo	Bajo	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Bajo	Bajo
		Terremoto	Bajo	Bajo
		Inundación	Bajo	Bajo
EQU-020	Impresora de Compras	Daño del hardware	Bajo	Bajo
		Robo	Bajo	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Bajo	Bajo
		Terremoto	Bajo	Bajo
		Inundación	Bajo	Bajo
EQU-021	Impresora de Funeraria	Daño del hardware	Bajo	Bajo
		Robo	Bajo	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Bajo	Bajo
		Terremoto	Bajo	Bajo
		Inundación	Bajo	Bajo
EQU-022	Modem de conexión a Internet	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Falla de energía	Medio	Bajo

		Incendio	Medio	Bajo
		Terremoto	Medio	Bajo
		Inundación	Medio	Bajo
EQU-023	Switch de conectividad LAN	Daño del hardware	Alto	Bajo
		Robo	Alto	Bajo
		Falla de energía	Alto	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Alto	Bajo
EQU-024	Centralilla telefónica	Daño del hardware	Alto	Bajo
		Robo	Alto	Bajo
		Falla de energía	Alto	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Alto	Bajo
EQU-025	Servidor	Daño del hardware	Alto	Bajo
		Robo	Alto	Bajo
		Falla de energía	Alto	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Alto	Bajo
SOP-001	Disco externo de respaldos	Daño del hardware	Bajo	Bajo
		Robo	Bajo	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Bajo	Bajo

		Terremoto	Bajo	Bajo
		Inundación	Bajo	Bajo
RED-001	Red telefónica	Daño del hardware	Medio	Bajo
		Robo	Medio	Bajo
		Incendio	Medio	Bajo
		Terremoto	Medio	Bajo
RED-002	Red de datos	Daño del hardware	Alto	Bajo
		Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Alto	Bajo
RED-003	Red punto a punto	Daño del hardware	Bajo	Bajo
		Robo	Bajo	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Bajo	Bajo
		Terremoto	Bajo	Bajo
		Inundación	Bajo	Bajo
AUX-001	Ups del servidor	Daño del hardware	Bajo	Bajo
		Robo	Bajo	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Bajo	Bajo
		Terremoto	Bajo	Bajo
		Inundación	Bajo	Bajo
AUX-002	Ups de Compras	Daño del hardware	Bajo	Bajo
		Robo	Bajo	Bajo
		Falla de energía	Bajo	Bajo

		Incendio	Bajo	Bajo
		Terremoto	Bajo	Bajo
		Inundación	Bajo	Bajo
AUX-003	Ups de Ventas	Daño del hardware	Bajo	Bajo
		Robo	Bajo	Bajo
		Falla de energía	Bajo	Bajo
		Incendio	Bajo	Bajo
		Terremoto	Bajo	Bajo
		Inundación	Bajo	Bajo
INS-001	Edificio de la EMUCE	Incendio	Alto	Bajo
		Terremoto	Alto	Bajo
		Inundación	Alto	Bajo

CAPITULO III

POLITICAS DE SEGURIDAD

3.1 Introducción

La implementación de Políticas de Seguridad en la EMUCE y en especial en el área de tecnología de información y comunicación deben obedecer al convencimiento de todos los actores de la organización de la importancia que tiene la seguridad en el sentido de precautelar los activos institucionales y con mayor importancia la información que maneja la Empresa con la finalidad de prever contingencia que se puedan presentar y salvaguardar los principales activos, las personas y la información; activos sin los cuales la continuidad del negocio se verá seriamente afectada.

En base al análisis realizado en el capítulo II del presente trabajo, se realiza la recomendación de la implementación de un conjunto de políticas de seguridad, las mismas que ayudarán a disminuir las posibilidades de que se presente alguna contingencia; y en caso de presentarse, ayudarán a disminuir el impacto en la organización.

Las políticas que se presentan a continuación han sido divididas en cuatro grandes grupos: Seguridad Organizacional, Seguridad Lógica, Seguridad Física y Seguridad Legal.

Las políticas de seguridad Organizacional hacen referencia al control y mantenimiento de las políticas de seguridad en sí mismas, las responsabilidades de los usuarios con respecto a los incidentes de seguridad y manejo de los activos institucionales, la clasificación de la información, y capacitación de usuarios.

Las políticas de seguridad lógica tratan los aspectos del control de acceso, administración y responsabilidades de los usuarios de los sistemas de

información, el uso de correo electrónico e Internet, la utilización de información y recursos de TIC's por parte de terceras personas ajenas a la institución, acceso a las aplicaciones y sistemas operativos.

La seguridad física hace referencia a aspectos físicos de control de acceso, y seguridades generales en el área del Centro de Cómputo y los recursos de tecnología con los que cuenta la organización.

Finalmente, la cuarta sección trata sobre la seguridad legal, en la cual se abordan temas como: licenciamiento de software, cumplimiento técnico y auditoría de sistemas.

3.2 Seguridad Organizacional

3.2.1 Política de Políticas de Seguridad

3.2.1.1 Introducción

La presente política pretende establecer un marco de referencia para el manejo de los servicios informáticos perteneciente a la EMUCE así como la normativa para la designación de un equipo de seguridad al interior de la misma.

3.2.1.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.2.1.3 Desarrollo de la Política

Art. 1. Los servicios de la red de la EMUCE son de exclusivo uso institucional y para gestiones administrativas, cualquier cambio en la normativa de uso de los mismos, será expresa y adecuada como política de seguridad en este documento.

Art. 2. La EMUCE nombrará un comité de seguridad, que de seguimiento al cumplimiento de la normativa y propicie el entorno necesario

para crear un sistema de gestión de la seguridad de la información, el cual tendrá entre sus funciones:

a) Velar por la seguridad de los activos informáticos

b) Gestión y procesamiento de información.

c) Cumplimiento de políticas.

d) Aplicación de sanciones.

e) Elaboración de planes de seguridad.

f) Capacitación de usuarios en temas de seguridad.

g) Gestionar y coordinar esfuerzos, por crear un plan de contingencia, que dé sustento o solución, a problemas de seguridad dentro de la institución. El mismo orientará y guiará a los empleados, la forma o métodos necesarios para salir adelante ante cualquier eventualidad que se presente.

h) Informar sobre problemas de seguridad a la Gerencia.

i) Poner especial atención a los usuarios de la red institucional sobre sugerencias o quejas con respecto al funcionamiento de los activos de información.

El comité de seguridad estará integrado por los siguientes miembros:

I. Gerente

II. Jefe Administrativo

III. Administrados de Sistemas

Art. 3. El personal de cada unidad organizativa dentro de la red de la EMUCE es el único responsable de las actividades procedentes de sus acciones.

Art. 4. El Administrador de Sistemas es el encargado de mantener en buen estado los servidores dentro de la red institucional.

Art. 5. Todo usuario de la red institucional de la EMUCE, gozará de absoluta privacidad sobre su información, o la información que provenga de sus acciones, salvo en casos, en que se vea involucrado en actos ilícitos o contraproducentes para la seguridad de la red institucional, sus servicios o cualquier otra red ajena a la institución.

Art. 6. Los usuarios podrán tener acceso a Internet, siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la unidad de informática.

Art. 7. Las actividades administrativas tienen la primera prioridad, por lo que a cualquier usuario utilizando otro servicio (por ejemplo Internet o "Chat") sin estos fines, se le podrá solicitar dejar libre la estación de trabajo, si así, fuera necesario.

3.2.1.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.2.1.5 Versiones

Versión 1.0 de mayo de 2009

3.2.2 Política de Excepciones de Responsabilidad

3.2.2.1 Introducción

La presente política pretende normar las excepciones al cumplimiento de una determinada política institucional.

3.2.2.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

Para el caso del Gerente, será el comité de seguridad quien autorizará el no cumplimiento de la presente política.

3.2.2.3 Desarrollo de la Política

Art. 1. Los usuarios que por disposición de sus superiores realicen acciones que perjudiquen a otros usuarios o la información que estos procesan, deberán mantener dicha disposición por escrito.

Art. 2. Algunos usuarios pueden estar exentos de responsabilidad, o de seguir algunas de las políticas enumeradas en este documento, debido a la responsabilidad de su cargo, o a situaciones no programadas. Estas excepciones deberán ser solicitadas formalmente y aprobadas por el comité de seguridad, con la documentación necesaria para el caso, siendo la gerencia quien dé por sentada su aprobación final.

3.2.2.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.2.2.5 Versiones

Versión 1.0 de mayo de 2009

3.2.3 Política de Responsabilidad por los Activos

3.2.3.1 Introducción

Pretende normar la responsabilidad que tienen los diferentes departamentos de la EMUCE en el control y cuidado de los activos institucionales.

3.2.3.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.2.3.3 Desarrollo de la Política

Art. 1. Cada departamento, tendrá un responsable por el/los activo/s crítico/s o de mayor importancia para la el departamento y/o la EMUCE.

Art. 2. La persona o entidad responsable de los activos de cada unidad organizativa o área de trabajo, velará por la salvaguarda de los activos físicos (hardware y medios magnéticos, aires acondicionados, mobiliario.), activos de información (Bases de Datos, Archivos, Documentación de sistemas, Procedimientos Operativos, configuraciones), activos de software (aplicaciones, software de sistemas, herramientas y programas de desarrollo).

Art. 3. El administrador de Sistemas será el responsable de la seguridad de la información almacenada en esos recursos.

3.2.3.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.2.3.5 Versiones

Versión 1.0 de mayo de 2009

3.2.4 Política de Clasificación de la Información

3.2.4.1 Introducción

La presente normativa pretende identificar los diferentes tipos de información con los que cuenta la EMUCE.

3.2.4.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.2.4.3 Desarrollo de la Política

Art. 1. De forma individual, los departamentos de la EMUCE, son responsables, de clasificar de acuerdo al nivel de importancia, la información que en ella se procese.

Art. 2. Se tomarán como base, los siguientes criterios, como niveles de importancia, para clasificar la información:

a) Pública

b) Interna

c) Confidencial

Art. 3. Los activos de información de mayor importancia para la institución deberán clasificarse por su nivel de exposición o vulnerabilidad.

3.2.4.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.2.4.5 Versiones

Versión 1.0 de mayo de 2009

3.2.5 Política de Seguridad Ligada al Personal

3.2.5.1 Introducción

La presente política pretende normar el uso de la información por parte del personal que labora en la EMUCE.

3.2.5.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.2.5.3 Desarrollo de la Política

Referente a contratos

Art. 1. Se entregará al contratado, toda la documentación necesaria para ejercer sus labores dentro de la institución, en el momento en que se dé por establecido su contrato laboral.

Art. 2. El contrato de trabajo deberá complementar un acuerdo de no-divulgación y confidencialidad, donde el empleado se compromete a mantener en secreto información sensible de la organización.

Art. 3. Una vez terminado el trabajo y antes de dar por terminado el contrato laboral, el contratado deberá restituir toda la información entregada por parte de la EMUCE.

El empleado

Art. 1. Se deberá complementar el contrato de trabajo con un acuerdo de no-divulgación y confidencialidad, donde el empleado se compromete a mantener en secreto información sensible de la organización.

Art. 2. La información procesada, manipulada o almacenada por el empleado es propiedad exclusiva de la EMUCE.

Art. 3. La EMUCE no se hace responsable por daños causados provenientes de sus empleados a la información o activos de procesamiento, propiedad de terceros y/o daños efectuados desde sus instalaciones de red a equipos informáticos externos.

3.2.5.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.2.5.5 Versiones

Versión 1.0 de mayo de 2009

3.2.6 Política de Capacitación de Usuarios

3.2.6.1 Introducción

La presente política pretende concientizar a los empleados de la EMUCE sobre la importancia de la seguridad.

3.2.6.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.2.6.3 Desarrollo de la Política

Art. 1. Los usuarios de la red institucional, serán capacitados en cuestiones de seguridad de la información, según sea el área operativa y en función de las actividades que se desarrollan.

Art. 2. Se deben tomar todas las medidas de seguridad necesarias, antes de realizar una capacitación a personal ajeno o propio de la institución, siempre y cuando se vea implicada la utilización de los servicios de red o se exponga material de importancia considerable para la institución.

3.2.6.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.2.6.5 Versiones

Versión 1.0 de mayo de 2009

3.2.7 Política de Respuesta a Incidentes o Anomalías de Seguridad

3.2.7.1 Introducción

La presente política pretende normar el respaldo de la información institucional de la EMUCE.

3.2.7.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.2.7.3 Desarrollo de la Política

Art. 1. Se realizarán respaldos de la información, diariamente, para los activos de mayor importancia o críticos, un respaldo semanal que se utilizará en caso de fallas y un tercer respaldo efectuado mensualmente, el cual deberá ser guardado y evitar su utilización a menos que sea estrictamente necesaria.

Art. 2. Las solicitudes de asistencia, efectuados por dos o más empleados o áreas de proceso, con problemas en las estaciones de trabajo, deberá dárseles solución en el menor tiempo posible.

Art. 3. El Administrador de Sistemas deberá elaborar un documento donde deba explicar los pasos que se deberán seguir en situaciones contraproducentes a la seguridad y explicarlo detalladamente en una reunión ante el personal de respuesta a incidentes.

Art. 4. Cualquier situación anómala y contraria a la seguridad deberá ser documentada, posterior revisión de los registros o Log de sistemas con el objetivo de verificar la situación y dar una respuesta congruente y acorde al problema, ya sea está en el ámbito legal o cualquier situación administrativa.

3.2.7.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.2.7.5 Versiones

Versión 1.0 de mayo de 2009

3.3 Seguridad Lógica

3.3.1 Política de Control de Accesos

3.3.1.1 Introducción

La presente política pretende normar la utilización de la información perteneciente a la EMUCE.

3.3.1.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.1.3 Desarrollo de la Política

Art. 1. El Administrador de Sistemas proporcionará toda la documentación necesaria para agilizar la utilización de los sistemas, referente a formularios, guías, controles, otros.

Art. 2. Cualquier petición de información, servicio o acción proveniente de un determinado usuario o departamento, se deberá efectuar siguiendo los canales de gestión formalmente establecidos por la institución, para realizar dicha acción; no dar seguimiento a esta política implica:

a) Negar por completo la ejecución de la acción o servicio.

b) Un informe completo dirigido al comité de seguridad, el mismo que será realizado por el Administrador de Sistemas con copia al departamento al cual solicita el servicio.

c) Sanciones aplicables por la gerencia, previamente discutidas con el comité de seguridad.

3.3.1.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.1.5 Versiones

Versión 1.0 de mayo de 2009

3.3.2 Política de Administración del Acceso de Usuarios

3.3.2.1 Introducción

La presente política pretende normar el acceso de los usuarios a la red institucional.

3.3.2.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.2.3 Desarrollo de la Política

Art. 1. Son usuarios de la red institucional los empleados de planta, administrativos, y toda aquella persona, que tenga contacto directo como empleado y utilice los servicios de la red institucional de la EMUCE.

Art. 2. Se asignará una cuenta de acceso a los sistemas de la intranet, a todo usuario de la red institucional, siempre y cuando se identifique previamente el objetivo de su uso o permisos explícitos a los que este accederá, junto a la información personal del usuario.

Art. 3. Los empleados de la EMUCE, son usuarios limitados, estos tendrán acceso únicamente a los servicios de Internet y recursos compartidos de la red institucional, cualquier cambio sobre los servicios a los que estos tengan acceso, será motivo de revisión y modificación de esta política, adecuándose a las nuevas especificaciones.

Art. 4. Se consideran usuarios externos o terceros, cualquier entidad o persona natural, que tenga una relación con la institución fuera del ámbito de empleado y siempre que tenga una vinculación con los servicios de la red institucional.

Art. 5. El acceso a la red por parte de terceros es estrictamente restrictivo y permisible únicamente mediante firma impresa y documentación de

aceptación de confidencialidad hacia la institución y comprometido con el uso exclusivo del servicio para el que le fue provisto el acceso.

Art. 6. No se proporcionará el servicio solicitado por un usuario o departamento, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución.

Art. 7. Se creará una cuenta temporal del usuario, en caso de olvido o extravío de información de la cuenta personal, para brindarse al usuario que lo necesite, siempre y cuando se muestre un documento de identidad personal.

Art. 8. La longitud mínima de caracteres permisibles en una contraseña se establece en 8 caracteres, los cuales tendrán una combinación alfanumérica, incluida en estos caracteres especiales.

Art. 9. La longitud máxima de caracteres permisibles en una contraseña se establece en 12 caracteres, siendo esta una combinación de Mayúsculas y minúsculas.

3.3.2.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.2.5 Versiones

Versión 1.0 de mayo de 2009

3.3.3 Política de Responsabilidades del Usuario

3.3.3.1 Introducción

La presente política pretende normar las responsabilidades de los usuarios sobre el uso de los activos informáticos de la EMUCE

3.3.3.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.3.3 Desarrollo de la Política

Art. 1. El usuario es responsable exclusivo de mantener a salvo su contraseña.

Art. 2. El usuario será responsable del uso que haga de su cuenta de acceso a los sistemas o servicios.

Art. 3. Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta se guardada en un lugar seguro.

Art. 4. El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por el Administrador de Sistemas, que contenga información que pueda facilitar a un tercero la obtención de la información de su cuenta de usuario.

Art. 5. El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de sus parientes, como fechas de cumpleaños o alguna otra fecha importante.

Art. 6. El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en

el, mediante una herramienta de bloqueo temporal (protector de pantalla), protegida por una contraseña, el cual deberá activarse en el preciso momento en que el usuario deba ausentarse.

Art. 7. Cualquier usuario que encuentre un hueco o falla de seguridad en los sistemas informáticos de la institución, está obligado a reportarlo al Administrador de Sistemas.

Art. 8. Los usuarios son responsables de guardar sus trabajos en discos flexibles, siempre y cuando hayan sido revisados por el administrador del Centro de Cómputo o persona encargada de dicha unidad, y así evitar cualquier pérdida de información valiosa.

3.3.3.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.3.5 Versiones

Versión 1.0 de mayo de 2009

3.3.4 Política de Uso de Correo Electrónico

3.3.4.1 Introducción

La presente política pretende normar el uso del servicio de correo electrónico de la EMUCE.

3.3.4.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.4.3 Desarrollo de la Política

Art. 1. El servicio de correo electrónico, es un servicio gratuito, y no se puede garantizar su confiabilidad, se debe hacer uso de él, acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red institucional.

Art. 2. El correo electrónico es de uso exclusivo, para los empleados de la EMUCE.

Art. 3. Todo uso indebido del servicio de correo electrónico, será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación total de la cuenta dentro del sistema.

Art. 4. El usuario será responsable de la información que sea enviada con su cuenta.

Art. 5. El Comité de Seguridad, se reservará el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la red institucional.

Art. 6. El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor.

3.3.4.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.4.5 Versiones

Versión 1.0 de mayo de 2009

3.3.5 Política de Seguridad en Acceso de Terceros

3.3.5.1 Introducción

La presente política pretende normar el acceso de terceras personas a la red institucional de la EMUCE.

3.3.5.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.5.3 Desarrollo de la Política

Art. 1. El acceso de terceros será concedido siempre y cuando se cumplan con los requisitos de seguridad establecidos en el contrato de trabajo o asociación para el servicio, el cual deberá estar firmado por las entidades involucradas en el mismo.

Art. 2. Todo usuario externo, estará facultado a utilizar única y exclusivamente el servicio que le fue asignado, y acatar las responsabilidades que devengan de la utilización del mismo.

Art. 3. Los servicios accedidos por terceros acataran las disposiciones generales de acceso a servicios por el personal interno de la institución, además de los requisitos expuestos en su contrato con la EMUCE.

3.3.5.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.5.5 Versiones

Versión 1.0 de mayo de 2009

3.3.6 Política de Control de Acceso a la Red

3.3.6.1 Introducción

La presente política norma el acceso de los usuarios a la red institucional de la EMUCE.

3.3.6.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.6.3 Desarrollo de la Política

Art. 1. El acceso a la red interna, se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, y éste será permitido mediante un mecanismo de autenticación.

Art. 2. Se debe eliminar cualquier acceso a la red sin previa autenticación o validación del usuario o el equipo implicado en el proceso.

Art. 3. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoria de seguridad.

Art. 4. El Administrador de sistemas deberá emplear dispositivos de red para el bloqueo, enrutamiento, o el filtrado de tráfico evitando el acceso o flujo de información, no autorizada hacia la red interna o desde la red interna hacia el exterior.

Art. 5. Los accesos a la red interna o local desde una red externa de la institución o extranet, se harán mediante un mecanismo de autenticación seguro y el tráfico entre ambas redes o sistemas será cifrado con una encriptación de mínimo 128 bits.

Art. 6. Se registrara todo acceso a los dispositivos de red, mediante archivos de registro o Log, de los dispositivos que provean estos accesos.

Art. 7. Se efectuara una revisión de Log de los dispositivos de acceso a la red en un tiempo máximo de 48 horas.

3.3.6.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.6.5 Versiones

Versión 1.0 de mayo de 2009

3.3.7 Política de Control de Acceso al Sistema Operativo

3.3.7.1 Introducción

La presente política pretende normar las configuraciones básicas del sistema operativo en los equipos de la EMUCE.

3.3.7.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.7.3 Desarrollo de la Política

Art. 1. Se deshabilitarán las cuentas creadas por ciertas aplicaciones con privilegios de sistema, (cuentas del servidor de aplicaciones, cuentas de herramientas de auditoría, etc.) evitando que estas corran sus servicios con privilegios nocivos para la seguridad del sistema.

Art. 2. Al terminar una sesión de trabajo en las estaciones, los operadores o cualquier otro usuario, evitara dejar encendido el equipo, pudiendo proporcionar un entorno de utilización de la estación de trabajo.

Art. 3. El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido al usuario administrador.

Art. 4. Los administradores de servicios, tendrán acceso único a los módulos de configuración de las respectivas aplicaciones que tienen bajo su responsabilidad.

Art. 5. Todo servicio provisto o instalado en los servidores, correrá o será ejecutado bajo cuentas restrictivas, en ningún momento se obviaran situaciones de servicios corriendo con cuentas administrativas, estos privilegios tendrán que ser eliminados o configurados correctamente.

3.3.7.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.7.5 Versiones

Versión 1.0 de mayo de 2009

3.3.8 Política de Control de Acceso a las Aplicaciones

3.3.8.1 Introducción

La presente política pretende normar la configuración de los sistema que se ejecutan sobre los equipos de la empresa.

3.3.8.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.8.3 Desarrollo de la Política

Art. 1. Las aplicaciones deberán estar correctamente diseñadas, con funciones de acceso especificas para cada usuario del entorno operativo de la aplicación.

Art. 2. Se deberá definir y estructurar el nivel de permisos sobre las aplicaciones, de acuerdo al nivel de ejecución o criticidad de las aplicaciones o archivos, y haciendo especial énfasis en los derechos de escritura, lectura, modificación, ejecución o borrado de información.

Art. 3. Se deberán efectuar revisiones o pruebas minuciosas sobre las aplicaciones, de forma aleatoria, sobre distintas fases, antes de ponerlas en un entorno operativo real, con el objetivo de evitar redundancias en las salidas de información u otras anomalías.

Art. 4. Las salidas de información, de las aplicaciones, en un entorno de red, deberán ser documentadas, y especificar la terminal por la que deberá ejecutarse exclusivamente la salida de información.

Art. 5. Se deberá llevar un registro mediante Log de aplicaciones, sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.

3.3.8.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.8.5 Versiones

Versión 1.0 de mayo de 2009

3.3.9 Política de Monitoreo del Acceso y Uso del Sistema

3.3.9.1 Introducción

La presente política norma el registro del uso de las aplicaciones informáticas de la EMUCE.

3.3.9.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.9.3 Desarrollo de la Política

Art. 1. Se registrará y archivará toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de Log o bitácoras de sistemas.

Art. 2. Los archivos de Log, almacenarán nombres de usuarios, nivel de privilegios, IP de terminal, fecha y hora de acceso o utilización, actividad desarrollada, aplicación implicada en el proceso, intentos de conexión fallidos o acertados, archivos a los que se tuvo acceso, entre otros.

Art. 3. Se efectuará una copia automática de los archivos de Log, y se conducirá o enviara hacia otra terminal o servidor, evitando se guarde la copia localmente donde se produce.

3.3.9.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.9.5 Versiones

Versión 1.0 de mayo de 2009

3.3.10 Política de Responsabilidades y Procedimientos Operativos

3.3.10.1 Introducción

La presente política norma los procedimientos operativos que deben llevar a cabo los administradores de las aplicaciones y servicios que se encuentran en ejecución en la EMUCE.

3.3.10.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.10.3 Desarrollo de la Política

Art. 1. El personal administrador de algún servicio, es el responsable absoluto por mantener en óptimo funcionamiento ese servicio, coordinar esfuerzos con el Administrador de Sistemas, para fomentar una cultura de administración segura y servicios óptimos.

Art. 2. Las configuraciones y puesta en marcha de servicios, son normadas por el Centro de Computo, y el Comité de Seguridad.

Art. 3. El personal responsable de los servicios, llevará archivos de registro de fallas de seguridad del sistema, revisara, estos archivos de forma frecuente y en especial después de ocurrida una falla.

3.3.10.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.10.5 Versiones

Versión 1.0 de mayo de 2009

3.3.11 Política de Planificación y Aceptación de Sistemas

3.3.11.1 Introducción

La presente política norma el proceso de aceptación de software adquirido a terceros.

3.3.11.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.11.3 Desarrollo de la Política

Art. 1. El Centro de Cómputo, o el personal del mismo, dedicado o asignado en el área de programación o planificación y desarrollo de sistemas, efectuarán todo el proceso propio de la planificación, desarrollo, adquisición, comparación y adaptación del software necesario para la EMUCE.

Art. 2. La aceptación del software se hará efectiva por la Gerencia de la institución, previo análisis y pruebas efectuadas por el personal de informática.

Art. 3. Únicamente se utilizará software certificado o en su defecto software previamente revisado y aprobado, por personal calificado en el área de seguridad.

Art. 4. La aceptación y uso de los sistemas no exonera, de responsabilidad alguna sobre el Administrador de Sistemas, para efectuar pruebas o diagnósticos a la seguridad de los mismos.

Art. 5. El software diseñado localmente o llámese de otra manera desarrolladas por programadores internos, deberán ser analizados y aprobados, por el Administrador de Sistemas, antes de su implementación.

Art. 6. Es tarea de programadores el realizar pruebas de validación de entradas, en cuanto a:

- Valores fuera de rango.
- Caracteres inválidos, en los campos de datos.
- Datos incompletos.
- Datos con longitud excedente o valor fuera de rango.
- Datos no autorizados o inconsistentes.
- Procedimientos operativos de validación de errores
- Procedimientos operativos para validación de caracteres.
- Procedimientos operativos para validación de la integridad de los datos.
- Procedimientos operativos para validación e integridad de las salidas.

Art. 7. Toda prueba de las aplicaciones o sistemas, se deberá hacer teniendo en cuenta las medidas de protección de los archivos de producción reales.

Art. 8. Cualquier prueba sobre los sistemas, del ámbito a la que esta se refiera deberá ser documentada y cualquier documento o archivo que haya sido necesario para su ejecución deberá ser borrado de los dispositivos físicos, mediante tratamiento electrónico.

3.3.11.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.11.5 Versiones

Versión 1.0 de mayo de 2009

3.3.12 Política de Protección Contra Software Malicioso

3.3.12.1 Introducción

La presente política norma el uso de software para prevenir el uso de programas maliciosos.

3.3.12.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.12.3 Desarrollo de la Política

Art. 1. Se adquirirá y utilizará software únicamente de fuentes confiables.

Art. 2. En caso de ser necesaria la adquisición de software de fuentes no confiables, este se adquirirá en código fuente.

Art. 3. Los servidores, al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus actualizable y activada la protección en tiempo real.

3.3.12.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.12.5 Versiones

Versión 1.0 de mayo de 2009

3.3.13 Política de Mantenimiento

3.3.13.1 Introducción

La presente política pretende normar el mantenimiento de las aplicaciones que se ejecutan en los equipos de la EMUCE.

3.3.13.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.13.3 Desarrollo de la Política

Art. 1. El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del personal del Centro de Computo, o del personal de soporte técnico.

Art. 2. El cambio de archivos de sistema, no es permitido, sin una justificación aceptable y verificable por el gestor de seguridad.

Art. 3. Se llevará un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

3.3.13.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.13.5 Versiones

Versión 1.0 de mayo de 2009

3.3.14 Política de Manejo de Seguridad y Medios de Almacenamiento

3.3.14.1 Introducción

La presente política pretende normar el manejo de los medios de almacenamiento y de respaldos de la información institucional.

3.3.14.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.3.14.3 Desarrollo de la Política

Art. 1. Los medios de almacenamiento o copias de seguridad del sistema de archivos, o información de la institución, serán etiquetados de acuerdo a la información que almacenan u objetivo que suponga su uso, detallando o haciendo alusión a su contenido.

Art. 2. Los medios de almacenamiento con información crítica o copias de respaldo deberán ser manipulados única y exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de su salvaguarda.

Art. 3. Todo medio de almacenamiento con información crítica será guardado bajo llave en una caja especial a la cual tendrá acceso únicamente, el Administrador de Sistemas o el Gerente, esta caja no debería ser removible, una segunda copia será resguardada por un tercero, entidad financiera o afín.

Art. 4. Se llevará un control, en el que se especifiquen los medios de almacenamiento en los que se debe guardar información y su uso.

3.3.14.4. Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.3.14.5 Versiones

Versión 1.0 de mayo de 2009

3.4 Seguridad Física

3.4.1 Política de Seguridad de los Equipos

3.4.1.1 Introducción

La presente política pretende normar la seguridad física de los equipos informáticos de la EMUCE.

3.4.1.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.4.1.3 Desarrollo de la Política

Art. 1. El cableado de red, se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias.

Art. 2. Los servidores, sin importar al grupo al que estos pertenezcan, con problemas de hardware, deberán ser reparados localmente, de no cumplirse lo anterior, deberán ser retirados sus medios de almacenamiento.

Art. 3. Los equipos o activos críticos de información y proceso, deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el Administrador de Sistemas y las personas responsables por esos activos, quienes deberán poseer su debida identificación.

3.4.1.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.4.1.5 Versiones

Versión 1.0 de mayo de 2009

3.4.2 Política de Controles Generales

3.4.2.1 Introducción

La presente política establece los parámetros de controles generales sobre los activos pertenecientes a la EMUCE.

3.4.2.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.4.2.3 Desarrollo de la Política

Art. 1. Las estaciones o terminales de trabajo, con procesamientos críticos no deben de contar con medios de almacenamientos extraíbles, que puedan facilitar el robo o manipulación de la información por terceros o personal que no deba tener acceso a esta información.

Art. 2. En ningún momento se deberá dejar información sensible de robo, manipulación o acceso visual, sin importar el medio en el que esta se encuentre, de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a esta información.

Art. 3. Deberá llevarse un control exhaustivo del mantenimiento preventivo y otro para el mantenimiento correctivo que se les haga a los equipos.

Art. 4. Toda oficina o área de trabajo debe poseer entre sus inventarios, herramientas auxiliares (extintores, alarmas contra incendios, lámpara de emergencia), necesarias para salvaguardar los recursos tecnológicos y la información.

Art. 5. Toda visita a las oficinas de tratamiento de datos críticos e información (Centro de Computo, sala de servidores entre otros) deberá ser

registrada mediante un formulario de accesos a las salas de procesamiento crítico, para posteriores análisis del mismo.

Art. 6. La sala o cuarto de servidores, deberá estar separada de las oficinas administrativas de la unidad de informática o cualquier otra unidad, departamento o sala de recepción del personal, mediante una división en la unidad de informática, recubierta de material aislante o protegido contra el fuego, Esta sala deberá ser utilizada únicamente por las estaciones prestadoras de servicios y/o dispositivos a fines.

Art. 7. El suministro de energía eléctrica debe hacerse a través de un circuito exclusivo para los equipos de cómputo, o en su defecto el circuito que se utilice no debe tener conectados equipos que demandan grandes cantidades de energía.

Art. 8. El suministro de energía eléctrica debe estar debidamente polarizado, no siendo conveniente la utilización de polarizaciones locales de tomas de corriente, sino que debe existir una red de polarización.

Art. 9. Las instalaciones de las áreas de trabajo deben contar con una adecuada instalación eléctrica, y proveer del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.

Art. 10. Las salas o instalaciones físicas de procesamiento de información deberán poseer información en carteles, sobre accesos, alimentos o cualquier otra actividad contraria a la seguridad de la misma o de la información que ahí se procesa.

3.4.2.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.4.2.5 Versiones

Versión 1.0 de mayo de 2009

3.5 Seguridad Legal

3.5.1 Política de Licenciamiento de Software

3.5.1.1 Introducción

La presente política norma la utilización de software propietario que se ejecuta en la EMUCE.

3.5.1.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.5.1.3 Desarrollo de la Política

Art. 1. La EMUCE, se reserva el derecho de respaldo, a cualquier miembro facultativo miembro de las áreas administrativas, ante cualquier asunto legal relacionado a infracciones a las leyes de copyright o piratería de software.

Art. 2. Todo el software comercial que utilice la EMUCE, deberá estar legalmente registrado, en los contratos de arrendamiento de software con sus respectivas licencias.

Art. 3. La adquisición de software por parte de personal que labore en la institución, no expresa el consentimiento de la institución, la instalación del mismo, no garantiza responsabilidad alguna para la EMUCE, por ende la institución no se hace responsable de las actividades de sus empleados.

Art. 4. Tanto el software comercial como el software libre son propiedad intelectual exclusiva de sus desarrolladores, la EMUCE respeta la propiedad intelectual y se rige por el contrato de licencia de sus autores.

Art. 5. El software comercial licenciado a la EMUCE, es propiedad exclusiva de la institución, la misma se reserva el derecho de reproducción de

éste, sin el permiso de sus autores, respetando el esquema de cero piratería y/o distribución a terceros.

Art. 6. En caso de transferencia de software comercial a terceros, se harán las gestiones necesarias para su efecto y se acataran las medidas de licenciamiento relacionadas con la propiedad intelectual.

Art. 7. Las responsabilidades inherentes al licenciamiento de software libre son responsabilidad absoluta de la EMUCE.

Art. 8. Cualquier cambio en la política de utilización de software comercial o software libre, se hará documentado y en base a las disposiciones de la respectiva licencia.

Art. 9. El software desarrollado internamente, por el personal que labora en la institución es propiedad exclusiva de la EMUCE.

Art. 10. La adquisición del software libre o comercial deberá ser gestionada con las autoridades competentes y acatando sus disposiciones legales, en ningún momento se obtendrá software de forma fraudulenta.

Art. 11. Los contratos con terceros, en la gestión o prestación de un servicio, deberán especificar, las medidas necesarias de seguridad, nivel de prestación del servicio, y/o el personal involucrado en tal proceso.

3.5.1.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.5.1.5 Versiones

Versión 1.0 de mayo de 2009

3.5.2 Política de Revisión de Políticas de Seguridad y Cumplimiento Técnico

3.5.2.1 Introducción

La presente política norma la revisión y cumplimiento de las políticas de seguridad establecidas para la EMUCE.

3.5.2.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.5.2.3 Desarrollo de la Política

Art. 1. Toda violación a las políticas de licenciamiento de software, será motivo de sanciones aplicables al personal que incurra en la violación.

Art. 2. El documento de seguridad será elaborado y actualizado por el Administrador de Sistemas, junto al Comité de Seguridad, su aprobación y puesta en ejecución será responsabilidad de la Gerencia.

Art. 3. Cualquier violación a la seguridad por parte del personal que labora, para la EMUCE, así como terceros que tengan relación o alguna especie de contrato con la institución se harán acreedores a sanciones aplicables de ley.

3.5.2.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.5.2.5 Versiones

Versión 1.0 de mayo de 2009

3.5.3 Política de Consideraciones Sobre Auditorías de Sistemas

3.5.3.1 Introducción

La presente política norma los procesos de auditoría de sistemas y de seguridad que se realicen en la EMUCE.

3.5.3.2 Alcance

El alcance de la presente política abarca todo el personal que labora en la EMUCE.

3.5.3.3 Desarrollo de la Política

Art. 1. Se debe efectuar una auditoria de seguridad a los sistemas de acceso a la red, trimestral, enmarcada en pruebas de acceso tanto internas como externas, desarrolladas por personal técnico especializado o en su defecto personal capacitado en el área de seguridad.

Art. 2. Toda auditoria a los sistemas, estará debidamente aprobada, y tendrá el sello y firma de la Gerencia.

Art. 3. Cualquier acción que amerite la ejecución de una auditoria a los sistemas informáticos deberá ser documentada y establecida su aplicabilidad y objetivos de la misma, así como razones para su ejecución, personal involucrada en la misma y sistemas implicados.

Art. 4. La auditoria no deberá modificar en ningún momento el sistema de archivos de los sistemas implicados, en caso de haber necesidad de modificar algunos, se deberá hacer un respaldo formal del sistema o sus archivos.

Art. 5. Las herramientas utilizadas para la auditoria deberán estar separadas de los sistemas de producción y en ningún momento estas se quedaran al alcance de personal ajeno a la elaboración de la auditoria.

3.5.3.4 Cumplimiento

El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

3.5.3.5 Versiones

Versión 1.0 de mayo de 2009

CAPITULO IV

PLAN DE CONTINGENCIAS

4.1 Introducción

Ante el incremento de la cultura informática derivada del creciente empleo de la Tecnología de la Información, surge la necesidad y responsabilidad de la protección de la misma, de sus medios de almacenamiento y de su ambiente de operación. La información que se maneja en la EMUCE, por ser materia prima para la propia gestión y toma de decisiones, es considerada como un activo importante y como tal, debe ser sujeta de custodia y protección para asegurar su integridad, confidencialidad y disponibilidad.

La cantidad de datos guardados en los medios y equipos de almacenamiento se acrecienta día con día y su integridad va relacionada con su pérdida, destrucción, alteración, etc. intencional o no intencional. Es por ello, que los usuarios o personal directamente relacionado con el uso y operación de bienes informáticos deben propiciar la adopción de medidas de seguridad para proteger su información.

El Plan de Contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, suficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible. Pese a todas las medidas de seguridad implementadas puede ocurrir un desastre.

El Plan de Contingencias es el instrumento de gestión para el buen manejo de las Tecnologías de la Información y las Comunicaciones. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de la institución.

Así mismo, este plan de contingencias sigue el conocido ciclo de vida iterativo "plan-do-check-act", es decir, "planifica-actúa-comprueba-corrige". Surge de un análisis de riesgos, donde entre otras amenazas, se identifican aquellas que afectan a la continuidad de la operación de la institución.

El plan de contingencias deberá ser revisado semestralmente. Así mismo, es revisado/evaluado cuando se materializa una amenaza.

Con base en esta guía cada una de las áreas que componen la EMUCE, deberán perseguir los siguientes fines:

- Establecer mecanismos y procedimientos para proporcionar confidencialidad, integridad y disponibilidad de la información.
- Estimular la creación de una cultura de seguridad informática, así como fomentar la ética entre los miembros de la EMUCE.
- Definir los requerimientos mínimos de seguridad en cada área, dependiendo del tipo de información que se procese: confidencial, restringida, de uso interno, general o público, estableciendo los procedimientos para identificación y uso de cada categoría de información.
- Promover el establecimiento de procedimientos alternos en previsión a contingencias de cualquier naturaleza que garanticen en la medida de lo posible, la continuidad del procesamiento de la información y la prestación de servicios, mismos que al incorporarse al presente documento lo irán enriqueciendo y de

esta manera se logrará contar cada vez con una mejor herramienta que apoye a superar las contingencias que se presenten.

4.2 Propósito

El propósito de este plan es mantener la continua ejecución de los procesos de misión crítica y sistemas de información tecnológica de la EMUCE en el caso extraordinario que un evento pudiera ocasionar que los sistemas fallen en el mínimo de su producción. El Plan de Contingencia de la EMUCE contiene las necesidades y requerimientos de tal forma que la institución pueda estar preparada para responder a un evento y, en su caso, hacer eficiente la restauración de los sistemas que hayan estado inoperables por el evento.

4.3 Alcance

Proveer información sobre los sistemas, lugares, medidas, limitantes técnicos y limitantes físicas del Plan de Contingencia de la EMUCE.

4.4 Objetivo

Proporcionar a la EMUCE un Plan de Contingencia Informático, que contenga los procedimientos e instructivos necesarios para poder continuar con las operaciones, procesos y servicios informáticos críticos, en caso de que se llegara a presentar algún siniestro o contingencia. Así como minimizar el impacto que dichos daños pudieran causar.

Para asegurar su correcto funcionamiento, la EMUCE, deberá efectuar las pruebas necesarias de las actividades que así lo requieran, y establecer un proceso continuo para darle un correcto mantenimiento.

El plan busca los siguientes objetivos:

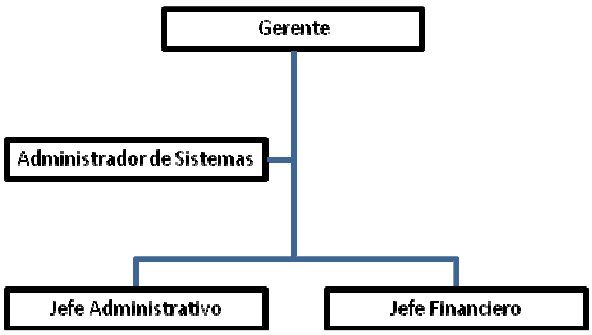
- Minimizar el número de decisiones que deben ser tomadas durante una contingencia

- Identificar los recursos necesarios para ejecutar las acciones definidas por este plan.
- Identificar las acciones a ser tomadas por equipos pre-diseñados
- Identificar información critica, así como el responsable de recuperarla en las operaciones de restauración
- Definir el proceso para probar y mantener este plan y entrenamiento para equipos de contingencia de la organización.

4.5 Organización

En el caso de un desastre u otra circunstancia que conlleve la necesidad de operaciones de contingencia, la organización normal de la EMUCE deberá cambiar a una organización de contingencia. La EMUCE deberá centrarse en cambiar, la estructura actual y funciones de un “día normal de trabajo”, a la estructura y funciones requeridas por la contingencia trabajando en conjunto para la restauración en tiempo de las operaciones de la misma.

Una estructura propuesta es la que se presenta en el siguiente diagrama:



4.6 Fases de la Contingencia

El Coordinador del Plan de Contingencia de la EMUCE, en conjunto con sus directivos, deberá determinar cuáles equipos y miembros son responsables de cada función durante las fases:

- Fase de Respuesta
- Fase de Reasunción
- Fase de Recuperación
- Fase de Restauración

4.7 Plan de Acción

4.7.1 Realizar un levantamiento de los servicios informáticos.

Llevar a cabo un Inventario de equipo de cómputo, software y mobiliario, para determinar cuál es la información crítica que se tiene que resguardar, adicionalmente levantar un inventario de los servicios de cómputo, telecomunicaciones, Internet, etc., que son requeridos para que los usuarios estén en posibilidad de llevar a cabo sus actividades normales.

4.7.2 Identificar un conjunto de amenazas.

Identificar los tipos de siniestros a los cuales está propenso cada uno de los procesos críticos, tales como falla eléctrica prolongada, incendio, terremoto, etc.

Identificar el conjunto de amenazas que pudieran afectar a los procesos informáticos, ya sea por causa accidental o intencional.

4.7.3 Revisar la seguridad, controles físicos y ambientales existentes, evaluando si son adecuados respecto a las amenazas posibles.

Se debe estar preparado para cualquier percance, verificando que dentro de la EMUCE se cuente con los elementos necesarios para salvaguardar sus activos.

4.7.4 Identificar los servicios fundamentales de la EMUCE.

Se deben analizar las funciones de mayor prioridad de la EMUCE, por medio de flujo gramas de procesos específicos para medir el alcance de cada actividad.

4.8 Etapas de la Metodología

En el Plan de Contingencia Informático se establecen procedimientos preventivos para el manejo de casos de emergencia que se presenten en la EMUCE al sufrir una situación anormal, protegiendo al personal, las instalaciones, la información y el equipo.

En el momento que sea necesario aplicar el Plan de Contingencia, la reanudación de las actividades puede ser el mayor reto con el que la EMUCE se enfrente, probablemente no pueda regresar a su lugar habitual de trabajo o no disponga de las herramientas usuales para desempeñar normalmente sus actividades. Incluso es posible tener que hacer el trabajo sin el equipo de gestión y colaboradores.

No se debe dejar el Plan de Contingencia para una ocasión posterior debido a cargas excesivas de trabajo, es necesario presupuestar tiempo y recursos para crear un programa de contingencia completo y útil.

La preparación ante un desastre comienza asegurándose de que se tienen los datos a recuperar. Un programa de contingencia no incluye solamente operaciones de copia de seguridad como parte de su contenido; sin embargo, la realización de copias de seguridad fiables es un requisito previo.

Existen diferentes tipos de contingencia de acuerdo a los daños sufridos:

- Menor.- Es la que tiene repercusiones sólo en la operación diaria y se puede recuperar en menos de 8 horas.
- Grave.- Es la que causa daños a las instalaciones, pero pueden reiniciar las operaciones en menos de 24 horas.
- Crítica.- Afecta la operación y a las instalaciones, este no es recuperable en corto tiempo y puede suceder por que no existen normas preventivas o bien porque estas no son suficientes. También puede suceder por ocurrir algún tipo de desastre natural como un terremoto.

Tipos de Contingencias de acuerdo al grado de afectación:

- En el mobiliario.
- En el equipo de cómputo en general (procesadores, unidades de disco, impresoras etc.).
- En comunicaciones (hubs, ruteadores, nodos, líneas telefónicas).
- Información.
- Instalaciones.

4.9 Determinación de activos a proteger

- Vidas humanas.
- La documentación, Base de datos y los sistemas Informáticos con los que cuenta la EMUCE.
- Infraestructura mobiliaria e instalaciones.

- Mobiliario y suministro de oficina.
- Equipos de cómputo y conectividad.
- Software de aplicaciones y copias de respaldo.

4.10 Riesgos en la Seguridad Informática (equipos y archivos).

El análisis de riesgos supone más que el hecho de observar la posibilidad de que ocurran cosas negativas. Se ha de poder obtener una evaluación económica del impacto de estos sucesos negativos. La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada institución.

Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado. Este plan debe ser diseñado por cada institución.

El análisis de riesgos supone responder a preguntas del tipo:

- ¿Qué puede ir mal?
- ¿Con qué frecuencia puede ocurrir?
- ¿Cuáles serían sus consecuencias?
- ¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?

En lo fundamental la evaluación de riesgos que se ha de llevar a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:

- ¿Qué se intenta proteger?
- ¿Frente a qué se intenta proteger?

Los principales riesgos considerados en el presente trabajo son:

4.10.1 Incendios.

La EMUCE tiene una deficiente protección contra incendios, por la falta de extintores, detectores de humo que imposibilita a los empleados a que estén preparados para afrontar un desastre de tal magnitud. Un evento de esta naturaleza ocasionaría pérdidas totales o parciales e irreparables.

4.10.2 Robo común.

El personal de seguridad debe estar ubicado en zonas estratégicas de las instalaciones del local de la EMUCE, evitando así que personas inescrupulosas puedan llevarse los equipos y con ellos los archivos.

4.10.3 Fallas en los equipos.

Por no realizar mantenimiento preventivo ni continúo de los equipos y a la depreciación del hardware. Este evento ocasionaría pérdidas totales o parciales, por lo tanto, se produce una interrupción forzada en las actividades, hasta solucionar el problema.

4.10.4 Equivocaciones.

El nivel de preparación del empleado para afrontar una equivocación. Durante las vacaciones de los empleados, se deberán sustituir personal capacitado.

4.10.5 Desconocimiento de la Normatividad.

El personal de la EMUCE, no conoce la Misión ni Visión de la empresa, esto se debe a la inexistencia de documentos, esto con lleva a que los procesos se dupliquen y se desconozcan los responsables inmediatos en caso de desastre, sin sabes quién es el que debe asumir el control de la situación.

4.10.6 Acción de virus.

A la utilización de software en la EMUCE sin dar un respectiva capacitación. Al incumplimiento de los controles preventivos.

4.10.7 Terremotos.

Las oficinas deben tener una infraestructura que cumpla con las normas antisísmicas para prevenir daños físicos en los equipos, archivos y el personal.

4.10.8 Accesos no autorizados.

Los niveles de acceso a la información deben estar monitoreados para que ninguna entidad externa a la oficina tenga acceso sin previa autorización.

4.10.9 Robo de datos.

Por la deficiente seguridad física y lógica a la base de datos de los Sistemas produciéndose la perdida de información valiosa de toda la organización.

4.10.10 Fraude.

La ausencia de un sistema para la autorización de ingreso a las instalaciones y los sistemas puede dar pie a la modificación fraudulenta de la base de datos u otra documentación.

4.10.11 Inundaciones.

Un incremento en las precipitaciones pluviales hiciera que las alcantarillas se colapsen provocando el deterioro de la infraestructura de la oficina, así como la documentación, y el adecuado ambiente de trabajo para el personal.

4.10.12 Fallo en el suministro eléctrico.

Provocado por la discontinuidad en el servicio de energía eléctrica para el uso de los equipos.

4.10.13 Falla total o parcial del cableado.

Ocasiona pérdidas totales o parciales por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema.

4.10.14 A la falla de Software

Se produce debido a que no se hicieron las pruebas y la validación correspondiente del software para su utilización.

4.11 Probabilidad de Ocurrencia de Riesgos

TIPOS DE RIESGO	PROBABILIDAD
Fallo de Software	Alta
Acción de virus	Alta
Incendios	Media
Desconocimiento de la normatividad	Alta
Fallas en los equipos	Media
Fraude	Media
Equivocaciones	Media
Accesos no autorizados	Baja
Fallo en el suministro eléctrico	Alta
Fallo en el Cableado	Baja
Robo de datos	Baja
Robo común	Media

Terremotos	Baja
Inundaciones	Muy Baja
Vandalismo	Muy Baja

4.12 Plan de Contingencia para Cuidar la Integridad del Personal

4.12.1 Acciones antes de la contingencia

- Programar 2 simulacros al año
- Conocer el manejo de los extintores
- Contar con botiquines de primeros auxilios en áreas estratégicas
- Contar con capacitación de primeros auxilios
- Implementar alarmas de emergencia en lugares estratégicos dentro de la EMUCE
- Establecer puntos de reunión dentro y fuera de la EMUCE
- Difundir las rutas de evacuación, así como los sitios de localización de alarmas y extintores
- Establecer procedimientos de evacuación
- Capacitación permanente y actualizada a los comités de Seguridad
- Contar con un directorio del personal

4.12.2 Acciones durante la contingencia

- Accionar las alarmas de emergencia
- Dirigir a los usuarios en la evacuación e información de salidas de emergencia
- Priorizar la evacuación
- Llamar al 911

4.12.3 Acciones después de la contingencia

- Brindar los primeros auxilios a las personas que lo requieran.
- Realizar un recuento de los daños causados.
- Realizar un informe con los hallazgos y emitir a la Dirección.
- Tomar acciones de acuerdo al informe emitido.
- Retroalimentar los planes de contingencia con lo aprendido en la última contingencia.

4.12.4 Documentos necesarios previos a las contingencias

- Contar con una copia del inventario del mobiliario y equipo existente en el área.
- Contar con un listado de configuraciones del equipo de cómputo y telecomunicaciones que reside en el área.
- Contar con documentación al día de contratos de mantenimiento de infraestructura.

4.13 Plan de Contingencia en Caso de Incendio

4.13.1 Acciones antes de la contingencia

- Verificar periódicamente que las instalaciones eléctricas estén en perfecto estado.
- No concentrar grandes cantidades de papel, ni fumar cerca de químicos o sustancias volátiles.
- Verificar las condiciones de extintores e hidrantes y capacitarse para su manejo.
- No arrojar las colillas de cigarrillos a los cestos de basura, verificar que se hayan apagado bien los cigarrillos y no dejarlas en cualquier sitio, utilizar ceniceros.
- No almacenar sustancias y productos inflamables.
- No hacer demasiadas conexiones en contactos múltiples, evitar la sobrecarga de circuitos eléctricos.
- Por ningún motivo mojar las instalaciones eléctricas, recordar que el agua es un buen conductor de la electricidad.
- Si se detecta cualquier anomalía en los equipos de seguridad (Extintores, hidrantes, equipo de protección personal, etc.) y en las instalaciones eléctricas, reportar de inmediato al personal encargado de la seguridad.
- Mantener siempre limpia y en orden el área de trabajo, ya que no hacerlo es una de las causas que provocan incendios.
- Tener a la mano los números telefónicos de emergencia.

4.13.2 Acciones durante la contingencia

- Si se descubre un conato de incendio, actuar tranquilamente.
- Si se conoce sobre el manejo de extintores, intentar sofocar el fuego; si éste es considerable no tratar de extinguirlo con los propios medios, solicitar ayuda.
- Si el fuego esta fuera de control, realizar una evacuación del inmueble, siguiendo todas las indicaciones del personal de seguridad.
- Si hay humo donde se encuentra y no puede salir, mantenerse al ras del piso, cubriendo tu boca y nariz con un pañuelo bien mojado y respirar a través de él, intentar el traslado a pisos superiores.
- Si es posible, mojar la ropa.
- Verificar si las puertas están calientes antes de abrirlas, si lo están, busca otra salida.

4.12.3 Acciones después de la contingencia

- Retirarse inmediatamente del área incendiada y ubicarse en una zona de seguridad externa.
- No obstruir las labores del personal especializado, dejar que los profesionales se encarguen de sofocar el incendio.
- Personal calificado realizará una verificación física del inmueble y definirá si está en condiciones de ser utilizado normalmente.
- Colaborar con las autoridades.

4.14 Plan de Contingencia en Caso de Fallas de Hardware o Software

Analizar y evaluar el daño causado por la alteración del software o hardware.

4.14.1 En el caso de que la alteración haga imposible el inicio inmediato de las operaciones se procede como sigue:

- Recoger los respaldos de datos, programas, manuales y claves del lugar en el que se encuentren resguardados.
- Si las fallas se derivan del mal funcionamiento de un equipo (Hardware) proceder a su reemplazo inmediato o remitirse a la póliza de garantía.
- Instalar (sí lo amerita) el sistema operativo.
- Restaurar la información de las bases de datos y programas.
- Revisar y probar la integridad de los datos.
- Iniciar las operaciones.

4.14.2 En los casos en que la alteración puede ser corregida sin problemas graves, se procede conforme a lo siguiente:

- Corrección de las alteraciones que se localicen en los servidores Hardware.
- Corrección de las alteraciones que se localicen en los servidores Software.
- Revisar y probar la integridad de los datos.
- Iniciar las operaciones.

Las alteraciones que sufran los servidores tanto en Software y Hardware pueden ser corregidas en la mayoría de los casos, sin embargo en algunas ocasiones, las alteraciones llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días sin tener la absoluta certeza de que las correcciones que se hicieron fueron las necesarias, por tal motivo es mejor acudir a los respaldos de información y restaurar los datos, de esta forma las operaciones del día no se verán afectadas y al mismo tiempo se ponen al día los datos faltantes de la operación del día anterior.

4.15 Plan de Contingencia en Caso de Fallas de la Red de Datos

- Evaluación de las fallas.
- Si las fallas se derivan del mal funcionamiento de un equipo se procede a su reemplazo inmediato o remitirse a la póliza de mantenimiento.
- Si resulta ser un problema de configuración, se procede a su reconfiguración inmediata.
- Revisar y probar la integridad de las comunicaciones.
- Iniciar de las operaciones.

Las fallas del sistema de red pueden deberse al mal funcionamiento de los equipos ó a la pérdida de configuración de los mismos por lo que se deben evaluar las fallas para determinar si estas se derivan del mal funcionamiento de un equipo ó de la pérdida de su configuración.

CAPÍTULO V

PROCEDIMIENTOS DE SEGURIDAD

5.1 Procedimiento de Respaldo de Información

5.1.1 Objetivo

Definir la información de la EMUCE que será respaldada y establecer un esquema para su respaldo. Definir los controles para verificar el correcto desarrollo de los respaldos, así como pruebas periódicas de recuperación, con el objeto de asegurar la posibilidad de recuperar la información de la EMUCE en caso de ocurrir algún incidente que provoque la pérdida de información.

5.1.2 Alcance

El presente procedimiento será aplicado a toda la información almacenada en los equipos de procesamiento de la EMUCE

5.1.3 Responsabilidades

5.1.3.1 Propietario

El propietario del presente procedimiento es responsable del Centro de Cómputo**.** Sus responsabilidades son:

- Establecer las medidas de seguridad necesarias para garantizar el adecuado almacenamiento del presente documento.
- Definir los perfiles que tendrán acceso al documento.
- Asegurar la accesibilidad del documento para quienes necesiten consultarlo.
- Comunicar la existencia del documento y asesorar sobre el mismo a los responsables de su cumplimiento.
- Solicitar actualizaciones fuera del esquema normal.

5.1.3.2 Responsables de cumplimiento

Es responsable del cumplimiento del presente procedimiento es el responsable del Centro de Cómputo, quien está a cargo de realizar el respaldo de la información.

5.1.3.3 Responsables de actualización

El responsable de la actualización del presente procedimiento es el responsable del Centro de Cómputo. Su responsabilidad es revisar y actualizar en caso que corresponda, el presente documento de acuerdo al esquema de revisión y actualización establecido y a las solicitudes efectuadas por el responsable del mismo.

5.1.4 Régimen de revisión y actualización

El presente documento será revisado semestralmente y actualizado en el caso de detectarse la necesidad de efectuar modificaciones que permitan mantenerlo actualizado en relación a la realidad de la estructura funcional y del ambiente informático.

Por otra parte, se realizarán las modificaciones que sean necesarias en el caso que se produjeran cambios que lo requieran, fuera de las revisiones programadas.

5.1.5 Desarrollo

A continuación se definen en primera instancia, los requisitos de respaldo que se adoptarán para los diferentes tipos de información de la EMUCE. Luego se establece el esquema de respaldo para cada tipo de información, así como su rotulado y almacenamiento.

5.1.5.1 Requisitos de respaldo

A continuación se detallan los requisitos de respaldo para cada tipo de información, de acuerdo a lo manifestado por sus propietarios. Dichos

requisitos serán los que determinen el tipo de respaldo a ser implementado para la información.

REQUISITOS DE RESPALDO			
Tipo de Información	Dueño(*)	Requisitos de Respaldo	Observaciones

(*) De acuerdo con lo establecido en la Política de Seguridad de la Información

Los requisitos de respaldo pueden ser, por ejemplo, asegurar la recuperación de la información del día anterior, la necesidad de guardar copias de respaldo históricos por un determinado período, etc.

5.1.6 Características del respaldo

5.1.6.1 Periodicidad

Para cada tipo de información se establece la periodicidad con la cual se realizarán los respaldos. Los períodos establecidos son:

- ANUAL: el respaldo se realiza una vez al año, generalmente el último día hábil
- MENSUAL: el respaldo se realiza una vez al mes, generalmente el último día hábil.
- SEMANAL: el respaldo se realiza una vez a la semana, generalmente el último día hábil.
- DIARIO: el respaldo se realiza una vez al día.
- OTROS: destinado al tipo de información que requiere ser resguardada con mayor frecuencia.

5.1.6.2 Tipo

Los respaldos pueden ser de diferente tipo de acuerdo a la información que contienen respecto del respaldo anterior. A continuación se definen los tipos de respaldo utilizados:

• COMPLETO: se resguarda toda la información

• INCREMENTAL: se resguarda la información que se haya incorporado desde el último respaldo realizado

• DIFERENCIAL: se resguarda sólo la información que se haya modificado desde el último respaldo realizado.

5.1.6.3 Rotación de las copias

Se establece el siguiente criterio para la reutilización de los dispositivos físicos de respaldo:

ANUALES: se conservarán todas las copias anuales, por lo que dichos dispositivos no tienen rotación.

MENSUALES: se mantienen 12 copias anuales, por lo que su rotación es anual.

SEMANALES: se mantienen cuatro copias semanales, por lo que su rotación es mensual.

DIARIAS: se mantienen cinco copias diarias (o bien la cantidad de días hábiles en una semana), por lo que su rotación es semanal.

Los dispositivos serán reutilizados un máximo de 12 veces.

A continuación se presenta una planilla de control de reutilización de cintas:

Tipo de Información		Utilización Máxima	Vencimiento
Mensual	Enero aaaa	x veces	Enero (aaaa + x)
	Febrero aaaa		
	Marzo aaaa		
	Abril aaaa		
	Mayo aaaa		
	Junio aaaa		
	Julio aaaa		
	Agosto aaaa		
	Septiembre aaaa		
	Octubre aaaa		
	Noviembre aaaa		
	Diciembre aaaa		
Semanal	1°Semana		
	2°Semana		
	3°Semana		
	4°Semana		
Diario	Lunes		
	Martes		
	Miércoles		
	Jueves		
	Viernes		

Aclaraciones:

Utilización máxima se refiere a la cantidad de veces que el proveedor del dispositivo aconseja utilizarlo como máximo.

“aaaa” corresponde al año.

Los dispositivos que deban ser dados de baja debido a la imposibilidad de reutilizarlos serán eliminados de acuerdo a lo establecido en la Política de Seguridad en relación a la eliminación segura de medios que contienen información.

5.1.6.4 Esquema de respaldo

A continuación se describe el esquema de respaldo de cada tipo de información definida en requisitos de respaldo:

<table>
<tr><td colspan="4">ESQUEMA DE RESPALDO</td></tr>
<tr><td>Tipo de Información:</td><td colspan="3"></td></tr>
<tr><td>Ubicación</td><td colspan="3"></td></tr>
<tr><td rowspan="12">Mensual</td><td rowspan="3">Diario</td><td>Completo</td><td></td></tr>
<tr><td>Incremental</td><td>Lunes a Viernes a las 21 horas</td></tr>
<tr><td>Diferencial</td><td></td></tr>
<tr><td rowspan="3">Semanal</td><td>Completo</td><td></td></tr>
<tr><td>Incremental</td><td>Sábado a las 04 horas</td></tr>
<tr><td>Diferencial</td><td></td></tr>
<tr><td rowspan="3">Mensual</td><td>Completo</td><td>Último día hábil del mes a las 23 horas</td></tr>
<tr><td>Incremental</td><td></td></tr>
<tr><td>Diferencial</td><td></td></tr>
<tr><td rowspan="3">Anual</td><td>Completo</td><td>Primer día hábil del año siguiente a las 04 horas</td></tr>
<tr><td>Incremental</td><td></td></tr>
<tr><td>Diferencial</td><td></td></tr>
<tr><td>Dispositivo:</td><td colspan="3"></td></tr>
<tr><td>Responsable:</td><td colspan="3"></td></tr>
</table>

El esquema planteado es sólo un ejemplo.

Consideraciones:

- La “Ubicación” se refiere al equipo en el cual se ubica físicamente la información.

- En cada caso, se deberá describir el horario en el que se realizará el respaldo. En los casos en que no aplique un tipo de respaldo, se completará con “N/A”.

- El “Dispositivo” se refiere al soporte físico en el cual se resguardará la información.

- El “Responsable” es la persona que deberá garantizar que cada respaldo se realice de forma adecuada, en tiempo y forma.

5.1.6.5 Rotulado de dispositivos físicos

Los respaldos serán realizados en cinta magnética.

En primera instancia se define la siguiente codificación para cada tipo de información:

Tipo de Información	Ubicación	Codificación(*)

(*) Consiste en tres letras.

Cada unidad de respaldo contará con una etiqueta en la que se escribirá lo siguiente:

Anual	Mensual	Semanal	Diario
IIATaaaa Donde: III es el tipo de información (campo codificación de la tabla anterior) A indica que se trata de una copia anual T es el tipo de respaldo donde “C” corresponde a completo “I” a Incremental y “D” a diferencial aaaa es el año al que corresponde.	**IIIMTmm** Donde: III es el tipo de información. M indica que se trata de una copia mensual. T es el tipo de respaldo donde “C” corresponde a completo “I” a incremental y “D” a diferencial. mm es el mes	**IIISTn** Donde: III es el tipo de información. S indica que se trata de una copia semanal. T es el tipo de respaldo donde “C” corresponde a completo “I” a incremental y “D” a diferencial n es “1” si corresponde a la 1º semana “2” a la 2º “3” a la 3º, “4” la 4º.	**IIIDTndd** Donde III es el tipo de información D indica que se trata de una copia diaria. T es el tipo de respaldo donde “C” corresponde a completo, “I” a incremental y “D” a diferencial n es “1” si corresponde a 1º quincena “2” si corresponde 2º. dd es “Lu” si corresponde al lunes, “Ma” al martes, “Mi” al Miércoles “Ju” a jueves “Vi” a viernes y “Sa” al sábado

5.1.6.6 Almacenamiento de las copias

Las copias de respaldo serán almacenadas de acuerdo al siguiente esquema:

Las copias anuales y mensuales se trasladarán para su almacenamiento en un sitio externo a la EMUCE.

Tener en cuenta que el mismo debe contemplar las medidas de seguridad física adecuadas para la conservación de las copias y que las mismas deben permanecer accesibles en caso de ser necesario recuperarlas.

El responsable de su traslado, a dicho sitio y su recuperación para la reutilización es el responsable del Centro de Cómputo.

Durante el traslado se tomarán las medidas de seguridad correspondientes para resguardar los dispositivos de posibles robos o daño físico.

A continuación se detalla el personal con acceso a las copias de respaldo:

Sitio de Respaldo	Ubicación	Personal Autorizado
Gabinete de cintas		
Sitio externo		

5.1.6.7 Control del proceso de respaldo

Con el objeto de asegurar la correcta ejecución de los procesos de respaldo de información de la EMUCE cada responsable de respaldo, definido en el esquema de respaldo, se verificará la ejecución de los mismos mediante las herramientas definidas a continuación:

Tipo de Información	Herramienta de respaldo	Herramienta de control del proceso de respaldo

Ejemplos de herramientas de control son los logs del sistema operativo (registros de auditoria) o de la herramienta de respaldo, o consolas propias de dichas herramientas.

Como resultado de este control, el responsable de cada respaldo completará la siguiente planilla:

PLANTILLA DE CONTROL DE PROCESOS DE RESPALDO					
Tipo de información:					
Responsable:					
Respaldo	Resultado(*)	Fecha	Hora	Acciones Tomadas	Nuevos Resultado
BDXDC1Lu					
BDXDC1Ma					
BDXDC1Mi					
BDXDC1Ju					
BDXDC1Vi					
BDXSC1012005					
BDXDC2Lu					
BDXDC2Ma					
BDXDC2Mi					
BDXDC2Ju					
BDXDC2Vi					
BDXSC2012005					
BDXMC012005					
Etc.					

(*) Indicar si el proceso se ha completado en forma correcta (C) o (I).

Esta planilla debe ser completada luego de finalizado cada respaldo, indicando si el proceso concluyó correctamente, o bien si presentó problemas y qué acciones fueron tomadas.

5.1.6.8 Verificación de la restauración

Se realizará la verificación de la recuperación de las copias de respaldo de acuerdo al procedimiento detallado en el punto procedimientos de recuperación del Procedimiento Recuperación de información", con el siguiente esquema para cada tipo de información:

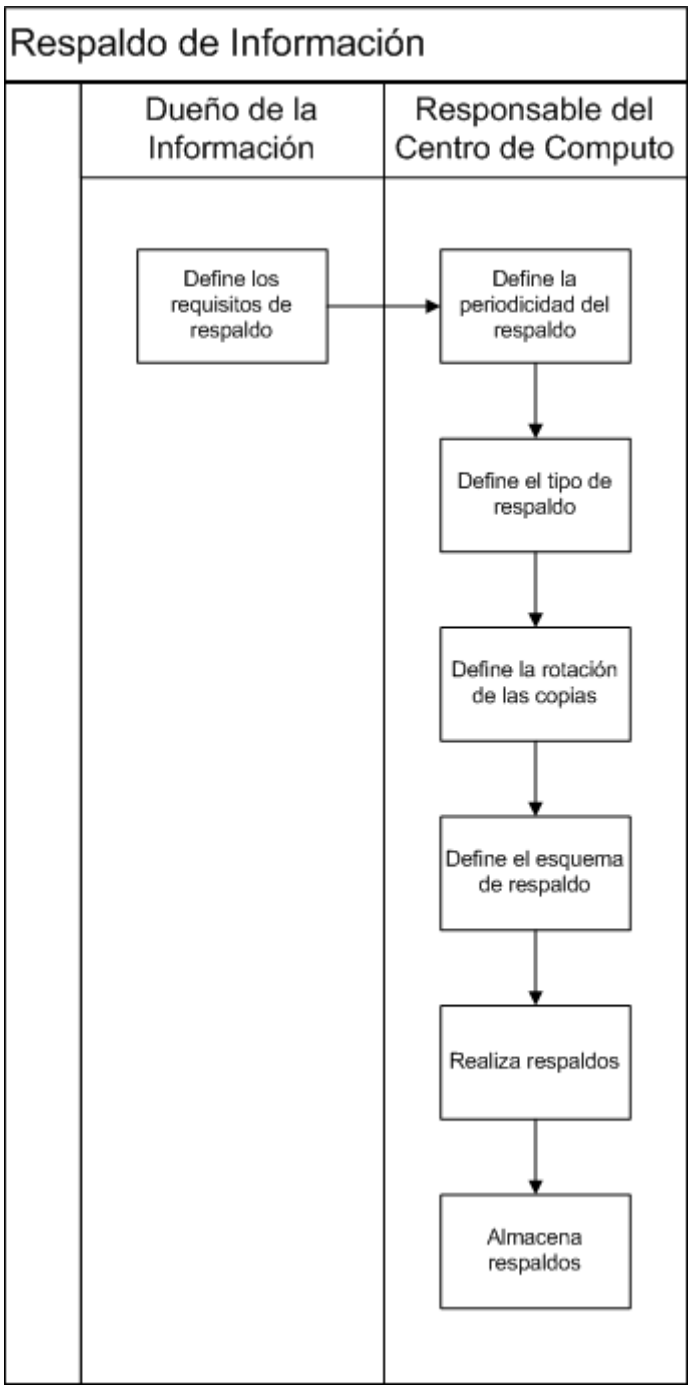
- Semanalmente se restaurará una copia diaria realizada
- Trimestralmente se restaurará la última copia mensual realizada

La recuperación se realizará en un ambiente de prueba para evitar que dicho proceso afecte al ambiente de producción.

Como resultado de la prueba, se completará la siguiente planilla:

PLANILLA DE VERIFICACION DE LA RESTAURACION			
Tipo de Información:			
Responsable:			
Fecha de Prueba	Respaldo (etiqueta)	Resultado	Acciones Tomadas

5.1.7 Esquema del proceso de respaldo de información



5.2 Procedimiento de Administración de Usuarios

5.2.1 Objetivo

Documentar un proceso de solicitud, análisis, aprobación e implementación de acceso lógico a los recursos de la EMUCE.

Estandarizar formularios para la solicitud de altas, bajas o modificaciones de accesos a los recursos de manera de contemplar todos los posibles requerimientos de un usuario.

Disponer la documentación administrativa e informáticamente organizada a los fines de establecer un sistema eficiente para los usuarios que operan en la red.

5.2.2 Alcance

El presente procedimiento será aplicado al control de acceso lógico a los siguientes componentes del ambiente informático:

- Información de la EMUCE
- Plataformas de procesamiento (o sistemas operativos)
- Bases de datos con información de la EMUCE
- Sistemas que procesan información de la EMUCE
- Servicios de red informática (ej.: correo electrónico, Internet, impresoras, etc.)

5.2.3 Responsabilidades

5.2.3.1 Propietario

El propietario del este procedimiento es el responsable del Centro de Cómputo. Sus responsabilidades principales son:

- Establecer las medidas de seguridad necesarias para garantizar el adecuado almacenamiento del presente documento.
- Definir los perfiles que tendrán acceso al documento.
- Asegurar la accesibilidad del documento para quienes necesiten consultarlo.
- Comunicar la existencia del documento y asesorar sobre el mismo a los responsables de su cumplimiento.
- Solicitar actualizaciones fuera del esquema normal.

5.2.3.2 Responsables de cumplimiento

Son responsables del cumplimiento del este procedimiento todos los empleados de la EMUCE, así como terceros que hagan uso de cualquier recurso informático perteneciente a la misma.

5.2.3.2 Responsables de actualización.

El responsable de la actualización del presente procedimiento es el responsable del Centro de Cómputo en su carácter de responsable de la seguridad informática de la EMUCE. Su responsabilidad es revisar, actualizar en caso que corresponda, y archivar el presente documento de acuerdo al esquema de revisión y actualización establecido y a las solicitudes efectuadas por el propietario del mismo.

5.2.4 Régimen de revisión y actualización

El presente documento será revisado semestralmente y actualizado en el caso de detectarse la necesidad de efectuar modificaciones que permitan mantenerlo actualizado en relación a la realidad de la estructura funcional y del ambiente informático.

5.2.5 Desarrollo

De acuerdo a lo establecido en la Política de Seguridad, todos los usuarios tendrán un identificador único (ID de usuario) solamente para su uso exclusivo, de manera que las transacciones puedan rastrearse con posterioridad hasta llegar al individuo que las haya efectuado. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

No se permite utilizar un mismo usuario identificador compartido para un grupo de personas. A continuación se definen términos que serán empleados en el presente procedimiento:

Cuenta: se entiende por cuenta, al ID de usuario y su contraseña asociada que le permiten ingresar de forma autorizada a un entorno (de red, plataforma o sistema).

Perfil: conjunto de permisos o funciones que puede realizar un usuario. Los perfiles se asocian a las cuentas de usuario.

5.2.5.1 Alta de un usuario

El alta de una cuenta se realizará mediante los siguientes pasos:

5.2.5.1.1 Forma:

Se solicita a través de nota/memorándum al Centro de Cómputo.

5.2.5.1.2 Contenido:

- La misma deberá contener nombre y apellido del usuario.
- Sector en el que prestará servicios.
- Sistemas a los que debería tener acceso
- Número de legajo ó número de documento.

5.2.5.1.3 Personas habilitadas para la solicitud de altas de usuarios:

La solicitud de alta de usuarios, únicamente podrá ser efectuada por los Jefes departamentales.

5.2.5.1.4 Documentación a presentar:

Dicha nota/memorándum, deberá acompañarse de un formulario de "Solicitud de alta de usuario". El formulario de "Solicitud de Alta de Usuario" deberá ser elaborado por el responsable del Centro de Cómputo.

5.2.5.1.5 Presentación:

Luego de completado, el formulario debe ser presentado al Centro de Cómputo, para su aprobación.

5.2.5.1.6 Registro:

Toda vez que se adicione un usuario, se debe registrar el cambio en sus archivos administrativos.

5.2.5.1.7 Aviso al Usuario:

Por último, se debe proveer al nuevo usuario la información necesaria para comenzar a utilizar su cuenta. Dicha información refiere al nombre de usuario y a la contraseña del recurso solicitado. De esta forma se concreta la finalización del proceso de alta.

5.2.5.1.8 Aclaraciones:

Cabe aclarar que el formulario se completa solamente de manera personalizada, mientras que la nota/memorándum puede que sea conjunta, es decir que contenga la solicitud de alta de varios usuarios a la vez.

Ante esto, es necesario otorgarle a cada nota/memorando un número interno, que permitirá operativizar su búsqueda en la documentación en papel.

Teniendo en cuenta que, varios formularios pueden remitir a una misma nota/memorando es fundamental que cada uno contenga el número interno al que se remite, para obtener un mejor control.

5.2.5.2 Nombre de un usuario

Este nombre es asignado por el Centro de Cómputo, quien lo comunicará directamente al usuario.

Este nombre será la "identificación" del usuario y se ingresará al ejecutar el usuario el inicio del sistema operativo.

5.2.5.1.1 Pautas y Características:

Tendrá una longitud mínima de 4 (cuatro) y una longitud máxima de 16 (dieciséis) caracteres.

Como norma se utilizará la inicial del nombre y el apellido del usuario (Ej. Juan Pérez será jperez; en el caso de apellidos muy extensos, podrá utilizarse parte del apellido)

Para los apellidos compuestos se tendrán en cuenta siempre el primer nombre y el primer apellido. Puede suceder que ya exista un usuario con la misma identidad, por lo que se utilizarán las iníciales del primero y segundo nombre para no repetir el ID del usuario.

5.2.5.3 Contraseña (password)

5.2.5.3.1 Asignación de contraseña

Para el primer ingreso al sistema, el responsable del Centro de Cómputo le comunica su nombre de usuario y le asigna como contraseña su número de documento de identificación del usuario.

Asimismo, el responsable del Centro de Cómputo debe seleccionar la opción para que el usuario al entrar por primera vez, le aparezca la advertencia de que su contraseña ha caducado y comience con el proceso de cambio de su contraseña.

5.2.5.3.2 Cambio de contraseña.

Cuando inicie la sesión de red con su nombre de usuario (por Ej.: agarcia), aparecerá una ventana indicando que su contraseña ha caducado.

Deberá hacer clic en el botón Aceptar.

Luego se presentará una segunda ventana donde ya aparecerá escrita su contraseña actual en el campo correspondiente a la contraseña anterior y dos campos donde deberá ingresar la contraseña nueva.

Las reglas de la política, que rige la nueva contraseña son:

- Longitud mínima de 8 (ocho) caracteres y máxima de 12 (doce) caracteres.
- Puede ser alfanumérica (combinación de números y letras). Condición no excluyente.
- Los caracteres permitidos son: letras mayúsculas y minúsculas; números entre el 0 (cero) y el 9 (nueve). No utilizar acentos y/u otros símbolos.
- La contraseña es sensible a mayúsculas y minúsculas, es decir, ‘a’ no es lo mismo que ‘A’.
- No podrá repetirse la contraseña anterior, al menos las correspondientes a los 3 últimos cambios.
- De no cumplirse con una de estas reglas, aparecerá una ventana advirtiendo el error, y que vuelva a escribir su nueva contraseña respetando las reglas anteriormente especificadas.
- Por el contrario si se cumple con las reglas, el proceso de cambio de contraseña será exitoso.

Para ingresos sucesivos, el usuario deberá identificarse, ingresando su nombre de usuario y a continuación la contraseña nueva que ha elegido.

La contraseña es confidencial, de uso exclusivo del usuario, no podrá ser igual al nombre de usuario y no debe **"prestarse"** a otros usuarios.

En lo referente a correo electrónico, como la contraseña de correo es la misma que la de usuario de red, al revisar su casilla de correo o hacer click en "enviar y recibir" se le solicitará también que ingrese la nueva contraseña.

Esta última operación, deberá ejecutarse por lo menos 15 minutos después de haber cambiado la contraseña de red.

Si se presenta un problema o anomalía durante el proceso deberá comunicarse con el Centro de Cómputo de la EMUCE.

5.2.5.4 Modificación de una cuenta/perfil existente

La modificación de una cuenta se realizará mediante los siguientes pasos:

5.2.5.4.1 Forma:

Se solicita a través de nota/memorándum al Centro de Cómputo.

5.2.5.4.2 Contenido:

- La misma deberá contener nombre y apellido del usuario.
- Sector en el que prestará servicios.
- Perfiles o accesos que se quieren modificar.
- Número de legajo ó número de documento.

5.2.5.2.3 Personas habilitadas para la solicitud de modificaciones de usuarios:

La modificación de usuarios, únicamente podrá ser efectuada por los Jefes Departamentales.

Dicha nota/memorándum, deberá acompañarse de un formulario de "Solicitud de modificación de usuario" que deberá ser elaborado para el Centro de Cómputo.

Completo el formulario, debe ser presentado al responsable del Centro de Cómputo, para su aprobación.

Toda vez que el responsable del Centro de Cómputos modifique el perfil de un usuario, deberá registrar el cambio en sus archivos administrativos.

Por último, se debe proveer al nuevo usuario la información necesaria para comenzar a utilizar el sistema. Dicha información refiere al nombre de usuario y a la contraseña del recurso solicitado. La misma se entrega en un formulario sellado. Así finaliza el proceso de modificación.

Cabe aclarar que el formulario se completa solamente de manera personalizada, mientras que la nota/memorándum puede que sea conjunta, es decir que contenga la solicitud de modificación de varios usuarios a la vez.

Antes esto, es necesario otorgarle a cada nota/memorando un número interno, que permitirá operativizar su búsqueda en la documentación en papel. Teniendo en cuenta que varios formularios pueden remitir a una misma nota/memorando, es fundamental que cada uno contenga el número interno al que se remite, para obtener un mejor control.

5.2.5.2.4 Por cambio de funciones

En los casos en los que un usuario cambie de función, o pase a depender de otra área o sección, se debe modificar el perfil con el que contaba hasta el momento. Para ello se seguirán los siguientes pasos:

La autoridad del usuario cuya cuenta debe ser modificada deberá enviar un memorándum con la información detallada a continuación, lo firmará y lo remitirá a Coordinación Informática.

Información a completar en el formulario:

- Datos del usuario
- Tipo de Modificación
- Fecha de Modificación: Si es “Programada” o “Inmediata” según corresponda. En caso de tratarse de una modificación programada, se indicará asimismo la fecha prevista.

El Responsable de Seguridad Informática controlará la existencia de toda la información requerida en el formulario y evaluará el posible impacto de la baja en otras áreas de incumbencia (por ej. la necesidad de solicitar cambios de perfiles como consecuencia).

Luego de finalizadas las tareas operativas, el sector a cargo de la administración de usuarios deberá Informar al superior que solicitó la modificación.

La nueva autoridad del usuario cuya cuenta debe ser modificada para ser utilizada eficazmente en su nueva sección de trabajo, completará el formulario de “Solicitud de Modificación de usuario” y lo remitirá al Centro de Cómputo.

Información a completar en el formulario:

- Datos del usuario
- Tipo de Modificación
- Fecha de Modificación: Si es “Programada” o “Inmediata” según corresponda. En caso de tratarse de una modificación programada, se indicará asimismo la fecha prevista.

5.2.5.3 Acciones por incumplimiento

5.2.5.3.1 Bloqueo de un usuario

El Centro de Cómputo cuenta con una estructura de recursos de hardware que permite realizar un monitoreo de las actividades de cada servidor, motivo por el cual ante la violación de cualquiera de los puntos anteriormente descriptos, sin previo aviso se procederá a:

- Borrado de todo tipo de archivo y/o acceso no permitido, Ej. Música, Messenger, videos, software sin licencia y otros.
- Bloqueo de la cuenta de usuario y restricción de acceso a la red del organismo, situación que podrá revertirse, mediante la solicitud de reconexión de servicio.

5.2.5.3.2 Reconexión de un usuario

La Reconexión de un Usuario deberá ser solicitada cuando éste último no haya cumplido con alguna de las normativas especificadas en el manual de Políticas para Internet u otras.

Cuando esto sucede, al usuario se le restringe el acceso al servidor y para recuperarlo debe solicitar la reconexión.

Para esto, es necesario que se presente al Centro de Cómputo, un memorándum especificando las causas que provocaron la restricción al servidor y solicitando la reconexión.

Dicho memorándum debe estar firmado por el solicitante y por el responsable del área administrativa a la que pertenece el usuario.

5.2.5.3.3 Recomendaciones generales

Se sugiere eliminar de los servidores archivos viejos, inútiles a la fecha y/o que no se utilicen.

Se recuerda que todos los archivos que se encuentran en discos de terminales NO son responsabilidad del Centro de Cómputo. En caso de necesitarse un respaldo especial, éste debe solicitarse en forma puntual.

5.2.5.4 Baja de un usuario

5.2.5.4.1 Por desvinculación

Cuando un empleado se desvincule de la EMUCE, la baja de su cuenta se efectuará mediante los siguientes pasos:

El Jefe Departamental que tenga a su cargo al usuario que se desvincula, deberá completar el formulario de “Solicitud de baja de usuario”. El formulario de Solicitud de Baja de Usuario deberá ser generado por el Centro de Cómputo.

Información a completar en el formulario:

- Datos del usuario
- Tipo de baja
- Fecha de baja: Si es “Baja Programada” o “Baja Inmediata” según corresponda. En caso de tratarse de una baja programada, se indicará asimismo la fecha prevista de baja.

El Responsable de Seguridad Informática realizará lo siguiente:

- Controlar la veracidad de toda la información requerida en el formulario.

- Completar la información relacionada a “Cuentas a dar de baja”, detallando las cuentas a eliminar e indicando a qué sistema/ambiente pertenecen.

- Firmar el formulario y solicitar la baja al sector a cargo de la administración de usuarios.

El sector a cargo de la administración de usuarios procederá a realizar las tareas operativas para luego:

- Firmar el formulario y remitirlo al Responsable de Seguridad Informática

- Informar al Responsable solicitante.

Es importante que estos pasos se realicen con suma URGENCIA al momento de decidirse o recibirse la comunicación indicando la desvinculación inmediata.

5.2.5.5 Manejo interno de administración de usuarios

5.2.5.5.1 Recepción de Documentación

Para el inicio del procedimiento de alta-baja-modificación, se debe presentar al Centro de Cómputo los siguientes dos documentos, que deben estar firmados y sellados por el responsable del área o sector emisor:

- Memorándum

- Formulario de Solicitud de Usuario

El Memorándum debe ser presentado por duplicado, uno para el Centro de Cómputo y el otro que se sellará y se devolverá para que el solicitante tenga un comprobante de la recepción del trámite.

Asimismo, el Centro de Cómputo debe recibir conjuntamente con el Memorándum respectivo, el Formulario de Solicitud del usuario/s. En el mismo, se debe detallar los mismos datos que se solicitan en el memorándum, junto a los datos personales del usuario. Si lo solicitado entre el memorándum y la solicitud no coincide, se deberá pedir al solicitante que rehaga la documentación. Hasta que esto no se cumpla no se dará curso a lo solicitado.

5.2.5.5.2 Manejo Interno de Documentación

Una vez ingresada la Documentación el centro de Cómputo se encargará de procesar la información de la siguiente manera:

- Dar curso a la Solicitud
- Cargar en “Base Solicitud de Usuarios”
- Aviso al Usuario
- Archivo de la Documentación

Los Administradores del Sistema, son los encargados de actualizar los servicios que la solicitud pide.

Es muy importante que el Usuario que hace el requerimiento sea avisado a la brevedad sobre el destino de la solicitud.

Tanto el memo, como la solicitud deberán ser archivadas, por los encargados administrativos de la documentación.

5.2.5.5.3 Archivo de documentación (memorándum/formularios)

Como del Memorándum pueden depender varias solicitudes, se le debe asignar un número interno, que será escrito también en cada formulario que derive de dicho memorándum, y deben ordenarse en el archivo de acuerdo a dicho número.

En tanto, los formularios que son personalizados, uno para cada usuario, deben archivarse por orden alfabético en sus respectivas carpetas.

De esta manera, al buscar un formulario, se puede detectar rápidamente el memorándum que lo acompaña, mediante el número interno que le fue asignado, tornando operativo el procedimiento y agilizando la búsqueda de la documentación en papel.

5.2.5.6 Inexistencia de documentación

En caso de efectuar un alta, cambio o baja de usuario, sin previa entrega de Formulario y Memorándum al Centro de Computo, los administradores deben avisar a los encargados de los archivos, para que tomen las medidas correspondientes para adquirir la documentación.

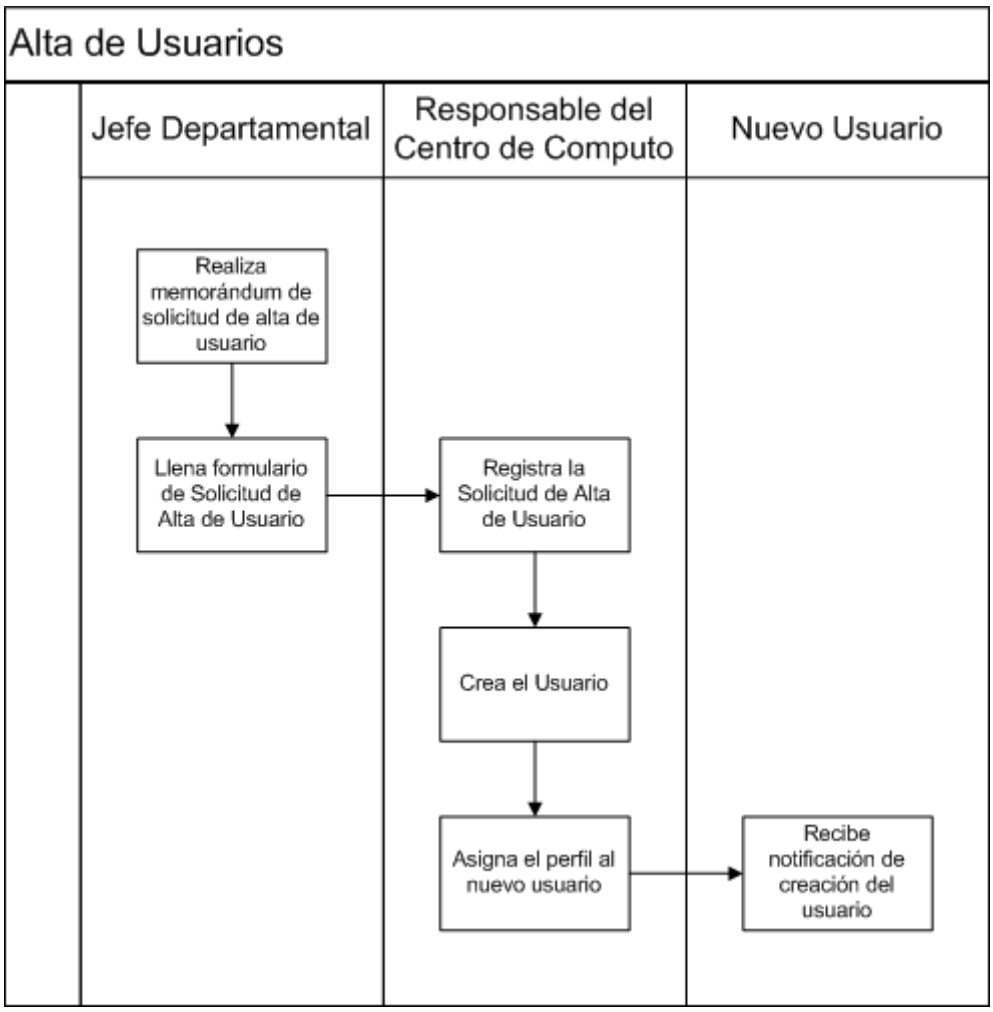
Este caso solo se acepta de manera excepcional si la solicitud es expedida por algún alto funcionario que manifiesta urgencia en el requerimiento.

Caso contrario, todas las altas, cambios o bajas de usuario deben solicitarse mediante memorándum y formulario con anterioridad.

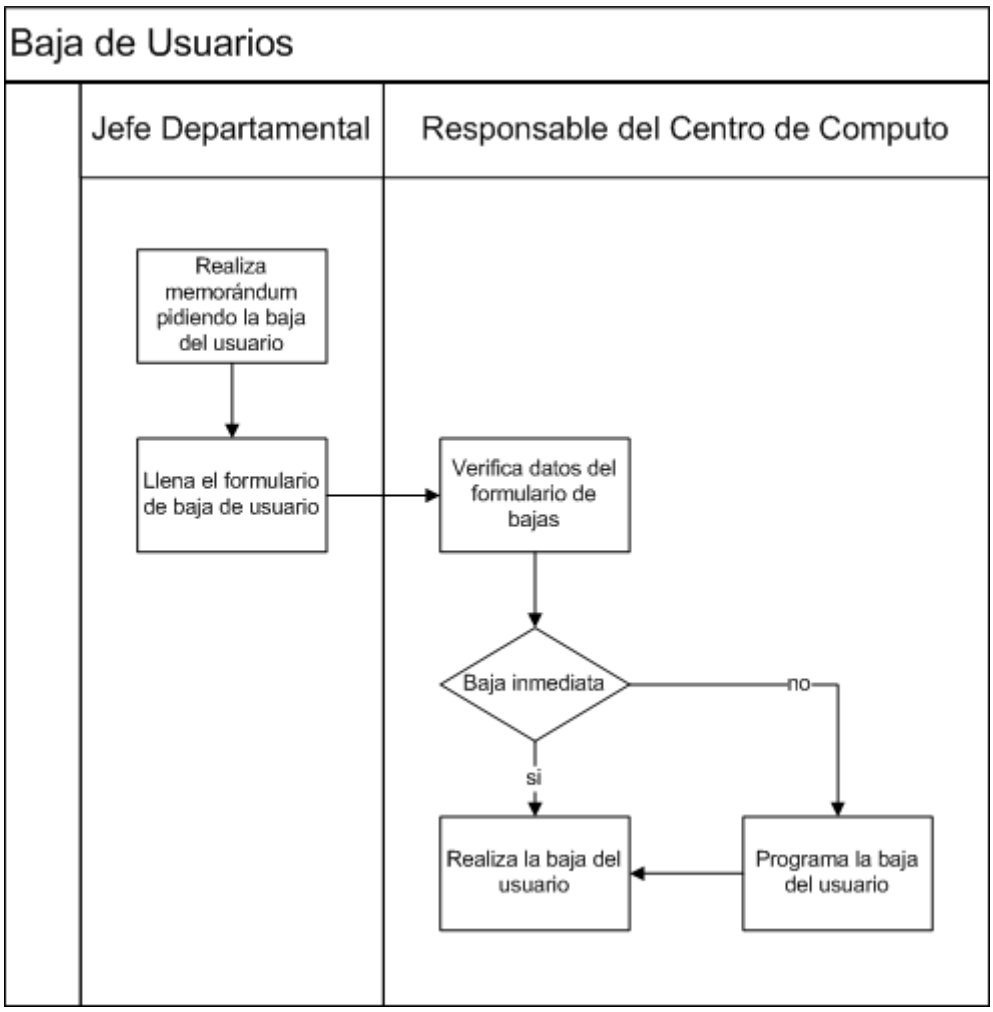
Si no existiese la documentación de usuarios ya existentes, se les solicitará que regularicen su situación, o en caso contrario en 48 hs. se dará de baja su cuenta automáticamente.

Si aún así no se regulariza la documentación, desde el Centro de Computo se le facilitará al usuario el formulario y memorándum, para que proceda a completarlo y hacerlo firmar por la autoridad correspondiente.

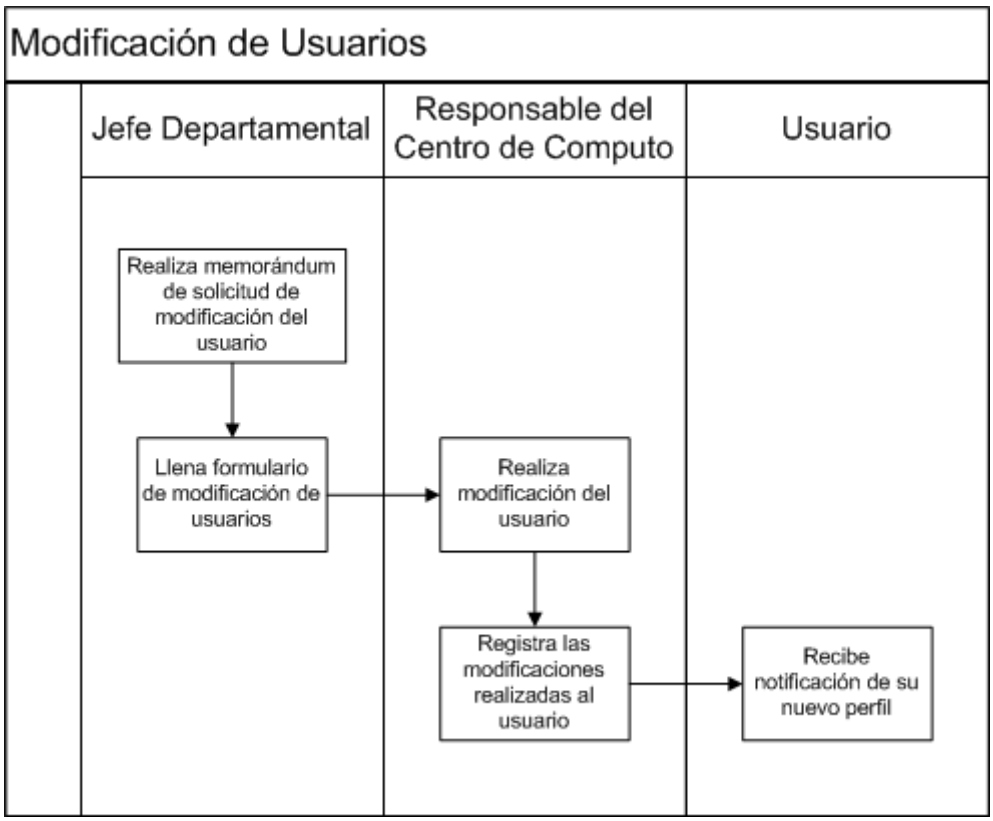
5.2.6 Esquema del proceso de alta de usuarios



5.2.7 Esquema del proceso de baja de usuarios



5.2.8 Esquema del proceso de modificación de usuarios



5.3 Procedimiento de Administración de Políticas para Internet

5.3.1 Objetivo

Desarrollar y mantener los recursos institucionales para el acceso a Internet.

5.3.2 Alcance

El presente procedimiento será aplicado todas las personas que cuentan con acceso a Internet tanto a nivel de navegabilidad como de correo electrónico.

5.3.3 Responsabilidades

5.3.3.1 Propietario

El propietario del presente procedimiento es el responsable del Centro de Cómputo. Sus responsabilidades son:

- Establecer las medidas de seguridad para garantizar el adecuado almacenamiento del presente documento.
- Definir los perfiles que tendrán acceso al documento.
- Asegurar la accesibilidad del documento para quienes necesiten consultarlo.
- Comunicar la existencia del documento y asesorar sobre el mismo a los responsables de su cumplimiento.
- Solicitar actualizaciones fuera del esquema normal.

5.3.3.2 Responsables de cumplimiento

Son responsables del cumplimiento del presente procedimiento todos los empleados de la EMUCE, así como terceros que hagan uso de cualquier recurso informático perteneciente al mismo.

5.3.3.3 Responsables de actualización

El responsable de la actualización del presente procedimiento es el responsable del Centro de Cómputo. Su responsabilidad es revisar y actualizar en caso que corresponda, el presente documento de acuerdo al esquema de revisión y actualización establecido y a las solicitudes efectuadas por el propietario del mismo.

5.3.4 Régimen de revisión y actualización

El presente documento será revisado semestralmente y actualizado en el caso de detectarse la necesidad de efectuar modificaciones que permitan mantenerlo actualizado en relación a la realidad de la estructura funcional y del ambiente informático. Por otra parte, se realizarán las modificaciones que sean necesarias en el caso que se produjeran cambios que lo requieran, fuera de las revisiones programadas.

5.3.5 Desarrollo

5.3.5.1 A nivel de Servicio de Navegación

El servicio de navegación en Internet se encuentra regulado de acuerdo a las posibilidades de seguridad y de prestación del equipamiento existente a nivel comunicaciones, hardware y networking.

El Centro de Cómputo resuelve, según sea:

Restringir navegación en horarios pico y todas aquellas restricciones que se hagan necesarias a efectos de mantener los niveles de velocidad en forma distribuida para todos los usuarios habilitados.

Asimismo, está prohibida cualquier acción destinada a bajar archivos de música, videos, etc., que ponen en riesgo la seguridad informática de los equipos y de la red.

La restricciones de navegación están implementadas sobre páginas no permitidas con contenidos pornográficos, musicales, webmails, mensajeros instantáneos, chat y otros indebidos.

5.3.5.2 A nivel de Servicio de Correo Electrónico

Este servicio debe ser utilizado únicamente para fines laborales, quedando terminantemente prohibida su utilización en cuestiones de índole personal.

Al momento de enviar un correo electrónico se debe tener en cuenta que sólo se manda a un máximo de 20 destinatarios, ya que ese es el límite permitido.

La capacidad del buzón del Correo Electrónico no puede superar los 13 MB.

Los archivos que se adjuntan para ser enviados por e-mail no pueden superar los 10MB, de manera contraria el servidor rechazará el envío.

De igual forma, se da a conocer que se encuentra bloqueada la descarga de archivos con extensiones dudosas como por ejemplo “.exe”, “.scr”, “.piff”, etc., pudiendo sólo abrir archivos con extensiones convencionales como por ej. los “.doc”, “.xls”, y “.pdf”

5.4 Procedimiento Auditoría Automática de los Sistemas

5.4.1 Objetivo

Definir las pautas generales para asegurar una adecuada identificación y seguimiento de los eventos de seguridad de los sistemas.

5.4.2 Alcance

Todo el personal de la EMUCE y los terceros, que interactúan de manera habitual u ocasional, que accedan a información y/o a los recursos informáticos.

5.4.3 Responsabilidades

5.4.3.1 Propietario

El propietario del presente procedimiento es el responsable del Centro de Cómputo en su carácter de responsable de Seguridad Informática de la EMUCE. Sus responsabilidades son:

- Establecer las medidas de seguridad necesarias para garantizar el adecuado almacenamiento del presente documento.
- Definir los perfiles que tendrán acceso al documento.
- Asegurar la accesibilidad del documento para quienes necesiten consultarlo.
- Comunicar la existencia del documento y asesorar sobre el mismo a los responsables de su cumplimiento.
- Solicitar actualizaciones fuera del esquema normal.

5.4.3.2 Responsables de cumplimiento

Es responsable del cumplimiento del presente procedimiento todo el personal de la EMUCE, así como terceros que hagan uso de cualquier recurso informático perteneciente al mismo.

5.4.3.3 Responsables de actualización

El responsable de la actualización del presente procedimiento es el responsable del Centro de Cómputo en su carácter de responsable de Seguridad Informática la EMUCE. Su responsabilidad es revisar y actualizar en

caso que corresponda, el presente documento de acuerdo al esquema de revisión y actualización establecido y a las solicitudes efectuadas por el propietario del mismo.

5.4.4 Régimen de revisión y actualización

El presente documento será revisado trimestralmente y actualizado en el caso de detectarse la necesidad de efectuar modificaciones que permitan mantenerlo actualizado en relación a la realidad de la estructura funcional y del ambiente informático.

Por otra parte, se realizarán las modificaciones que sean necesarias en el caso que se produjeran cambios que lo requieran, fuera de las revisiones programadas.

5.4.5 Desarrollo

5.4.5.1 Solicitantes de eventos a registrar

El responsable del Centro de Cómputo es responsable de la definición de los eventos de seguridad a ser registrados automáticamente en los sistemas.

Exclusivamente los Dueños de Datos / Delegados deben solicitar al responsable del Centro de Computo el registro de eventos adicionales en la medida que se correspondan con su información o personal a su cargo.

Para situaciones de excepción, el Dueño de Datos / Delegado del área de Recursos Humanos y/o de Auditoría Interna puede solicitar la registración de eventos de algún usuario.

El Centro de Cómputo es el responsable de implementar todos los eventos de seguridad en cada uno de los sistemas.

5.4.5.2 Tipos de eventos

Se deben registrar todos los eventos relacionados con las configuraciones de seguridad de los sistemas.

Todo software utilizado debe permitir el registro automática y explotación de la información de los eventos de seguridad.

5.4.5.3 Acceso a los registros

Exclusivamente el responsable del Centro de Cómputo y los Operadores (para los procesos de generación de copias de respaldo) deberían acceder a los registros de eventos de seguridad en la medida que lo permitan los sistemas.

5.4.5.4 Eventos generales a registrar para todos los usuarios

- Accesos fallidos de ingreso de usuarios
- Encendido y apagado de equipos centrales de procesamiento
- Desconexión forzada de usuarios
- Alta, baja o modificación de usuarios y grupos
- Cambios en la configuración de la seguridad
- Instalación de software de aplicación
- Procesos de depuración de información no automatizados

5.4.5.5 Eventos especiales

- Todos los accesos no autorizados a información clasificada como de acceso autorizado.
- Todos los eventos de un usuario cuando sean específicamente solicitados.

- Todos los accesos para cualquier usuario que acceda a la información clasificada como sensible.

- Todos los accesos del Responsable de Seguridad, de los usuarios de máximo riesgo y de los usuarios especiales del personal de Desarrollo de Sistemas cuando acceden al ambiente de Producción.

5.4.5.6 Agotamiento de espacio disponible para almacenamiento

El responsable del Centro de Cómputo en conjunto con los correspondientes Dueños de Datos / Delegados debe definir cuáles son los eventos que se consideren críticos que determinen la suspensión del servicio de procesamiento cuando se llegue al límite de la capacidad de almacenamiento en los equipos.

Para el resto de los eventos, debe definir la opción de suspender el registro o la sobre escritura de los datos.

5.4.5.7 Acciones ante situaciones de anormalidad

El Administrador debe:

- analizar diariamente los eventos

- informar al Responsable de Seguridad ante incidentes observados

El Responsable de Seguridad debe informar al Dueño de Datos / Delegado y cuando corresponda al Dueño de Datos / Delegado del área de Recursos Humanos y de Auditoría Interna.

El Responsable de la Seguridad debe conservar todos los soportes enviados y eventualmente comunicar al área de Operaciones de Sistemas la

necesidad de conservar los registros de eventos por períodos mayores a los previstos.

5.4.5.8 Depuraciones

En situaciones de emergencia en la performance del equipo debido al excesivo volumen de los registros automáticos de auditoría, el área de Operaciones de Sistemas debe generar una copia de respaldo de estos registros antes de proceder a su depuración y notificar del hecho al Responsable de Seguridad.

5.5 Procedimiento de Comunicaciones

5.5.1 Objetivo

Definir las pautas generales para asegurar una adecuada protección de la información en los procesos de transmisión y recepción de datos en las redes internas y externas de la EMUCE.

5.5.2 Alcance

Todo el personal del Centro de Cómputo de la EMUCE y los terceros que interactúan de manera habitual u ocasional que estén vinculados a los procesos de transmisión de datos en el desarrollo de sus tareas habituales.

5.5.3 Responsabilidades

5.5.3.1 Propietario

El propietario del presente procedimiento es el el responsable del Centro de Computo en su carácter de responsable de seguridad de la EMUCE. Sus responsabilidades son:

- Establecer las medidas de seguridad necesarias para garantizar el adecuado almacenamiento del presente documento.

- Definir los perfiles que tendrán acceso al documento.
- Asegurar la accesibilidad del documento para quienes necesiten consultarlo.
- Comunicar la existencia del documento y asesorar sobre el mismo a los responsables de su cumplimiento.
- Solicitar actualizaciones fuera del esquema normal.

5.5.3.2 Responsables de cumplimiento

Es responsable del cumplimiento del presente procedimiento todo el personal de la EMUCE, así como terceros que hagan uso de cualquier recurso informático perteneciente al mismo.

5.5.3.3 Responsables de actualización

El responsable de la actualización del presente procedimiento es el Responsable del Centro de Cómputo en su carácter de responsable de seguridad de la EMUCE. Su responsabilidad es revisar y actualizar en caso que corresponda, el presente documento de acuerdo al esquema de revisión y actualización establecido y a las solicitudes efectuadas por el propietario del mismo.

5.5.4 Régimen de revisión y actualización

El presente documento será revisado semestralmente y actualizado en el caso de detectarse la necesidad de efectuar modificaciones que permitan mantenerlo actualizado en relación a la realidad de la estructura funcional y del ambiente informático.

Por otra parte, se realizarán las modificaciones que sean necesarias en el caso que se produjeran cambios que lo requieran, fuera de las revisiones programadas.

5.5.5 Desarrollo

5.5.5.1 Conexiones internas

Adicionalmente a las medidas de protección física y de acceso de usuarios ya definidas en las respectivas normas, se deben tener en cuenta las siguientes consideraciones adicionales:

- Utilizar switches, no sólo para conectar los distintos segmentos de la red interna, sino también para conectar las distintas estaciones de trabajo y servidores entre sí.

- Verificar que existan los adecuados mecanismos de encriptación para la información sensible propia de los sistemas (contraseñas, bases de datos de seguridad o similares).

- Utilizar un esquema de direccionamiento IP teniendo en cuenta las direcciones privadas definidas en la normativa internacional respectiva para evitar que éstas sean enrutadas desde el exterior.

- Utilizar sistemas de detección de intrusos que permitan la detección posibles ataques y tomen acciones automáticas para prevenirlos.

5.5.5.2 Conexiones externas

En forma general, todas las conexiones externas a la red de la EMUCE deben cumplir las siguientes consideraciones:

El origen de todas las conexiones remotas debe ser autenticada utilizando un nivel aceptado de autenticación.

Todo acceso a la red interna de la compañía debe realizarse a través de una red segmentada (DMZ - zona desmilitarizada).

Las conexiones externas podrán acceder solamente a los servicios, sistemas y/o aplicaciones a los que están autorizados.

Deben transmitirse en forma encriptada todos los datos considerados de acceso autorizado y/o sensibles, a través redes virtuales permanentes utilizando clave pública y privada o certificados.

Los accesos externos deben ser registrados a fin de determinar posibles intentos de accesos no autorizados.

Debe incluirse en los contratos con los proveedores la utilización de otra vía alternativa ante interrupciones en el servicio.

5.5.6 Aspectos particulares de los distintos tipos de accesos externos:

5.5.6.1 Internet

Todo contrato con un proveedor de servicios de Internet debe contemplar la descripción de todos los servicios provistos y de todos aquellos que en un futuro pudiera requerir la compañía.

Todas las conexiones deben realizarse a través de un Firewall. En el caso particular de las conexiones salientes, éstas deben ser validadas a través de un servidor del tipo “AAA” (que verifica la autenticidad - Authentication, la autorización – Authorization y el monitoreo – Accounting de la cuenta de usuario) a fin de controlar los accesos de los usuarios, para lo cual se debe llevar un registro de los servicios utilizados y como mínimo la cuenta de usuario, la dirección IP accedida, la dirección URL accedida, la fecha y la hora.

En el caso de las conexiones entrantes, se debe llevar registro de los intentos fallidos que contenga la dirección IP de origen, el servicio requerido, el motivo del rechazo, la fecha y la hora.

5.5.6.2 Accesos remotos

El servicio de Acceso Remoto será utilizado solamente para conexiones entrantes y en función al perfil del usuario que se conecta se establecen los servicios y direcciones habilitadas para dicho usuario.

Debe registrarse todo evento relacionado con cambios de derechos de acceso y accesos exitosos y fallidos, la identificación del usuario responsable, la fecha y hora de inicio, tiempo de conexión, las líneas y protocolos empleados y, para los cambios en los derechos de acceso, el estado anterior y posterior de los cambios realizado.

5.6 Procedimiento de Manejo de Incidentes

5.6.1 Objetivo

Establecer pautas para el reporte, registro, tratamiento y seguimiento de los incidentes ocurridos; así como la comunicación y solución de debilidades identificadas en el ambiente informático.

Mitigar los efectos causados por los incidentes ocurridos en el ambiente informático.

Generar conocimiento a partir del cual sea posible reducir la posibilidad de ocurrencias de incidentes futuros.

5.6.2 Alcance

El presente procedimiento será aplicado ante la ocurrencia de cualquier tipo de incidente que afecte la seguridad de la información del Organismo o el correcto funcionamiento de los componentes que integran el ambiente informático. Cabe aclarar que se considerará como incidente tanto a aquel que presente consecuencias de cualquier tipo como el que haya sido detenido antes de producir un impacto, no ocasionando daños.

Asimismo, se aplicará en forma preventiva, a las debilidades detectadas en cualquier componente del ambiente informático, aunque los mismos no hayan sido víctimas de un ataque concreto.

5.6.3 Responsabilidades

5.6.3.1 Propietario

El propietario del presente procedimiento es el responsable del Centro de Cómputo. Sus responsabilidades son:

- Establecer las medidas de seguridad necesarias para garantizar el adecuado almacenamiento del presente documento.
- Definir los perfiles que tendrán acceso al documento.
- Asegurar la accesibilidad del documento para quienes necesiten consultarlo.
- Comunicar la existencia del documento y asesorar sobre el mismo a los responsables de su cumplimiento.
- Solicitar actualizaciones fuera del esquema normal.

5.6.3.2 Responsables de cumplimiento

Es responsable del cumplimiento del presente procedimiento es todo el personal de la EMUCE, así como terceros que hagan uso de cualquier recurso informático perteneciente al mismo.

5.6.3.3 Responsables de actualización

El responsable de la actualización del presente procedimiento es responsable del Centro de Cómputo en su carácter de Responsable de Seguridad. Su responsabilidad es revisar y actualizar en caso que corresponda, el presente documento de acuerdo al esquema de revisión y actualización establecido y a las solicitudes efectuadas por el propietario del mismo.

5.6.4 Régimen de revisión y actualización

El presente documento será revisado semestralmente y actualizado en el caso de detectarse la necesidad de efectuar modificaciones que permitan mantenerlo actualizado en relación a la realidad de la estructura funcional y del ambiente informático.

Por otra parte, se realizarán las modificaciones que sean necesarias en el caso que se produjeran cambios que lo requieran, fuera de las revisiones programadas.

5.6.5 Desarrollo

Un evento es una ocurrencia observada u observable en un sistema, una red o en los procesos. Un evento será considerado como incidente si éste puede producir efectos adversos en el ambiente informático.

Se define a un incidente de seguridad como un evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

Como de se aclara en el “Alcance”, un incidente puede lograr el cumplimiento del objetivo para el cual se ha producido, o bien puede ser detenido antes de ello.

5.6.5.1 Clasificación de un incidente

Todo Incidente detectado será clasificado por el Responsable de Seguridad en el marco del procedimiento descrito en siguientes puntos.

Se establecen tres niveles en base a la criticidad e impacto del incidente sobre el ambiente informático:

Alto	
Daño, modificación o pérdida significativa de información crítica/estratégica (posiblemente irremplazable) del Organismo. Impacto significativo en la operatoria del organismo. Daño significativo a la infraestructura informática del Organismo,	Ejemplos: Acceso no autorizado al sistema. Información crítica comprometida. Infección de virus no controlado. Ataques a infraestructura crítica: DNS, firewll, routers, switches o sistemas productivos. Ataques a correo electrónico o al servidor de aflicciones web. Detección de herramientas no autorizadas para efectuar escuchas del cable, software de hacking. Agujeros de seguridad o falta de controles. Violaciones de seguridad por parte de un empleado o un tercero.
Medio	
Daño, modificación o pérdida de información recuperable sin compromiso de la operatoria. Posible impacto moderado en la operatoria del Organismo. Errores no intencionales del administrador.	Ejemplos: Mal uso o abuso de accesos autorizados Contraseñas compartidas Pérdida o robo de propiedad intelectual o información propietaria/confidencial. Acceso/Modificación accidental de información crítica de los sistemas. Infección de virus controlada. Sospechas de violaciones de seguridad por parte de un empleado o un tercero.
Bajo	
Daño, modificación o pérdida no intencional de información recuperable. Bajo o nulo impacto sobre la operatoria del Organismo. Acciones no intencionales de un usuario.	Ejemplos: Errores en la configuración de estaciones de trabajo. Errores en la configuración de aplicaciones.

5.6.5.2 Detección de un incidente

La primera etapa del proceso de manejo de incidentes es la detección, en la cual se produce el conocimiento por parte del usuario, de la ocurrencia de un incidente. La detección de un incidente puede ser efectuada en cualquier área de la EMUCE, tanto por usuarios funcionales como por usuarios del Área Informática. Por otra parte, existe también la posibilidad de que un incidente sea detectado por un componente de control automático, implementado en el ambiente informático, como ser algún software de monitoreo de red con alarma.

A continuación se citan algunos de los incidentes que pueden ser detectados:

- Infección de virus, gusanos o troyanos
- Modificación de la página Web (Web-defacement)
- Interrupción o denegación de servicio por medios electrónicos
- Escaneos de puertos o pruebas maliciosas
- Intercepción de las comunicaciones
- Acceso no autorizado a archivos de datos o sistemas
- Modificación de archivos de datos o sistemas
- Fraude por medios electrónicos
- Robo electrónico de información confidencial
- Robo de equipamiento
- Fallas de hardware
- Catástrofes naturales

Cabe destacar que este procedimiento se aplicará asimismo al manejo de debilidades o anomalías que, sin ser incidentes, representan un riesgo para la seguridad del ambiente de sistemas. Es por ello que los usuarios deberán efectuar asimismo el reporte de:

- Debilidades identificadas en los componentes informáticos
- Anomalías en materia de seguridad del software o hardware

El usuario recolectará toda aquella información susceptible de ser perdida, que fuera de utilidad para el análisis del incidente o anomalía, como ser, pantallas de error. Por el contrario, el usuario no realizará ninguna modificación ni intento de reparación del problema.

5.6.5.3 Reporte de un incidente

Una vez detectado el incidente, se procederá al reporte del mismo.

El usuario que haya detectado el incidente es responsable de reportar inmediatamente el mismo al Centro de Cómputo.

El Centro de Cómputo procederá a notificar el incidente al Responsable de Seguridad, quien evaluará si realmente se trata de un incidente o sólo es un evento que no presenta efectos adversos. En el caso de tratarse de un incidente, procederá a su clasificación.

Una vez clasificado el incidente, comunicará al Centro de Cómputo.

5.6.5.4 Tratamiento de un incidente

5.6.5.4.1 Incidente concretado

Acción inmediata

En primer lugar, el Responsable de Seguridad llevará a cabo las acciones necesarias para mitigar los efectos del incidente:

Habiendo tomado conocimiento del incidente ocurrido, se evaluará la criticidad del impacto del incidente y la necesidad de solicitar la asistencia para la solución del mismo.

Se identificarán los componentes afectados aislándolos de la red para evitar la propagación de los daños.

Se definirán las medidas a ser implementadas para la restauración de los daños ocasionados.

El responsable del Centro de Cómputo tendrá a cargo la implementación de las medidas definidas de acuerdo a los procedimientos operativos existentes.

Acciones posteriores

Una vez solucionado el incidente se seguirán los siguientes pasos:

El Responsable de Seguridad Informática procederá a:

Efectuar un análisis de las causas que ocasionaron la ocurrencia del incidente con el objeto de implementar medidas tendientes a prevenir la repetición del mismo en un futuro.

Notificar a las Autoridades de la EMUCE.

Comunicar al propietario de la información afectada (de corresponder) las medidas llevadas a cabo para la solución del incidente

Comunicar al usuario que efectuó el reporte, el cierre del incidente

5.6.5.4.2 Incidente no concretado

En el caso de que el incidente no se hubiera concretado, es decir, que no hayan ocurrido daños a ser reparados, sólo se efectuará el reporte y documentación del mismo.

Estos casos pueden corresponder a:

Incidentes cuyo efecto fue detenido por alguna medida de seguridad existente.

Debilidades identificadas en los componentes informáticos.

Anomalías en materia de seguridad del software o hardware

5.6.5.5 Documentación del incidente

La documentación de los incidentes de seguridad es muy importante en el proceso de manejo de incidentes, dado que permite efectuar una gestión eficiente de los mismos, realizar análisis estadísticos y disminuir su ocurrencia y efectos producidos.

5.6.5.5.1 Documentación interna

La documentación interna de los incidentes será efectuada por el Centro de Cómputo, en función a la información reportada por el usuario acerca del incidente y acerca de su tratamiento y solución.

Se utilizará para la documentación un registro de Incidentes con la siguiente información:

Datos del incidente

Identificador único: se asignará un identificador por incidente documentado.

Categoría: tipo de incidente. El objetivo es agrupar en una misma categoría varios incidentes de manera de facilitar su posterior análisis.

Descripción: definición detallada del incidente.

Concretado / No Concretado

Nivel de criticidad.

Datos del reporte

Informado por: nombre del usuario que reportó el incidente

Fecha

Hora

Efectos producidos: detalle de las consecuencias producidas por el incidente concretado.

Datos sobre la atención

Responsable: será la persona responsable de la atención del incidente

Encargado: será la persona asignada a la atención del incidente.

Datos sobre la solución

Estado:

Pendiente	Si bien el incidente ha sido reportado, aún no se lo ha comunicado al Responsable de Seguridad Informática.
Informado	El incidente ha sido reportado al Responsable de Seguridad Informática pero aún no se lo ha tratado.
En curso	El incidente ha sido reportado al Responsable de Seguridad Informática y se encuentra en tratamiento
Resuelto	El incidente ha sido resuelto.
Demorado	El tratamiento ha sido interrumpido por motivos a detallar.

Encargado: designado para la solución del incidente

Fecha de cierre

Detalle: se describe en detalle y cronológicamente, indicando la fecha correspondiente, cada una de las tareas efectuadas para la solución del incidente, así como los gastos insumidos (de corresponder)

5.6.5.6 Control de incidentes

El control de incidentes será efectuado por el Responsable de Seguridad Informática, mediante la utilización de un Tablero de Seguimiento *(planilla*

disponible en el sitio). El objetivo de dicho control es efectuar un análisis periódico de los incidentes ocurridos, de manera de:

Detectar debilidades y vulnerabilidades en los componentes informáticos

Analizar patrones de ataques

Delinear medidas para reducir la cantidad de incidentes ocurridos y mitigar sus consecuencias

Efectuar reportes al Comité de Seguridad de la Información con información estadística respecto de los incidentes ocurridos

Para ello, mensualmente se completará la tabla de Seguimiento de incidentes con la siguiente información (gran parte de la cual surgirá del registro de incidentes):

Datos del incidente:

Identificador único: se asignará un identificador por categoría de incidente.

Categoría: tipo de incidente.

Concretado / No Concretado

Nivel de criticidad: Porcentaje de incidentes con nivel de criticidad ALTO/MEDIO/BAJO en el período.

Métrica: unidad utilizada para contabilizar los incidentes, por ejemplo, cantidad de incidentes por mes.

Cantidad registrada:

Esperada: este valor debe ser establecido al comienzo del período evaluado, en función de los objetivos establecidos. Luego se buscará, mediante la implementación de medidas adecuadas, el logro de la cantidad esperada.

Período actual: cantidad de incidentes registrados en el período al que corresponden los datos.

Período anterior: cantidad de incidentes registrados en el período anterior.

Tendencia:

Creciente: en el caso en que la cantidad de incidentes registradas en el período anterior sea menor a la registrada en el actual.

Decreciente: en el caso en que la cantidad de incidentes registradas en el período anterior sea mayor a la registrada en el actual.

Alerta: criticidad definida en función a los incidentes registrados. Será evaluado de acuerdo a un criterio establecido en función a un análisis de impacto de los incidentes registrados. Un posible criterio a utilizar son las consecuencias potenciales o efectivas sufridas a causa de los incidentes ocurridos.

Comentarios

El Responsable de Seguridad Informática emitirá un reporte mensual del presente tablero, para ser entregado al Comité de Seguridad de la Información.

5.7 Procedimiento de Segregación de Ambientes

5.7.1 Objetivo

Definir una segregación entre los diferentes ambientes de procesamiento: desarrollo, prueba y producción, con el objeto de controlar el acceso a los mismos y proteger la información que cada uno contiene.

5.7.2 Alcance

El presente procedimiento será aplicado a todos los entornos que cuenten con más de una instancia de procesamiento, por ejemplo, producción y desarrollo o producción y prueba, etc.

5.7.3 Responsabilidades

5.7.3.1 Propietario

El propietario del presente procedimiento es el responsable del Centro de Cómputo en su carácter de Responsable de Seguridad Informática de la EMUCE. Sus responsabilidades son:

Establecer las medidas de seguridad necesarias para garantizar el adecuado almacenamiento del presente documento.

Definir los perfiles que tendrán acceso al documento.

Asegurar la accesibilidad del documento para quienes necesiten consultarlo.

Comunicar la existencia del documento y asesorar sobre el mismo a los responsables de su cumplimiento.

Solicitar actualizaciones fuera del esquema normal.

5.7.3.2 Responsables de cumplimiento

Es responsable del cumplimiento del presente procedimiento todo el personal del Organismo, así como terceros que hagan uso de cualquier recurso informático perteneciente al mismo.

5.7.3.3 Responsables de actualización

El responsable de la actualización del presente procedimiento es el responsable del Centro de Cómputo en su carácter de Responsable de Seguridad Informática de la EMUCE. Su responsabilidad es revisar y actualizar en caso que corresponda, el presente documento de acuerdo al esquema de revisión y actualización establecido y a las solicitudes efectuadas por el propietario del mismo.

5.7.4 Régimen de revisión y actualización

El presente documento será revisado semestralmente y actualizado en el caso de detectarse la necesidad de efectuar modificaciones que permitan mantenerlo actualizado en relación a la realidad de la estructura funcional y del ambiente informático.

Por otra parte, se realizarán las modificaciones que sean necesarias en el caso que se produjeran cambios que lo requieran, fuera de las revisiones programadas.

5.7.5 Desarrollo

Se definen tres ambientes de procesamiento:

Producción: Es donde se ejecutan las transacciones reales, con datos válidos y actuales

Pruebas: Es donde se realizan las pruebas sobre posibles cambios o actualizaciones a implementar en el ambiente de Producción

Desarrollo: Es donde se efectúan tareas de programación, modificación o mantenimiento de los sistemas.

Cabe aclarar que en ocasiones es posible implementar sólo dos ambientes: Producción y Desarrollo/Prueba, incorporando las tareas realizadas en ambos en un mismo ambiente.

El objetivo de segregar los ambientes mencionados es proteger la información almacenada en cada uno de ellos de accesos indebidos, modificación no autorizada, eliminación errónea o pérdida. Separando los ambientes es posible otorgar acceso a los mismos sólo a los usuarios que lo necesitan de acuerdo a sus funciones.

Como premisas generales, y citando lo definido en la Política de Seguridad de la Información, se definen:

El personal de desarrollo (programadores) no accede al ambiente de Producción, sino únicamente al ambiente de Desarrollo.

Los usuarios finales no acceden al ambiente de Desarrollo sino únicamente al ambiente de Producción y a través de las aplicaciones.

El ambiente de Prueba es accedido por los usuarios, “testers” y demás personal que tiene a cargo la prueba del sistema en cuestión. Los usuarios encargados de probar los sistemas serán aquellos que tengan conocimiento del mismo y cuenten con la capacidad de evaluarlo.

Los administradores del Centro de Cómputos acceden a todos los ambientes.

NOTA: “Tester”: Persona encargada de probar un sistema con el objeto de verificar que cumple sus funciones adecuadamente y de detectar posibles aspectos a mejorar, modificar o corregir.

5.7.5.1 Ambientes de procesamiento

A continuación luce la planilla modelo que deberá mantenerse actualizada como documentación en el Centro de Cómputos :

Sistema	Ambientes de Procesamiento		
	Producción	Pruebas	Desarrollo

Por cada sistema se indicará en qué ambiente se encuentra la versión más actualizada.

5.7.5.2 Segregación de ambientes

De acuerdo a lo definido en la Política de Seguridad de la Información, los diferentes ambientes de procesamiento de un sistema serán segregados físicamente si es posible, o lógicamente como mínimo.

El administrador del Centro de Cómputos mantendrá actualizada la siguiente planilla a efectos de poder realizar con comodidad y seguridad las operaciones necesarias con cada sistema donde la “Ubicación” se refiere al lugar donde se ubica el ambiente: servidor y ruta.

Los accesos a los diferentes ambientes para los sistemas del Organismo serán solicitados de acuerdo a lo definido en el “Procedimiento - Administración de usuarios”.

Sistema	Ambientes de Procesamiento					
	Producción		Pruebas		Desarrollo	
	Ubicación	Usuarios Autorizados	Ubicación	Usuarios Autorizados	Ubicación	Usuarios Autorizados

5.7.5.3 Pasar información entre ambientes

El pasar información entre los diferentes ambientes es una operación crítica que debe ser controlada exhaustivamente. El personal autorizado a efectuar dicho pasaje será autorizado expresamente y sus actividades serán controladas.

El Administrador del Centro de Cómputo será el encargado de asignar dichos permisos de acceso, los cuales se detallan a continuación:

Sistema	Usuarios Autorizados al Pasaje de Información		
	Producción a Desarrollo	Desarrollo a Pruebas	Pruebas a Producción

5.8 Procedimiento para el uso de recursos

5.8.1 Objetivo

Establecer pautas para regular el uso de los recursos informáticos pertenecientes al Organismo.

5.8.2 Alcance

El presente procedimiento se aplica al equipamiento informático (Hardware), a la información (archivos), a los servicios (ejemplo Internet y correo electrónico), a los sistemas (software) del Organismo.

5.8.3 Responsabilidades

5.8.3.1 Propietario

El propietario del presente procedimiento es el responsable del Centro de Cómputo en su carácter de Responsable de Seguridad Informática de la EMUCE. Sus responsabilidades son:

Establecer las medidas de seguridad necesarias para garantizar el adecuado almacenamiento del presente documento.

Definir los perfiles que tendrán acceso al documento.

Asegurar la accesibilidad del documento para quienes necesiten consultarlo.

Comunicar la existencia del documento y asesorar sobre el mismo a los responsables de su cumplimiento.

Solicitar actualizaciones fuera del esquema normal.

5.8.3.2 Responsables de cumplimiento

Es responsable del cumplimiento del presente procedimiento todo el personal del Organismo, así como terceros que hagan uso de cualquier recurso informático perteneciente al mismo.

5.8.3.3 Responsables de actualización

El responsable de la actualización del presente procedimiento es el responsable del Centro de Cómputo en su carácter de responsable de Seguridad Informática de la EMUCE. Su responsabilidad es revisar y actualizar en caso que corresponda, el presente documento de acuerdo al esquema de revisión y actualización establecido y a las solicitudes efectuadas por el propietario del mismo.

5.8.4 Régimen de revisión y actualización

El presente documento será revisado anualmente y actualizado en el caso de detectarse la necesidad de efectuar modificaciones que permitan mantenerlo actualizado en relación a la realidad de la estructura funcional y del ambiente informático.

Por otra parte, se realizarán las modificaciones que sean necesarias en el caso que se produjeran cambios que lo requieran, fuera de las revisiones programadas.

5.8.5 Desarrollo

El Organismo brinda a su personal y a toda persona externa que realice trabajos para el mismo, las herramientas necesarias para su desempeño. Es responsabilidad de los depositarios de dichas herramientas, el uso apropiado de las mismas.

5.8.5.1 Uso de la información

La información perteneciente al Organismo será utilizada únicamente dentro del marco de las actividades propias del mismo. Con lo cual, se encuentran prohibidas, entre otras actividades:

- Utilizar la información del Organismo para beneficio propio.
- Efectuar daños o destrucción de información del Organismo o cualquier acción que pueda impedir el acceso legítimo a la misma.

Se respetarán las pautas de manejo y resguardo de información establecida en la Política de Seguridad de la Información.

Los Propietarios de la Información mantendrán actualizada la clasificación de la misma, y el resto del personal conocerá el nivel de clasificación de cada tipo de información que deba manejar, almacenar o transferir.

5.8.5.2 Uso del equipamiento

El Organismo provee al personal de equipamiento para el desarrollo de sus tareas, como ser, PCs, impresoras, scanners, CDs y otros dispositivos informáticos. El usuario dará el tratamiento que corresponde a dicho equipamiento, de forma de evitar cualquier daño físico o lógico al mismo como consecuencia de un uso inadecuado.

El equipamiento del Organismo será utilizado únicamente para propósitos relacionados con las actividades del mismo. Entre las actividades que se prohíben detallamos:

- Utilizar los recursos del Organismo para desarrollar cualquier actividad comercial personal.

- Utilizar la red para fomentar o conducir al personal a la realización de actividades lucrativas.

- Realizar actividades tendientes a obtener mayores derechos de acceso que los otorgados por las autoridades.

- Desarrollar actividades (ej.: ejecución de programas) que produzcan la disminución en el rendimiento de la red.

- Iniciar cualquier actividad que comprometa la seguridad de la red o de cualquiera de sus componentes.

- Otorgar acceso a la red o a cualquiera de sus componentes y equipamiento a una persona no autorizada.

- Realizar cambios en la configuración del equipamiento, excepto expresa y previa autorización.

En caso de detectarse fallas se deberá seguir el Procedimiento correspondiente

- Efectuar la conexión o desconexión de equipamiento, como ser, PCs, impresoras, etc. En caso de ser necesario, el usuario deberá comunicarse con la Coordinación de Informática

- Entorpecer o detener la verificación periódica efectuada por el software antivirus en equipos.

Respondiendo a la política de pantallas limpias establecida en la Política de Seguridad, los usuarios deberán bloquear el acceso a su PC durante períodos prolongados de inactividad. Se entiende como “período prolongado” aquel mayor a 30 minutos.

Se recomienda lo siguiente:

- Evitar que alimentos (sólidos y líquidos) se encuentren cerca del equipamiento.
- Evitar que celulares y radios se encuentren cerca del equipamiento.
- No obstruir la salida de ventilación de los equipos.

5.8.5.3 Almacenamiento de información

Los usuarios disponen de los siguientes tipos de medios de almacenamiento:

De red

Espacio privado: cada usuario puede poseer un directorio privado en el servidor de archivos, en el cual puede almacenar información de manera que sólo él pueda accederla. Dicho directorio posee una capacidad máxima de almacenamiento.

Espacio compartido: el servidor de archivos presenta carpetas compartidas entre algunos o todos los usuarios, de manera de facilitar el proceso de compartir información.

La información almacenada en el servidor de archivos es resguardada periódicamente de acuerdo al Procedimiento de Resguardo de la información

Espacio Local

Se trata del/los discos locales de cada PC. Cada usuario es responsable de administrar el espacio de su/sus propios discos. Cabe destacar que la información de los discos locales no es resguardada periódicamente, por lo que cada usuario debe copiar al servidor de archivos la información importante que desee resguardar.

En caso de requerir la restauración de una copia de resguardo, el usuario deberá comunicarse con la Coordinación de Informática para efectuar el pedido.

Se encuentra prohibido el almacenamiento, tanto en la red como a nivel local, de material no relacionado con las actividades laborales de los usuarios, como ser:

Material pornográfico

Material que evidencia tendencias políticas, religiosas u otras ideologías

Software u otro material protegido por la Ley de Propiedad Intelectual

Software gratuito no relacionado con las actividades del Organismo

Fotografías personales

Archivos multimedia (música, video, etc.) no relacionados con las actividades laborales

5.8.5.4 Uso de los sistemas

El Organismo provee a su personal el software para el desarrollo de sus actividades laborales, el cual es instalado por el Área Informática y debe ser utilizado únicamente para propósitos relacionados con las actividades del Organismo. Entre las actividades que se prohíben detallamos:

- Mantener software no licenciado en equipamiento del Organismo.
- Efectuar copias ilegales de software perteneciente al Organismo.
- Adquirir software sin la autorización previa y expresa del funcionario que corresponda.

- Intentar el acceso a información o sistemas restringidos dentro del Organismo.

- Atentar contra el correcto funcionamiento de los sistemas, por ejemplo, mediante la introducción de código malicioso.

5.8.5.5 Uso del acceso a Internet

El Organismo otorga acceso a Internet a parte de su personal con el objeto de que dicho servicio beneficie el desarrollo de sus actividades. Por ello, el acceso a Internet por parte de los usuarios habilitados, así como su utilización deben responder únicamente a necesidades laborales.

Entre las actividades que se prohíben detallamos:

- Instalar y/o utilizar herramientas de navegación que no son las aprobadas por el Área de Informática.

- Acceder a sitios que contengan material pornográfico o en cualquier aspecto obsceno o agresivo.

- Publicar información del Organismo o de su personal, excepto autorización previa y expresa.

Transmitir por Internet o descargar:

- Material pornográfico

- Material que evidencia tendencias políticas, religiosas u otras ideologías

- Software u otro material protegido por la Ley de Propiedad Intelectual (infringiendo derechos de autor de terceros)

- Software gratuito no relacionado con las actividades del Organismo

- Fotografías personales
- Utilizar cualquier software de “chat” o participar de foros de “chat” en línea.
- Participar en listas de discusión y otros servicios que no se encuentren relacionados con sus actividades en el Organismo.
- Realizar actividades ilegales en el ámbito de Internet.

Los servicios de Internet se encuentran operativos desde los días Lunes a las 07:00 hasta los Viernes a las 23:00 hs.

Con el objeto de minimizar el riesgo de violación a la seguridad a través del uso incorrecto del servicio de correo electrónico, se requiere el cumplimiento de lo siguiente:

- Analizar los archivos descargados con la herramienta antivirus instalada en las estaciones clientes.
- Desactivar la ejecución automática de código Java, JavaScript y ActiveX en la herramienta de navegación utilizada.
- Evitar el ingreso de datos personales confidenciales en sitios Web, excepto que los mismos cuenten con mecanismos de encriptación para la transferencia de su información. Ante la duda, solicitar asistencia a Coordinación de Informática.

5.8.5.6 Uso del correo electrónico

La casilla de correo otorgada al usuario es propiedad del Organismo, por lo que su utilización debe relacionarse sólo con fines laborales, relacionados con las actividades del Organismo.

Entre las actividades que están prohibidas las detallamos a continuación:

- Enviar o recibir correo electrónico con contenido relacionado con temas ajenos a las actividades que el usuario desempeña en el Organismo. Algunos ejemplos son:
    - Saludos personales
    - Material fotográfico
    - Cadenas
    - Anuncios comerciales
    - Material pornográfico u obsceno
    - Material que evidencie tendencias políticas, religiosas u otras ideologías
    - Software u otro material protegido por la Ley de Propiedad Intelectual
    - Software gratuito no relacionado con las actividades del Organismo
    - Fotografías personales
- Utilizar el correo electrónico para efectuar amenazas u hostigamiento.
- Leer, interceptar o revelar comunicaciones electrónicas pertenecientes a otro usuario sin autorización previa expresa del mismo.
- Instalar y/o utilizar herramientas de navegación que no son las aprobadas por el Área de Informática.
- Utilizar lenguaje inapropiado en cualquier mensaje.

- Emitir juicio u opinar en forma personal frente a terceros. Tener en cuenta que al utilizar las direcciones de correo electrónico del Organismo están actuando en su representación.

- Enviar información perteneciente al Organismo a un tercero externo al mismo, excepto autorización previa expresa.

- Emitir comentarios peyorativos acerca del Organismo o su personal en foros públicos u otros medios de publicación electrónica.

- Utilizar el servicio de correo electrónico para ejercer actividades ilegales.

- Violar la Política de Seguridad del Organismo en cuanto a la seguridad de la información.

Con el objeto de minimizar el riesgo de violación a la seguridad a través del uso incorrecto del servicio de correo electrónico, se requiere el cumplimiento de lo siguiente:

- Eliminar los mensajes de origen desconocido que contengan adjuntos, sin abrirlos y/o guardarlos localmente.

- Analizar los archivos recibidos antes de su descarga o ejecución con la herramienta antivirus instalada en las estaciones clientes.

- Bloquear la notificación automática de mensajes recibidos.

- Utilizar técnicas criptográficas en los casos en que se necesite garantizar autenticación, integridad y confidencialidad de la información incluida en el mensaje.

Con el objeto de optimizar el funcionamiento del servicio de correo electrónico, es deseable:

- Controlar la cantidad de destinatarios de los mensajes, enviando correos masivos sólo si es necesario y se cuenta con una adecuada justificación. EL máximo de destinatarios no puede superar las (20) direcciones de correo.

- No adjuntar archivos mayores a 7MB. Es conveniente utilizar herramientas de compresión para minimizar el tamaño de los adjuntos.

- Solicitar la confirmación de un mensaje enviado sólo cuando sea necesario.

- Guardar los mensajes enviados sólo cuando sea de utilidad o necesidad.

- Realizar resguardos parciales de la casilla de correo con el objeto de asegurar la disponibilidad de los mensajes almacenados en la misma en caso de falla del servidor de correo, y liberar espacio ocupado innecesariamente en el servidor de correo.

- Eliminar los mensajes (enviados y recibidos) que no sea necesario conservar.

- La capacidad del buzón del Correo Electrónico no puede superar los 13 MB.

5.8.5.7 Monitoreo

Dado que tanto el equipamiento como los sistemas y los servicios de Internet y correo electrónico mencionados en el presente procedimiento son propiedad del Organismo, el mismo puede monitorear y/o auditar:

- El uso de la red y el equipamiento informático.

- El uso de los sistemas.

- El uso del servicio de acceso y navegación en Internet.

- El uso del servicio de correo electrónico, así como los mensajes enviados y recibidos por los usuarios. Para ello, el Organismo puede hacer uso de herramientas específicas diseñadas para tal fin.

5.8.5.8 Utilización de antivirus

Es norma del Organismo:

En Programas Automáticos

- Se debe implementar un sistema automático de control antivirus para prevenir y eliminar las consecuencias de la acción de los virus informáticos.

- Los programas deben ser instalados por el área de Coordinación de Informática en los equipos centralizados de procesamiento y en las estaciones de trabajo de modo residente para que estén activados durante su uso.

Actualizaciones

- Se deben actualizar periódicamente las versiones de los programas antivirus y dicha situación debe estar reflejada en los contratos con el proveedor.

Archivos enviados y recibidos

- Los programas antivirus deben permitir la detección de virus en archivos enviados y recibidos via el servicio de correo electrónico o desde otras redes de datos/Internet.

Otras medidas complementarias

- Adicionalmente se pueden realizar una ejecución periódica de otro programa antivirus en los equipos de procesamiento centralizado a los efectos de reforzar el control sobre todo eñ disco.

- El horario de operación de red es de 08:00 a 22:00 Hs. En caso de excepciones, éstas deberán solicitarse por escrito a la Coordinación de Informática y serán analizadas.

5.9 Compromiso de confidencialidad y aceptación de la política

5.9.1 Objetivo

Desarrollar y mantener actualizado un “Compromiso de confidencialidad y aceptación de la Política de Seguridad de la Información” a ser firmado por todos los usuarios.

5.9.2 Alcance

El “Compromiso de confidencialidad y aceptación de la Política de Seguridad de la Información” será firmado por todo el personal de la EMUCE, cualquiera fuese su situación de revista.

5.9.3 Responsabilidades

5.9.3.1 Propietario

El propietario del presente procedimiento es el responsable del Centro de Cómputo, responsable de la Seguridad de la Información de la EMUCE**.** Sus responsabilidades son:

- Establecer las medidas de seguridad necesarias para garantizar el adecuado almacenamiento del presente documento.

- Definir los perfiles que tendrán acceso al documento.

- Asegurar la accesibilidad del documento para quienes necesiten consultarlo.

- Comunicar la existencia del documento y asesorar sobre el mismo a los responsables de su cumplimiento.

- Solicitar actualizaciones fuera del esquema normal.

5.9.3.2 Responsables de actualización.

El responsable de la actualización del presente procedimiento es el responsable del Centro de Cómputo, responsable de la Seguridad de la Información de la EMUCE. Su responsabilidad es revisar, actualizar en caso que corresponda, y archivar el presente documento de acuerdo al esquema de revisión y actualización establecido y a las solicitudes efectuadas por el propietario del mismo.

5.9.4 Régimen de revisión y actualización

El presente documento será revisado anualmente y actualizado en el caso de detectarse la necesidad de efectuar modificaciones que permitan mantenerlo actualizado en relación a la realidad de la estructura funcional y del ambiente informático.

Por otra parte, se realizarán las modificaciones que sean necesarias en el caso que se produjeran cambios que lo requieran, fuera de las revisiones programadas.

5.9.5 Desarrollo

5.9.5.1 Instrumentación de la firma del compromiso

Una copia del Modelo de Compromiso será firmada por todo el personal actual de la EMUCE y aquel que se incorpore en adelante, cualquiera fuese su situación de revista.

La Dirección Administrativa de la EMUCE será la encargada de instrumentar la firma y de archivar las copias de Compromisos firmados en los respectivos legajos del personal.

5.9.5.2 Modificación del compromiso

En caso que el Compromiso sea modificado, el responsable de actualización informará a la Dirección Administrativa sobre la existencia de una nueva versión del Compromiso.

La Dirección Administrativa evaluará si las modificaciones ameritan la renovación de la firma por parte de los empleados. De ser así, lo comunicará a la Gerencia, donde se instrumentará la nueva firma para todo el personal.

Cabe aclarar que la Dirección Administrativa, por su competencia en el marco legal que reviste el compromiso, puede solicitar modificaciones al mismo en caso de que lo crea conveniente o necesario. En este caso, se deberá coordinar la modificación con el responsable de actualización.

5.10 Modelo de compromiso de aceptación de la política de Seguridad de la información, confidencialidad y utilización de Recursos informáticos

El que suscribe, ... con C.I. ..... , declara conocer y aceptar todas las obligaciones emergentes de la POLITICA DE SEGURIDAD DE LA INFORMACION adoptada por la EMUCE, en el marco de la POLITICA DE SEGURIDAD DE LA INFORMACION MODELO aprobada por Disposición del la Gerencia.

En tal sentido, me comprometo a utilizar la información adquirida con motivo del ejercicio de mis funciones exclusivamente para su uso oficial y a no comunicar, diseminar o de alguna otra forma de hacer pública dicha información a ninguna persona o entidad, salvo en caso de que el funcionario responsable del sector con facultad de clasificar la información de acuerdo de acuerdo con el grado de sensibilidad y criticidad de ésta, así lo autorice mediante su aprobación previa y por escrito, haciéndome responsable de todos los daños y perjuicios que pudiera irrogar una utilización de la información con fines distintos a los asignados.

Consiente que los recursos de procesamiento de información de la EMUCE se suministran con un propósito determinado, me comprometo a utilizar los que me fueran asignados para el desempeño de mis funciones de manera racional, evitando su abuso, derroche o desaprovechamiento, aceptando a tales fines que las actividades de ……. sean objeto de permanente control y monitoreo.

Para el caso de ser necesario el intercambio de información con terceras personas, me comprometo a verificar previamente lo concerniente a la suscripción de un compromiso o acuerdo de confidencialidad que obligue a los destinatarios de la información y/o el organismo en el cual desempeñan sus tareas, a no divulgar ésta a terceros, haciéndome responsable por los daños y perjuicios que pudiere irrogar su difusión en caso de no tomar esta medida.

La obligación de reserva o confidencialidad asumida en virtud del presente seguirá vigente después de finalizada la tarea encomendada y aún después de la rescisión o resolución del contrato o cese o interrupción de la relación de empleo que me vincula con la EMUCE haciéndome responsable de los daños y perjuicios que pudiera irrogar la difusión de datos o informes no publicados.

El presente compromiso de ninguna manera sustituye la normativa vigente aplicable a la función que desempeño.

Conclusiones

Una organización puede ser más competitiva gestionando de una mejor manera su seguridad; teniendo en cuanta que la tecnología asumida como soporte de sus procesos de negocio está sujeta a innumerables contingencias provocadas por la misma utilización de la tecnología o por terceras persona con o sin mala intensión.

Si la organización está de acuerdo en emprender un proyecto de seguridad a nivel informática, en primera instancia deberá contar con el convencimiento, compromiso y firme propósito de la alta gerencia y directivos, caso contrario será un proyecto que de por un resultado un documento que se archivará y nunca se pondrá en práctica.

Las políticas y procedimientos de seguridad informática planteadas en este documento deben tomarse como punto de partida en la búsqueda de la seguridad, deben ser documentos dinámicos que deberán irse adaptando conforme los requerimientos organizacionales.

La administración de la seguridad informática no puede estar desligada de la administración de toda la organización ya que esta es parte fundamental de la misma y no podrá ser puesta en práctica sin un esfuerzo administrativo.

Recomendaciones

Mejorar la competitividad de una empresa es uno de los objetivos de la misma y la implementación de un conjunto de políticas y procedimientos de seguridad informática ayuda a alcanzar éste objetivo, por lo cual, debe ser una prioridad dentro de las organizaciones.

Para emprender en un proyecto de creación de políticas y procedimientos de seguridad al interior de una institución es necesario contar con el respaldo de los altos directivos si se desea que el proyecto tenga una altísima probabilidad de éxito

Se debe tener presente que las políticas y procedimientos de seguridad en una institución no pueden ser algo estático, deben ser revisadas de acuerdo con el crecimiento y el cambio institucional, así como por el cambio tecnológico que sufra la organización.

Vincular la administración de la seguridad informática a la práctica común de la administración empresarial. Son dos mundos que deben marchar por la misma senda.

El uso de redes de almacenamiento, SAN, puede convertirse en una solución interesante para el almacenamiento de la información de la EMUCE, su utilización podría dar soporte a los actuales y futuros requerimientos de almacenamiento y acceso a la información, ya que, dan soporte a una gran cantidad de datos y es una de las opciones más eficientes y versátiles que se presentan actualmente, además el desarrollo de dispositivos de almacenamiento y en las telecomunicaciones facilitan de gran manera su implementación y uso de manera eficaz y eficiente.

Bibliografía

ALCIBAR Cesar, Convergencias entre normas y tecnología, Documento digital.

BONILLA Gustavo, Seguridad de la información – Norma ISO 17799, Documento Digital.

CASAL Gonzáles Concepción, La seguridad informática de las aplicaciones y el control interno, Documento Digital.

CORELITI Estrada Alejandro, Análisis de ISO-27001:2005, Documento Digital.

CORELITTI Estrada Alejandro, "ISO-27001- Los controles." Parte I. Documento Digital.

CORELITTI Estrada Alejandro, "ISO-27001- Los controles." Parte II. Documento Digital.

GARCIA Amo José Ramón, La gestión de la seguridad informática en el ministerio de agricultura, pesca y alimentación, Documento Digital.

GONZÁLES Breña Julio, Análisis de riesgos en la agencia estatal de meteorología mediante el empleo de MAGERIT y PILAR, Documento Digital.

JARAUTA Sánchez Javier, SIERRA José María, PALACIOS Hielscher Rafael, Seguridad informática, Documento Digital.

KERIK, Clempner Julio, GUTIÉRREZ Tornés Agustín, Planeación estratégica de tecnología de información en entornos dinámicos e inciertos. Documento digital.

MARTÍNEZ Martínez Cristina, Guía de implantación de sistemas de gestión de la seguridad de la información, Documento Digital.

RODRÍGUEZ de la Roa Gómez Álvaro, Sistemas de gestión de seguridad de la información. Documento Digital.

VIVEROS Aguirre Jerson, Fundamentos para el desarrollo de un sistema de gestión de seguridad de la información, Documento Digital.

CONTRALORÍA GENERAL DE LA REPÚBLICA DE COSTA RICA, Normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE), Documento Digital, Aprobada en el año 2007.

IT GOVERNACE INSTITUTE., Manual de objetivos de control, directrices gerenciales y modelo de madurez, Cobit 4.0

IT GOVERNANCE INSTITUTE, Reunión informativa del consejo sobre la gobernabilidad de TI, Documento Digital.

MINISTERIO DE ADMINISTRACIONES PÚBLICAS, Metodología de análisis y gestión de riesgo de los sistemas de información - I método, Madrid, 20 de junio de 2006

MINISTERIO DE ADMINISTRACIONES PÚBLICAS, Metodología de análisis y gestión de riesgo de los sistemas de información - II catálogo de elementos, Madrid, 20 de junio de 2006

MINISTERIO DE ADMINISTRACIONES PÚBLICAS, metodología de análisis y gestión de riesgo de los sistemas de información - III guía de técnicas, Madrid, 20 de junio de 2006

MINISTERIO ESPAÑOL DE ADMINISTRACIONES PÚBLICAS, Aplicaciones utilizadas para el ejercicio de potestades – Criterios de Conservación. Junio de 2004

MINISTERIO ESPAÑOL DE ADMINISTRACIONES PÚBLICAS, Aplicaciones utilizadas para el ejercicio de potestades – Criterios de Seguridad y Conservación, Junio de 2004

ISO/IEC 17799:2007 Norma Técnica Peruana, Documento Digital

UNIVERSIDAD NACIONAL DE COLOMBIA, Guía para la elaboración de políticas de seguridad, Documento Digital.

Anexo I

Glosario

EMUCE

Empresa Municipal de Servicios de Cementerios, Salas de Velación y Exequias – Cuenca

MGSI

Maestría en Gerencia de Sistemas de Información

ISO

Organización Internacional para la Normalización

SGSI

Sistema de Gestión de la Seguridad de la Información

COBIT

Objetivos de Control para la Información y Tecnologías Relacionadas

PSI

Plan de Seguridad de la Información

TI

Tecnología de la Información

TIC's

Tecnología de la Información y Comunicación

MAGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Anexo II

Listado de Activos

Datos - Información

DAT-001	Catálogo de usuarios de la red LAN
DAT-002	Datos del sistema.

Servicios

SER-001	Servicio de Internet
SER-002	Autenticación de usuarios en la red LAN
SER-003	Servicio de telefonía
SER-004	Servicio de conexión remota

Aplicaciones

APL-001	Subsistema de contabilidad
APL-002	Subsistema de inventarios
APL-003	Subsistema de recaudaciones
APL-004	Subsistema de servicios
APL-005	Subsistema de administración de accesos a aplicaciones
APL-006	Subsistema de nómina

Equipamiento informático

EQU-001	Equipo de Gerencia
EQU-002	Equipo de Jefatura Financiera
EQU-003	Equipo de Jefatura Administrativa

EQU-004	Equipo de Contabilidad
EQU-005	Equipo de Bodega
EQU-006	Equipo de Recaudación
EQU-007	Equipo de Compras
EQU-008	Equipo del Departamento Técnico
EQU-009	Equipo de Ventas
EQU-010	Equipo de Secretaría
EQU-011	Equipo de Funeraria
EQU-012	Equipo de la Casa de Velaciones
EQU-013	Equipo de Servicios
EQU-014	Equipo de Servicios
EQU-015	Impresora de Secretaría
EQU-016	Impresora de Recaudación
EQU-017	Impresora de la Jefatura Financiera
EQU-018	Impresora de Contabilidad
EQU-019	Impresora de la Jefatura Administrativa
EQU-020	Impresora de Compras
EQU-021	Impresora de Funeraria
EQU-022	Modem de conexión a Internet

EQU-023	Switch de conectividad LAN
EQU-024	Centralilla telefónica
EQU-025	Servidor

Soportes de Información

SOP-001	Disco externo de respaldos

Redes

RED-001	Red telefónica
RED-002	Red de datos
RED-003	Red punto a punto

Equipamiento auxiliar

AUX-001	Ups del servidor
AUX-002	Ups de Compras
AUX-003	Ups de Ventas

Instalaciones

INS-001	Edificio de la EMUCE

Anexo III

Modelos de Fichas de Control de Activos

Ficha de Levantamiento de Información de Activos

[D] Datos / Información	
Código	**Nombre**
Descripción	
Propietario	
Responsable	

Tipo (marque todos los adjetivos que procedan):

( ) [vr] datos vitales (vital records)
( ) [com] datos de interés comercial
( ) [adm] datos de interés para la administración pública
( ) [int] datos de gestión interna
( ) [source] código fuente
( ) [exe] código ejecutable
( ) [conf] datos de configuración
( ) [log] registro de actividad (log)
( ) [test] datos de prueba

( ) [per] datos de carácter personal
( ) [A] de nivel alto
( ) [M] de nivel medio
( ) [B] de nivel básico

( ) [label] datos clasificados
( ) [S] secreto
( ) [R] reservado
( ) [C] confidencial
( ) [DL] difusión limitada
( ) [SC] sin clasificar

Valoración		
Dimensión	**Valor**	**Justificación**
[I] Integridad		
[C] Confidencialidad		
[A_C] Autenticidad de quién accede a los datos		
[T_D] Trazabilidad de quén accede a los datos, cuándo y con qué hace		

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

Ficha de Levantamiento de Información de Activos

[S] Servicios	
Código	**Nombre**
Descripción	
Propietario	
Responsable	

Tipo (marque todos los adjetivos que procedan):

( ) [anon] anónimos (sin requerir identificación del usuario)
( ) [pub] al público en general (sin relación contractual)
( ) [ext] a usuarios externos (bajo una relación contractual)
( ) [int] interno (usuarios y medios de la propia organización)
( ) [cont] contratado a terceros (se presta con medios ajenos)

( ) [www] world wide web
( ) [telnet] acceso remoto a cuenta local
( ) [email] correo electrónico
( ) [ftp] transferencia de ficheros
( ) [edi] intercambio electrónico de datos

( ) [dir] servicio de directorio
( ) [idm] gestión de identidades
( ) [ipm] gestión de privilegios
( ) [pki] PKI – infraestructura de clave pública

Valoración		
Dimensión	**Valor**	**Justificación**
[D] Disponibilidad		
[A_S] Autenticidad de quién accede al servicio		
[T_S] Trazabilidad de qué accede al servicio, cuándo y qué hace		

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

Ficha de Levantamiento de Información de Activos

[SW] Aplicaciones (software)	
Código	**Nombre**
Descripción	
Propietario	
Responsable	
Tipo (marque todos los adjetivos que procedan): ( ) [prp] desarrollo propio (in house) ( ) [sub] desarrollo a medida (subcontratado) ( ) [std] estándar (off the shelf) ( ) [browser] navegador web ( ) [www] servidor de presentación ( ) [email_client] cliente de correo electrónico ( ) [app] servidor de aplicaciones ( ) [file] servidor de ficheros ( ) [dbms] sistema de gestión de bases de datos ( ) [tm] monitor transaccional ( ) [office] ofimática ( ) [av] anti virus ( ) [backup] sistema de backup ( ) [os] sistema operativo	

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

Ficha de Levantamiento de Información de Activos

[HW] Equipamiento Informático (hardware)	
Código	**Nombre**
Descripción	
Propietario	
Responsable	
Tipo (marque todos los adjetivos que procedan): ( ) [host] grandes equipos ( ) [mid] equipos medios ( ) [pc] informática personal ( ) [mobile] informática móvil ( ) [pda] agendas personales ( ) [easy] fácilmente reemplazable ( ) [data] que almacena datos ( ) [peripheral] periféricos ( ) [print] medios de impresión ( ) [scan] escáneres ( ) [crypto] dispositivos criptográficos ( ) [network] soporte de la red ( ) [modem] módems ( ) [hub] concentradores ( ) [switch] conmutadores ( ) [router] encaminadores ( ) [bridge] pasarelas ( ) [firewall] cortafuegos ( ) [pabx] centralita telefónica	

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

Ficha de Levantamiento de Información de Activos

[SI] Soportes de Información	
Código	**Nombre**
Descripción	
Propietario	
Responsable	
Tipo (marque todos los adjetivos que procedan): ( ) [electronic] electrónicos ( ) [disk] discos ( ) [disquette] disquetes ( ) [cd] cederrón (CD-ROM) ( ) [usb] dispositivos USB ( ) [dvd] DVD ( ) [tape] cinta magnética ( ) [mc] tarjetas de memoria ( ) [ic] tarjetas inteligentes ( ) [non_electronic] no electrónicos ( ) [printed] material impreso ( ) [tape] cinta de papel ( ) [film] microfilm ( ) [cards] tarjetas perforadas	

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

Ficha de Levantamiento de Información de Activos

[COM] Redes de Comunicación	
Código	**Nombre**
Descripción	
Propietario	
Responsable	
Tipo (marque todos los adjetivos que procedan): ( ) [PSTN] red telefónica ( ) [ISDN] rdsi (red digital) ( ) [X25] X25 (red de datos) ( ) [ADSL] ADSL ( ) [pp] punto a punto ( ) [radio] red inalámbrica ( ) [sat] satélite ( ) [LAN] red local ( ) [MAN] red metropolitana ( ) [Internet] Internet ( ) [vpn] red privada virtual	

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

Ficha de Levantamiento de Información de Activos

[AUX] Equipamiento Auxiliar	
Código	**Nombre**
Descripción	
Propietario	
Responsable	
Tipo (marque todos los adjetivos que procedan): ( ) [power] fuentes de alimentación ( ) [ups] sistemas de alimentación ininterrumpida ( ) [gen] generadores eléctricos ( ) [ac] equipos de climatización ( ) [cabling] cableado ( ) [robot] robots ( ) [tape] ... de cintas ( ) [disk] ... de discos ( ) [supply] suministros esenciales ( ) [destroy] equipos de destrucción de soportes de información ( ) [furniture] mobiliario: armarios, etc ( ) [safe] cajas fuertes	

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

Ficha de Levantamiento de Información de Activos

[L] Instalaciones	
Código	**Nombre**
Descripción	
Propietario	
Responsable	
Tipo (marque todos los adjetivos que procedan): ( ) [site] emplazamiento ( ) [building] edificio ( ) [local] local ( ) [mobile] plataformas móviles ( ) [car] vehículo terrestre: coche, camión, etc. ( ) [plane] vehículo aéreo: avión, etc. ( ) [ship] vehículo marítimo: buque, lancha, etc. ( ) [shelter] contenedores ( ) [channel] canalización	

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

Ficha de Levantamiento de Información de Activos

[P] Personal	
Código	**Nombre**
Descripción	
Propietario	
Responsable	
Tipo (marque todos los adjetivos que procedan): ( ) [ue] usuarios externos ( ) [ui] usuarios internos ( ) [op] operadores ( ) [adm] administradores de sistemas ( ) [com] administradores de comunicaciones ( ) [dba] administradores de BBDD ( ) [des] desarrolladores ( ) [sub] subcontratas ( ) [prov] proveedores	

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

Anexo IV

Fichas de relación de activos

[SW] Aplicaciones (software)	
Código: APL-001	**Nombre: Subsistema de Contabilidad**
Descripción: Permite el registro contable de las tranasacciones de la empresa	
Propietario: EMUCE	
Responsable: Econ. Gustavo Gavilanes	

Tipo (marque todos los adjetivos que procedan):
( ) [prp] desarrollo propio (in house)
(X) [sub] desarrollo a medida (subcontratado)
( ) [std] estándar (off the shelf)
( ) [browser] navegador web
( ) [www] servidor de presentación
( ) [email_client] cliente de correo electrónico
( ) [app] servidor de aplicaciones
( ) [file] servidor de ficheros
(X) [dbms] sistema de gestión de bases de datos
( ) [tm] monitor transaccional
( ) [office] ofimática
( ) [av] anti virus
( ) [backup] sistema de backup
( ) [os] sistema operativo

Dependencia de activos inferiores	
Activo: EQU-002	**Grado: Alt0**
¿Por qué? Es en el equipo en el cual se ejecuta el sistema	
Activo: EQU-001	**Grado: Bajo**
¿Por qué? Es utilizado para realizar las consultas financieras	
Activo: EQU-004	**Grado: Alto**
¿Por qué? Es el equipo en el cual se registran las transaciones contables	
Activo: EQU-006	**Grado: Alto**
¿Por qué? Es el equipo en el cual se registran los igresos financieros y se realiza el proceso de facturación	
Activo: EQU-013	**Grado: Alto**
¿Por qué? Es el equipo en el cual se registran los igresos financieros y se realiza el proceso de facturación	
Activo: EQU-014	**Grado: Alto**
¿Por qué? Es el equipo en el cual se registran los igresos financieros y se realiza el proceso de facturación	

[SW] Aplicaciones (software)	
Código: APL-002	**Nombre: Subsistema de Inventarios**
Descripción: Permite el registro de los inventarios que son propiedad de la EMUCE	
Propietario: EMUCE	
Responsable: Econ. Gustavo Gavilanes	

Tipo (marque todos los adjetivos que procedan):
( ) [prp] desarrollo propio (in house)
(X) [sub] desarrollo a medida (subcontratado)
( ) [std] estándar (off the shelf)
( ) [browser] navegador web
( ) [www] servidor de presentación
( ) [email_client] cliente de correo electrónico
( ) [app] servidor de aplicaciones
( ) [file] servidor de ficheros
(X) [dbms] sistema de gestión de bases de datos
( ) [tm] monitor transaccional
( ) [office] ofimática
( ) [av] anti virus
( ) [backup] sistema de backup
( ) [os] sistema operativo

Dependencia de activos inferiores	
Activo: EQU-005	**Grado: Alto**
¿Por qué? El ingreso de los activos se los realiza por bodega	
Activo: EQU-003	**Grado: Bajo**
¿Por qué? El departamento financiero es el encargado del control de los activos de la EMUCE	
Activo: EQU-004	**Grado: Bajo**
¿Por qué? Se debe contabilizar los activos en los cierres de los períodos contables	

[SW] Aplicaciones (software)	
Código: APL-003	**Nombre: Subsistema de recaudaciones**
Descripción: Registra los ingresos de la emuce por concepto de la venta de los diferentes servicios	
Propietario: EMUCE	
Responsable: Econ. Gustavo Gavilanes	

Tipo (marque todos los adjetivos que procedan):	
( ) [prp] desarrollo propio (in house)	
(X) [sub] desarrollo a medida (subcontratado)	
( ) [std] estándar (off the shelf)	
( ) [browser] navegador web	
( ) [www] servidor de presentación	
( ) [email_client] cliente de correo electrónico	
( ) [app] servidor de aplicaciones	
( ) [file] servidor de ficheros	
(X) [dbms] sistema de gestión de bases de datos	
( ) [tm] monitor transaccional	
( ) [office] ofimática	
( ) [av] anti virus	
( ) [backup] sistema de backup	
( ) [os] sistema operativo	

Dependencia de activos inferiores	
Activo: EQU-009	**Grado: Alto**
¿Por qué? Es donde se registra las ventas de los servicios proporcionados por la EMUCE	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[SW] Aplicaciones (software)	
Código: APL-005	**Nombre: Subsistema de acceso a aplicaciones**
Descripción: Permite el control de acceso a las aplicaciones. Otorga permisos de acceso	
Propietario: EMUCE	
Responsable: Econ. Gustavo Gavilanes	

Tipo (marque todos los adjetivos que procedan):	
( ) [prp] desarrollo propio (in house)	
(X) [sub] desarrollo a medida (subcontratado)	
( ) [std] estándar (off the shelf)	
( ) [browser] navegador web	
( ) [www] servidor de presentación	
( ) [email_client] cliente de correo electrónico	
( ) [app] servidor de aplicaciones	
( ) [file] servidor de ficheros	
(X) [dbms] sistema de gestión de bases de datos	
( ) [tm] monitor transaccional	
( ) [office] ofimática	
( ) [av] anti virus	
( ) [backup] sistema de backup	
( ) [os] sistema operativo	

Dependencia de activos inferiores	
Activo: APL-001	**Grado: Alto**
¿Por qué? Si no funciona el subsistema de control de acceso, no es posible acceder a los sistemas	
Activo: APL-002	**Grado: Alto**
¿Por qué? Si no funciona el subsistema de control de acceso, no es posible acceder a los sistemas	
Activo: APL-003	**Grado: Alto**
¿Por qué? Si no funciona el subsistema de control de acceso, no es posible acceder a los sistemas	
Activo: APL-004	**Grado: Alto**
¿Por qué? Si no funciona el subsistema de control de acceso, no es posible acceder a los sistemas	
Activo: APL-006	**Grado: Alto**
¿Por qué? Si no funciona el subsistema de control de acceso, no es posible acceder a los sistemas	

[SW] Aplicaciones (software)	
Código: APL-006	**Nombre: Subsistema de nómina**
Descripción: Permite la realización del cálculo de la nómina de los empleados	
Propietario: EMUCE	
Responsable: Econ. Gustavo Gavilanes	

Tipo (marque todos los adjetivos que procedan):
( ) [prp] desarrollo propio (in house)
(X) [sub] desarrollo a medida (subcontratado)
( ) [std] estándar (off the shelf)
( ) [browser] navegador web
( ) [www] servidor de presentación
( ) [email_client] cliente de correo electrónico
( ) [app] servidor de aplicaciones
( ) [file] servidor de ficheros
(X) [dbms] sistema de gestión de bases de datos
( ) [tm] monitor transaccional
( ) [office] ofimática
( ) [av] anti virus
( ) [backup] sistema de backup
( ) [os] sistema operativo

Dependencia de activos inferiores	
Activo: EQU-003	**Grado: Medio**
¿Por qué? Al final de cada mes es necesario emitir la nómina	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-001	**Nombre: Equipo de Gerencia**
Descripción: Equipo de utilización del Econ. Gustavo Gavilanes	
Propietario: EMUCE	
Responsable: Econ. Gustavo Gavilanes	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
( ) [mid] equipos medios
(X) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
( ) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-002	**Nombre: Equipo de Jefatura Financiera**
Descripción: Equipo de Jefatura Financiera	
Propietario: EMUCE	
Responsable: Jefe Financiero	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
( ) [mid] equipos medios
(X) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
( ) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-003	**Nombre: Equipo de Jefatura Administrativa**
Descripción: Equipo de Jefatura Administrativa	
Propietario: EMUCE	
Responsable: Jefe Financiero	

Tipo (marque todos los adjetivos que procedan):

( ) [host] grandes equipos
( ) [mid] equipos medios
(X) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
  ( ) [print] medios de impresión
  ( ) [scan] escáneres
  ( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
  ( ) [modem] módems
  ( ) [hub] concentradores
  ( ) [switch] conmutadores
  ( ) [router] encaminadores
  ( ) [bridge] pasarelas
  ( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-004	**Nombre: Equipo de Contabilidad**
Descripción: Equipo de Contabilidad	
Propietario: EMUCE	
Responsable: Contador General	

Tipo (marque todos los adjetivos que procedan):

( ) [host] grandes equipos
( ) [mid] equipos medios
(X) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
  ( ) [print] medios de impresión
  ( ) [scan] escáneres
  ( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
  ( ) [modem] módems
  ( ) [hub] concentradores
  ( ) [switch] conmutadores
  ( ) [router] encaminadores
  ( ) [bridge] pasarelas
  ( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-005	**Nombre: Equipo de Bodega**
Descripción: Equipo de Bodega	
Propietario: EMUCE	
Responsable: Bodeguero	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
( ) [mid] equipos medios
(X) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
( ) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-006	**Nombre: Equipo de Recaudación**
Descripción: Equipo de recaudación	
Propietario: EMUCE	
Responsable: Tesorero	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
( ) [mid] equipos medios
(X) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
( ) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo: EQU-016	**Grado: Alto**
¿Por qué? Es una impresora matricial conectada directamente al puerto del PC	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-007	**Nombre: Equipo de Compras**
Descripción: Equipo de Compras	
Propietario: EMUCE	
Responsable: Jefe de Compras	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
( ) [mid] equipos medios
(X) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
( ) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo: EQU-020	**Grado: Alto**
¿Por qué? Impresora conectada directamente al puerto del PC	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-008	**Nombre: Equipo del Departamento Técnico**
Descripción: Equipo del Departamento Técnico	
Propietario: EMUCE	
Responsable: Jefe del Departamento Técnico	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
( ) [mid] equipos medios
(X) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
( ) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-009	**Nombre: Equipo de Ventas**
Descripción: Equipo de Ventas	
Propietario: EMUCE	
Responsable: Recaudador	

Tipo (marque todos los adjetivos que procedan):

- ( ) [host] grandes equipos
- ( ) [mid] equipos medios
- (X) [pc] informática personal
- ( ) [mobile] informática móvil
- ( ) [pda] agendas personales
- ( ) [easy] fácilmente reemplazable
- ( ) [data] que almacena datos
- ( ) [peripheral] periféricos
  - ( ) [print] medios de impresión
  - ( ) [scan] escáneres
  - ( ) [crypto] dispositivos criptográficos
- ( ) [network] soporte de la red
  - ( ) [modem] módems
  - ( ) [hub] concentradores
  - ( ) [switch] conmutadores
  - ( ) [router] encaminadores
  - ( ) [bridge] pasarelas
  - ( ) [firewall] cortafuegos
- ( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-010	**Nombre: Equipo de Secretaria**
Descripción: Equipo de Secretaria	
Propietario: EMUCE	
Responsable: Secretaria de Gerencia	

Tipo (marque todos los adjetivos que procedan):

( ) [host] grandes equipos
( ) [mid] equipos medios
(X) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
  ( ) [print] medios de impresión
  ( ) [scan] escáneres
  ( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
  ( ) [modem] módems
  ( ) [hub] concentradores
  ( ) [switch] conmutadores
  ( ) [router] encaminadores
  ( ) [bridge] pasarelas
  ( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-011	**Nombre: Equipo de Funeraria**
Descripción: Equipo de Funeraria	
Propietario: Equipo de Funeraria	
Responsable: Jefe de Funeraria	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
( ) [mid] equipos medios
(X) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
( ) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-012	**Nombre: Equipo de la Casa de Velaciones**
Descripción: Equipo de la Casa de Velaciones	
Propietario: EMUCE	
Responsable: Jefe de Funeraria	

Tipo (marque todos los adjetivos que procedan):

- ( ) [host] grandes equipos
- ( ) [mid] equipos medios
- (X) [pc] informática personal
- ( ) [mobile] informática móvil
- ( ) [pda] agendas personales
- ( ) [easy] fácilmente reemplazable
- ( ) [data] que almacena datos
- ( ) [peripheral] periféricos
  - ( ) [print] medios de impresión
  - ( ) [scan] escáneres
  - ( ) [crypto] dispositivos criptográficos
- ( ) [network] soporte de la red
  - ( ) [modem] módems
  - ( ) [hub] concentradores
  - ( ) [switch] conmutadores
  - ( ) [router] encaminadores
  - ( ) [bridge] pasarelas
  - ( ) [firewall] cortafuegos
- ( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-013	**Nombre: Equipo de Servicios**
Descripción: Equipo de Servicios	
Propietario: EMUCE	
Responsable: Auxiliar de Servicios	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
( ) [mid] equipos medios
(X) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
( ) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-014	**Nombre: Equipo de Servicios**
Descripción: Equipo de Servicios	
Propietario: EMUCE	
Responsable: Auxiliar de Servicios	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
( ) [mid] equipos medios
(X) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
( ) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-015	**Nombre: Impresora de Secretaria**
Descripción: Impresora de Secretaria	
Propietario: EMUCE	
Responsable: Secretaria de Gerencia	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
( ) [mid] equipos medios
( ) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
(X) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-016	**Nombre: Impresora de Recaudación**
Descripción: Impresora de Recuadación	
Propietario: EMUCE	
Responsable: Tesorero	

Tipo (marque todos los adjetivos que procedan):

( ) [host] grandes equipos
( ) [mid] equipos medios
( ) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
(X) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-017	**Nombre: Impresora de la Jefatura Financiera**
Descripción: Impresora de la Jefatura Financiera	
Propietario: EMUCE	
Responsable: Director Financiero	

Tipo (marque todos los adjetivos que procedan):

- ( ) [host] grandes equipos
- ( ) [mid] equipos medios
- ( ) [pc] informática personal
- ( ) [mobile] informática móvil
- ( ) [pda] agendas personales
- ( ) [easy] fácilmente reemplazable
- ( ) [data] que almacena datos
- ( ) [peripheral] periféricos
  - (X) [print] medios de impresión
  - ( ) [scan] escáneres
  - ( ) [crypto] dispositivos criptográficos
- ( ) [network] soporte de la red
  - ( ) [modem] módems
  - ( ) [hub] concentradores
  - ( ) [switch] conmutadores
  - ( ) [router] encaminadores
  - ( ) [bridge] pasarelas
  - ( ) [firewall] cortafuegos
- ( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-018	**Nombre: Impresora de Contabilidad**
Descripción: Impresora de Contabilidad	
Propietario: EMUCE	
Responsable: Contador General	

Tipo (marque todos los adjetivos que procedan):

( ) [host] grandes equipos
( ) [mid] equipos medios
( ) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
(X) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-019	**Nombre: Impresora de la Jefatura Administrativa**
Descripción: Impresora de la Jefatura Administrativa	
Propietario: EMUCE	
Responsable: Jefe Administrativo	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
( ) [mid] equipos medios
( ) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
(X) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-020	**Nombre: Impresora de Compras**
Descripción: Impresora de Compras	
Propietario: EMUCE	
Responsable: Jefe Administrativo	

Tipo (marque todos los adjetivos que procedan):

( ) [host] grandes equipos
( ) [mid] equipos medios
( ) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
(X) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-020	**Nombre: Impresora de Funeraria**
Descripción: Impresora de Funeraria	
Propietario: EMUCE	
Responsable: Jefe Administrativo	

Tipo (marque todos los adjetivos que procedan):

- ( ) [host] grandes equipos
- ( ) [mid] equipos medios
- ( ) [pc] informática personal
- ( ) [mobile] informática móvil
- ( ) [pda] agendas personales
- ( ) [easy] fácilmente reemplazable
- ( ) [data] que almacena datos
- ( ) [peripheral] periféricos
  - (X) [print] medios de impresión
  - ( ) [scan] escáneres
  - ( ) [crypto] dispositivos criptográficos
- ( ) [network] soporte de la red
  - ( ) [modem] módems
  - ( ) [hub] concentradores
  - ( ) [switch] conmutadores
  - ( ) [router] encaminadores
  - ( ) [bridge] pasarelas
  - ( ) [firewall] cortafuegos
- ( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-021	**Nombre: Impresora de Funeraria**
Descripción: Impresora de Funeraria	
Propietario: EMUCE	
Responsable: Jefe de Fuenraria	

Tipo (marque todos los adjetivos que procedan):

( ) [host] grandes equipos
( ) [mid] equipos medios
( ) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
(X) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-022	**Nombre: Modem de conexión a Internet**
Descripción: Modem de conexión a Internet	
Propietario: ETAPA	
Responsable: Coordinador de Sistemas	

Tipo (marque todos los adjetivos que procedan):

( ) [host] grandes equipos
( ) [mid] equipos medios
( ) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
  ( ) [print] medios de impresión
  ( ) [scan] escáneres
  ( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
  (X) [modem] módems
  ( ) [hub] concentradores
  ( ) [switch] conmutadores
  ( ) [router] encaminadores
  ( ) [bridge] pasarelas
  ( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-023	**Nombre: Switch de conectividad LAN**
Descripción: Switch de conectividad LAN	
Propietario: EMUCE	
Responsable: Coordinador de Sistemas	

Tipo (marque todos los adjetivos que procedan):

( ) [host] grandes equipos
( ) [mid] equipos medios
( ) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
  ( ) [print] medios de impresión
  ( ) [scan] escáneres
  ( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
  ( ) [modem] módems
  ( ) [hub] concentradores
  (X) [switch] conmutadores
  ( ) [router] encaminadores
  ( ) [bridge] pasarelas
  ( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-024	**Nombre: Centralilla telefónica**
Descripción: Centralilla telefónica	
Propietario: EMUCE	
Responsable: Jefe Administrativo	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
( ) [mid] equipos medios
( ) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
( ) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
(X) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[HW] Equipamiento Informático (hardware)	
Código: EQU-025	**Nombre: Servidor**
Descripción: Servidor de datos y aplicaciones de la EMUCE	
Propietario: EMUCE	
Responsable: Coordinador de Sistemas	

Tipo (marque todos los adjetivos que procedan):
( ) [host] grandes equipos
(X) [mid] equipos medios
( ) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
( ) [print] medios de impresión
( ) [scan] escáneres
( ) [crypto] dispositivos criptográficos
( ) [network] soporte de la red
( ) [modem] módems
( ) [hub] concentradores
( ) [switch] conmutadores
( ) [router] encaminadores
( ) [bridge] pasarelas
( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Dependencia de activos inferiores	
Activo: APL-001	**Grado: Alto**
¿Por qué? Es en el servidor en el cual se encuentran los subsistemas	
Activo: APL-002	**Grado: Alto**
¿Por qué? Es en el servidor en el cual se encuentran los subsistemas	
Activo: APL-003	**Grado: Alto**
¿Por qué? Es en el servidor en el cual se encuentran los subsistemas	
Activo: APL-004	**Grado: Alto**
¿Por qué? Es en el servidor en el cual se encuentran los subsistemas	
Activo: APL-005	**Grado: Alto**
¿Por qué? Es en el servidor en el cual se encuentran los subsistemas	
Activo: APL-006	**Grado: Alto**
¿Por qué? Es en el servidor en el cual se encuentran los subsistemas	

[SI] Soportes de Información	
Código: SOP-001	**Nombre: Soporte de Información**
Descripción: Disco duro externo con la finalidad de obtener respaldos	
Propietario: EMUCE	
Responsable: Coordinador de Sistemas	

Tipo (marque todos los adjetivos que procedan):
( ) [electronic] electrónicos
(X) [disk] discos
( ) [disquette] disquetes
( ) [cd] cederrón (CD-ROM)
( ) [usb] dispositivos USB
( ) [dvd] DVD
( ) [tape] cinta magnética
( ) [mc] tarjetas de memoria
( ) [ic] tarjetas inteligentes
( ) [non_electronic] no electrónicos
( ) [printed] material impreso
( ) [tape] cinta de papel
( ) [film] microfilm
( ) [cards] tarjetas perforadas

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[COM] Redes de Comunicación	
Código: RED-001	**Nombre: Red Telefónica**
Descripción: Red que da soporte a los servicios telefónicos de la emuce	
Propietario	
Responsable	

Tipo (marque todos los adjetivos que procedan):
(X) [PSTN] red telefónica
( ) [ISDN] rdsi (red digital)
( ) [X25] X25 (red de datos)
( ) [ADSL] ADSL
( ) [pp] punto a punto
( ) [radio] red inalámbrica
( ) [sat] satélite
( ) [LAN] red local
( ) [MAN] red metropolitana
( ) [Internet] Internet
( ) [vpn] red privada virtual

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[COM] Redes de Comunicación	
Código: RED-002	**Nombre: Red de Datos**
Descripción: Cableado no estructurado para dar servicios de red al interior de la EMUCE	
Propietario: EMUCE	
Responsable: Coordinador de Sistemas	

Tipo (marque todos los adjetivos que procedan):
( ) [PSTN] red telefónica
( ) [ISDN] rdsi (red digital)
(X) [X25] X25 (red de datos)
( ) [ADSL] ADSL
( ) [pp] punto a punto
( ) [radio] red inalámbrica
( ) [sat] satélite
( ) [LAN] red local
( ) [MAN] red metropolitana
( ) [Internet] Internet
( ) [vpn] red privada virtual

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[AUX] Equipamiento Auxiliar	
Código: AUX-003	**Nombre: UPS de Ventas**
Descripción: UPS para dar protección a computador de recaudación	
Propietario: EMUCE	
Responsable: Tesorero	

Tipo (marque todos los adjetivos que procedan):

- ( ) [power] fuentes de alimentación
- (X) [ups] sistemas de alimentación ininterrumpida
- ( ) [gen] generadores eléctricos
- ( ) [ac] equipos de climatización
- ( ) [cabling] cableado
- ( ) [robot] robots
  - ( ) [tape] ... de cintas
  - ( ) [disk] ... de discos
- ( ) [supply] suministros esenciales
- ( ) [destroy] equipos de destrucción de soportes de información
- ( ) [furniture] mobiliario: armarios, etc
- ( ) [safe] cajas fuertes

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[L] Instalaciones	
Código: INS-001	**Nombre: Edificio de la EMUCE**
Descripción: Edificio principal en donde funciona la EMUCE	
Propietario: EMUCE	
Responsable: Gerente	

Tipo (marque todos los adjetivos que procedan):
( ) [site] emplazamiento
(X) [building] edificio
( ) [local] local
( ) [mobile] plataformas móviles
( ) [car] vehículo terrestre: coche, camión, etc.
( ) [plane] vehículo aéreo: avión, etc.
( ) [ship] vehículo marítimo: buque, lancha, etc.
( ) [shelter] contenedores
( ) [channel] canalización

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

[P] Personal	
Código: PER-001	**Nombre: Coordinador de Sistemas**
Descripción: Responsable de funcionamiento de los sistema en la EMUCE	
Propietario	
Responsable	

Tipo (marque todos los adjetivos que procedan):	
( ) [ue] usuarios externos	
( ) [ui] usuarios internos	
( ) [op] operadores	
(X) [adm] administradores de sistemas	
( ) [com] administradores de comunicaciones	
( ) [dba] administradores de BBDD	
( ) [des] desarrolladores	
( ) [sub] subcontratas	
( ) [prov] proveedores	

Dependencia de activos inferiores	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	
Activo	**Grado**
¿Por qué?	

Anexo V

Diagnóstico Nivel de Madurez en el área de TI

Análisis del entorno de la TIC[10]

El área de TIC en la empresa no se encuentra definida ni orgánicamente, ni funcionalmente; en el organigrama no consta el departamento o área, lo que pone en clara decadencia la utilización y potencialización de las tecnologías relacionadas con la gestión de información y comunicaciones. Esta problemática se acentúa al no contar con un profesional, dentro de sus funcionarios, con conocimientos y preparación en las aéreas de TIC.

Este acaecer se revierte lógicamente en la pobre generación de planes, organización, adquisición y renovación de activos relacionados, soporte y monitoreo de los recursos tecnológicos y de sistemas.

Para suplir la deficiencia orgánica y funcional respecto al espacio de las TIC, se le ha encargado a una funcionaria que ocupa el cargo de bodeguera para que entregue el soporte básico a los usuarios cuando se presentan problemas relacionados con el uso de los equipos informáticos y del sistema de información, sin que esta funcionaria tenga un grado adecuado de preparación para la toma de decisiones, aportaciones y atención en el área.

Cuando los casos de soporte superan el nivel de conocimiento de la funcionaria encargada, deben acudir a solicitar apoyo externo, que sin duda no entregan la atención en el tiempo optimo y muchas veces ni siquiera la adecuada, pues son resultados y decisiones asumidas reactivamente para salir del problema puntual, sin percibir y considerar el ámbito total del precursor del problema, de la consecuencia de la solución y de las posibles afecciones al total del entorno tecnológico y del sistema de información.

Existiendo la conciencia de la necesidad de contar con apoyo técnico externo, no existe tampoco contratos formales con profesionales y/o empresas

[10] Araneda, Delgado Ronnie. Trabajo de fin de maestría. Mayo 2009

que den un soporte outsorsing adecuado, simplemente se tiene identificado las “fuentes de socorro” a quienes se acude puntualmente cuando se presenta la necesidad.

Tampoco existe un área física destinada al centro de cómputo, donde se cuente con el ambiente adecuado para la tenencia de equipos, los mismos que se encuentran ubicados en las instalaciones según el “espacio y sitio” definido por comodidad de ordenamiento espacial, más que lineamientos técnicos.

Lo anterior a dado paso a que la red de datos comience a crecer desordenadamente y sin una planeación adecuada, teniendo que ir acomodando cables y dispositivos de red según se presente la necesidad y evidentemente sin las consideraciones técnicas debidas.

Gobierno y Gestión de las TIC

Para establecer el nivel de gobernabilidad y gestión de las TIC en la Empresa, se realizó una encuesta basada en los estándares sugeridos por COBIT, de la cual se puede desprender lo siguiente:

Planear y Organizar

No existe un plan estratégico de TIC, ni una arquitectura de información que provea una adecuada respuesta a los requerimientos de información que se integre con los procesos de negocio.

La dirección tecnológica es de tipo inicial, donde se cuenta con un sistema aplicativo “adaptado” a las necesidades, pero que se origina de un SI comercial, lo que no satisface la totalidad de requerimientos actuales y menos los futuros.

La definición de procesos y la organización de las TIC se lo realizan reactivamente, posesionando este aspecto en un nivel inicial, sin claras proyecciones de formalizarla.

La administración de la inversión en TIC, administración de los recursos humanos relacionados, la calidad y proyectos del área es inexistente, pues obedece al surgimiento de necesidades puntuales y sujetas a un presupuesto que no incluye rubros para estas líneas.

Donde se nota un poco de incidencia gerencial es en la comunicación de las aspiraciones de los servicios actuales y responsabilidades, sin embargo no se encuentra formalizado.

No existe un plan de gestión de riesgos, lo que conlleva a plantear soluciones a los problemas que se presentan de una manera reactiva.

Adquirir e implementar

La identificación de soluciones automatizadas, la adquisición y mantenimiento de software aplicativo, la adquisición y mantenimiento de infraestructura de TIC, la administración de la operación y el uso de las TIC, la adquisición de recursos y la administración de cambios esta en un estado inicial, que se la realiza reactivamente, según las necesidades, nunca se llega a repetir un procedimiento para estas tareas.

La planificación oportuna, la instalación y acreditación de soluciones y cambios es inexistente, pues tan solo se limitan a “sostener” lo existente, y aunque hay rasgos iníciales donde por lo menos se piensa en las necesidades de adquisición e implementación, estas no están dirigidas a soluciones integrales, si no a necesidades identificadas a nivel de usuarios y que corresponden a apreciaciones personales.

Entregar y dar Soporte

La definición y administración de niveles de servicio, la administración de servicios de terceros, la administración del desempeño y la capacidad, la garantía de la continuidad de los servicios y la seguridad de los sistemas, la identificación y asignación de costos para soporte, la educación y

entrenamiento a usuarios, la administración de la mesa de servicios e incidentes, la configuración del servicios de soporte, la administración de los datos y la administración de las operaciones se encuentran en un estado inicial y responden de modo reactivo a las circunstancias.

Se mantiene una “relación de confianza” con el proveedor del sistema de información, a quien se lo contacta en los casos de necesidad, pero no existe un contrato formal de outsourcing, ni un procedimiento que de respuestas claras a las necesidades de soportes y help desk.

Algo que sobresale dentro de este nivel de Ad Hoc sobre la administración y gestión del soporte es que si se han preocupado por adiestrar a los usuarios, por lo menos en un nivel adecuado para que puedan hacer uso de sus recursos informáticos, en alguna medida con cursos formales de formación de usuarios y en otros casos con ayuda de los mismos proveedores del sistema quien les enseña informalmente a los usuarios.

No existe una gestión sobre la administración de problemas, ni administración sobre el ambiente físico, situación que no permite prevenir y prepararse para salir adelante eficientemente y a tiempo de una necesidad de help desk.

Monitorear y Evaluar

El monitoreo y evaluación del control interno y el cumplimiento regulatorio están en nivel inicial, esto es porque al ser una empresa de servicio público está sujeta a fiscalización y control de las entidades regulatorias del estado y a fiscalización interna, donde tiene que cumplir con las normativas prevista para este tipo de Empresas, haciendo que de algún modo estas regulaciones y acciones de control “salpiquen” al área de TIC, mas no por una conciencia de que en esta área debería existir un monitorio y evaluación de su gestión.

Es así que el desempeño en lo que se refiere a TIC, que es un aspecto que ya está inmerso en el control y fiscalización correspondiente a las empresas de servicio público está en un nivel de inexistencia total.

Conclusiones

- A nivel institucional no existe una conciencia de la importancia de las TIC como herramientas de soporte y dinamizadora de la gestión de negocio, de lo que se desprende una falta de compromiso por parte de sus más altos directivos para fortalecer los aspectos técnicos-tecnológicos.

- En general no se posesiona el uso intensivo de las TIC como instrumento estratégico al servicio de la reforma y gestión administrativa, que debería caminar en forma paralela con la modernización tanto de la actividad y la cultura de los servidores públicos.

- El personal para soportar la gestión de TIC no es el más apropiado, dejándose muy descubierto este aspecto, lo que origina una alta dependencia en terceros, situación que aporta negativamente a muchos factores de seguridad y administrabilidad.

- Los recursos informáticos y de comunicaciones son los suficientes y necesarios para soportar la necesidad actual, subrayando que el sistema de información y los servicios asociados a las TIC pudiesen ser mejorados sustancialmente, con esto se desea enfatizar que no son los ideales para convertirse en una verdadera fortaleza competitiva del entorno de negocio.

- La arquitectura de la red de datos no responde a principios de buenas prácticas técnicas, tanto en su tendido físico, como en su

configuración lógica, de lo que se desprende un alto nivel de inseguridad y poquísimo cuidado por la información, extendiéndose esta situación al manejo de los activos en general.

- Del punto de vista de los estándares recomendados por COBIT, donde la gestión de TIC en general puede definirse en 6 niveles, que son: No existente, Inicial/Ad Hoc, Repetible pero intuitiva, Proceso definido, Administrado y medible, y Optimizado; donde cada uno corresponde a un nivel de madures en la forma de "manejar" los aspectos de gestión, la Empresa se encuentra en un primer nivel, esto es Inicial/Ad Hoc, dado que todos los aspectos son tratados reactivamente y sin planes previos, ni gestiones de prevención.

Recomendaciones

- Elaborar un plan estratégico de TIC que guíe la gestión del área, y permita que la Empresa y sus directivos cuenten con una adecuada herramienta que oriente y permita tomar decisiones en un ámbito de acción planificado y con objetivos concretos, a demás de permitir planificar con anterioridad el presupuesto necesario para solventar los requerimientos del área.

- Empoderar las TIC como herramienta de soporte y gestión de negocios, para lo cual la gerencia deberá asumir tal compromiso y proporcionar los mecanismos de comunicación para que los funcionarios lo adopten como parte de una cultura institucional.

- Ejecutar un plan de formación formal sobre los recursos informáticos que poseen, tanto a nivel de usuarios como técnicos, reclutar personal profesional en el área de TIC y/o formalizar planes y contratos de outsourcing.

- Elaborar un plan de seguridad sobre los activos informáticos, la red de datos y la información de la Empresa, que asegure el conjunto computacional y describa las políticas necesarias para salvaguardar los recursos y permita recuperarse de la mejor manera posible de los diferentes eventos negativos que pudiesen presentarse.

- Iniciar un plan de acción que permita mejorar el nivel de madurez de la gestión de las TIC, asumiendo procesos y actividades apoyadas y guiadas por estándares que denoten buenas prácticas, tales como ITIL, COBIT, etc.

ANEXO V

Medida de Precaución y Recomendación

En Relación al Centro de Cómputo

Es recomendable que el Centro de Cómputo no esté ubicado en las áreas de alto tráfico de personas o con un alto número de invitados.

Hasta hace algunos años la exposición de los Equipos de Cómputo a través de grandes ventanales, constituían el orgullo de la organización, considerándose necesario que estuviesen a la vista del público, siendo constantemente visitados. Esto ha cambiado de modo radical, principalmente por el riesgo de terrorismo y sabotaje.

Se deben evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol y calor (inconvenientes para el equipo de cómputo), puede ser un riesgo para la seguridad del Centro de Cómputo.

Otra precaución que se debe tener en la construcción del Centro de Cómputo, es que no existan materiales que sean altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.

El acceso al Centro de Cómputo debe estar restringido al personal autorizado. El personal de la Institución deberá tener su carné de identificación siempre en un lugar visible.

Se debe establecer un medio de control de entrada y salida de visitas al centro de cómputo. Si fuera posible, acondicionar un ambiente o área de visitas.

Se recomienda que al momento de reclutar al personal se les debe hacer además exámenes psicológicos y médico y tener muy en cuenta sus antecedentes de trabajo, ya que un Centro de Cómputo depende en gran medida, de la integridad, estabilidad y lealtad del personal.

El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.

Deben establecerse controles para una efectiva disuasión y detección, a tiempo, de los intentos no autorizados de acceder a los sistemas y a los archivos de información que contienen.

Se recomienda establecer políticas para la creación de los password y establecer periodicidad de cambios de los mismos.

Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.

Establecer políticas de control de entrada y salida del personal, así como de los paquetes u objetos que portan.

La seguridad de las terminales de un sistema en red podrán ser controlados por medios de anulación del disk drive, cubriéndose de esa manera la seguridad contra robos de la información y el acceso de virus informáticos.

Los controles de acceso, el acceso en sí y los vigilantes deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña. En caso que ingresara algún extraño al centro de Cómputo, que no pase desapercibido y que no le sea fácil a dicha persona llevarse un archivo.

Las cámaras fotográficas no se permitirán en ninguna sala de cómputo, sin permiso por escrito de la Dirección.

Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

El modelo de seguridad a implementar, estará basado en el entorno y en la política y estrategias de la instalación.

Recomendaciones para el Mantenimiento de Cintas Magnéticas y Cartuchos

Cintas Magnéticas

- La temperatura y humedad relativa del ambiente en que se encuentran almacenados deben estar en el siguiente rango:

  Temperatura: 4ºC a 32ºC

  Humedad relativa: 20 % a 80 %

  El ambiente debe contar con aire acondicionado.

- Las cintas deben colocarse en estantes o armarios adecuados.

- Deberá mantenerse alejados de los campos magnéticos.

- Se les debe dar un mantenimiento preventivo en forma periódica a fin de desmagnetizar impurezas que se hayan registrado sobre ellas.

Cartuchos

- La temperatura y humedad relativa del ambiente en que se encuentran almacenados deben estar en el siguiente rango:

  Temperatura: 16ºC a más

  Humedad Relativa: 20 % a 80 %

  La temperatura interna del Drive puede oscilar entre: 5ºC a 45ºC.

- Deben ser guardados dentro de su caja de plástico.

- Deben mantenerse alejados de campos magnéticos.

Recomendaciones para el Mantenimiento de los Discos Duros

Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.

El ordenador debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio.

Se debe evitar que la microcomputadora se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras.

No se debe mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.

Una de las medidas más importantes en este aspecto, es hacer que la gente tome conciencia de lo importante que es cuidar un Microcomputador.

Recomendación para el Cuidado del Equipo de Cómputo

Teclado. Mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función.

CPU. Mantener la parte posterior del CPU liberado en por lo menos 10 cm. para asegurar así una ventilación mínima adecuada.

Mouse. Poner debajo del mouse una superficie plana y limpia, de tal manera que no se ensucien los rodillos y mantener el buen funcionamiento de éste.

Protectores de pantalla. Estos sirven para evitar la radiación de las pantallas a color que causan irritación a los ojos.

Impresora. El manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel.