UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE CIENCIAS PURAS Y NATURALES

CARRERA DE INFORMATICA

TESIS DE GRADO

"METODOLOGIA PARA LA SEGURIDAD DE ENTORNOS INFORMATICOS, MSEI"

PARA OPTAR AL TITULO DE LICENCIATURA EN INFORMATICA

MENCION: INGENIERIA DE SISTEMAS INFORMATICOS

POSTULANTE: FERNANDO CONDORI CALLE

TUTOR: LIC. EFRAIN SILVA SANCHEZ

REVISOR: LIC. GROVER ALEX RODRIGUEZ RAMIREZ

LA PAZ – BOLIVIA

2011

AGRADECIMIENTOS

A mi queridísima madre Lucy Calle la cual ya no se encuentre a mi lado, pero estará por siempre al lado de nuestro familia bendiciéndonos y cuidándonos como siempre día a día desde el cielo, a mi papá Julio Jaime Condori quien supo guiarme y darme consejos acertados y terminar mi proyecto, a mis hermanos Milton Hugo Condori, Noemí Condori y Rosmery Condori, porque siempre estuvieron a mi lado incondicionalmente y me brindaron la fortaleza para poder culminar con éxito esta proyecto.

A mi tutor Lic. Efraín Silva Sánchez, que me ha colaborado con su capacidad y modesto conocimiento en la realización de la presente tesis.

Le doy mi más profundo agradecimiento al Lic. Grover Alex Rodríguez Ramírez, mi revisor por sus acertados consejos, elocuente paciencia y amplio conocimiento, que está plasmado en el presente trabajo.

Finalmente agradecer a todos los docentes y compañeros estudiantes de la Carrera de Informática y a la Universidad Mayor de San Andrés por permitir mi formación como profesional.

Fernando Condori Calle

RESUMEN

La metodología propuesta se compone de seis fases que agrupan etapas. Estas fases, a su vez, desde un aspecto macroscópico se pueden generalizar en dos grandes grupos: el estudio del entorno y la implantación de la solución.

El primer grupo de fases se encuentran: La definición del Alcance; El Relevamiento; y La Planificación. Aquí se fija como objeto conocer al entorno informatizado donde se implementara la metodología, a fin de asegurarlo.

Este conocimiento implica la intervención del usuario, que aportara el conocimiento personal desde su perspectiva, también aportara inquietudes y necesidades que ayudaran al Experto en Seguridad a dar la solución más satisfactoria para el cliente.

El segundo grupo de fases comprende: La Implantación de la Solución; La Estabilización del Entorno; El Mantenimiento de la solución, para guardar el entorno en condiciones confiables de seguridad.

En esta parte el Experto en Seguridad ya conoce el entorno objetivo, por lo que se dedica a hallar la solución que mejor se adapte al mismo.

La implantación de las técnicas que se eligieron en la etapa anterior, genera y desarrolla los modelos de análisis que forman parte del Plan de Aseguramiento.

Luego de la ejecución del Plan de Aseguramiento, el entorno objetivo se estabiliza determinando una adecuada capacitación de los usuarios, y verificando los beneficios logrados como resultado.

La implantación se ocupara del registro de incidencias, de cambios en los bienes físicos y lógicos, entre los que se consideran las periódicas actualizaciones de software antivirus y otras técnicas a aplicarse con regularidad para mantener el nivel de seguridad a medida que el entorno cambia.

ABSTRACT

The proposed methodology consists of six phases which grouped stages. These phases, in turn, from a macroscopic appearance can be generalized into two main groups: the study of the environment and the implementation of the solution.

The first sets of phases are: Defining the Scope, The Survey, and Planning. Here the object is set to meet the computing environment where the methodology was implemented in order to secure it.

This knowledge involves user intervention, which provided personal knowledge from their perspective, it also brings concerns and needs to assist the Security Expert to give the most satisfactory solution for the customer.

The second group of stages includes: The Implementation of the Solution, The Neighborhood Stabilization, maintenance of the solution, to keep the environment safe reliable conditions.

In this part of the security expert known as the target environment, so that is dedicated to finding the solution that best suits it.

The implementation of the techniques that were chosen in the previous step, generates and develops analytical models that are part of the Assurance Plan.

After execution of the Assurance Plan, the target environment stabilizes determining adequate training of users, and verifying the benefits achieved as a result.

The introduction should address the event log, changes in physical and logical assets, among which are considered regular updates of antivirus software and other techniques to be applied regularly to maintain the level of security as the environment changes.

INDICE GENERAL

ANEXOS

CAPITULO I

INTRODUCCIÓN

1.1 INTRODUCCIÓN

La Seguridad Informática es una disciplina cuya importancia crece día a día. Aunque la seguridad es un concepto difícil de medir, su influencia afecta directamente a todas las actividades de cualquier entorno informatizado en los que interviene el Informático, por lo que es considerada una vital importancia.

La seguridad como "una característica de cualquier sistema (informática o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo y que es, en cierta manera infalible "....." para el caso de sistemas informáticos, es muy difícil de conseguir (según la mayoría de los expertos, imposible) por lo que pasa a hablar de *confiabilidad*" [Antonio Villalón Huerta, 2002].

"Seguridad de la información protege a esta de una amplia gama de amenazas, a fin de garantizar la continuidad comercial, minimizar el daño al negocio y maximizar el retorno sobre las inversiones y las oportunidades" [ISO 17799, 2005].

Actualmente la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que desemboca en la aparición de nuevas amenazas en los sistemas informáticos.

Esto ha llevado a que muchas organizaciones hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas tecnologías para obtener el mayor provecho de las ventajas que brindan. De esta manera las políticas de seguridad informática surgen como una herramienta para concienciar a los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

Las políticas de seguridad informática fijan los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Éstas políticas deben diseñarse "a medida" para así recoger las características propias de cada organización.

No son una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son más bien una descripción de lo que se desea proteger y el por qué de ello, es decir que pueden tomarse como una forma de comunicación entre los usuarios y los gerentes.

De acuerdo con lo anterior, el implementar políticas de seguridad requiere un alto compromiso con la organización, agudeza, destreza y experiencia técnica para detectar fallas y debilidades, y constancia para renovar y actualizar dichas políticas en función del dinámico ambiente que rodea las organizaciones modernas.

1.2 PLANTEAMIENTO DEL PROBLEMA

Básicamente, los problemas de Seguridad Informática son sucesos que no deseamos que ocurran. La mayoría son inesperados, aunque en muchos casos se puedan prevenir.

Cuando hablamos de incidencias de seguridad, o problemas de Seguridad de Informática nos referimos a:

- Acceso no autorizado a la información
- Descubrimiento de información
- Modificación no autorizada de datos
- Invasión a la privacidad
- Denegación de servicios
- Etc.

Cada entorno informatizado es diferente, y maneja distintos tipos de información, y por ende, es distinta la forma en que se tratan los datos.

Los componentes de los entornos informatizados son distintos, por lo que las especificaciones de seguridad asociados a cada uno varía notablemente

dependiendo de la tecnología utilizada a nivel de plataforma, software base y dispositivos físicos.

La funcionalidad y características técnicas de los componentes de los entornos varían notablemente según la marca, en particular en los aspectos concernientes a la seguridad.

Hoy en día la amenaza más común en los ambientes informatizados se centra en la eliminación o disminución de la disponibilidad de los recursos y servicios que utiliza el usuario.

El crecimiento de las telecomunicaciones y la estricta dependencia que existe entre el negocio de las empresas y la tecnología informática hace crítica la inversión en seguridad.

Cada vez más los procesos comerciales se ven estrechamente ligados a procesos informáticos. Prácticamente toda la información vital para el negocio de una compañía comercial se encuentra informatizada, no solo almacenada en dispositivos electrónicos, sino que, en la mayor parte de los casos, se encuentra distribuida físicamente y viaja constantemente a través de medios públicos como redes de telefonía e internet. Es por eso que se pone énfasis en el crecimiento de soluciones para el problema de la Seguridad Informática, por lo que el conocimiento en esta área ha crecido enormemente en los últimos años, al punto en que somos capaces de afirmar que es posible lograr una completa enumeración de las fallas de seguridad de los sistemas y los entornos en los que viven,

Estas fallas de seguridad son las que se convierten en amenazas susceptibles de ser aprovechadas por usuarios malintencionados para causar daño o algún tipo de invasión a la confidencialidad. Protegerse contra accesos no autorizados es el problema más sencillo a resolver, ya que durante años se han desarrollado y perfeccionado algoritmos matemáticos para la encriptación de datos, para el intercambio seguro de información, para garantizar el correcto funcionamiento del

software, que se ha traducido en herramientas capaces de proporcionar soluciones rápidas y sencillas a problemas técnicos de seguridad.

Desafortunadamente, no es suficiente simplemente arreglar los errores o eliminar las fallas técnicas de seguridad. El problema va mucho más allá. La Seguridad Informática es un problema cultural, en la que el usuario juega un rol protagónico.

La responsabilidad sobre la seguridad de los datos y equipos ya no recae solamente en el personal técnico especializado encargado de resguardar los bienes y servicios brindados por el entorno, sino que es el usuario el que debe velar por la seguridad de los bienes físicos y lógicos que maneja.

Para ello debe existir una conciencia de trabajo seguro, de resguardo de la confidencialidad y de protección de los activos utilizados a diario en el trabajo de cada individuo. Por esta razón la seguridad Informática debe estar incorporada desde el principio de todo proceso, desde el diseño para garantizar la evaluación de todos los factores funcionales (y no solamente los técnicos) a tener en cuenta para el uso seguro del entorno. Si esto sucede, el objetivo inicial de la seguridad habrá sido logrado.

Luego de lograr eso se deben implantar medidas de índole técnica que garanticen el adecuado uso de los recursos y servicios solamente a los usuarios autorizados, y la disponibilidad de los mismos. Pero lo importante es ver que la Seguridad Informática ya no es un problema de la gente especializada en sistemas, sino que ha salido de los laboratorios y los centros de cómputo para instalarse en el escritorio del usuario, en donde nacen los Problemas de Seguridad.

En el ámbito nacional se cuenta con las siguientes propuestas:

- Seguridad y Protección en Redes LAN conectadas a Internet, tesis realizado por Marco Antonio Quisbert Ayala en la Universidad Mayor de San Andrés, La Paz Bolivia, 2002.
- Encriptación de Datos Comprimidos, tesis realizado por Patricia Bacarreza Córdova en la Universidad Mayor de San Andrés, La Paz Bolivia, 2008.

- Guía Práctica para Analizar, Detectar y Solucionar Vulnerabilidades Físicas Lógicas en Sistemas de Informáticos, tesis realizado por Raúl Genero Silva García en la Universidad Mayor de San Andrés, La Paz Bolivia, 2008.

- IPSVOFSL Sistema Inteligente de Prevenciones de Intrusiones, tesis realizado por Marco Antonio Villegas Pacasi en la Universidad Mayor de San Andrés, La Paz Bolivia, 2008

1.3 HIPÓTESIS

H_0 La Metodología para la Seguridad de Entornos Informáticos basada en la norma ISO 17799 proporciona un método estructurado y ordenado para facilitar y guiar en la tarea de aseguramiento de un entorno informatizado.

H_1 La Metodología para la Seguridad de Entornos Informáticos basada en la norma ISO 17799 no proporciona un método estructurado y ordenado para facilitar y guiar en la tarea de aseguramiento de un entorno informatizado.

1.4 OBJETIVOS

1.4.1 Objetivo General

Diseñar un método para la seguridad de entornos informáticos basado en la norma ISO 17799.

1.4.2 Objetivos Específicos

- Plantear un modelo de seguridad que sea considerado una herramienta más para el ingeniero informático, esto para reducir el tiempo de trabajo que pueda implicar errores que se presenten a futuro.

- Determinar las fases por la que estará compuesta la presente metodología donde se aplicaran procedimientos y se buscara el conocimiento de los procesos, y a su vez, una completa documentación que avale y acompañe

al proyecto y que sirva de referente a lo largo de la vida operativa del entorno.

1.5 ALCANCES

En esta tesis se desarrollara una metodología de trabajo. Se describirán las tareas y subtareas a realizar para obtener resultados específicos, se indicaran un orden para realizarlas, se servirá de documentación a desarrollar para completar informes y relevamientos, se dará un marco general para el desarrollo del proyecto de aseguramiento del entorno en estudio.

1.6 LIMITES

No se entrara en detalle en los siguientes temas:

- Administración del proyecto:

  No se entrara en detalles en la formalización del Alcance, ni en la estimación de tiempos y costos del proyecto, ya que son tareas puramente administrativas que no hacen al problema de aseguramiento del entorno informatizado.

- Vulnerabilidades conocidas en sistemas operativos y aplicaciones:

  No se enumeran las vulnerabilidades conocidas en software base ni en aplicativos, ya que estas cambian y se incrementa día a día, lo que restaría escalabilidad y vigencia en el tiempo a la tesis.

- Implantación:

No se entrara en detalle en configuraciones ni ejecución de procesos específicos para solucionar problemas de seguridad en sistemas operativos ni software aplicativo pues pretende hacer una metodología portable, independiente de la plataforma tecnológica.

CAPITULO II

MARCO TEORICO

2.1 MARCO TEORICO

¿Qué es seguridad de la información?

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades. La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida [Norma ISO 17799, 2005].

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio [Norma ISO 17799, 2005].

¿Por qué se necesita seguridad de la información?

La información y los procesos, sistemas y redes de apoyo son activos comerciales importantes. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una ventaja competitiva, el flujo de caja, rentabilidad, observancia legal e imagen comercial. Las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas [Norma ISO 17799, 2005].

La seguridad de la información es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de la información funcionará como un facilitador; por ejemplo para lograr e-gobierno o e-negocio, para evitar o reducir los riesgos relevantes. La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado [Norma ISO 17799, 2005].

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de una planeación cuidadosa y prestar atención a los detalles. La gestión de la seguridad de la información requiere, como mínimo, la participación de los accionistas, proveedores, terceros, clientes u otros grupos externos. También se puede requerir asesoría especializada de organizaciones externas [Norma ISO 17799, 2005].

¿Cómo establecer los requerimientos de seguridad?

Es esencial que una organización identifique sus requerimientos de seguridad. Existen tres fuentes principales de requerimientos de seguridad, una fuente se

deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial. Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente socio-cultural [Norma ISO 17799, 2005].

¿Qué queremos proteger?

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Por hardware entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, etc.) o tarjetas de red. Por software entendemos el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones, y por datos el conjunto de información lógica que manejan el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos. Aunque generalmente en las auditorias de seguridad se habla de un cuarto elemento a proteger, los fungibles (elementos que se gastan o desgastan con el uso continuo, como papel de impresora, toners, cintas magnéticas, etc.), aquí no consideraremos la seguridad de estos elementos por ser externos [Antonio Villalón Huerta, 2002].

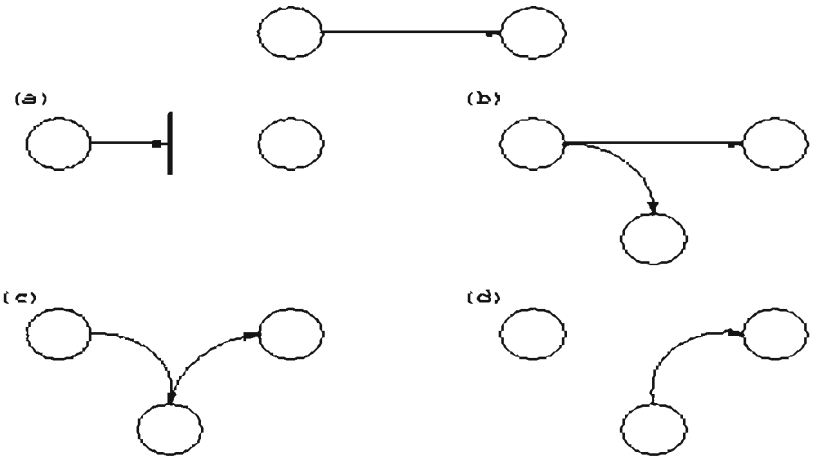


Figura 1.1: Flujo normal de información entre emisor y receptor y posibles amenazas: (a) interrupción, (b) interceptación, (c) modificación y (d) fabricación [Antonio Villalón Huerta, 2002].

2.2 Evaluando los riesgos de la seguridad

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debiera ser equilibrado con el daño comercial probable resultado de fallas en la seguridad. Los resultados de la evaluación del riesgo ayudarán a guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de seguridad de la información, e implementar los controles seleccionados para protegerse contra esos riesgos. La evaluación del riesgo se debiera repetir periódicamente para tratar cualquier cambio que podría influir en los resultados de la evaluación del riesgo [Norma ISO 17799, 2005].

2.2.1 Selección de controles

Una vez que se han identificado los requerimientos y los riesgos de seguridad y se han tomado las decisiones para el tratamiento de los riesgos, se debieran seleccionar los controles apropiados y se debieran implementar para asegurar que los riesgos se reduzcan a un nivel aceptable. Los controles se pueden seleccionar a partir de este estándar o de otros conjuntos de controles, o se pueden diseñar

controles nuevos para cumplir con necesidades específicas conforme sea apropiado. La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio de aceptación del riesgo, opciones de tratamiento del riesgo y el enfoque general para la gestión del riesgo aplicado a la organización, y también debieran estar sujetas a todas las regulaciones y legislación nacionales e internacionales relevantes [Norma ISO 17799, 2002].

Algunos de los controles en este estándar se pueden considerar principios guías para la gestión de la seguridad de la información y aplicables a la mayoría de las organizaciones. Se explican con mayor detalle más abajo bajo el título "Punto de inicio de la seguridad de la información" [Norma ISO 17799, 2005].

2.2.2 Punto de inicio de la seguridad de la información

Se pueden considerar un número de controles como un buen punto de inicio para la implementación de la seguridad de la información. Estos se basan en requerimientos legislativos esenciales o pueden ser considerados como una práctica común para la seguridad de la información.

Los controles considerados como esenciales para una organización desde el punto de vista legislativo incluyen, dependiendo de la legislación aplicable:

a) protección de data y privacidad de la información personal;

b) protección de los registros organizacionales;

c) derechos de propiedad intelectual.

Los controles considerados práctica común para la seguridad de la información incluyen:

a) documento de la política de seguridad de la información;

b) asignación de responsabilidades de la seguridad de la información;

c) conocimiento, educación y capacitación en seguridad de la información;

d) procesamiento correcto en las aplicaciones;

e) gestión de la vulnerabilidad técnica;

f) gestión de la continuidad comercial;

g) gestión de los incidentes y mejoras de la seguridad de la información.

Estos controles se aplican a la mayoría de las organizaciones y en la mayoría de los escenarios. Se debiera notar que aunque los controles en este estándar son importantes y debieran ser considerados, se debiera determinar la relevancia de cualquier control a la luz de los riesgos específicos que enfrenta la organización. Por lo tanto, aunque el enfoque arriba mencionado es considerado como un buen punto de inicio, no reemplaza la selección de controles basada en la evaluación del riesgo [Norma ISO 17799, 2005].

2.2.3 Factores de éxito críticos

La experiencia ha demostrado que los siguientes factores con frecuencia son críticos para una exitosa implementación de la seguridad de la información dentro de una organización:

a) política, objetivos y actividades de seguridad de información que reflejan los objetivos comerciales;

b) un enfoque y marco referencial para implementar, mantener, monitorear y mejorar la seguridad de la información que sea consistente con la cultura organizacional;

c) soporte visible y compromiso de todos los niveles de gestión;

d) un buen entendimiento de los requerimientos de seguridad de la información, evaluación del riesgo y gestión del riesgo;

e) marketing efectivo de la seguridad de la información con todos los gerentes, empleados y otras partes para lograr conciencia sobre el tema;

f) provisión para el financiamiento de las actividades de gestión de la seguridad de la información;

g) proveer el conocimiento, capacitación y educación apropiados;

h) establecer un proceso de gestión de incidentes de seguridad de la información;

i) implementación de un sistema de medición que se utiliza para evaluar el desempeño en la gestión de la seguridad de la información y retroalimentación de sugerencias para el mejoramiento [Norma ISO 17799, 2005].

2.3 Alcance

Este Estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados [NORMA ISO 17799, 2005].

Los objetivos de control y los controles de este Estándar Internacional son diseñados para ser implementados para satisfacer los requerimientos identificados por una evaluación del riesgo.

Este Estándar Internacional puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales [NORMA ISO 17799, 2005].

2.3.1 Categorías de seguridad principales

Cada categoría de seguridad contiene:

a) un objetivo de control que establece lo que se debiera lograr; y

b) uno o más controles que se pueden aplicar para lograr el objetivo de control.

Las descripciones del control están estructuradas de la siguiente manera:

2.3.2 Lineamiento de implementación

Proporciona información más detallada para apoyar la implementación del control y cumplir con el objetivo de control. Parte de este lineamiento puede no ser adecuado en todos los casos y por lo tanto, pueden ser adecuadas otras maneras para implementar el control. Otra información Proporciona más información que tal vez se deba considerar, por ejemplo consideraciones legales y referencias a otros estándares [Norma ISO 17799, 2005].

2.3.3 Evaluación de los riesgos de seguridad

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar un número de veces para abarcar las diferentes partes de la organización o sistemas de información individuales. La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo) [Norma ISO 17799, 2005].

Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo;

por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones del riesgo se debieran realizar de una manera metódica capaz de producir resultados comparables y reproducibles. La evaluación del riesgo de seguridad de la información debiera tener un alcance claramente definido para ser efectiva y debiera incluir las relaciones con las evaluaciones del riesgo en otras áreas, si fuese apropiado [Norma ISO 17799, 2005].

2.3.4 Tratamiento de los riesgos de seguridad

Antes de considerar el tratamiento del riesgo, la organización debiera decidir el criterio para determinar si se pueden aceptar los riesgos, o no. Los riesgos pueden ser aceptados si, por ejemplo, se ha evaluado que el riesgo es bajo o que el costo del tratamiento no es efectivo en costo para la organización. Estas decisiones debieran ser registradas [Norma ISO 17799, 2005].

Para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión de tratamiento del riesgo. Las opciones posibles para el tratamiento del riesgo incluyen:

a) aplicar los controles apropiados para reducir los riesgos;

b) aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización de la organización;

c) evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra;

d) transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.

Los controles debieran asegurar que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:

a) los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales:

b) objetivos organizacionales;

c) requerimientos y restricciones operacionales;

d) costo de implementación y operación en relación a los riesgos que se están reduciendo, y manteniéndolo proporcional a los requerimientos y restricciones de la organización;

e) la necesidad de equilibrar la inversión en implementación y operación de los controles con el daño probable resultado de fallas en la seguridad.

Los controles se pueden seleccionar a partir de este estándar o de otros conjuntos de controles, o se pueden diseñar controles nuevos para cumplir con necesidades específicas de la organización [Norma ISO 17799, 2005].

2.3.5 Política de seguridad de la información

Objetivo: Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes. La gerencia debiera establecer claramente la dirección de la política en línea con los objetivos comerciales y demostrar su apoyo, y su compromiso con, la seguridad de la información, a través de la emisión y mantenimiento de una política de seguridad de la información en toda la organización [Norma ISO 17799, 2005].

2.3.6 Documento de la política de seguridad de la información

El documento de la política de seguridad de la información debiera ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes. El documento de la política de seguridad de la información debiera enunciar el compromiso de la gerencia y establecer el enfoque de la organización para manejar la seguridad de la información. El documento de la política debiera contener enunciados relacionados con:

a) una definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información (ver introducción);

b) un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales;

c) un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo;

d) una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización, incluyendo:

1. conformidad con los requerimientos legislativos, reguladores y restrictivos,

2. educación, capacitación y conocimiento de seguridad,

3. gestión de la continuidad del negocio,

4. consecuencias de las violaciones de la política de seguridad de la información;

e) una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información,

f) referencias a la documentación que fundamenta la política; por ejemplo, políticas y procedimientos de seguridad más detallados para sistemas de información específicos o reglas de seguridad que los usuarios debieran observar [Norma ISO 17799, 2005].

2.4 Organización de la seguridad de la información

Se debiera establecer un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización. La gerencia debiera aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en toda la organización. Si fuese necesario, se debiera establecer una fuente de consultoría sobre seguridad de la información y debiera estar disponible dentro de la organización. Se debieran desarrollar contactos con los especialistas o grupos de seguridad externos, incluyendo las autoridades relevantes, para mantenerse actualizado con relación a las tendencias industriales, monitorear los estándares y evaluar los métodos y proporcionar vínculos adecuados para el manejo de los incidentes de seguridad de la información [Norma ISO 17799, 2005].

2.4.1 Compromiso de la gerencia con la seguridad de la información

La gerencia debiera apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información, la gerencia debiera:

a) asegurar que los objetivos de seguridad de la información estén identificados, cumplan con los requerimientos organizacionales y estén integrados en los procesos relevantes;

b) formular, revisar y aprobar la política de seguridad de la información;

c) revisar la efectividad de la implementación de la política de seguridad de la información;

d) proporcionar una dirección clara y un apoyo gerencial visible para las iniciativas de seguridad;

e) proporcionar los recursos necesarios para la seguridad de la información;

f) aprobar la asignación de roles y responsabilidades específicas para la seguridad de la información a lo largo de toda la organización;

g) iniciar planes y programas para mantener la conciencia de seguridad de la información;

La gerencia debiera identificar las necesidades de consultoría especializada interna o externa para la seguridad de la información, y revisar y coordinar los resultados de la consultoría a través de toda la organización [Norma ISO 17799, 2005].

2.5 Seguridad física y ambiental

Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización. Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia [Norma ISO 17799, 2005].

2.5.1 Trabajo en áreas aseguradas

Se debiera diseñar y aplicar la protección física y los lineamientos para trabajar en áreas aseguradas, se debieran considerar los siguientes lineamientos:

a) el personal debiera estar al tanto de la existencia o las actividades dentro del área asegurada sólo conforme las necesite conocer;

b) se debiera evitar el trabajo no-supervisado en el área asegurada tanto por razones de seguridad como para evitar las oportunidades para actividades maliciosos;

c) las áreas aseguradas vacías debieran ser cerradas físicamente bajo llave y revisadas periódicamente;

d) no se debiera permitir equipo fotográfico, de vídeo, audio y otro equipo de grabación; como cámaras en equipos móviles; a no ser que sea autorizado [Norma ISO 17799, 2005].

2.6 Áreas de acceso público, entrega y carga

Se debieran controlar los puntos de acceso como las áreas de entrega y carga y otros puntos por donde personas no-autorizadas puedan ingresar al local y, si fuese posible, debieran aislarse de los medios de procesamiento de información para evitar el acceso no autorizado, se debieran considerar los siguientes lineamientos:

a) el acceso al área de entrega y carga desde fuera del edificio se debiera restringir al personal identificado y autorizado;

b) se debiera diseñar el área de entrega y carga de manera que se pueda descargar los suministros sin que el personal de entrega tenga acceso a otras partes del edificio;

c) las puertas externas del área de entrega y carga debieran estar aseguradas cuando se abren las puertas internas;

d) se debiera inspeccionar el material que ingresa para evitar amenazas potenciales (ver 9.2.1d) antes que el material sea trasladado del área de entrega y carga al punto de uso;

e) se debiera registrar el material que ingresa en concordancia con los procedimientos de gestión de activos (ver también 7.1.1) a su ingreso al local;

f) cuando fuese posible, los embarques que ingresan y salen debieran estar segregados. A riesgo que la información sea vista por personas no autorizadas durante su uso; y se debieran asegurar los medios de almacenaje para evitar el acceso no autorizado;

c) se debieran aislar los ítems que requieren protección especial para reducir el nivel general de la protección requerida;

d) se debieran adoptar controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo;

e) se debieran establecer lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información;

f) se debieran monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información;

g) se debiera aplicar protección contra rayos a todos los edificios y se debieran adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones;

h) se debieran considerar el uso de métodos de protección, como membranas de teclado, para el equipo en el ambiente industrial;

i) se debiera proteger el equipo que procesa la información confidencial para minimizar el riesgo de escape de información debido a emanación.

2.6.1 Ubicación y protección del equipo

Se debiera ubicar o proteger el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no-autorizado, se debieran considerar los siguientes lineamientos para la protección del equipo:

a) el equipo se debiera ubicar de manera que se minimice el acceso innecesario a las áreas de trabajo;

b) los medios de procesamiento de la información que manejan data confidencia debieran ubicarse de manera que se restrinja el ángulo de visión para reducir el riesgo que la información sea vista por personas no autorizadas durante su uso;

c) se debieran aislar los ítems que requieren protección especial para reducir el nivel general de la protección requerida;

d) se debieran adoptar controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo;

e) se debieran establecer lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información;

f) se debieran monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información;

g) se debiera aplicar protección contra rayos a todos los edificios y se debieran adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones;

h) se debieran considerar el uso de métodos de protección, como membranas de teclado, para el equipo en el ambiente industrial;

i) se debiera proteger el equipo que procesa la información confidencial para minimizar el riesgo de escape de información debido a emanación.

2.7 Vulnerabilidades a nivel físico

Las amenazas a las instalaciones serán:

- Acceso libre a todos los sectores de la empresa a cualquier usuario: Si cualquier usuario puede acceder a todas las oficinas de la empresa, sin controles ni barreras físicas, es muy probable que acceda un intruso a las instalaciones provocando actos ilícitos como hurtos, daños físicos o espionaje de información confidencial;

- Falta de un perímetro de seguridad: Si no se establece un perímetro de seguridad, la empresa se convierte en una continuación física de la vereda;

- Falta de áreas protegidas que guarden los equipos críticos. Permitiendo el acceso indiscriminado de personas;

- Falta de barreras físicas que protejan los activos: Permite el ingreso a la organización de intrusos;

- Existencia de múltiples puntos de acceso: Esto facilita el ingreso no autorizado de intrusos;

- Falta de autentificación de usuarios: Esto dificulta la identificación de usuarios no autorizados;

- Ausencia de métodos confiables de autentificación de usuarios: Un método no confiable de autentificación de usuarios es levemente mejor que ningún método de autentificación de usuarios;

- Áreas de procesamiento de información y de entrega y carga de materiales comunicadas: Facilita el acceso de intrusos al sector de cómputos;

- Áreas de entrega y carga de materiales descuidadas: Facilita la circulación de personas no autorizadas con los efectos consecuentes;

- Integración del área de procesamiento de información administrativa por la organización y la administrada por terceros: Provoca una alteración a la

confidencialidad de datos y la exposición a ataques internos por parte de terceros;

- Señalización indiscreta del edificio o sobre indicación: Toda la ayuda que se dé para acceder a los sectores protegidos será una herramienta útil para el intruso que desee perpetrar las instalaciones;

- Falta de sistemas de detección de intrusos;

- Hacer pública información sensible: Toda la información delicada debe de ser cuidadosamente administrada, pues todo dato es una llave para el sistema, que un intruso experimentado puede utilizar. Por ejemplo, es común hacer públicas todas las extensiones telefónicas, incluso las de los sectores restringidos. Si un usuario no autorizado accede a uno de estos números, sería capaz de implementar la ingeniería social para obtener información o accesos que no le pertenecen [ISO 1977, 2005].

2.7.1 Amenazas a los equipos

- Mala distribución física de los activos: Los equipos pueden estar ubicados en forma descuidada, expuesta a catástrofes naturales (cerca de ventanas) o hurto (cerca de puertas o pasillos);

- Almacenamiento de materiales dañinos cerca de los equipos: Como combustibles o químicos;

- Humo de cigarrillo: El humo de cigarrillo ataca los discos magnéticos y ópticos y provoca trastornos en la ventilación de los artefactos eléctricos. Además el cigarrillo puede provocar incendios;

- Permitir comer y beber en sectores con equipos: La comida y bebida puede provocar deterioros en los equipos y cortocircuitos y hasta quemar elementos eléctricos;

- Exposición a temperaturas extremas: Exponer los equipos a temperaturas extremas daña sus circuitos, provocando cortocircuitos e incendios;

- Terminales abandonadas: Las terminales encendidas en desuso son un riesgo alto, ya que cualquier persona puede hacer uso de sus recursos, sin siquiera la necesidad de loguearse;

- Falta de higiene: La falta de higiene en oficinas puede provocar daño en los documentos impresos y en los equipos por acumulación del polvo, grasa, etc.

- Descuido de las unidades de soporte de información: Tener en mal estado o en lugares inseguros las unidades de backup y recuperación de sistemas es casi lo mismo que no tenerlas;

- No llevar un control de los cambios en los equipos: No registrar cada alta, baja o modificación en los equipos conlleva a un desconocimiento del capital invertido, con lo que cualquier hurto pasaría por desapercibido [ISO 1977, 2005].

2.7.2 Amenazas generadas por el uso de una red física de datos

Cuando un mensaje "M" es enviado por un usuario origen "A" a un usuario destino "B" determinado a través de una red, como se muestra en la figura1, este mensaje viaja por el medio físico con el riesgo de sufrir alguno de los siguientes ataques por parte de un intruso "I".

En el medio del viaje del origen al destino, el mensaje puede sufrir de ataques de intrusos para su lectura, modificación, o eliminación [ISO 1977, 2005].

2.7.3 Tipos de amenazas

1) Interrupción: Sucede cuando el destinatario nunca recibe el mensaje emitido por el origen;

2) Intercepción: El mensaje enviado por el origen es interceptado por un intruso que recibe el mensaje tanto como el verdadero destino;

3) Modificación: El mensaje enviado por el origen nunca es distribuido ; en su lugar el intruso envía otro mensaje en reemplazo del original [ISO 1977, 2005].

2.7.4 Factores de riesgo

- Conectores de LAN inutilizados al descubierto: Cualquier usuario no autorizado puede conectar una laptop y sumarse a la red directamente;

- Cables al descubierto: Pueden ser dañados con facilidad provocando una negación de servicio.

- Cables atravesando zonas públicas: Pueden ser interceptadas por intrusos que desvíen o modifiquen los paquetes transmitidos; tender cables de energía junto con cables de comunicaciones pueden provocar interferencias en las comunicaciones [ISO 1977, 2005].

2.8 Vulnerabilidades a nivel lógico

2.8.1 Amenazas generadas por el uso del correo electrónico

- Virus: Son porciones de código que son insertadas dentro de un archivo llamado host, de manera que cuando el archivo es ejecutado, se ejecuta también la porción de código insertada, la cual puede efectuar distintas acciones malintencionadas, destructivas y hasta copiarse en otros archivos;

- Gusanos (worms): Son programas independientes que se expanden a través de la red realizando distintas acciones como instalar virus, o atacar una PC como un intruso;

- Troyanos: Programas que tienen una porción de código oculta que dicen hacer una cosa y en realidad hacen otra o simplemente hacen lo que dicen;

- Conejos: Son programas que no dañan directamente al sistema por alguna acción destructiva, sino que tienen la facilidad de reproducirse exponencialmente de manera de provocar en poco tiempo una negación de servicio al consumir los recursos (memoria, disco, procesador, etc.);

- Empleados pueden comprometer a la organización enviando correos electrónicos difamatorios llevando a cabo practicas de hostigamiento, o realizando compras no autorizadas;

- Acceso remoto a las cuentas de correo electrónico sin control;

- Falta de una política de eliminación de mensajes: Puede suceder que se eliminen mensajes que, si se almacenaran, podrían ser hallados en caso de litigio;

- Es un servicio vulnerable a ser modificado por personas no autorizadas;

- Es un servicio vulnerable al descubrimiento (de información confidencial;

- Se pueden producir errores como por ejemplo la consignación incorrecta de la dirección de destino o la publicación de direcciones de personal jerárquico de la empresa [ISO 1977, 2005].

2.8.2 Amenazas generadas por el uso de software dañino

- Bombas lógicas: Son un conjunto de instrucciones que se ejecutan bajo condiciones especiales (una fecha, etc.);

- Backdoors y trapdoors: Son instrucciones que permiten a un usuario acceder a otros procesos o a una línea de comandos;

- Timeouts: Son programas que se pueden utilizar durante un periodo de tiempo determinado;

- Herramientas de seguridad: Son utilitarios que sirven para identificar vulnerabilidades en un sistema [ISO 1977, 2005].

2.8.3 Amenazas generadas por la presencia de intrusos

- Eaves dropping: Es la escucha no autorizada de conversaciones, claves, datos, etc.;
- Ingeniería social: Consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían, como revelar su contraseña o cambiarla;
- Shoulder Surfing: Consiste en espiar físicamente a los usuarios para obtener claves de acceso al sistema, números validos de tarjetas de crédito, etc.;
- Masquerading: Un intruso puede usar la identidad de un usuario autorizado que no le pertenece simplemente apoderándose de un nombre de usuario y contraseña validos;
- Piggy backing: Ocurre cuando un usuario accede a una zona restringida gracias al permiso otorgado a otra persona que si está autorizada;
- Basurero: La información de los desperdicios dejados alrededor de un sistema puede ser aprovechada por intrusos provocar un hurto o daño [ISO 1977, 2005].

2.8.4 Vulnerabilidades en los sistemas operativos

- Existencia de cuentas de usuarios no utilizadas: Muchas cuentas de usuario son creadas por defecto en la instalación del sistema operativo y nunca son deshabilitadas, a pesar de que no se utilicen. Esta situación en un puerta abierta para los intrusos que conocen estas vulnerabilidades de los sistemas operativos;

- Existencia de cuentas de usuario con permisos excesivos: Generada por la falta de control de los permisos asignados a los usuarios;

- Existencia de servicios no utilizados: Muchos servicios son instalados por defecto con el sistema operativo o para la corrida de procesos especiales y nunca son eliminados. Estos pueden ser utilizados por intrusos para manipular en forma remota y acceder a los recursos;

- Malas configuraciones de seguridad del sistema operativo: Como la existencia de cuentas de usuario creadas en la instalación, que son default, aumentando el riesgo de ataques a la integridad y confidencialidad mediante un acceso no autorizado;

- Errores en los archivos de configuración existentes y sus valores;

- Falta de un esquema de backup,

- Ausencia de una estrategia de recuperación ante desastres: El Plan de Recuperación del Entorno ante Desastres cubre las aplicaciones, equipos y software base que soporta el negocio para su recuperación. No poseer un plan de acción ante la emergencias implica de las prestaciones y una potencial perdida de información vital para el negocio;

- Contraseñas almacenadas en texto plano: Algunos sistemas operativos almacenan las contraseñas en texto plano permitiendo el acceso autorizado de intrusos si ellos lograran acceder a la información de passwords;

- Falta de registros de las pistas de auditoría: Las pistas de auditoría o logs sirven para dejar registro de las acciones de los usuarios y los procesos. No llevar un adecuado registro y recuperación de información [ISO 1977, 2005].

2.8.5 Vulnerabilidades en las aplicaciones

A nivel funcional:

- Falta de documentación: La ausencia de documentación dificulta la capacitación de los usuarios y el seguimiento de los proyectos y procesos, provocando incoherencias en el trabajo;
- Mala organización del área de sistemas,
- Mala administración de la seguridad informática;
- Fallas en la metodología de desarrollo de las aplicaciones;
- Planificación deficiente;
- Pobre separación de tareas;
- Falta de separación de ambientes: La separación de ambientes es fundamental, más allá de las ventajas metodológicas en el proceso de desarrollo de software, en la conservación de la integridad de los datos a través de la separación lógica y física de los entornos de producción, desarrollo y prueba;
- Mala configuración de entornos: Generalmente en los entornos de desarrollo se otorgan permisos excesivos a los programadores que provocan fallas en la confidencialidad e integridad de los datos;
- Falta de las pruebas en el desarrollo de aplicaciones;
- Mal manejo de datos;
- Datos utilizados para las pruebas: Muchas veces se utilizan para las pruebas de datos de producción. Esto no es crítico si la base de datos de prueba es independiente, pero tiene un riesgo asociado cuando se manejan datos de carácter personal, protegidos por las leyes de todo mundo, para las cuales hay que tomar medidas de seguridad adicionales. La falta de estos controles o el uso indebido de datos puede tener consecuencias legales graves;

- Clasificación, manejo y protección de los datos productivos: La falta de análisis de criticidad de los datos y categorización hace que no se brinden los controles que garanticen la correcta manipulación de datos con la consecuente pérdida de confidencialidad e integridad;
- Falta de control de cambios,
- Defectos en la funcionalidad general de la aplicación,
- Falta de coherencia con los objetivos del negocio;
- Mala administración de la aplicación:
    - Falta de organización de los perfiles de usuarios;
    - Formas de erróneas de asignación de permisos;
    - Mal manejo de incidencias.
- Prestaciones limitadas;
- Pobre análisis de control interno:
    - Falta de separación de tareas;
    - Análisis de asignación de funciones incompatibles.
- Falta de asignación de responsabilidades de seguridad.

Aspectos lógicos:

- Mala estructura de navegación del menú/paginas de la aplicación;
- Errores en las interfaces e interacción con otros servicios;
- Malas configuraciones de seguridad del sistema operativo;
- Vulnerabilidades en los servicios prestados por el mismo servidor;

- Errores en los archivos de configuración existentes y sus valores;
- Mal manejo de transacciones;
- Mal manejo de la concurrencia;
- Falta de un esquema de backup;
- Ausencia de una estrategia de recuperación ante desastres;
- Mala administración de la base de datos;
- Mala configuración de seguridad de las bases de datos utilizadas;
- Formas inseguras de comunicación con la aplicación;
- Contraseñas almacenadas en texto plano;
- Falta de registro de las pistas de auditoría;
- Mal manejo de datos:
    - Falta de validación de los datos de entrada;
    - Falta de validación de los datos de salida;
- Mal manejo de errores de la aplicación [ISO 1977, 2005].

2.8.6 Amenazas generadas por mala administración de la información

- No controlar el acceso a los sistemas: Cualquier usuario podría utilizar y modificar los archivos sin tener que pasar ninguna barrera que filtre a los intrusos;
- No llevar un registro de las incidencias;

- No contar con un sistema de perfiles de usuario: Un sistema de perfiles permite asignar distintos privilegios a los usuarios de manera que todos tengan las mismas posibilidades de acceso a los recursos, según la tarea.

- No llevar un control de los cambios en el software: No registrar cada alta, baja o modificación en los programas de software conlleva a un desconocimiento del capital invertido con lo que cualquier hurto o modificación pasaría desapercibido;

- Ausencia de control de impacto del nuevo software: Puede haber una incoherencia entre los requerimientos de capacidad de procesamiento y almacenamiento del nuevo software y los disponibles o una incompatibilidad con la plataforma de hardware utilizada;

- No mantener actualizado el software de detección y reparación del antivirus;

- Falta de backups: Sin copias de respaldo la recuperación de la información y la restauración del sistema luego de incidente es imposible;

- Realización de backups incompletos puede llegar a no servir de mucho a la hora de reconstruir un sistema caído;

- Acceso limitado o no controlado a los datos: Permite el libre acceso de intrusos a los datos facilitando los ataques anónimos;

- Documentación desprotegida: Un intruso o espía puede hacer mal uso de la documentación para distintos fines de espionaje, sabotaje, hurto, o para obtener información que le sirva como puerta al sistema objetivo [ISO 1977, 2005].

2.9 Vulnerabilidades a nivel de la organización

- Superposición o mala asignación de roles: [CISA] realizo un estudio de compatibilidades de funciones y desarrollo una matriz de compatibilidad donde se refleja que funciones son compatibles o no con otras, por lo que

deberían llevarse a cabo por distintas personas. Este criterio es utilizado para reforzar el control interno por oposición de intereses;

- Ausencia de administradores y responsables por la seguridad del sistema: Esta falta implica una gran falta en la seguridad ya que se omite el primer paso en el camino a la protección, el control, que provocara:
    - Ausencia o mal manejo de incidencias;
    - Mala administración de los recursos;
    - Falta de control lógico;
    - Falta de registro o monitorización de la actividad del sistema;
    - Etc.
- Falta de políticas contra ataques internos;
- Ausencia de una Normativa de Seguridad;
- Descuido de los escritorios y las pantallas: Dejando el acceso libre a los documentos y archivos de la oficina;
- Sectores de desarrollo, de prueba y producción unificados: Provoca fallas en la calidad del software y falta de control en las distintas etapas del desarrollo de software, además de problemas en la implantación en el ambiente de producción;
- Falta de registro del flujo del personal: No permite detectar intrusos, provocando hurtos y otros ataques;
- Falta de protección de las operaciones de comercio electrónico [ISO 1977, 2005].

2.10 Protección de la información

[ISO 17799, 2005] indica: "los medios que contienen información sensible deben de ser eliminados de manera segura, por ej. Incinerándolos o rompiéndolos en pequeños trozos, o eliminando los datos y utilizando los medios en otra aplicación dentro de la organización." Se debe prestar especial atención a la eliminación segura de:

- Prevención de ataques externos:
    - Eaves dropping: Es la escucha no autorizada de conversaciones, claves, datos, etc.
    - Ingeniería social: La Ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían, como revelar su contraseña o cambiarla.
    - Shoulder Surfing: Consiste en espiar físicamente a los usuarios para obtener claves de acceso al sistema, números válidos de tarjetas de crédito, etc. Se recomienda prevenir a los usuarios sobre estos temas a fin de concientizarlos para que tomen los cuidados necesarios;
    - Masquerading: Un intruso puede usar la identidad de un usuario autorizado que no le pertenece simplemente apoderándose de un nombre de usuario y contraseña válidos;
    - Piggy backing: Se lo llama así al ataque en que un usuario no autorizado accede a una zona restringida gracias al permiso otorgado a otra persona que sí está autorizada.
    - Basurero: Basurero es la obtención de información de los desperdicios dejados alrededor de un sistema: Es de vital importancia destruir toda documentación que ya no se utilice, con una máquina

trituradora de papel y borrar los documentos en "forma segura" según el sistema operativo que se use.

- Clasificación de la información: La información se debe clasificar en cuanto a su acceso (que perfiles de usuario tienen acceso a lectura, ejecución o modificación de los datos) y en cuanto a su criticidad. Para clasificarla según acceso, se hace uso de la Tabla de Accesos Sobre Activos Lógicos, y para clasificarla según su criticidad, se hace referencia al inventario de Activos Lógicos;

- Establecer medidas de protección según la clasificación de la información: Según el tipo de información que se trate, se deberán garantizar controles como se indica a continuación:

    - Para la información pública o no restringida: No es necesario establecer restricciones especiales, más allá de las recomendaciones sobre su buen uso y conservación;

    - Para la información restringida y/o secreta: Dependiendo que la información se haya clasificado como restringida o secreta se deben cumplir con los siguientes requerimientos mínimos y obligatorios para su protección:

        - Autorización: Los usuarios a quienes por la naturaleza de su trabajo se les permita el acceso a la información clasificada como confidencial o secreta, deben estar expresamente autorizados.

        - El dueño de los datos debe de mantener un detalle de los usuarios autorizados a acceder a la información. El Administrador de Seguridad debe conservar la documentación respaldatoria de las autorizaciones recibidas para los cambios de permisos. Limitar el acceso a las aplicaciones a través de un adecuado sistema de control de accesos. No permitir el uso

de información secreta para propósitos de prueba durante los desarrollos o implantaciones. En cuanto a la información restringida, solo debe utilizarse teniendo en cuenta las autorizaciones definidas en la Norma de Ambientes de procesamiento. El Dueño de los Datos debe de autorizar expresamente el acceso a la información en el ambiente de producción por parte de personal del área de Sistemas, siempre y cuando lo considere absolutamente necesario y debido a situaciones de emergencia. En estos casos documentar la autorización y las tareas efectuadas, de acuerdo al Procedimiento de Administración de Usuarios Recursos.

- Conservación: La información clasificada como secreta y los medios físicos donde se almacene, deben protegerse utilizando cajas de seguridad cuya llave y/o combinación debe de ser conservada por el Dueño de los Datos, quien debe autorizar toda copia adicional de dicha información así como la transmisión, envió, impresión y/o destrucción de la misma. La conservación de soportes impresos de esta información debe efectuarse en archivos cerrados cuyo acceso físico debe estar restringido únicamente a los usuarios autorizados, según lo especificado en la Norma de Protección física del Manual de Seguridad de la Organización. Realizar el proceso de generación y/o restauración de la información de acuerdo a lo definido en la Norma de Copias de Respaldo.

- Impresión: imprimir los reportes que contienen información confidencial en impresoras de acceso exclusivo para usuarios autorizados;

- Entrega/Traslado: Realizar toda entrega de documentación que contenga información secreta/confidencial en sobre cerrado. Asimismo, establecer mecanismos que permitan asegurarte al remitente de la documentación que esta fue recibida por el destinatario correspondiente;

- Divulgación de terceros: Instrumentar convenios de confidencialidad con los terceros que deben acceder a información de la empresa.

- Destrucción: Destruir toda información secreta y sus correspondientes soportes físicos cuando se considere no vigente y se discontinué su utilización y/o conservación.

- Informar a los usuarios sobre el manejo de la información: Toda la información conservada en los equipos informáticos (archivos y correos electrónicos residentes en servidores de datos centralizados y/o estaciones de trabajo) puede ser considerada propiedad de la compañía y no de los usuarios, dependiendo de su Política de Seguridad, por lo que podrá ser administrada y/o monitoreada por los responsables del área de Sistemas de acuerdo con las pautas de seguridad definidas. Esto debe estar claramente establecido en la Norma de Clasificación y Tratamiento de la Información de la empresa y pertinentemente informado a todos los usuarios.

CAPITULO III

MARCO APLICATIVO

DESARROLLO DE LA METODOLOGIA DE SEGURIDAD DE ENTORNOS INFORMATICOS (MSEI)

La Metodología para la Seguridad de Entornos Informáticos, MSEI se desarrolla en las siguientes fases:

- Definición del Alcance
- Relevamiento
- Planificación
- Implantación
- Estabilización
- Mantenimiento

Estas fases se categorizan formando dos grandes grupos según el objetivo que persiguen: el estudio del entorno y la implantación de la solución. Partiendo de un entorno inseguro o desprotegido, a través de las primeras tres fases de la Metodología, se logra un estudio del entorno del conocimiento necesario para encarar la solución de los problemas de seguridad detectados. Es en esta parte en que el Experto en Seguridad delimita el entorno elaborando el Alcance, que abarca los activos lógicos y físicos afectados en el análisis.

Una vez delimitado el área de trabajo o entorno objetivo, se procede a realizar el sondeo que conducirá al conocimiento funcional y técnico detallado del entorno, sus activos, los empleados, los procesos y procedimientos involucrados que se registrara en los respectivos documentos de relevamiento. Para finalizar esta primera parte del trabajo, el Experto en Seguridad construye un plan de Seguridad de Entorno que contendrá todos los objetivos de control deseados y la forma de implantarlos en el entorno para asegurarlo.

Todas las tareas desarrolladas en esta etapa inicial conducen a la familiarización del experto con el entorno y su conocimiento. Esto permitirá al Experto determinar las mejores medidas a tomar para asegurar el entorno objetivo.

Esta tesis se basa en estándares internacionales [ISO 19977], normas y las mejores prácticas profesionales, por lo que no es necesario poseer un conocimiento especializado en Seguridad. Sin Embargo, se confía en el buen criterio del Ingeniero en Sistemas o Licenciado en Informática, que la utilice para lograr la mejor implementación de la solución.

Continuando con la metodología, la segunda parte del trabajo consiste en llevar a la práctica de los controles planificados antes, en la fase que llamamos *Implantación*.

Luego de la implementación de los controles y las mejoras en los procesos que conducen a la obtención de los objetivos fijados en el plan, el Experto en Seguridad deberá realizar un balance ponderando los objetivos fijados al principio con los resultados obtenidos en la última etapa. Su trabajo aquí es evaluar la implantación, su grado de éxito y realizar los ajustes al Plan que sean necesarios para completar el aseguramiento del entorno. A esta fase la llamamos *Estabilización*.

Finalmente nace una fase que se mantendrá a lo largo de toda la vida del entorno: la fase de Mantenimiento, que acompaña todos los cambios en el entorno persiguiendo la preservación de su seguridad. En esta etapa, la etapa final de la Metodología, el entorno se convierte en seguro y se mantiene de esa forma hasta que se implanten cambios lo suficientemente grandes como para que se deba considerar la construcción de un nuevo Plan de Seguridad. En este caso la metodología de seguridad permite reiniciar el proceso haciendo mucho más cortas las etapas iníciales, saltando tareas de sondeo como la realización del *Relevamiento General* y el *Relevamiento de Usuario*, que ya han sido realizados

no requieren mayor detalle. Como vimos, entonces, partiendo de un entorno inseguro, realizando las tareas que forman parte de las primeras tres fases de la Metodología de Seguridad, en una primera etapa se logra el conocimiento del entorno. Siguiendo con la implantación de la solución, a través de las tres últimas fases compuestas por tareas de implantación, control y mejora continua, se obtiene un entorno seguro, que es el objetivo de este trabajo.

3.1 DEFINICION DEL ALCANCE

3.1.1 Análisis de Requerimientos de Usuario

En esta etapa él Experto en Seguridad (ES) se pone en contacto con el cliente (la persona o entidad interesada en asegurar el entorno objetivo) y se escucha e interpreta lo que el usuario le pide. En general el usuario no sabe qué es lo que quiere asegurar, por eso, es tarea del Experto en Seguridad orientarlo en el campo mostrándole los distintos aspectos que se deberían asegurar, para determinar a qué nivel el usuario desea que se realice el proyecto de aseguramiento. A partir de esta decisión él Experto en Seguridad concentrará su esfuerzo en el Relevamiento General y en el Relevamiento de usuario, haciendo foco en el o los aspectos que el usuario señaló.

Muy probablemente el usuario no tenga claro siquiera qué nivel desea proteger (físico, lógico u organizacional) y dejará la decisión en manos de Experto en Seguridad. El Experto en Seguridad puede, entonces, pasar a las etapas siguientes de esta fase de la metodología MSEI para detectar a grandes rasgos las mayores falencias en cuanto a seguridad por nivel y ofrecer los resultados al cliente para que este decida el camino a seguir.

3.1.1.1 Documento de Requerimientos de Usuario

De una forma u otra, el ES registrará el pedido del usuario en un documento llamado *Documento de Requerimientos de Usuario*, que contendrá la voluntad del usuario respecto de los niveles y elementos a asegurar.

El Documento de Requerimientos de Usuario contendrá la siguiente información:

Niveles a asegurar:

- Nivel físico: Elementos a asegurar del nivel físico.
- Nivel lógico: Elementos a asegurar del nivel lógico.
- Nivel de la organización: Elementos a asegurar del nivel de la organización.

3.1.2 Elaboración del Alcance

A partir de los requerimientos obtenidos del usuario se establece el alcance que tendrá el proyecto de aseguramiento del entorno informatizado objetivo.

En esta etapa se determinan claramente todos los puntos sobre los que se elaborará el Plan de Aseguramiento y se registran en un documento elaborado para tal fin. Este documento se llamará *Alcance*. Cabe mencionar que el Alcance es elaborado por el Experto en Seguridad con una adecuada colaboración del cliente, que deberá asumir responsabilidad sobre los temas que se decida dejar fuera del proyecto. Este deberá reflejar objetivos claros y puntuales que se deberán cumplir en el proceso de seguridad.

3.1.2.1 Alcance

Se define claramente lo que se pretende lograr en el proyecto. Los objetivos deben responder al acrónimo SMART, que enmarca las prácticas fundamentales necesarias para alcanzar alta motivación y mejora para conseguir el objetivo propuesto:

S: Simple, específico con un significado preciso.

M: Meaningful (con significado), motivante, mensurable.

A: Aceptable, alcanzable orientado a la acción, acordado, activable, asignable.

R: Realístico, a una revisión orientado a resultados relevantes a una misión.

T: Timelines (líneas de tiempo), con registro de fecha, relacionado con el tiempo, tangible, basado en tiempo, específico en el tiempo, limitado por el tiempo, relacionado con el tiempo, verdadero.

Participantes del proyecto

- Responsable por la empresa objetivo: Ejecutivo de nivel gerencial que avala el proyecto.
- Experto en Seguridad (ES): Profesional responsable del diseño y planificación del Plan de Aseguramiento del entorno.
- Recursos afectados al proyecto: Son personas que colaborarán durante todo el proyecto liderado por el ES.

Definición del Entorno

Se deberá determinar con precisión cuál será el entorno donde se implementara el proyecto. El alcance estará circunscrito a ese entorno y todas las referencias que se hagan a él serán en relación a esta definición.

El entorno puede ser desde un equipo informático hasta una corporación distribuida en distintas regiones geográficas; puede definirse como el edificio que alberga a la empresa objetivo o como el Centro de Cómputos (CC) o Centro de Procesamientos de Datos (CPD) donde se encuentran los servidores.

Niveles que cubrirá el proyecto

Esto es, definir a qué nivel se hará al estudio para lograr el aseguramiento. Como se definió en la introducción, el estudio se puede enfocar en alguno o todos estos niveles: Nivel físico, Nivel lógico, Nivel de la organización.

Hitos a cubrir en cada nivel:

Definir a alto nivel qué hitos se deberán cumplir a lo largo del proyecto.

Elementos fuera del Alcance:

Ítems que se haya decidido dejar fuera del proyecto por diversos motivos.

Planificación del trabajo:

Definición de las etapas o fases en que se desarrollará el proyecto, a nivel macro, sin entrar en detalle.

Entregables de cada etapa:

El cliente debe ver el avance del proyecto a medida que transcurre el tiempo. Para eso se define una serie de documentos o entregables de cada etapa del proyecto que reflejarán el trabajo hecho.

Consideraciones adicionales:

Consideraciones que él Experto de Seguridad crea necesarias para el proyecto.

3.1.3 Aprobación del Alcance

Como documento inicial del proyecto el Alcance deberá ser aprobado por los responsables del lado del cliente, previo consenso con él Experto de Seguridad encargado de la elaboración del Plan de Aseguramiento del entorno informatizado objetivo.

3.1.4 Estimación de tiempos y costos.

Como en todo proyecto, es necesario realizar una estimación del tiempo que se deberá invertir y los recursos a asignar para culminar con éxito y en un tiempo finito el proyecto de aseguramiento del entorno. Para la estimación de tiempos no existe una fórmula que determine el tiempo que llevará cada tarea. La duración de las mismas depende de muchos factores:

- De la cantidad de recursos asignados;

- De la calidad de esos recursos;
- De la carga que se les pueda asignar a esos recursos;
- De la experiencia de los recursos humanos involucrados;
- Del tamaño del entorno;
- De la complejidad del entorno;
- De la estabilidad económico-financiera de la empresa objetivo (pues el proyecto puede perder prioridad ante situaciones de crisis);
- Del apoyo del nivel gerencial y la seriedad con que tomen el proyecto pues muchas decisiones surgirán a ese nivel.

Es por eso que la experiencia le dará al Experto en Seguridad la capacidad para medir el tiempo que le llevará hacer cada tarea según los parámetros antes mencionados. La estimación de costos, por otro lado, es una variable fundamental a determinar, en la que la experiencia del Experto en Seguridad se utiliza para la asignación de recursos, a partir de la cual se calculan los costos. Para ello existen métodos, pero no es el fin de este trabajo entrar en detalle al respecto. En esta sección mencionaremos los costos que se deberán tener en cuenta a nivel general. Como en todo este trabajo, se deja la responsabilidad al Experto en Seguridad de bajar el nivel de análisis, para que siguiendo esta Metodología para la Seguridad de Entornos Informáticos, llegue al punto de reflejar el caso en el que está trabajando.

Los costos que genera un proyecto como éste se pueden categorizar en 3 clases: Costos capitales; Costos recurrentes; Costos no recurrentes.

3.1.4.1 Costos capitales

Son los costos para adquirir, desarrollar, o instalar los principales bienes o activos. Un activo principal es una ventaja palpable que tiene una vida útil de más que un

año y se pretende continuar su uso con el tiempo. Activos capitales estándar incluyen hardware de computadora y software comprado como un paquete o desarrollado ha pedido. Los siguientes son algunos ejemplos de costos capitales:

- Equipos de procesamiento de datos:
    - CPUs;
    - Workstations;
    - Laptops;
    - Unidades de almacenamiento externo (Discos rígidos externos);
    - Monitores;
    - Impresoras;
    - Scanners;
    - Etc.

- Equipos de telecomunicaciones:
    - Routers;
    - Switches;
    - Hubs;
    - Modems;
    - Servidores;
    - Cableado de red.

- Software
    - Sistemas operativos;
    - Aplicaciones;
    - Software de comunicaciones;
    - Utilitarios; Firewalls; IDSs.
- Otros:
    - UPSs o SAIs
    - Generadores de energía eléctrica;
    - Mueblería.

3.1.4.2 Costos recurrentes

Los costos recurrentes son los costos que se presentan con regularidad. En contraste con los costos capitales, los costos recurrentes deben ser tratados como si fueran a ser pagados completamente al ser facturados. Los costos recurrentes en general son costos operativos, en muchos casos fáciles de definir como alquileres de equipos y salarios. Otros son más difíciles de distinguir de los costos capitales, como por ejemplo la compra de hardware y software, que pueden ser tratados como costos capitales o recurrentes. En el entorno de Information Technology (IT), los costos recurrentes son los siguientes:

- Salarios:
    - Incluye los costos por todos los empleados involucrados directa o indirectamente con el proyecto, encargados del manejo, el soporte y la administración del proyecto en todas sus fases.
- Contratos:

- Contratos de mantenimiento de hardware;
- Contratos de mantenimiento de software.

- Hardware:
  - Alquiler de equipos;
  - Actualización de equipos;
  - Mantenimiento interno.
- Software:
  - Actualización de software;
  - Licencias de software;
  - Mantenimiento interno.
- Telecomunicaciones:
  - Alquileres;
  - Transmisión de datos;
  - Mantenimiento.
- Recursos humanos:
  - Salarios;
  - Seguros;
  - Capacitación;
  - Provisiones;

- Viajes.

3.1.4.3 Costos No recurrentes

Los costos no recurrentes son los que se presentan una sola vez durante la vida del proyecto de seguridad. Aunque aparecen una vez, suelen ser los mayores costos del proyecto.

- Salarios;
- Contratos;
- Estudios
- Análisis de requerimientos, diseño, performance, estudios de viabilidad, etc.;
- Conversión de costos;
- Provisión de datos;
- Auditorías internas;
- Acondicionamiento del entorno;
- Costos incidentales;
- Entrenamiento;
- Viajes;
- Documentación.

Una vez estimados los tiempos y costos a invertir en el proyecto, el Experto en Seguridad está en condiciones de elaborar la propuesta de trabajo que contendrá el Plan de trabajo que especifique las tareas y los recursos necesarios para desarrollarlas.

3.1.5 Elaboración del Plan de Trabajo

El paso siguiente a la elaboración del Alcance, y una vez aprobado por los responsables, es la elaboración del *Plan de Trabajo*. Este Plan de Trabajo no es más que la organización de las tareas a desarrollar durante la duración estimada del proyecto.

En todo plan se fijan objetivos o hitos a cumplir. Estos hitos están asociados a una serie de tareas necesarias para lograr el objetivo, que tendrán un periodo asignado. Una buena práctica es fijar las fechas de inicio y fin de la tarea para que los periodos no se extiendan demasiado. Cada subetapa del proyecto tendrá (o no) entregables, documentos o resultados para que los que se trabaja en el periodo asignado. A su vez, el comienzo de una tarea puede depender del resultado de otras tareas, por lo que no podrá comenzar hasta que todas las tareas de las que depende hayan finalizado. Puede haber tareas que se solapen, cuyo resultado alimenta otra tarea, etc. Las posibilidades de dependencia son múltiples por lo que es importante organizarlas con anticipación previendo posibles retrasos o inconvenientes.

El Plan de Trabajo deberá incluir, como mínimo:

- Nombre del proyecto;
- Duración total del proyecto;
- Períodos laborales;
- Períodos laborales;
- Tareas;
- Fases;
- Duración de las tareas;

- Fecha de Inicio del proyecto;
- Fecha de Inicio de cada tarea;
- Fecha de Inicio de cada tarea;
- Fecha de Inicio de cada tarea;
- Fecha de Inicio de cada tarea;
- Solapamiento de tareas;
- Tareas predecesoras o tareas dependientes de otras;
- Entregables por hito;
- Entregables por tarea.

3.2 RELEVAMIENTO

3.2.1 Elaboración del Relevamiento General.

Para desarrollar un Plan de Aseguramiento, el Experto en Seguridad debe conocer la empresa objetivo, su organización y sus procesos de negocio. Sobre esta información se basará una serie de estudios que dependerá de muchos de los factores aquí relevados.

Es por eso que aquí se propone una serie de puntos de control sobre los que se deberá investigar, cuestionar y observar:

- El rubro de la empresa, y conocer sobre su negocio;
- La calidad de la sede en cuanto al manejo del negocio (Administrativa, productiva, comercial, etc.);
- El tamaño de la empresa y su distribución física;

- Detalles sobre la infraestructura edilicia (cantidad de edificios, pisos u oficinas) y su distribución física;
- Que exista una definición de funciones y estructura de comunicación en la empresa;
- Que exista un área de Seguridad Informática;
- Organización de personal – jerarquías dentro de la empresa;
- Que exista un encargado de soporte para las aplicaciones y equipos tratados;
- La arquitectura de la red;
- La tecnología que maneja la empresa (hardware y software);
- La tecnología que maneja la empresa (hardware y software);
- Las aplicaciones especificas que apoyan al negocio;
- Analizar la existencia de documentación en relación a:
    - Un marco normativo que defina la política de la empresa y se siente las bases para el desarrollo de procedimientos y estándares técnicos;
    - Relaciones formales y conocidas por el personal, referidas a la documentación de carácter obligatorio y deseable que debe ser desarrollada y mantenida.
    - Los requerimientos de tecnología de procesamiento de archivos y de interfaces para los usuarios.

Para verificar estos puntos de control el Experto en Seguridad puede realizar las siguientes tareas:

- Revisar la documentación del proceso de negocio de la empresa objetivo con el fin de conocer su estructura y funcionamiento.

- Entrevistar a los responsables del nivel gerencial para obtener información sobre el manejo del negocio y sobre los aspectos críticos del mismo;

- Entrevistar a los responsables del nivel gerencial para obtener información sobre el manejo del negocio y los activos de información que los soportan;

- Obtener de los usuarios, la información adicional sobre el entorno a relevar, tales como:

    - La satisfacción funcional de los requerimiento de información de los usuarios;

    - Confianza de los usuarios en la información que manejan estos equipos y aplicaciones;

- Entrevistar al personal del Área de Sistemas a fin de identificar la documentación existente y los procedimientos formales e informales relacionados con el desarrollo, autorización y mantenimiento de la misma;

- Analizar la documentación existente en cuanto a estructura, niveles de aprobación, vigencia, contenido, publicación y distribución entre los involucrados;

- Identificar los componentes de hardware presentes en las instalaciones;

- Entrevistar al personal de comunicaciones para comprender globalmente las facilidades de acceso a través de internet y los mecanismos de seguridad implantados para prevenir el acceso a dichas facilidades.

3.2.1.1 Relevamiento General

El sondeo propuesto en el *Relevamiento General* deberá documentarse como parte de los entregables del proyecto de aseguramiento del entorno. Para esto se propone el siguiente esquema que resume los puntos de control básicos a relevar:

- Rubro de la empresa
- Calidad de la sede:
    - Administrativa, productiva, comercial, etc.;
- Negocio:
    - Descripción;
    - Procesos de negocio;
    - Productos;
    - Servicios;
    - Actividades rutinarias;
    - Actividades extraordinarias;
    - Actividades excepcionales.
- Dependencia:
    - ¿Es una empresa con presencia multinacional?
    - ¿El negocio se ve afectado por la actividad de la empresa en otros países?
    - ¿El negocio se ve afectado por la actividad de la empresa en otras provincias?
    - ¿El negocio se ve afectado por la actividad de la empresa en otras ciudades?

- ¿El negocio se ve afectado por la actividad de la empresa en otros edificios?

- Si es multinacional:
    - ¿Se trata de una sede o de la corporación?
    - Cantidad de países donde opera;
    - Listado de países donde opera.
- Información edilicia:
    - Cantidad de edificios;
    - Cantidad de pisos por edificio;
    - Cantidad total de pisos;
    - Cantidad de oficinas por piso;
    - Cantidad total de oficinas.
- Red:
    - Arquitectura física, lógica, protocolos;
    - Cableado.
- Hardware:
    - Tipos de maquinarias (mainframes, terminales, PCs);
    - Cantidad de equipos por tipo;
    - Elementos de Red (switches, routers, hubs, etc.);
    - Cantidad de elementos de red;

- Telefonía (centrales telefónicas, teléfonos);
- Cantidad de teléfonos;
- Otros elementos (UPSs, impresoras, scanners, etc.);
- Cantidad de elementos por tipo.

- Software:
  - Sistemas Operativos;
  - Utilitarios;
  - Bases de datos;
  - Software de gestión;
  - Cantidad de licencias.
- Personal:
  - Jerarquía;
  - Cantidad de áreas;
  - Cantidad de sectores;
  - Personal: Contabilización por puesto (gerentes, administrativos, usuarios, no usuarios, externos)
- Administración:
  - ¿Existe un área de desarrollo de software?
  - ¿Existe un área de control de calidad de software?
  - ¿Existe de un área de Seguridad Informática?

- ¿De quién es la responsabilidad de la administración de los equipos?
- ¿De quién es la responsabilidad de la operación de los equipos (de la corporación, del país, de la sucursal, del sector)?
- ¿Cuántas personas abarcan?

3.2.2 Elaboración del Relevamiento de Usuario

En esta etapa del relevamiento él Experto de Seguridad realiza una investigación sobre el entorno objetivo con el fin de obtener un panorama de la situación actual y conocer su forma de funcionamiento, y detectar, a grandes rasgos, fuentes de debilidades para luego realizar un estudio profundo enfocado en los puntos hallados, en la etapa llamada Análisis de Vulnerabilidades.

En este análisis, el Experto de Sistemas verificará los siguientes objetivos de control:

- Que se haya definido y documentado un modelo de administración de la seguridad;
- Que existan estándares y procedimientos de trabajo definidos para todas las tareas del área;
- Que el circuito de trabajo responda a criterios de seguridad, eficiencia y productividad;
- Que exista un perímetro de seguridad para los equipos de procesamiento critico;
- Que se apliquen medidas de seguridad física en el entorno de trabajo de los usuarios finales;
- Que los equipos informáticos sean utilizados sólo con fines autorizados y siguiendo los procedimientos establecidos;

- Que exista un encargado de soporte del mantenimiento para las aplicaciones analizadas;
- Que los usuarios tienen conciencia de los problemas de seguridad informática y están informados acerca de los riesgos existentes;
- Que existen adecuados procedimientos manuales o automatizados de control de cambios a los programas y de toma de nuevos requerimientos de usuarios;
- Que existen acuerdos de confidencialidad firmados por los usuarios para el manejo de la información que tratan los sistemas;
- Que exista un marco normativo que defina la política de la empresa y sienta las bases para el desarrollo de procedimientos y estándares técnicos;
- Que exista documentación de usuario que especifique los requerimientos de tecnología, de procesamiento, de archivos y de interfaces.
- Que se encuentre implantado adecuadamente un ambiente general de control de accesos propio de las aplicaciones y recursos a efectos de prevenir el uso no autorizado de funciones interactivas, tanto desde conexiones desde la red interna como desde internet.

Para verificar estos puntos de control el Experto en Seguridad y su equipo de trabajo puede realizar las siguientes tareas:

- Entrevistar a los usuarios a fin de obtener información sobre el entorno a relevar, en los siguientes aspectos: Físico; Lógico; De la organización.
- Para ello el Experto en Seguridad explicara a los usuarios el objetivo de la charla y dará todo el detalle necesario para que las respuestas de los mismos sean validas.

En estas entrevistas se sugiere realizar un test en cada uno de los diferentes departamentos de la organización y dentro de estos, en los distintos sectores.

Este test tiene por obtener una medida de lo expuesto que se encuentra el ambiente a vulnerabilidades, fallas en la cultura de trabajo, vicios en la organización, el nivel de información que manejan los empleados y su nivel de información que manejan los empleados y su nivel de conciencia respecto de la seguridad, etc. O sea, una medida general de lo expuesto que se encuentra el sistema los ataques informáticos por nivel.

Esto servirá como introducción al Experto en Seguridad para la construcción del Mapa de Vulnerabilidades y para fijar los objetivos del Plan de Aseguramiento del sistema. Una vez recompilado como mínimo esta información, la Metodología MSEI prevé la intervención del usuario como fuente de conocimiento del Experto en Seguridad. A continuación se especifica el documento formal que se materializa la intervención directa del usuario como referente de las características del entorno en estudio.

3.2.2.1 Relevamiento de usuario

El Relevamiento de Usuario consiste en una serie de preguntas separadas en tres módulos por nivel. Los módulos corresponden a los niveles físico, lógico y de la organización respectivamente. El Experto en Seguridad evaluara la criticidad de cada punto asignado un valor según la respuesta obtenida.

3.2.2.2 Asignación de puntaje

Para la asignación del puntaje se siguió el criterio adecuado para el estudio que se lleva a cabo en este Relevamiento. Se definen los valores posibles y su significado como sigue:

- 0: No representa amenaza alguna;
- 1: Amenaza leve;

- 2: Gran amenaza al sistema.

Para medir la criticidad se utiliza el siguiente criterio:

No representa amenaza alguna: Si están presentes elementos que provean información que no es del sistema que pueda ser usada para efectuar ataques estructurados en un objetivo, pero que no otorgan acceso autorizado directamente.

Amenaza leve: Si existen eventos que tengan el potencial de otorgar acceso o permitir ejecución de código por medio de procedimientos largos o complejos, o elementos de bajo riesgo aplicados a componentes importantes.

Gran amenaza al sistema: Si existen elementos que permiten acceso local o remoto inmediato a los servicios.

3.2.2.3 Aclaración sobre las preguntas

Se realizaran preguntas en tres distintos niveles los cuales son el Nivel Físico, el Nivel Lógico y el Nivel de Organización esta aclaración estará en la parte de Anexos. Las preguntas apuntan a determinar si el usuario tiene conciencia de la criticidad de la información que maneja y si se ha realizado alguna vez una clasificación de la información de la organización.

Resultados de la evaluación

Según la cantidad de puntos obtenidos en cada nivel se establece la calificación del entorno en cuanto a seguridad informática:

Nivel físico:

- De 0 a 6 puntos: Seguro/protegido;
- De 7 a 16 puntos: Medianamente vulnerable;
- De 17 a 32 puntos: Altamente vulnerable.

Nivel lógico:

- De 0 a 10 puntos: Seguro/protegido;
- De 11 a 14 puntos: Medianamente vulnerable;
- De 15 a 28 puntos: Altamente vulnerable.

Nivel de la organización:

- De 0 a 4 puntos: Seguro/protegido;
- De 5 a 9 puntos: Medianamente vulnerable;
- De 10 a 20 puntos: Altamente vulnerable.

Evaluación del entorno

Referencias al puntaje obtenido en el test por nivel:

- 0: Seguro/protegido;
- 1: Medianamente vulnerable;
- 2: Altamente vulnerable; x: 0 o 1.

Configuraciones de resultados:

- 000: Entorno seguro.
- 001, 010, 001, 011, 110, 101, 111: Entorno medianamente vulnerable. Asegurable a corto plazo;
- xx2, x2x, xx2: Entorno altamente vulnerable. Asegurable de mediano a corto plazo;
- x22, 22x, 2x2: Entorno altamente vulnerable. Asegurable a mediano/ largo plazo;

- 222: Entorno altamente vulnerable. Requiere una planificación completa a largo plazo.

3.2.3 Análisis de vulnerabilidades.

Esta etapa comprende la determinación de las amenazas que enfrenta el entorno respecto de la seguridad de la información. Los datos almacenados en los servidores de la red, los almacenados en cada estación de trabajo, los equipos e instalaciones, las aplicaciones, los documentos y todo mensaje, corren riesgos reales, potenciales y latentes a cada instante.

Estos mensajes, datos, activos deben cumplir su función conservando los tres pilares de la seguridad intactos: las vulnerabilidades pueden generar amenazas en el entorno en estudio, sin son conocidos por un atacante, pueden causar la pérdida de alguna de las características deseables de la información, antes mencionadas.

Conocer al enemigo

Es muy importante conocer el entorno en estudio para predecir el tipo de atacante que puede atraer.

Según las características del entorno, se estará expuesto a un abanico de atacantes más o menos peligrosos y más o menos experto, los usuarios inexpertos son atraídos por entornos inseguros (como una computadora hogareña conectada a internet), mientras que los intrusos más hábiles se ven atraídos por ambientes más confidenciales y protegidos (instituciones financieras, de gobierno).

Es por eso que el Experto en Seguridad debe de analizar qué tipo de entorno maneja para predecir a qué tipo de ataques probablemente se deberá enfrentar.

Análisis de Vulnerabilidades

En esta etapa se analizan las fallas de seguridad en el entorno según los estándares internacionales referenciados en la bibliografía de este trabajo.

Se considera una vulnerabilidad a toda diferencia entre los parámetros deseados recomendados por dichos estándares y las mejores prácticas profesionales en cuanto a Seguridad Informática. Los objetivos de control considerados según [IRAM/ISO/IEC17799], [BS779], [Cobit], [AAW-ISI] son los siguientes:

Aspectos funcionales

- Que exista una adecuada definición de funciones y estructura de comunicación en el área;
- Que las tareas incompatibles sean adecuadamente segregadas;
- Que existan licencias de uso del producto para cada recurso / usuario;
- Que las aplicaciones activas en el entorno contribuyan a perseguir los objetivos del negocio;
- Que se haya definido y documentado un modelo de administración de la seguridad;
- Que existan estándares y procedimientos de trabajo definidos para todas las tareas de área.
- Que el circuito de trabajo responda a criterios de seguridad, eficiencia y productividad;
- Que los procedimientos adoptados estén de acuerdo con normas estándares en la materia;
- Que estén definidos y se encuentren documentados para cada puesto del organigrama perfiles de usuario modelo a los cuales se les asocian las identificaciones individuales de cada persona.
- Que los equipos informáticos sean utilizados solo con fines autorizados y siguiendo los procedimientos establecidos.

- Que todo procesamiento este debidamente autorizado por los responsables correspondientes;

- Que existan procedimientos de control de los resultados que surgen del procesamiento en los equipos;

- Que existan estándares definidos a seguirse para la realización de pruebas de los desarrollos y/o mantenimientos;

- Que el acceso a la documentación de los sistemas de aplicación de producción solo se permita a personal autorizado;

- Que exista encargado de soporte del mantenimiento para las aplicaciones analizadas;

- Que existen adecuadas procedimientos manuales o automatizados de control de cambios a los programas;

- Que existen clausulas de confidencialidad en los contratos con los proveedores de software y/o terceros que trabajen en las aplicaciones.

Este análisis permitirá visualizar el nivel de adhesión que tiene la estructura del proceso a los estándares, metodológicos que se tengan establecidos para el desarrollo y mantenimiento, así como para la documentación de las etapas del proceso. Además se podrán establecer los criterios que fueron utilizados para definir y establecer las características de los controles internos y las validaciones. El análisis funcional permite visualizar las distintas etapas que se suceden en el proceso, así como también identificar etapas de alto, medio y bajo riesgo.

Para verificar estos puntos de control él ES y su equipo de trabajo puede realizar las siguientes tareas:

- Revisar la documentación del proceso de negocio de la empresa objetivo con el fin de conocer su estructura y funcionamiento;

- Entrevistar a los analistas/programadores/técnicos responsables del mantenimiento de las aplicaciones y equipos y comparar el procedimiento que cada uno está aplicando;

- Entrevistar a los analistas/programadores responsables del desarrollo.

- Entrevistar a los analistas/programadores/técnicos responsables del desarrollo de las aplicaciones y equipos para validar la adecuada concientización del personal a fin de cumplir con la documentación vigente;

- Conocer los procesos y funciones de administración de las bases de datos y de "back-up" de archivos y programas (fuentes ejecutables) de cada una de las aplicaciones;

- Entrevistar a ciertos usuarios finales, elegidos al azar, a efectos de verificar cuan involucrados están con las distintas fases de desarrollo/mantenimiento de sistemas (diseño, desarrollo, prueba y aceptación).

- Relevar y probar los procedimientos de administración, control, control de los cambios efectuadas a las aplicaciones e identificar a los responsables de llevar a cabo los mismos;

- Identificar y entrevistar al personal responsable de implantar cambios de realizar controles sobre las incidencias que involucren las aplicaciones para verificar que se cumpla con los procedimientos vigentes;

- Solicitar (en caso de existir) y analizar el log utilizado para priorizar y monitorizar la recepción y progreso de los cambios de sistemas;

- Solicitar y analizar muestras de documentos relacionados con modificaciones de los programas:

    - Documentos aprobados por los supervisores de desarrollo autorizando la puesta en producción de los programas modificados;

- Documentos que demuestren que los usuarios finales han aprobado los desarrollos/modificaciones efectuados antes de migrar los nuevos programas al área de producción;

- Formularios que formalmente comuniquen el orden de ejecución de los programas modificados al área de operaciones;

- Identificar una muestra de requerimientos de cambios a las aplicaciones relevadas en el log requerido y verificar que para cada uno de ellos se haya cumplimentado adecuadamente el procedimiento de modificación de programas y catalogación en producción, con su respectivo control.

Análisis de la documentación

Los objetivos de control que se deben verificar son los siguientes:

- Que exista un marco normativo que defina la política de la empresa y se sienta las bases para el desarrollo de procedimientos y estándares técnicos;

- Que existan relaciones formales y conocidas por el personal, referidas a la documentación de carácter obligatorio y deseable que debe ser desarrollada y mantenimiento;

- Que se cumpla con las definiciones formales e informales relacionadas al desarrollo, mantenimiento y cadenas de autorización referidas a la documentación.

- Que se encuentren implantados métodos efectivos de distribución y comunicación entre los involucrados;

- Que los procesos tecnológicos estén alineados con las normas establecidas y sean adecuados;

- Que los procedimientos alcancen los niveles de servicio;

- Que exista documentación de usuario que especifique los requerimientos de tecnología, de procedimientos, de archivos y de interfaces;
- Que exista un procedimiento formal para realizar el control de cambios, niveles de revisión, autorización y publicación;
- Entrevistar al personal del Área de Sistemas a fin de identificar la documentación existente y los procedimientos formales e informales;
- Analizar la documentación existente en cuanto a niveles de aprobación, vigencia, contenido, publicación y distribución entre los involucrados;
- Evaluar los niveles de cumplimiento de los procedimientos existentes;
- Seleccionar un grupo de personas para evaluar el nivel de conocimiento y utilización de la documentación existente;
- Identificar los puntos débiles de la documentación y procedimientos existentes.

Análisis de las aplicaciones y equipos

Los objetivos de control que debe verificar el ES en este aspecto son los siguientes:

- Que existan roles adecuados para la supervisión de la seguridad de las aplicaciones y equipos que existan en el entorno;
- Que se encuentre implantado adecuadamente un control de accesos a la red de datos y sus equipos que eviten el uso no autorizado de los recursos,
- Que se encuentran implantado adecuadamente un control de accesos a la red de datos y sus equipos que eviten el uso no autorizado de los recursos, el descubrimiento y divulgación de información y el mal uso y abuso de la información tratada por los mismos;

- Que se encuentran implantado adecuadamente un ambiente general de control de accesos propio de las aplicaciones y recursos a efectos de prevenir el uso no autorizado de funciones interactivas, tanto desde conexiones desde la red interna como desde internet.

- Que se encuentran implantado adecuadamente un ambiente general de control de accesos para el procesamiento "batch";

- Que exista una adecuada política de configuración de los equipos informáticos y de comunicaciones;

- Que se encuentre implantada adecuadamente la estructura de control de accesos del ambiente de procesamiento de forma de evitar que se puedan modificar o leer archivos de datos o programas de las aplicaciones analizadas en forma no autorizada;

- Que las aplicaciones gestionen los errores de forma estándar y que se realicen las validaciones adecuadas en la entrada y salida de datos;

- Que exista un plan de contingencia que permita recuperar las aplicaciones del entorno ante desastres o situaciones de emergencia;

- Identificar y analizar el sistema de autentificación de usuarios utilizado por la aplicación, el sistema operativo que la soporta;

- Realizar una toma de la configuración lógica de los equipos mediante:

    - Scripts de relevamiento técnico que lean los archivos de configuración más importantes y los vuelquen en informes;

    - Generalización de listados;

- Realizar pruebas de cumplimiento para verificar que los accesos a los diferentes recursos informáticos están adecuadamente otorgados y/o restringidos;

- Realizar un intento de penetración con el fin de vulnerar barreras de acceso existentes para utilizar desde una conexión proveniente de internet (intento de penetración externo), o desde la red interna de la compañía (intento de penetración interno).

Intento de Penetración

Un intento de penetración es un análisis que permite detectar vulnerabilidades en un entorno informatizado de vulnerabilidades. Su alcance se extiende a:

- Equipos de comunicación;
- Servidores;
- Estaciones de trabajo,
- Aplicaciones,
- Bases de datos;
- Servicios informáticos;
- Casillas de correo electrónico;
- Portales de internet;
- Intranet corporativa;
- Acceso físico a recursos y documentación;
- Ingeniería social (la ingeniería social es la técnica por la cual se obtiene información convenciendo al usuario que otorgue información confidencial, haciéndose pasar por usuarios con altos privilegiados como administradores y técnicos).

Para realizar un intento de Penetración es necesario realizar las siguientes tareas:

- Reconocimiento de los recursos disponibles mediante el empleo de herramientas automáticas;
- Identificación de las vulnerabilidades existentes mediante herramientas automáticas;
- Explotación manual y automática de las vulnerabilidades para determinar su alcance;
- Análisis de resultados;

Este análisis otorga información referente a:

- Versiones desactualizadas de software;
- Versiones de software con vulnerabilidades conocidas,
- Contraseñas triviales;
- Usuarios default;
- Configuraciones default;
- Utilización de servicios inseguros;
- Recursos compartidos desprotegidos;
- Errores en la asignación de permisos.

Herramienta de análisis de vulnerabilidades

Existe una serie de herramientas que ofrecen datos útiles para el análisis de vulnerabilidades, como analizadores de configuraciones, analizadores de logs, herramientas de escaneo o puertos (Port Scanners), sniffers, Network Mapping Testing Tools y otras herramientas, sobre las que no se dará detalle por su constante evolución. No es objetivo de esta Tesis dar detalles sobre implementaciones en particular, sin embargo, se considera interesante remarcar la

importancia del uso de estas herramientas para la detección de vulnerabilidades sobre todo porque reducen considerablemente los tiempos de búsqueda y recolección de datos.

Mapa de Vulnerabilidades

El Mapa de Vulnerabilidades es un documento que se propone con la idea de registrar y contabilizar las vulnerabilidades presentes en el entorno en estudio antes de la implantación del Plan de Aseguramiento.

Para registrar las vulnerabilidades detectadas en el análisis anterior se divide el estudio del entorno en tres partes:

- Nivel físico;
- Nivel lógico;
- Nivel de la organización.

El ES incluirá en el Mapa de Vulnerabilidades del entorno objetivo los niveles que se hayan determinado en el Alcance.

Aquí se enumera una serie de aspectos concernientes a seguridad que implican vulnerabilidades y que él ES incluirá en el Mapa de Vulnerabilidades:

3.2.4 Análisis de Riesgos

A partir del Mapa de Vulnerabilidades construido en la etapa anterior de la fase de Definición del Alcance de la MSEI, se analiza el riesgo que corren los activos de la organización para determinar la probabilidad de ocurrencia de incidencias de seguridad y su impacto en el sistema.

Los riesgos pueden ser:

- Tecnológicos: si tienen origen o afectan aspectos técnicos del entorno (como deterioro de equipamientos, falta de disponibilidad de recursos, etc.);

- Funcionales: si tienen origen o afectan aspectos funcionales del entorno (como posible descubrimiento de información por la existencia de usuarios con contraseña por default, o el acceso no autorizado a los recursos por una pobre autentificación de usuarios).

Todos los entornos están expuestos a amenazas. Todos los entornos tienen vulnerabilidades, algunas conocidas, otras no, pero están presentes, esperando ser usadas por un atacante para penetrar las barreras de seguridad y apoderarse de información, denegar servicios, o provocar toda clase de daño. No importa la plataforma tecnológica, no importa la marca de software que se usa. Tampoco importa la infraestructura edilicia, los equipos, el cableado. Siempre existen riesgos.

Existe una relación entre tipo de desastres y sus afectos, y, por supuesto, su probabilidad de ocurrencia. Los riesgos reales y potenciales son variables en el tiempo y lugar.

En el análisis de vulnerabilidades se vieron los distintos tipos de amenazas que pueden presentarse a nivel lógico, físico y de la organización.

No es posible eliminar todos los riesgos sino que se pueden mitigar (empleando medida para reducirlos), transferir (ceder su responsabilidad a otra persona) o asumir (cuando se decide correr el riesgo con sus posibles consecuencias). Sin embargo siempre existen riesgos remanentes y desconocidos. Es más, cada día surgen nuevos riesgos a medida que la tecnología avanza y los sistemas cambian. Los entornos informatizados suelen acompañar estos cambios adaptándose a los requerimientos tecnológicos del momento. Es por eso que surgen nuevos riesgos día a día.

Es tarea del ES en esta parte de la metodología examinar las vulnerabilidades halladas y evaluar su riesgo asociado, determinar su probabilidad de ocurrencia y medir su impacto en el entorno.

Los riesgos observados que presentan una probabilidad de ocurrencia no despreciable en función de las características del entorno varían desde los factores climáticos y meteorológicos que afectan a la región hasta el factor humano de los recursos de la empresa. Para la evaluación de riesgos es posible utilizar métodos muy variados en composición y complejidad, pero para todos ellos es necesario realizar un diagnostico de la situación.

Este análisis de riesgos permite al ES ofrecer un informe de los riesgos entorno, los peligros que corre e identificar los requerimientos de seguridad del sistema objetivo y su prioridad, de manera de poder encarar la elaboración del Plan de Aseguramiento del proyecto junto a los requerimientos planteados por el usuario.

El análisis de riesgos se realiza en cada área de la empresa, mediante métodos de adquisición de información como entrevistas con los usuarios.

Informe de Riesgos

A continuación se presenta un documento que ayuda a la formalización de estos conceptos para su estudio: el *Informe de Riesgos*.

Este documento recompila todas las vulnerabilidades halladas en la etapa anterior de la metodología, para evaluar su riesgo, su criticidad, la probabilidad de que ocurran y determinar su impacto en el entorno informatizado y en el negocio.

Esta es una adaptación de la Tabla de Riesgos utilizada en el análisis de sistemas en la que se ha agregado la criticidad que implica la vulnerabilidad en estudio.

Se recomienda agrupar las vulnerabilidades con algún criterio, como por ejemplo por nivel de criticidad, que puede clasificarse en: Alto; Medio; Bajo. U ordenarlas en forma decreciente según su impacto o probabilidad de ocurrencia.

3.3 PLANIFICACIÓN

3.3.1 Elaboración del plan de Aseguramiento

En esta parte de la fase de planificación se establece, en base al Alcance y al Relevamiento anteriormente realizado, el *Plan de Aseguramiento*.

Este documento describe en forma precisa y detallada las medidas, cambios y controles que se implementarán a fin de proteger el sistema objetivo, mitigando los riesgos descubiertos en la fase anterior de la Metodología para la Seguridad de Entornos Informáticos, MSEI.

Los objetivos de control planteados por el Experto en la etapa de Análisis de Vulnerabilidades se reflejan aquí en medidas de control que garanticen la reducción del riesgo asociado a las vulnerabilidades halladas, tanto en aspectos tecnológicos como funcionales.

[ISO - 17799] indica: "Una vez identificados los requerimientos de seguridad, deben seleccionarse e implementarse controles para garantizar que los riesgos sean reducidos a un nivel aceptable"..."Los controles deben seleccionarse teniendo en cuenta el costo de implantación en relación con los riesgos a reducir y las pérdidas que podrían producirse de tener lugar una violación de la seguridad. También deben tenerse en cuenta los factores no monetarios, como el daño en la reputación". Se detalló en etapas anteriores de la MSEI cómo a partir de un análisis de vulnerabilidades, de requerimientos de usuario y de riesgos se llega a establecer el Alcance. Sin embargo, no es el fin de este trabajo dar detalles sobre las técnicas a implementar para conseguir resultados, entendiéndose por buenos resultados el aseguramiento del elemento en cuestión. Se limitara a dar las pautas procedimientos para asegurar el entorno informatizado que es objetivo, y el Experto en Seguridad que lo implemente deberá realizar el trabajo de investigación especifico para obtener los resultados propuestos por este trabajo, según la tecnología involucrada.

3.3.2 Protección física

Protección de las Instalaciones

Se analiza en esta parte la protección del edificio, salas e instalaciones a nivel físico. Se evalúa la implantación de alguna de las siguientes técnicas:

- Definición de áreas de la organización en cuanto a seguridad: En esta etapa se deberán diferenciar los sectores de acceso común a todos los usuarios (como el comedor, la sala de reuniones, etc.) de los sectores de acceso restringido (como el área de cómputo o tesorería) y los distintos niveles de seguridad requeridos.

- Definición de un perímetro de seguridad: Un perímetro de seguridad es un área considerada segura. Al definir un perímetro de seguridad, se establece un área donde se implementaran medidas de protección que garanticen cierto grado de seguridad, como por ejemplo barreras físicas, paredes, alarmas, sistemas automáticos de autenticación de usuarios, etc.

- Verificación del perímetro de seguridad: Realizar pruebas de penetración de las barreras físicas, para determinar su fortaleza;

- Determinación de áreas protegidas: Un área protegida es una zona que se desea mantener segura a la que no tiene acceso todo el personal, sino un grupo reducido de este, a la que acceden con fines específicos y bajo severos controles de autentificación. Puede ser una oficina cerrada con llave o diversos recintos dentro de un perímetro de seguridad física donde se realicen operaciones confidenciales, como el centro de procesamiento de información, etc. Se deben definir las zonas u oficinas que tienen estos requerimientos;

- Controles en las áreas protegidas:

    - Controlar el trabajo en las áreas protegidas tanto por razones de seguridad como para evitar la posibilidad de que se lleven a cabo actividades maliciosas;

- Bloquear físicamente las áreas protegidas desocupadas e inspeccionar periódicamente;
- Prohibir el ingreso de equipos fotográficos, de video, audio u otro tipo de de equipamiento que registre información.

- Determinación de uno o varios métodos de autentificación de usuarios: Autentificar usuarios implica verificar a los usuarios que intentan acceder al entorno, a la red o al sistema, comprobando que estos sean quienes dicen ser.

Existen muchos métodos de autenticación de usuarios, y se clasifican según lo que utilizan para la verificación de la identidad:

- Métodos que se basan en algo que el usuario sabe:
  - Contraseñas (passwords);
  - Frases secretas (passphrases);
- Métodos que autentican a través de un elemento que el usuario posee o lleva consigo:
  - Tarjetas magnéticas;
  - Tarjetas de identidad inteligentes (chipcards o smartcards).
- Métodos que utilizan características físicas del usuario o actos inconscientes:
  - Verificación del aspecto físico;
  - Reconocimiento por huella digital;
  - Reconocimiento por el patrón de la retina del ojo;

- Reconocimiento por el patrón del iris del ojo;
- Reconocimiento de la voz;
- Firmas es un acto inconsciente, ya que no se razona cómo se hace cada trazo;
- Verificación de la geometría de la mano;

- Determinación de la forma de registro del flujo de personas en los distintos sectores: Por ejemplo, mediante un sistema de tarjetas magnéticas:
  - Registrar la hora de ingreso y egreso de cada usuario que ingrese al edificio;
  - Registrar la hora de ingreso y egreso de cada usuario que recurra al centro de cómputos;
- Separación del área de procesamiento de información de las áreas de entrega y carga de materiales;
- Controles en las áreas de entrega y carga de materiales: Controlar el acceso a las áreas de depósito, desde el exterior de la sede de la organización;
- Diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio;
- Implantación de sistemas de detección de intrusos: Implantar adecuados sistemas de detección de intrusos que se instalan según estándares profesionales y probados periódicamente. Estos sistemas comprenden todas las puertas exteriores y ventanas accesibles. Las áreas vacías deben tener alarmas activadas en todo momento. También se considera la protección de otras áreas, como la sala de cómputos o las salas de comunicaciones;

- No hacer pública información sensible;

Protección de los equipos

Se analiza en esta parte la protección de los distintos Activos a nivel físico. Se evalúa la posibilidad de implementar alguna de las siguientes técnicas:

- Evaluación de la distribución física de los activos: Se realiza a fin de evitar accidentes, o para prevenir, mediante la ubicación estratégica de los bienes, hurtos o deterioros de activos:
    - Ubicar las instalaciones clave en lugares a los cuales no pueda acceder el público;
    - Ubicar las funciones y el equipamiento de soporte compartidas por los usuarios, por ejemplo, fotocopiadoras, máquinas de fax, dentro del área protegida para evitar solicitudes de acceso, que podrían comprometer la información;
- Mantener alejados los suministros: Almacenar los materiales peligrosos o combustibles en lugares seguros a una distancia prudencial del área protegida;
- Individualización de los elementos de red: Es fundamental tener un conocimiento completo de la red, individualizar todos sus elementos, su respectiva ubicación física y su dirección lógica.
- Rotulación de activos físicos:
    - Los equipos, dispositivos externos, cintas de backup y demás activos físicos deben ser rotulados según la nomenclatura fijada en el Inventario de Activos Físicos de forma clara y legible;
- Control de cambios en equipos:

- Mantener el equipamiento de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor;
- Mantener registro de todas las fallas supuestas o reales en el Registro de Incidencias y de todo el mantenimiento preventivo, correctivo y actualizaciones de hardware en el documento de ABM Activos y en el Inventario de Activos Físicos.

- Prevención de catástrofes:
  - Incendios: Provocados por rayos, por fallas eléctricas o descuido de los usuarios (cigarrillos, hornallas). Colocar extinguidores automáticos en los techos y extinguidores manuales en todo el edificio;
  - Humo: Provocado por incendios y por el cigarrillo. El huno ataca los discos magnéticos y ópticos y provoca trastornos en la ventilación de los artefactos eléctricos. Se considera prohibir fumar en las oficinas y colocar detectores de humo en techos;
  - Temperaturas extremas: Los artefactos eléctricos y electrónicos funcionan correctamente dentro de un rango determinado de temperaturas, en general entre los 0 y los 70 grados centígrados. Si se exceden estos extremos se corre el riesgo de que los materiales dejen de ser ferros magnéticos. Consultar los manuales de los fabricantes y mantener la temperatura dentro de los rangos sugeridos. Se aconseja la utilización de equipos de aire acondicionado en todas las salas;
  - Polvo: El polvo se deposita sobre los artefactos removibles y entra por los ventiladores de las CPU y daña los circuitos. Es necesario tener una rutina de limpieza y aspiración de los ambientes;

- Explosiones;
- Vibraciones: Ciertos objetos presentes en oficinas provocan vibraciones indeseadas. Impresoras, maquinas expendedoras de bebidas, provocan estas vibraciones. Instalar plataformas anti vibración;
- Electricidad: Trastornos o fallas en la línea eléctrica pueden provocar cortocircuitos, subidas de tensión, cortes en el flujo eléctrico y hasta incendios. Instalar cables a tierra y estabilizadores de tensión. También se sugiere la utilización de baterías o unidades de alimentación ininterrumpida;
- Tormentas eléctricas: Las tormentas eléctricas pueden provocar altísimas subidas de tensión que queman los equipos.
- Ruido eléctrico: El ruido eléctrico es generado por motores, equipos eléctricos y celulares. Colocar filtros en la línea de alimentación y alejar los equipos de otros artefactos;
- Humedad: El exceso de humedad en equipos eléctricos provoca cortocircuitos y la escasez de humedad provoca estática. Se recomienda instalar alarmas anti humedad y mantener la misma al 20%.
- Inundaciones: Colocar los equipos alejados del piso, instalar un falso suelo o ubicar sensores en el piso que corten el suministro de energía eléctrica al detectar agua;
- Terremotos: Para proteger los equipos más críticos de los terremotos se fijan estos de manera que no se puedan desplazar y se trata de ubicar todo equipo alejado de las ventanas;
- Insectos;

- Comida y bebidas: La organización debe analizar su política respecto de comer, beber y fumar cerca de las instalaciones de procesamiento de información. Se recomienda prohibir estas actividades para proteger los equipos e instalaciones

- Terminales abandonadas: Las terminales encendidas en desuso son un riesgo alto. Utilizar un sistema automático de detección y apagado de terminales encendidas en desuso.

- Vandalismo;

- Hurto;

- Ubicación de la información crítica en lugares seguros:

  - Mantener el equipamiento de sistemas de soporte UPC (usage parameter control), de reposición de información perdida (fallback) y los medios informáticos de respaldo (backups) a una distancia prudencial de la fuente de información, en lugares protegidos contra intrusos y catástrofes naturales que permitan evitar daños ocasionados por eventuales desastres en el sitio original;

- Protección de las copias de respaldo:

  - Los medios que contienen las copias de respaldo o backup como cintas o discos deben ser cuidadosamente almacenados en lugares alejados de la fuente de datos y protegidos contra robo, incendio e inundación;

- Restricción del acceso a unidades removibles:

  - Únicamente los usuarios locales deben tener acceso a las unidades removibles como discos removibles, CD-ROM, DVD, ETC;

- Garantizar el adecuado suministro de energía:
    - Proteger el equipamiento con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas:
- Protección del cableado: Proteger contra interceptación o daño del cableado de energía eléctrica y de comunicaciones, que transporta datos o brinda apoyo a los servicios de información:
    - Instalar líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información subterráneas, o sujetas a una adecuada protección alternativa;
    - Proteger el cableado de red contra interceptación no autorizada o daño, evitando trayectos que atraviesen áreas públicas;
    - Separar los cables de energía de los cables de comunicaciones para evitar interferencias;
    - Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de control.
- Protección de los equipos utilizados fuera de la organización: El nivel gerencial debe proveer seguridad de forma equivalente a la suministrada dentro del ámbito de la organización, para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma:
    - Controlar el equipamiento y dispositivos retirados del ámbito de la organización para que no estén desatendidos en lugares públicos;
    - Transportar las computadoras personales como equipaje de mano y de ser posible enmascaradas, durante el viaje;

- Respetar permanentemente las instrucciones del fabricante, por ejemplo, protección por exposición a campos electromagnéticos fuertes;
- Contar con una adecuada cobertura de seguro proteger el equipamiento fuera del ámbito de la organización;
- Contar con medios de protección de las comunicaciones entre los equipos portables (como Laptops) mediante técnicas de encriptación de los canales.

- Control de la baja de equipos:
  - Controlar los equipos que se den de baja para evitar la utilización indebida de la información que transporten;
  - Verificar el borrado seguro de datos sobrescribiendo las pistas de discos antes de desecharlos;
  - Procurar la destrucción física de diskettes y unidades de cinta y todo artefacto removible capaz de contener información;
- Control de la disponibilidad de almacenamiento:
  - Verificar la disponibilidad de espacio de almacenamiento físico de datos;
  - Monitorear las demandas de capacidad requeridas por los elementos de software;
  - Realizar proyecciones sobre los futuros requerimientos de capacidad.

3.3.3 Protección lógica

Se analiza en esta parte la protección de los distintos Activos a nivel lógico.

Protección de la información

En este apartado se pretende establecer reglas para la protección de la información de la organización objetivo, o sea, técnicas de prevención del hurto, modificación o deterioro de la confidencialidad de los datos con significado para la institución:

- Prevención de ataques externos.

- Clasificación de la información: La información se debe clasificar en cuanto a su acceso (que perfiles de usuario tienen acceso a lectura, ejecución o modificación de los datos) y en cuanto a su criticidad. Para clasificarla según acceso, se hace uso de la Tabla de Accesos Sobre Activos Lógicos, y para clasificarla según su criticidad, se hace referencia al inventario de Activos Lógicos;

- Establecer medidas de protección según la clasificación de la información: Según el tipo de información que se trate, se deberán garantizar controles como se indica a continuación:

    - Para la información pública o no restringida: No es necesario establecer restricciones especiales, más allá de las recomendaciones sobre su buen uso y conservación;

    - Para la información restringida y/o secreta: Dependiendo que la información se haya clasificado como restringida o secreta se deben cumplir con los siguientes requerimientos mínimos y obligatorios para su protección.

    - Conservación: La información clasificada como secreta y los medios físicos donde se almacene, deben protegerse utilizando cajas de seguridad cuya llave y/o combinación debe de ser conservada por el Dueño de los Datos, quien debe autorizar toda copia adicional de

dicha información así como la transmisión, envió, impresión y/o destrucción de la misma.

- Entrega/Traslado: Realizar toda entrega de documentación que contenga información secreta/confidencial en sobre cerrado para una mayor confidencialidad.
- Divulgación de terceros: Instrumentar convenios de confidencialidad con los terceros que deben acceder a información de la empresa.
- Destrucción: Destruir toda información secreta y sus correspondientes soportes físicos cuando se considere no vigente y se discontinué su utilización y/o conservación.
- Informar a los usuarios sobre el manejo de la información: Toda la información conservada en los equipos informáticos (archivos y correos electrónicos residentes en servidores de datos centralizados y/o estaciones de trabajo) puede ser considerada propiedad de la compañía y no de los usuarios, dependiendo de su Política de Seguridad, por lo que podrá ser administrada y/o monitoreada por los responsables del área de Sistemas de acuerdo con las pautas de seguridad definidas.

Protección del Sistema Operativo.

- Actualización de del Sistema Operativo:
  - Actualizar periódicamente los Sistemas Operativos de Servidores y estaciones de trabajo para las diferentes plataformas. En Unix-Linux, actualizar el kernel y en la plataforma Microsoft, actualizar el SO con la versión que se considere necesaria de acuerdo con las necesidades funcionales y las mejoras implementadas por el fabricante;

- Aplicar los parches (hot fixes, service packs) que publican los proveedores de software en todos los equipos;

- Estandarización de servidores: La configuración de seguridad de los equipos puede ser tediosa, pero es necesaria. Los servidores deben seguir un estándar para su identificación y para su configuración. El Manual de Seguridad incluye estándares técnicos que se elaboran para estos fines. El ES deberá evaluar la posibilidad de elaborar uno para facilitar la tarea de homogenización de configuraciones de seguridad por plataforma deben tener los equipos respecto de la seguridad, que se aplique a todos los servidores existentes, y cada vez que se dé de alta a uno nuevo;

- Protección del inicio del sistema: Permitir la configuración del arranque de los equipos según lo establecido en el Manual de Seguridad. La practica más recomendable es deshabilitar la posibilidad de booteo de los servidores desde el CD-ROM;

- Control de la instalación de programas y dispositivos: Permitir únicamente a usuarios con privilegios de administrador que instalen software y dispositivos en los equipos;

- Creación de subsistemas en el sistema operativo limitada: Sistemas Operativos como la serie Windows permite la creación de subsistemas OS/2 y POSIX. Los de la familia Unix permiten la creación de shells hijos donde correr procesos en segundo plano. Ambos casos deben de evaluar según la funcionalidad del equipo que se trate, y restringir el uso de estas facilidades cuando no sean estrictamente necesarias para el desarrollo de las tareas y servicios que prestan;

- Desconexión de todas las unidades de red inutilizadas: Muchas veces se conectan unidades de red con fines específicos para la instalación remota, etc;

- Limpieza de memoria: Cada vez que el sistema se cierra se debe limpiar la paginas de memoria virtual;

- Apagado seguro: No permitir el apagado de equipos sin la autenticación (login del usuario). La única excepción es durante la utilización de medios alternativos de alimentación eléctrica (como UPSs) durante una emergencia;

- Implantación de un sistema de perfiles y grupos de usuarios: La administración de usuarios es clave para el mantenimiento de la seguridad del entorno; Todos los sistemas operativos actuales permiten la creación de usuarios, perfiles de usuario y grupos. Los perfiles son los tipos de usuarios existentes. Los grupos son conjuntos de usuarios. Por lo general se crea grupos para identificar a los usuarios que realizan una misma tarea. Las mejores prácticas de seguridad sugieren crear un conjunto de grupos de usuarios y asignar los permisos en caso de cambios o recupero de información de cintas y backup, puesto que solamente hay que modificar los permisos de los grupos y no individualmente los de los usuarios, que, serán muchos más en número. En cambio si los permisos son otorgados por grupo, simplemente alcanza con eliminar al usuario del grupo y asignarlo al nuevo, con la automática asignación de permisos al que pertenece.

- Implantación de una Política sobre las cuentas de usuarios: El manual de Seguridad de la organización debe contener, entre sus normas y procedimientos, la política de ABM de Usuarios. En ella se debe especificar los parámetros que deben cumplir la identificación de usuario (como estándar de nomenclatura, responsabilidad del usuario sobre su uso), la cuenta (como vencimiento, bloqueo por inutilización, etc.). El ABM se usuarios consiste en la Alta, Baja y Modificación de usuarios en el sistema, entendiéndose por:

    - Alta de un usuario: Requerimiento de acceso a una aplicación o un servicio para un usuario inexistente;

- Modificación de un usuario, requerimiento de:
    - Diferentes tipos de acceso a las aplicaciones o servicios;
    - Acceso a una nueva aplicación o servicio;
    - Eliminación de acceso a una aplicación o servicio;
- Baja de un usuario: Requerimiento de eliminar los derechos de acceso de ese usuario a toda aplicación o servicio;
- Deshabilitacion de un usuario: Requerimiento de negar los derechos de acceso de ese usuario a toda aplicación o servicio, sin eliminarlo definitivamente del dominio de usuarios; el Dueño de Datos del área o sector al cual pertenece el usuario en el desempeño de sus funciones, debe de solicitar la creación, modificación o borrado de la cuenta de usuario; en una empresa con Help Desk, una operación (ABM) sobre una cuenta de usuario deberá registrarse como un caso y llevarse a cabo según lo establecido en el correspondiente Procesamiento de Administración de Usuarios y Recursos.

Tipos de cuentas de usuarios

Las cuentas de usuarios generadas en cada uno de las aplicaciones deben de contener, al menos los siguientes datos:

- El nombre y apellido completo del propietario de la misma y el área de trabajo, en el caso de los usuarios personales;
- En el caso de las cuentas de servicios debe figurar la función para la que fue creada;
- Debe crearse una cuenta para cada servicio individual con los mínimos privilegios posibles y no utilizar una misma cuenta para varios servicios;

Todo usuario se debe comprometer a:

- Mantener la confidencialidad de la información a la que acceda;
- Utilizar en forma personal y exclusiva su identificación de usuario;
- Responsabilizarse del uso que se haga de su identificación de usuario.

Implantación de una Política de Contraseñas de Usuarios;

- Longitud mínima (por ejemplo de 6 caracteres y sin contener blancos);
- Longitud máxima (por ejemplo de 16 caracteres);
- Vida máxima (para obligar a los usuarios a realizar el cambio de clave cada cierto periodo, por ejemplo 45 días);
- Vida mínima (para evitar que un usuario realice el cambio obligatorio de la clave a su vencimiento y luego vuelve inmediatamente a la clave anterior);
- Cantidad mínima de caracteres numéricos;
- Cantidad mínima de caracteres alfabéticos;
- Cantidad mínima de caracteres especiales ($%&@?)
- Cantidad mínima de caracteres distintos de la ultima contraseña;
- Tiempo mínimo que debe transcurrir antes de reutilizar un password (por ejemplo, un año);
- Cantidad mínima de contraseñas distintas antes de reutilizar una. Es una variante del control anterior, utilizada para el mismo fin;
- Determinar si se debe ser cambiada obligatoriamente la primera vez que el usuario ingrese al sistema;

Además debe de cumplir las siguientes características:

- Debe poder ser cambiada toda vez que el usuario lo requiera;
- No debe ser compartida;
- Se debe preservar su confidencialidad;
- No debe ser fácil de adivinar, para lograr esto existe varias soluciones:
    - Utilizar un software generador de passwords: Utilizar un software que analice la password (por ejemplo comparando la contraseña ingresada por el usuario con una lista contenida en un diccionario de contraseñas prohibidas) y rechace contraseñas fáciles al momento de ingreso;
- Administración de usuarios: Garantizar que todos los usuarios posean los privilegios mínimos necesarios para la realización de su tarea.
- Las practicas recomendadas para la cuentas de usuarios son las siguientes:
    - Renombrar la cuenta de Administrador Local.
    - Deshabilitar la cuenta de Administrador ficticia;
    - Deshabilitar la cuenta de invitado o Guest;
    - Nunca usar cuentas grupales (de uso masivo). Las cuentas deben ser de uso individual exclusivo;
    - Todos los usuarios personales deben autenticarse en el sistema. No se deben permitir cuentas de usuario personales sin password;
    - Establecer una nomenclatura para la denominación de las cuentas de usuarios personales y para los servicios (como por ejemplo utilizar las iníciales del nombre seguidas por el apellido);
    - Utilizar descripciones de usuarios claras y completas que permitan la identificación y clasificación de los usuarios.

Para lograr una adecuada y efectiva implantación de un sistema de grupos y perfiles de usuarios, sin superposición de roles ni de permisos, y con el fin de detectar cualquier inconsistencia, se sugiere relevar los usuarios con sus respectivos permisos y roles en un documento generado para tal fin llamado *Mapa de Usuarios,* que permite la rápida visualización de inconsistencias en la asignación de perfiles.

Mapa de Usuarios

El siguiente documento presenta una alternativa para visualizar, documentar y administrar los grupos de usuarios:

Descripción de los campos

GRUPO: nombre del grupo que se está relevando;

USUARIOS: nombre completo de los usuarios que pertenecen a ese grupo;

NOMBRE DE INICIO DE SESIÓN: por ejemplo: jdominguez;

OTROS GRUPOS A LOS QUE PERTENECE: en este campo se agregan todos los grupos a los que pertenece el usuario, excepto en el que se está definiendo, esto sirve para detectar inconsistencias.

También él ES deberá interiorizarse con los permisos proporcionados por perfil, y deberá verificar que, según la estructura de la organización, ningún usuario está abusando del sistema con permisos que no le corresponden, y, asimismo, que no existan usuarios donde sus accesos estén indebidamente restringidos y así, dificultar o impedir su trabajo.

- Revisión de las cuentas de usuario: El administrador de seguridad debe realizar una periódica revisión de las cuentas de los usuarios del sistema, a fin de detectar usuarios inactivos y realizar las bajas correspondientes, según el procedimiento de seguridad de administración de usuarios;

- Revisión de los permisos de los usuarios: Realizar una periódica revisión de los permisos otorgados sobre el file system y sobre los recursos. Un control básico consiste en restringir los permisos para los grupos genéricos, e ir otorgándolos individualmente o por grupo según la necesidad. En los sistemas operativos de la línea Microsoft Windows el grupo genérico mas abarcado es el llamado Everyone. En la línea de Linux, es Others (el último octeto de los permisos).

- Revisión de los servicios de red: Revisar periódicamente los servicios de red habilitados y eliminar todos aquellos que no se necesiten, en particular los que permiten hacer conexiones remotas o transporte de datos en texto plano (como FTP);

- Revisión de los protocolos de red: Revisar periódicamente los protocolos de red habilitados y eliminar todos aquellos que no se necesiten, en particular los protocolos antiguos e inseguros (como NetBIOS);

- Control del inicio de sesión: Establecer un número máximo de intentos fallidos de inicio de sesión de los usuarios, luego del cual se bloquee la cuenta hasta que el usuario solicite su desbloqueo mediante el procedimiento vigente.

- Nombre del último usuario logueado: Evitar que se muestra la identificación del último usuario que se logueo en el sistema;

- Bloqueo de cuentas de usuario: Las cuentas bloqueadas por intentos fallidos de sesión o por permanecer inactivas durante un periodo determinado deben permanecer bloqueados durante un tiempo, para impedir el inicio de sesión.

A continuación se exponen controles sobre las cuentas de usuarios, que deben estar explicitas en las Normas de Usuarios, y deben ser de conocimiento de todos los usuarios del Sistema:

- Toda cuenta de usuario que haya intentado cuatro (4) veces el acceso al sistema en forma fallida y consecutiva, debe ser automáticamente bloqueada;

- Toda cuenta de usuario que no haya accedido al sistema por un periodo de 60 días será bloqueada y se iniciara la gestión de baja de la misma, que comprende:

    - Verificación por parte de Recursos Humanos y del Dueño de los Datos de la inexistencia del usuario;

    - Aprobación por parte de este ultimo para la eliminación definitiva de la cuenta.

  En caso de comprobar la necesidad de la baja, el Administrador de Seguridad deberá proceder a su inmediata eliminación. Transcurrida una cantidad de días (por ejemplo 120 días) sin utilización de la cuenta, la misma se dará automáticamente de baja.

- Registros de pistas de auditoría o logs: Registrar pistas de auditoría, más conocidas como "logs", con el fin de asegurar un adecuado monitoreo de los eventos que pudieran afectar a la seguridad de la información de la compañía objetivo.

  Toda aplicación utilizada en el entorno productivo debe permitir el registro automático y la explotación de la información de las siguientes pistas de auditoría:

  - Trazas generales a activar en sistemas operativos y equipos de comunicaciones:

    - Intentos exitosos y fallidos de ingreso de usuarios;

    - Desconexión forzada de usuarios;

- Alta, baja o modificación de usuarios, grupos y/o perfiles;
- Cambios en la configuración de la seguridad;
- Instalación del software de aplicación;
- Encendido y apagado de servidores y equipos de comunicaciones;
- Procesos de depuración de información no automatizados,

- Trazas generales a activar en aplicaciones:
  - Intentos exitosos y fallidos de usuarios;
  - Desconexión automática de sesiones de usuario por inactividad;
  - Alta, baja o modificación de usuarios, grupos y/o perfiles;
  - Cambios en la configuración de la seguridad;
  - Instalación del software de aplicación;
  - Procesos manuales de depuración de datos;
  - Las acciones llevadas a cabo por los usuarios especiales.
- Trazas especiales a activar:
  - Todos los accesos a información clasificada como confidencial;
  - Todos los eventos de un usuario cuando sean específicamente solicitados por los Dueños de los Datos;
  - Todos los accesos de aquellas cuentas de usuarios con altos privilegios sobre los sistemas;

Protección de los datos.

Controlar y administrar el acceso de los usuarios sobre los activos lógicos: Se debe administrar correctamente los recursos lógicos como archivos, bases de datos, programas de software y data warehouses, y llevar un control sobre ellos para detectar posibles accesos no autorizados, hurto de datos o descubrimiento de información.

Para este fin se propone la elaboración de una tabla que refleje la asignación de permisos sobre los activos lógicos por perfil y por usuario.

Este documento llamado *Tabla de Permisos Sobre Activos Lógicos* se exhibe a continuación: Llevar un adecuado control y documentación de los cambios realizados en el software ya sea:

- Una actualización;
- Un cambio de plataforma;
- Agregados de funcionalidad.

Todos los cambios se registran adecuadamente en el ABM Activos, como se especifica en la etapa 4.5 Control de Cambios de esta metodología y en el Documento de Actualización de Software.

A continuación se presenta el *Documento de Actualización de Software* para su actualización cuando se realicen puntualmente actualizaciones de software (upgrades). Este documento que tiene como fin especifico ayudar al administrador a controlar el proceso de actualizaciones de software en forma masiva.

Por ejemplo, cuando se actualiza el software antivirus, que es una tarea ardua ya que mucho programas no permiten que las actualizaciones sean instaladas por usuarios sin permisos de administrador, este es el que debe pasar maquina por maquina instalando software. El Documento de Actualización de Software se usura como ayuda para el control de las actualizaciones registrando cada máquina a medida que se avanza con las Workstation de la red.

Documento de Actualización de Software

- Control de impacto del nuevo software: Antes de instalar nuevo software en los equipos se realiza un control de compatibilidades y aprobación por parte de gerencia:
    - Controlar las licencias de software de actualizaciones;
    - Verificar los requerimientos de capacidad de procesamiento y almacenamiento del nuevo software;
    - Verificar compatibilidad con la plataforma de hardware utilizada;
    - Preparar los ambientes para la actualización;
    - Realizar pruebas de instalación antes de la instalación definitiva;
    - Verificar la compatibilidad del nuevo software con otros elementos existentes;
    - Capacitar a los usuarios.
- Instalación y continua actualización de software de detección y reparación de antivirus
    - Comprobar diariamente la existencia de nuevo software antivirus y sus actualizaciones (y documentar las actualizaciones en el ABM Activos y en el Documento de Actualizaciones de Software);
    - Comprobar la ausencia de virus antes de utilizar archivos transportados a través de la red, o en medios magnéticos como zips, u otros.
    - Comprobar la ausencia de virus en archivos adjuntos a mensajes en los servidores de mail;

- Comprobar la ausencia de virus en los archivos bajados de internet antes de su ejecución o instalación;
- Realizar planes de continuidad de los negocios ante ataques de virus.

- Realización de copias de seguridad (backups):
  - Guardar en forma segura los datos críticos, información de recuperación de sistemas y registros exactos de las aplicaciones en forma periódica;
  - Mantener siempre al menos los tres últimos ciclos de backup;
  - Comprobar periódicamente los medios de almacenamiento de los backups (cintas) para garantizar una recuperación exitosa;
  - Comprobar periódicamente el correo funcionamiento de las unidades de cinta para la recuperación de datos desde los medios físicos de almacenamiento;
  - Verificar los procedimientos y procesos de recuperación a partir de los backups, para garantizar su eficacia y la adecuada restitución del sistema ante eventualidades;
  - Borrar en forma segura el contenido de los dispositivos de backup que estén fuera de uso o que contengan información vencida;
  - Volcar el procedimiento de backup a un documento para el registro y control de las unidades de almacenamiento, y su relación con el contenido electrónico;

Aquí se presenta un registro para llevar ese control de forma ordenada: *el Inventario de Backup*.

Inventario de Backup

El ES determinará la técnica más conveniente para realizar el Backup en su sistema objetivo.

Para la aplicación de cualquier técnica él ES deberá documentar el resguardo de datos que hizo y proteger ese documento con claves u otros métodos para prohibir su acceso a extraños.

- Establecer en forma univoca los permisos otorgados a cada perfil de usuario para evitar accesos no autorizados en los distintos entornos:
    - Archivos;
    - Bases de datos;
    - Aplicaciones;
    - Servicios.
- Protección de la documentación del sistema:
    - Almacenar la documentación del sistema en forma segura: bajo llave en archivos o armarios de acceso restringido;
    - Los documentos de administración de la seguridad deben estar protegidos de manera especial y solo debe tener accesos a ellos el o los responsables correspondientes. Son de critico manejo los siguientes documentos:
        - La Política de Seguridad;
        - Los Manuales de Procedimientos;
        - Los Estándares de Seguridad;
        - El Mapa de Vulnerabilidades;
        - El Diario de Incidencias.

- Proteger la documentación del sistema almacenada en una red local, implementando un sistema de acceso o privilegios por perfil;
- Suministrada a través de una red pública con métodos seguros:
    - Permitir solo acceso a la lectura de los documentos;
    - Implementar un sistema de verificación de integridad de los archivos contra las modificaciones no autorizadas;
    - Implementar métodos de intercambio de información seguro, protegiendo la confidencialidad de los datos;
    - Aplicar otros métodos que garanticen integridad de los datos, según la necesidad;
    - Ejemplos de herramientas que se pueden utilizar para lograr esto son: aplicar funciones HASH, aplicar MAC (Message Authentification Code) e implementar IPSec.
- Protección de la información publicada en la Web: la información publicada en Internet debe ser protegida contra modificación, ya que si se ve afectada la integridad de las publicaciones, la seguridad de la empresa y su reputación estarán en juego.
- Protección de correo electrónico: Implementar técnicas de encriptación de mensajes o firma digital para el intercambio seguro de correo electrónico.
- Protección del trafico cliente-servidor: Proteger el trafico entre equipos clientes y servidores mediante el recurso adecuado según corresponda:
    - Firma digital:
    - Cifrado de paquetes;

        - Autentificación Kerberos:
        - Métodos de Hash.
    - Protección del tráfico de los vínculos: Proteger el tráfico entre equipos distantes mediante el cifrado de paquetes.

3.3.1.3 Protección a nivel de la organización.

Se analiza en esta parte la protección de los distintos Activos a nivel de la organización. Se deben considerar algunos de los siguientes puntos:

- Elaboración/adecuación de una Normativa de seguridad: A nivel de la organización, el primer paso en la protección del entorno es establecer la normativa que dicte los lineamientos sobre los procedimientos, las tareas y procesos informáticos. La normativa se materializa en un "Manual de Seguridad" compuesto por:
    - La Política general de Seguridad;
    - Las Normas;
    - Los procedimientos;
    - Los estándares técnico;
    - Los Manuales de usuarios.
- Determinación de la necesidad de un cambio en la estructura de la organizacional:
    - Crear un sector dedicado a la seguridad informática: Si la empresa en cuestión no presenta la estructura organizacional que soporte el siguiente esquema de responsabilidades, será tarea de ES diseñar y proponer una serie de responsabilidades a crear en la organización,

pudiendo implicar la creación de un área de Seguridad Informática y una de Control Interno o Auditoria:

- Determinar los roles y responsabilidades: este proyecto consiste en dar una razonable protección a la información a través de la correcta administración de la seguridad por parte de los responsables asignados a cada una de las funciones dentro de la compañía objetivo.

A continuación se define los roles y responsabilidades de cada una de las funciones relacionadas con la seguridad:

Dueño de los datos

Se llama Dueño de los Datos a todo Director y/o Gerente de cada área de la empresa responsable sobre la información correspondiente a su ámbito de trabajo. El Dueño de los Datos podrá asignar las tareas de administración y control de las medidas de seguridad del área, a un colaborador, quien recibe el nombre de Dueño de los Datos Delegado. Son sus principales responsabilidades:

- Identificar toda la información de su área, cualquiera sea su forma y medio de conservación;
- Clasificar su información de acuerdo a su grado de criticidad, documentando y actualizando periódicamente esta clasificación;
- Determinar qué usuarios de su área pueden acceder a su información, asegurando que cada uno tenga garantizado el ingreso a los datos de acuerdo a sus respectivas funciones, y en el marco de lo especificado por la Norma de Administración de Usuarios, Accesos y Recursos;
- Proponer los eventos de seguridad adicionales que considere necesarios para proteger su información.

Oficial de Seguridad

El Oficial de Seguridad es quien tiene a su cargo la definición y el mantenimiento del marco normativo y el asesoramiento a todo el personal de la compañía para su implantación. En relación a esta función, es responsable de:

- Implantar un programa de concientización permanente de usuarios sobre la seguridad de la información y su mantenimiento a futuro;
- Mantener actualizada la normativa de seguridad y la lista de todos los Dueños de los Datos/ Delegados;
- Asistir al Administrador de Seguridad en la implantación de la normativa de seguridad informática;
- Participar en la investigación y recomendación de productos de seguridad en conjunto con el área de Sistemas, para la implantación de las medidas de seguridad en los sistemas;
- Participar en el proceso de evaluación de los riesgos emergentes ante una situación de interrupción no prevista del procesamiento de sistemas, definición de las distintas estrategias de recuperación, y en la prueba e implantación de los planes de recuperación ante desastres definidos;
- Participar en el diseño, desarrollo, mantenimiento o adquisición de sistemas de aplicación en cuanto a: Identificación y evaluación de los controles automatizados del sistema, menúes de usuarios y controles manuales adicionales a incluir en los procedimientos que acompañen a su operatoria.

Administrador de Seguridad

Se define como tal a la persona que tiene a su cargo la ejecución de las medidas de seguridad en algún equipo de procesamiento, servicio y/o aplicación. Sus principales responsabilidades relacionadas con la protección de la información son:

- Administrar todas las solicitudes de alta, baja y modificación de permisos relacionados con los accesos de los usuarios a los respectivos equipos y aplicaciones;

- Implantar en los sistemas todos los parámetros definidos en las normas, procedimientos y estándares específicos;

- Asistir a los usuarios en las tareas relacionadas con la protección de los datos;

- Analizar e informar cualquier evento que atente contra la seguridad informática, así como controlar periódicamente que solamente los usuarios autorizados posean acceso a los recursos.

Operador Responsable

Se establecen como Operadores Responsables de la información a:

- Los responsables de los archivos centralizados de la información en soportes.

- Los responsables de los Centros de Procesamiento de Datos o de los sitios donde se encuentren los equipos de procesamiento centralizado, de comunicación y/o de almacenamiento;

- Implantar las medidas de seguridad física definidas para la protección de la información en la normativa correspondiente;

- Disponer la efectiva custodia de las claves de mayor riesgo de los equipos/servicios/aplicaciones conservadas en medios impresos.

Comité de Cambios

- Planificar, priorizar, autorizar y coordinar las tareas a realizar por los distintos involucrados ante la necesidad de realización de cambios de sistemas en producción;

- Definir los criterios sobre los cuales se realiza la evaluación de impacto y criticidad de los cambios;

- Liderar los procesos de cambio a realizar ante situaciones de emergencia;

Usuarios

Se considera como tales a todos los sujetos que hacen uso de los equipos, servicios y aplicaciones y de la información de la empresa, para poder cumplir con sus respectivas tareas. Son sus responsabilidades: Cumplir con todas las medidas de seguridad definidas en el Manual de Seguridad; Resguardar los soportes de información que conserven en su poder, según lo establecido en el Procedimiento de Tratamiento de la Información; Firmar el Compromiso de Confidencialidad de la Información. Implantación de políticas para evitar ataques internos:

"El 80% de los fraudes, robos, sabotajes o accidentes relacionados con los sistemas informáticos son causados por el propio personal de la organización propietaria de dichos sistemas, lo que se suele denominar *insider factor*" esto significa que la mayoría de los ataques a los sistemas informáticos son perpetrados por el propio personal que trabaja actualmente en la empresa, o que ha trabajado con anterioridad [Antonio Villalón Huerta, 2002].

Estas son personas con envidia, codicia o ex empleados que desean vengarse por haber sido despedidos o por otras disconformidades. Las personas que trabajan en el área de administración de los sistemas, de redes o en desarrollo, tienen conocimiento de claves, formas de acceso, ubicación de información crítica y hasta tienen conocimiento de las fallas y debilidades del sistema. Es por esto que se aconseja tomar medidas preventivas acerca de esta realidad:

- Mínimo privilegio: A cada usuario se le debe otorgar el mínimo privilegio que necesita para realizar su actividad;

- Conocimiento parcial: Las actividades críticas de la organización deben ser conocidas y realizadas por varias personas competentes para que puedan respaldarse en caso de incidencias como accidentes o viajes.

- Rotación de funciones: Para evitar la complicidad de dos responsables, o evitar el mutuo sabotaje si están enemistados;

Implantación de políticas de escritorios y pantallas limpias:

- Implementar una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles para evitar robos, pérdidas o daño de la información, y protegerla de desastres naturales.

- Implementar una política de pantallas limpias para reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

Separación de las instalaciones de desarrollo, de prueba y producción:

- Es fundamental separar físicamente las instalaciones de desarrollo, prueba y producción para evitar confusiones, pérdida de información y fallas en la confidencialidad de los datos.

- Se debe trabajar en instalaciones separadas que garanticen integridad en el ambiente de desarrollo, estabilidad en el ambiente de pruebas y confidencialidad en al ambiente de producción u operación.

Autorizados al software operativo y a los datos del negocio.

- Registrar fecha y hora de entrada y salida del personal

Protección de las instalaciones.

Implantación de medidas de protección para el transporte de activos:

- Utilizar medios de transporte o servicios de mensajería confiables;
- Crear una lista de servicios de mensajería autorizados e implementar un procedimiento para verificar la identificación de los mismos;
- Proteger el bien contra eventuales daños físicos durante el tránsito con un adecuado embalaje, siguiendo las especificaciones de los fabricantes o proveedores;
- Adoptar controles especiales para proteger la información sensible contra divulgación o modificación no autorizadas;

Protección de las operaciones de comercio electrónico: Las transacciones de comercio electrónico comprenden un intercambio de información delicada, como precios, números de tarjetas de crédito, crédito disponible de un usuario, y otros datos personales como dirección, número de teléfono, número de documento, y hasta preferencias personales. Para prevenir el mal uso de nuestros datos, su manipulación o modificación, se debe hacer uso de herramientas y aplicar técnicas que lo eviten. Estas técnicas deben garantizar:

- Autenticación del cliente y el comerciante;
- Autorización para fijar precios, emitir o firmar los documentos comerciales;
- Confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos en los procesos de oferta y contratación;
- Confiabilidad y autenticación en la información sobre precios y descuentos;
- Confidencialidad e integridad de los datos suministrados con respecto a órdenes, pagos y direcciones de entrega, y confirmación de recepción en las transacciones de compra;
- Verificación de los datos del cliente;
- Cierre de la transacción;

- Determinar la forma de pago más adecuada para evitar fraudes;
- Confidencialidad e integridad de la información sobre órdenes de compra para evitar la pérdida o duplicación de transacciones;
- Determinar quién asume el riesgo de eventuales transacciones fraudulentas;

  Para implementar estas medidas se puede hacer uso de alguna de las siguientes herramientas:

  - Firma digital;
  - Encriptación de datos;
  - Certificados digitales;
  - IPSec;
  - SET (Secure Electronic Transaction).

El ES determinara, según el caso, la forma más adecuada de llevar a cabo esta tarea.

Protección del correo electrónico:

- Determinar cuáles son las cuentas no autorizadas para intercambio de correo;
- Determinar las consideraciones legales aplicables:
  - Publicación de direcciones corporativas;
  - Filtrado de contenido de los mensajes;
  - Necesidad de prueba de envió, origen, entrega y aceptación;

- Determinar las acciones aplicables a correo entrante al dominio para usuarios desconocidos;

Implantación de un proceso de autorización para la publicación de información electrónica de la empresa:

- A través de la publicación de páginas en Internet;
- A través de la difusión de noticias y contenido en mensajes de correo electrónico;

3.3.2 Aprobación del Plan de Aseguramiento

Una vez elaborado el plan de Aseguramiento, el cliente debe dar su aprobación para su implantación.

Como todo proyecto, debe estar acompañado del apoyo del nivel gerencial y de los responsables directos involucrados.

El proceso de aprobación variará según las costumbres y políticas del cliente, pero en todos los casos va acompañado de la asignación de un presupuesto a invertir en los recursos asignados en la planificación.

3.4 IMPLANTACION

Culminadas las fases correspondientes a la primera parte de esta metodología, el estudio del entorno, se da comienzo al segundo y último grupo de fases llamado Implantación de la solución. Dentro de este grupo se encuentra la fase que da título al presente capítulo. En el mismo se desarrolla la implantación de la solución.

En esta fase se lleva a la práctica lo planificado realizando los controles y ajustes necesarios según lo relevado anteriormente.

A su vez, y como en todo este trabajo, este capítulo se divide en etapas que describen tareas.

Se pretende llevar un orden en la ejecución de las etapas aquí presentadas, pues es de particular importancia para seguir el razonamiento desarrollado en esta tesis.

Las etapas a desarrollar son las siguientes:

- Elaboración de Relevamiento de Activos.
- Clasificación de la Información.
- Elaboración/adaptación de la Normativa de Seguridad.
- Publicación de la Normativa de Seguridad.
- Implantación del Plan de Aseguramiento.
- Elaboración del Plan de Recuperación del Entorno ante Desastres.

Cada una tiene un objetivo específico e individual, que contribuye en parte a lograr el objetivo de la fase, que es la implantación de las medidas de seguridad planificadas.

El ES considerará la necesidad de implementar todas o alguna de las etapas propuestas, pero de hacerlo, deberá respetar el orden sugerido ya que las tareas que se desarrollan alimentan muchas veces a otras que les siguen, aunque no necesariamente deben estar todas presentes.

La Clasificación de la Información no puede realizarse sin un relevamiento de los activos físicos y lógicos de la Organización, aunque no es estrictamente necesario que se formalice esto en un inventario como se sugiere en la etapa 4.1.

Más allá de la interdependencia entre etapas, la fase debe interpretarse como la unidad en la que se pretende materializar las medidas planificadas para lograr el aseguramiento del entorno.

3.4.1 Elaboración del Relevamiento de Activos.

Para mantener una adecuada protección de los activos de la organización se debe rendir cuentas por todos los recursos de información importantes y se debe designar un propietario para cada uno de ellos, según [ISO 17799] "

En esta etapa de la MSEI el Experto en Seguridad realiza un detallado relevamiento de los bienes o activos en posesión de la organización objetivo.

Para el desarrollo de esta tarea se presenta una tabla para la documentación de la existencia de los recursos de hardware, software y la información de una empresa y su clasificación, según su criticidad.

3.4.1.1 Inventario de Activos

El Inventario de Activos aquí propuesto pretende llevar una contabilidad de los bienes de la organización en cuestión, clasificándolos según el nivel de protección que cada uno necesita, según la valorización de los responsables. Se hará distinción entre los elementos físicos o tangibles y los lógicos o intangibles (como la información).

Para este fin se propone la elaboración de un *Inventario de Activos Físicos*, y un *Inventario de Activos Lógicos*.

El Inventario de Activos Físicos contendrá los siguientes elementos:

Elementos de hardware:

- Equipamiento informático: monitores, módems;

- Equipos de comunicaciones: routers, PABXs, hubs, switches, etc.;
- Medios magnéticos: cintas y discos removibles;
- Periféricos: impresoras, máquinas de fax, contestadores automáticos;
- Cableado: cables internos y externos;
- Mobiliario, lugares de emplazamiento;
- Se hará una distinción especial sobre las CPUs para facilitar su identificación.

CPUs: Se establece una distinción del resto de los elementos de hardware para su fácil identificación.

- Procesadores, computadoras portátiles.

Asimismo el Inventario de Activos Lógico contendrá estos elementos:

Elementos de software:

- Sistemas operativos;
- Software de aplicaciones;
- Software de sistemas;
- Herramientas de desarrollo;
- Utilitarios.

Servicios:

- Servicios informáticos;
- Servicios de comunicaciones;

- Servicios generales (calefacción, iluminación, energía eléctrica, aire acondicionado)

Datos:

- Bases de datos;
- Archivos;
- Documentación de sistemas.

Información archivada

- Backups:

3.4.1.3 Rotulación de activos

Luego de la clasificación de la información y de la elaboración del inventario de Activos Lógicos y del Inventario de Activos Físicos se procede a la identificación de los activos por medio de rótulos o labels. La ventaja de llevar actualizado los inventarios es que de esta forma se pueden rotular los activos con el código asignado en el Inventario, y no con la descripción explícita. Este mecanismo es muy útil para proteger la información contra hurtos y sabotajes. Un ejemplo claro es el caso de las cintas de backup. Si una cinta de backup contiene una indicación clara de la información que contiene, su criticidad, la fecha en que se realizó, etc.

3.4.1.4 Análisis de Criticidades

El análisis de criticidades es el paso previo a la Clasificación de la Información. Para clasificar la información de acuerdo a algún rango establecido en primer lugar hay que establecer cuán crítico es el activo en cuestión.

La criticidad se puede expresar mediante la necesidad de conservar tres atributos: La autenticidad; La disponibilidad; La integridad.

Cada Dueño de los Datos debe analizar su información para proceder a su clasificación, basándose principalmente en los perjuicios que pudiera ocasionarle a la Compañía objetivo y/o a su personal, el incumplimiento de alguno de los valores establecidos en la Política General.

La clasificación de la información debe estar sustentada por los siguientes criterios básicos:

- El valor estratégico de la información para la Compañía;
- La ventaja competitiva que puede darles a terceros su conocimiento;
- Los criterios específicos que definan las autoridades de la Compañía;
- Las leyes y reglamentaciones vigentes.

Asimismo, el impacto y probabilidad de una pérdida en seguridad se pueden clasificar en cuatro niveles:

- **Nivel 3:** Alto riesgo; Daño irreparable, Impacto a nivel corporativo de 2 a 5 años. Es un objetivo de ataque de alta probabilidad;
- **Nivel 2:** Nivel 2: Daño Significativo. Impacto a nivel de país de la empresa / sede hasta 2 años. Es un objetivo posible.
- **Nivel 1:** Daño Moderado. A nivel departamental. Impacto de menos de 1 año. Es un objetivo poco probable;
- **Nivel 0:** Ningún Daño. Con licencia completa. Dominio público. No es un objetivo de ataque.

3.4.2 Clasificación de la Información

La Clasificación de la Información de la Compañía debe estar alineada a la Política de Seguridad de la compañía, y se debe definir para cada una de las áreas de negocio. El tratamiento de la Información debe responder a su clasificación.

3.4.2.1 Identificación de la información

Los gerentes de las áreas o de las divisiones, que son Dueños de los Datos, tienen la responsabilidad primaria de clasificar la información y protegerla adecuadamente. La clasificación de datos y los procedimientos de manejo especial se usan para proteger los datos de divulgaciones no autorizadas.

Cada Dueño de los Datos debe identificar toda la información que se genera dentro del área que maneja, en todas sus formas y medios, tales como:

- Documentos propios y/o de terceros;
- Información en los sistemas/equipos de procesamiento, individuales y/o centralizados;
- Informes, reportes y listados;
- Medios magnéticos móviles;
- Cualquier otro soporte físico que contenga información.

La dirección de la empresa debe evaluar la probabilidad y el impacto producto de la divulgación, modificación y/o pérdida de información, como base para determinar el valor de la información.

Cada organización deberá establecer las categorías adecuadas para la clasificación de la información que maneja. En algunos casos manejara información confidencial, en otras será restringida o pública.

3.4.2.2 Tipos de información

Existen muchos modelos de clasificación de la Información, unos más populares que otros. Es importante entender el negocio de la empresa objetivo para

determinar el que más se ajusta a su realidad. Entre los modelos más utilizados está el siguiente, en el que la información se puede clasificar en tres categorías:

- **Restringida:** Información de acceso medianamente restringido (utilizada por usuarios de rango medio, empleados) sobre la que es necesario realizar suficientes controles para garantizar el acceso adecuado;
- **Pública:** Información de acceso libre, sobre la que se realizan los mínimos controles (información disponible para la comunidad);
- **Privada:** relacionada con los individuos, tal como evaluaciones de desempeño, compensaciones y beneficios, carpetas personales o registros médicos;
- **Uso Interno:** relacionada con la operatoria diaria, como por ejemplo planes de viajes y reuniones, iniciativas de proyectos, distribución física de usuarios y recursos, precios y demarcaciones.

3.4.2.3 Beneficios de la clasificación de la información

- Mejora de forma continúa la seguridad de la información;
- Establece los principales controles necesarios para evitar accesos externos o Internos no autorizados a la información;
- Brinda medidas de control para la protección de datos de carácter personal;
- Posiciona la utilización del correo electrónico e Internet como una herramienta de trabajo.

3.4.2.4 Riesgos de la información

Para establecer una clasificación es necesario realizar el paso previo según esta metodología, que consiste en hacer un análisis de la criticidad de los Activos lógicos y físicos.

Asimismo, el Dueño de los Datos debe identificar los riesgos a los cuales está expuesta su información, teniendo en cuenta la posibilidad de que personal interno y/o externo realice:

- Divulgación no autorizada;
- Modificación indebida;
- Destrucción de los soportes.

3.4.3 Elaboración/ adaptación de la Normativa de Seguridad

3.4.3.1 Interiorización del experto con la política y negocio de la organización

Para la elaboración o adaptación de un adecuado Marco Normativo él SE debe interiorizarse con el manejo del negocio, la estructura de la organización, la jerarquía de la empresa y el manejo de los empleados, pero sobre todo debe interpretar y conocer la estrategia de la empresa y sus políticas implícitas sobre el manejo de la información.

3.4.3.2 Elaboración/adaptación de la Normativa de Seguridad

En esta etapa de la MSEI, el Experto de Seguridad determinará si es conveniente hacer una adaptación de la Normativa de Seguridad, si existiera, o si se inclina por la elaboración de una nueva. La Normativa de Seguridad es el marco que regula el comportamiento de las personas en la empresa, su forma de trabajar y de efectuar las tareas que involucran los recursos del entorno informatizado.

El conjunto formado por los documentos que componen la Normativa de seguridad es llamado *Manual de Seguridad* de la empresa. El Manual de Seguridad está formado por la Política de Seguridad, las Normas, los Procedimientos, los Instructivos y Estándares técnicos.

La política de Seguridad es la más general. Contiene los lineamientos y definiciones independientes de plataformas y tecnologías. Las normas son

también leyes pero más puntuales que las políticas. Las normas generalmente tratan temas específicos a alto nivel. Los Procedimientos, en cambio bajan el nivel a una serie de pasos a seguir, siempre independientemente de la plataforma con que se trabaje. Los Esquemas, en cambio son procedimientos dependientes de la tecnología, por lo que se debe especificar la plataforma, sistema operativo o aplicativo para el que se deba aplicar.

Finalmente, los Estándares técnicos son documentos que describen la configuración de cierto sistema, aplicación o hardware. Por ejemplo se puede establecer un estándar técnico para la configuración de los servidores, para que cada vez que se dé de alta a un nuevo servidor se garantice que siguiendo ese estándar se obtendrá la misma configuración de los demás servidores, ayudando a la automatización, por medio de scrips, de dicha configuración.

Para la elaboración del Manual de Seguridad de la Información, que es el conjunto de documentación que avala el Marco Normativo de una empresa, el Experto en Seguridad debe de realizar un relevamiento de aspectos organizados y políticos, además de los técnicos.

El Experto de Seguridad deberá descubrir la forma de comunicación que maneja la empresa, sobre todo deberá estudiar el lenguaje que emplea la alta gerencia para emitir sus comunicados detectando la forma gramatical que se utiliza para las expresiones imperativas y las enunciativas.

Debe prestar especial atención en esto, ya que la Política y las Normas son enunciadas con carácter exclusivamente imperativo, ya que son leyes a cumplir algunas veces por gran parte del personal y en su mayoría por todos. La forma en que se enuncien las oraciones será crucial para las futuras auditorias, al mal momento de verificar el cumplimiento de las Normas.

3.4.4 Política de Seguridad

La Política de Seguridad es un documento que establece las pautas, según el enfoque de la organización y su negocio, en cuanto a la gestión de la seguridad.

La Política de Seguridad contiene los principios de seguridad sobre los cuales deben basarse las normas, procedimientos y estándares detallados. Debe ser conocida y acatada por todos y cada uno de los miembros de la organización, y debe ser concebida bajo el total consentimiento y apoyo de la gerencia.

Entre estos principios se encuentran:

- Eficacia: Garantizar que toda información que sea utilizada es necesaria y entregada de forma oportuna, correcta consistente y útil para el desarrollo de las actividades;
- Eficiencia: Asegurar que el tratamiento de la información se realice mediante una optima utilización de los recursos humanos y materiales;
- Confiabilidad: Garantizar que los sistemas informáticos brinden información correcta para ser utilizada en la operatoria de cada uno de los procesos;
- Integridad: Asegurar que sea procesada toda la información necesaria y suficiente para la marcha de las actividades en cada uno de los sistemas informatizados y procesos transaccionales;
- Exactitud: Asegurar que toda la información se encuentre libre de errores y/o irregularidades de cualquier tipo;
- Disponibilidad: Garantizar que la información y la capacidad de su tratamiento manual y automático, sean resguardados y recuperados eventualmente cuando sea necesario de manera tal que no se interrumpa significativamente la marcha de las actividades;
- Legalidad: Asegurar que toda la información y los medios físicos que la contienen, procesen y/o transporten, cumplan con las regulaciones legales vigentes en cada ámbito;

- Confidencialidad: Garantizar que toda la información este protegida del uso no autorizado, revelaciones accidentales, espionaje industrial, violación de la privacidad y otras acciones similares de accesos de terceros no permitidos;

- Autorización: Garantizar que todos los accesos a datos y/o transacciones que los utilicen, cumplan con los niveles de autorización correspondientes para su utilización y divulgación;

- Protección Física: Garantizar que todos los medios de procesamiento y/o conservación de información cuenten con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado;

- Propiedad: Asegurar que todos los derechos de propiedad sobre la información utilizada en el desarrollo de las tareas, estén adecuadamente establecidos a favor de sus propietarios;

- No Repudio: Garantizar los medios necesarios para que el receptor de una comunicación pueda corroborar fehacientemente la autenticidad del emisor.

3.4.4.1 Ámbitos de aplicación y personal afectado

La Política de Seguridad, junto con sus extensiones, como los Manuales de Procedimiento y Estándares de Seguridad, formaliza las medidas a implementar en los distintos ámbitos determinados en el Alcance de la documentación respectiva, y que afecta a:

- Personal efectivo del área de sistemas;

- Personal efectivo de otras áreas;

- Personal de mantenimiento;

- Externos (soporte de hardware, contratistas, etc.);

- Pasantes;

- Consultores;
- Clientes.

3.4.5 Normas y Procedimientos

Una Norma es toda definición concreta sobre cada uno de los temas de seguridad que luego serán adaptados a cada servicio informático en forma específica.

Un Procedimiento es toda especificación de las pautas a seguir para el desarrollo de una tarea en particular. Incluye el desarrollo de instrucciones operativas y procedimientos apropiados de respuesta a incidencias y recuperación de las prestaciones frente a una catástrofe.

Ambos son independientes de la plataforma, y lo suficientemente genéricos como para poder ser aplicados en distintos entornos.

Las Normas y Procedimientos deberán contener:

- Definición de la seguridad de la información, sus objetivos y alcance generales;
- Declaración del propósito de los responsables del nivel gerencial, apoyando los objetivos y principios de la seguridad de la información;
- Explicación de la Políticas, principios, normas y requisitos de cumplimiento en materia de seguridad, que son especialmente importantes para la organización;
- Definición de los responsables en materia de gestión de la seguridad de la información:
- Definición de los responsables sobre los activos afectados:
    - Hardware;

- CPUS;
- Software o servicios o datos;
- Backups.

- Definición del procedimiento a seguir ante la ocurrencia de incidencias relativos a la seguridad;
- Referencias a documentos que puedan respaldar la política, por ejemplo:
  - Estándares de Seguridad más detallados para sistemas de información específicos o normas de seguridad que deben cumplir los usuarios;
  - Instructivos que definen la forma de proceder ante la sucesión de ciertos eventos, la administración de las contraseñas, el uso de los recursos específicos y el manejo de los datos;
  - Normativa internacionales

3.4.5.1 Espectro de las Normas y los Procedimientos

En un entorno informatizado se pueden generar Normas y Procedimientos en los distintos aspectos de la seguridad, haciendo foco en los niveles físico, lógico y de la organización.

Un Marco Normativo completo está compuesto por Políticas, Normas y sus respectivos Procedimientos, Instructivos y Estándares.

En general, se puede elaborar la normativa abarcando los siguientes tópicos, siempre dependiendo del negocio y de la estructura de la organización objetivo:

A nivel físico

- Correo electrónico;

- Uso de internet;
- Uso de antivirus;
- Seguridad física;
- Seguridad del entorno, centro de cómputos, oficinas, escritorios, etc.;
- Backups;
- Separación física de ambientes de procesamiento, controles y documentación;
- Destrucción de información;
- Destrucción de la información contenida en distintos soportes magnéticos, borrado seguro y eliminación de medios impresos;
- Utilización de equipos;
- Utilización de celulares;
- Recuperación del Entorno de Desastres;
- Administración de la Seguridad de Acceso;
- Reinicio de sistemas: para procesos críticos de tiempo real o que poseen un alto nivel de disponibilidad los cuales deben ser reiniciados bajo condiciones especificas y siguiendo procedimientos especiales;
- Eliminación segura de salidas de tareas fallidas: se establece las pautas para terminar procesos o tareas de las que dependen o de las que esperaba un resultado.

A nivel lógico

- Clasificación y manejo de la información;

- Modo de procesamiento de los datos;
- Acceso a datos;
- Administración de usuarios;
- Administración de contraseñas;
- Procedimientos de solicitud de permisos de usuarios;
- Desarrollo de software;
- Requerimientos de programación (schedulling), incluyendo dependencias con otros sistemas, tiempos de inicio de primeras tareas y tiempos de terminación de ultima tareas;
- Separación lógica de ambientes: requerimiento de metodologías de desarrollo de software, ciclo de vida;
- ABM aplicaciones;
- Uso de software;
- Normas para el manejo de salidas (outputs), como el uso de papelería especial o la salidas administración de salidas confidenciales;
- Continuidad del procesamiento – Recuperación del Entorno ante Desastres;
- Administración de registros de eventos de auditoría;
- Conexión a la LAN;
- Conexiones de Terceros;
- Accesos Remotos;
- Concientización y capacitación;

- Normas para usuarios;
- Seguridad en Bases de Datos;
- Administración de la Seguridad de la Red;
- Intercambio de archivos a través de la red;
- Acuerdo de Confidencialidad.

A nivel de la organización

- Responsabilidad de Seguridad;
- Licencias legales de software;
- Auditoria de sistemas;
- Administración y respuesta ante incidencias;
- Denominación de responsables sobre los activos de la empresa;
- Identificación y registro de cambios en el sistema;
- Procedimiento de aprobación formal de los cambios propuestos;
- Comunicaciones a usuarios;
- Puestas operativas: reglas para la transferencia de software desde el ambiente de desarrollo hacia el ambiente de prueba y al de producción;
- Procedimiento de ABM de usuarios.

3.4.6 Publicación de la Normativa de Seguridad

Luego de la aprobación correspondiente, se debe dar a conocer el Manual de Seguridad de la organización.

En esta etapa se deben firmar los convenios de confidencialidad existentes y la confirmación de lectura y conocimiento de las Normas por parte de los usuarios, si así se haya dispuesto.

Es recomendable que esta etapa dispare el comienzo de la fase de concientización y capacitación de usuarios como se sugiere en esta metodología.

3.4.6.1 Implantación de una campaña de concientización

Para lograr el conocimiento del Manual de seguridad y su correcta interpretación se debe realizar una campaña de concientización para que los usuarios adquieran los conceptos de Seguridad que se defienden a través de la normativa, y comprendan la importancia de de su implantación.

La protección de la información debe convertirse en un factor cultural dentro de la empresa. Los usuarios deben incorporar los conceptos a su desenvolvimiento diario para realizar su trabajo cumpliendo con prácticas seguras de manera casi implícita. Para ello la campaña de concientización debe remachar en conceptos como la confidencialidad, la legalidad, la autorización, la información de incidencias, etc.

Para lanzar una campaña de concientización se puede recurrir a herramientas de marketing, como publicación de afiches, reparto de pines, elementos de escritorio y librería, mensajería masiva, publicación de noticias, foros de discusión, cursos y seminarios, charlas informales y cafés inductivos que promuevan conceptos e incentiven a la incorporación de prácticas que lleven a la implantación de la seguridad.

3.4.6.2 Capacitación de los usuarios

Además de la concientización, se debe realizar una adecuada capacitación de los usuarios que garantice que poseen los conocimientos mínimos para el manejo de

la información y la implantación de las medidas impuestas en las Normas de Seguridad vigentes.

Es responsabilidad de la empresa y no de los usuarios en particular la capacitación técnica y administrativa correspondiente.

En particular, las personas que tienen asignados roles específicos de Seguridad, o que intervengan en el manejo de la información deberán informarse de sus que intervengan en el manejo de la información deberán informarse de sus un convenio de confidencialidad o firmando la lectura y aceptación del marco Normativo de la Organización. En los casos en que sea preciso una capacitación formal, como en los aspectos técnicos, se debe garantizar la adquisición de los conocimientos necesarios para poder implementar las Normas correspondientes, proveyendo a los usuarios de los medios educativos adecuados (cursos, manuales, bibliografía, etc.).

3.4.7 Implantación del Plan de Aseguramiento

En esta etapa se implantarán todas las medidas planificadas especialmente para el entorno objetivo, y específicamente en cada nivel estudiado: físico, lógico y de la organización. Cada tarea desarrollada en esta etapa implica un período de pruebas o revisión de los controles efectuados. Así, por ejemplo luego de efectuar una restricción de permisos de usuarios se debe realizar una revisión sobre los accesos para verificar su correcta asignación, y una prueba de acceso a los recursos para detectar excesos de autorización o restricciones que no permitan desarrollar el trabajo normal del usuario afectado. Dado que un proyecto de esta clase puede tener una magnitud considerable en un entorno amplio, se sugiere realizar las revisiones y pruebas necesarias luego de finalizada cada subetapa, correspondiente a los niveles antes mencionados.

3.4.7.1 Implantación a nivel físico

La metodología aquí propuesta invita a llevar a la práctica los controles seleccionados para obtener el nivel de seguridad deseado en el aspecto físico. En esta parte se implanta la solución correspondiente sobre los activos físicos:

Protección de las Instalaciones

Se hacen efectivas las medidas planificadas sobre las instalaciones físicas del entorno.

Protección de los equipos

Se implantan los procedimientos de protección sobre los equipos informáticos.

Revisiones y pruebas

Luego de realizar los cambios o controles, se realizan las revisiones y pruebas pertinentes sobre equipos de procesamiento, equipos de comunicación, dispositivos

3.4.7.2 Implantación a nivel lógico

Aquí se implantan los controles sobre los activos lógicos de la organización:

Protección de la información

En esta parte se procede a proteger la información del entorno como activo

Protección del sistema operativo

Se implantan medidas de protección en el software de base del sistema.

Protección de los datos

Se establecen las medidas preventivas al menor nivel de granularidad de los activos lógicos: los datos.

Revisiones y pruebas

Una vez realizados los cambios o controles, se realizan las revisiones y pruebas sobre las aplicaciones, el software de base como sistemas operativos y bases de datos y los datos.

3.4.7.3 Implantación a nivel de la organización

Aquí se implantan los controles en la organización, en la estructura de la empresa, en las tareas y procesos, en los roles y responsabilidades asignadas.

Protección de la organización

Se realiza la implantación de medidas correctivas y preventivas sobre la estructura de la organización, sobre los roles y responsabilidades de los individuos involucrados con el entorno, el comportamiento de los empleados en la oficina, etc.

Revisiones y pruebas

Siempre luego de realizar los cambios o controles, se realizan las revisiones y pruebas para asegurar un control interno adecuado.

3.4.8 Elaboración del Plan de Recuperación del Entorno ante Desastres (PRED)

El *Plan de Recuperación del Entorno ante Desastres*, en adelante PRED, tiene como objetivo detectar los riesgos presentes en el entorno, analizar su probabilidad de ocurrencia, establecer su criticidad según cómo afectan la continuidad del negocio, y finalmente proponer un plan que logre mitigar en cierta medida estos riesgos, y que permita la recuperación de la disponibilidad de los recursos lógicos, físicos y humanos para mantener la continuidad del proceso del negocio. Muchas veces desastres naturales o accidentes, como incendios, inundaciones, hasta cortes en el suministro de energía eléctrica provocan pérdidas enormes no sólo a nivel de bienes, sino pérdidas provocadas por la interrupción del negocio. Hoy en día el negocio es más y más dependiente de la informática, ya que la mayoría de las empresas tiene sus sistemas productivos y financieros automatizados y computarizados. De esta forma es crucial contar con un plan para sostener el flujo

de los negocios entorno completo. En esta tesis se utilizarán indistintamente los términos "emergencia", "contingencia" y "desastre". Por lo tanto, el hecho de utilizar la palabra "contingencia" no indica menor gravedad que las situaciones en las que se referencia al hecho acontecido como un "desastre". El PRED contiene las siguientes partes:

- Establecimiento del escenario considerado;
- Determinación de los tipos de operación en una contingencia;
- Establecimiento de criticidades:
  - Criticidades por equipo;
  - Criticidades por servicios;
  - Criticidades por aplicaciones;
- Determinación de las prestaciones mínimas;
- Análisis de riesgos:
  - Probabilidad de ocurrencia de desastres;
  - Determinación de los niveles de desastre;
- Presentación de las distintas estrategias posibles de recuperación;
- Selección de la estrategia de recuperación;
- Elaboración de la estrategia de recuperación:
- Formación del Equipo de Recuperación del Entorno ante Desastres (ERED):
  - Roles y responsabilidades;
  - Asignación de roles;

- Establecimiento de los procedimientos:
  - Declaración de la emergencia;
  - Restablecimiento de las condiciones normales.

A continuación se detallará cada una de las partes que componen el PRED.

3.4.8.1 Determinación del escenario considerado

Se deberá hacer un relevamiento de:

- Las condiciones físicas del entorno;
- Los servicios y aplicaciones existentes;
- Los equipos presentes;

3.4.8.2 Determinación de los tipos de operación en una contingencia

Los principales tipos de operaciones considerados ante una situación de contingencia son:

Operación normal inicial: Es la operatoria que se registraba antes de ocurrir el desastre. Asimismo, define las condiciones que se deben alcanzar como objetivo final mediante la ejecución del Plan De Recuperación Del Entorno Ante Desastres;

Operación alternativa: Mientras se trabaja en la recuperación de las prestaciones afectadas por la contingencia, los usuarios deberán utilizar una operatoria alternativa, constituida fundamentalmente por procesos manuales, durante la cual se genera información. A partir del momento en que los servicios y aplicaciones están disponibles, existe un tiempo de "catch up" o actualización de la información del sistema, en el cual se ingresan las novedades ocurridas desde la ocurrencia de la emergencia;

Operación normal en desastre: Mediante la ejecución de los procedimientos que reciben el nombre de "Recuperación de las prestaciones", se llega a esta instancia en la cual todos los servicios y aplicaciones han sido recuperados, pero no se encuentran ejecutando en su lugar original o bajo las mismas condiciones en que se encontraba originalmente.

Operación normal restablecida: Mediante la ejecución de los procedimientos que reciben el nombre de "Restablecimiento de las condiciones normales" se alcanza esta última instancia, en la cual todos los servicios y aplicaciones se encuentran ejecutando correctamente y bajo las mismas condiciones que presentaba antes de la contingencia.

Operación normal: Es la operación del servidor utilizando su disco local;

Operación alternativa: En el momento en que se recupere las prestaciones del servidor de archivos, como parte del proceso de actualización de la información o "catch up", los archivos distribuidos se copian en el sitio habilitado;

Operación normal en desastre: Se considera desde el momento en que la información del disco local del servidor se encuentra copiada en un disco de la cabina, la unidad ha sido montada en el servidor y todos los archivos generados cabina, la unidad ha sido montada en el servidor y todos los archivos generados adicionalmente, a partir de la declaración de la emergencia, se debe realizar el reclamo al servicio técnico del proveedor del servidor, para que repare o reemplace el disco que ha fallado;

Operación normal restablecida: se alcanza esta operatoria en el momento en que el servidor nuevamente utiliza su disco local;

3.4.8.3 Establecimiento de criticidades

En función del impacto producido por la suspensión de las prestaciones del entorno informatizado, se determina la criticidad y el tiempo máximo de tolerancia de corte de las mismas.

A continuación se presenta el análisis realizado desde la perspectiva de los equipos y desde el punto de vista de servicios y aplicaciones. Los documentos que registran las criticidades los organizamos en tablas llamadas: *Tabla de Criticidades por Equipo, Tabla de Criticidades por Servicios* y *Tabla de Criticidades por Aplicaciones*.

3.4.8.4 Determinación de las prestaciones mínimas

Ante una situación de desastre se debe tener en claro cuál debe ser la prestación mínima que debe recuperarse de manera prioritaria, para preservar la continuidad del negocio. Asimismo se debe estimar el tiempo máximo para recuperar esta prestación.

3.4.9 Análisis de riesgos

En esta etapa se analizan los riesgos presentes en el entorno como se ha explicado en la fase 2 de esta metodología, para determinar qué riesgos se pueden mitigar, cuáles se pueden transferir y cuáles se deben asumir.

3.4.9.1 Probabilidad de ocurrencia de desastres

Los riesgos considerados para el plan de recuperación ante desastres, son aquellos que presentan una probabilidad de ocurrencia no despreciable en función de las características del entorno:

- Ubicación geográfica;
- Características meteorológicas de la región;
- Características generales del edificio;
- Condiciones ambientales;

- Condiciones de acceso;
- Condiciones de las oficinas contiguas.

3.4.9.2 Determinación de los niveles de desastre

En función del impacto producido se definen tres grandes tipos de desastres:

Total o Mayor: En el caso en que:

- El lugar físico no pueda disponerse por un período máximo tolerado para la interrupción de las prestaciones mínimas.
- El tiempo que demoran las tareas de restablecimiento de todas o algunas de las prestaciones sea mayor al período máximo aceptable.

Parcial: En el caso en que:

- Los equipos han sufrido daños menores que permiten su funcionamiento parcial o sus prestaciones pueden ser realizadas por otros equipos, y es necesaria la acción de alguien externo (proveedores, mantenimiento, etc.).

Menor: En el caso en que:

- Los desperfectos se solucionan mediante la reinstalación y/o reconfiguración de los equipos.

Roles y responsabilidades

El Equipo de Recuperación del Entorno ante Desastres (ERED) tiene las siguientes responsabilidades:

- Definir las medidas preventivas necesarias y factibles de aplicar, a fin de disminuir la probabilidad de ocurrencia de desastres;
- Definir, probar, ajustar y mantener actualizado el Plan de Recuperación del Entorno ante Desastres;

- Recuperar las prestaciones en el menor tiempo posible;
- Restablecer las condiciones normales que se presentaban antes del desastre;
- Analizar las causas del desastre y la forma en que se ha procedido a fin de emitir un informe y modificar las medidas preventivas y plan de recuperación.

A su vez, el ERED está compuesto por sub-equipos con distintas obligaciones, estos equipos son:

- Equipo de recuperación de hardware [ERH]
- Equipo de recuperación de software [ERS]
- Equipo de recuperación de comunicaciones [ERC]
- Equipo de comunicaciones a usuarios [ECU]

- **Equipo de dirección estratégica y coordinación**: Las responsabilidades de este equipo son:
  - Dirigir y coordinar las actividades del resto de los equipos que conforman el Equipo de Recuperación del Entorno ante Desastres;
  - Realizar las declaraciones de los distintos estados: emergencia, contingencia y restablecimiento de las condiciones normales;
  - Determinar el nivel de desastre producido por una contingencia;
  - Elaborar los planes de recuperación de las prestaciones y restablecimiento de las condiciones normales;
  - Interactuar con personal de mantenimiento para la resolución de contingencias físicas del Centro de Cómputos.

- **Equipo de recuperación de hardware:** Las responsabilidades de este equipo son:
    - Identificar los elementos de hardware que hayan sido dañados por una contingencia;
    - Coordinar con los proveedores de hardware el cumplimiento de los contratos de mantenimiento, garantías y niveles de soporte;
    - Participar en las instalaciones de sistemas operativos que realicen los proveedores;
    - Verificar el correcto funcionamiento de los elementos de hardware que hayan sido restaurados o reemplazados por los proveedores.
- **Equipo de recuperación de software:** Las responsabilidades de este equipo son:
    - Identificar los servicios, procesos, bases de datos y aplicaciones que hayan sido afectados por una contingencia;
    - Instalar, configurar y ajustar todo el software que haya sido afectado.
- **Equipo de recuperación de comunicaciones:** Las responsabilidades de este equipo son:
    - Identificar los elementos de comunicaciones que hayan sido dañados por la contingencia;
    - Detectar los problemas de conectividad de los equipos del CPD y determinar las causas;
    - Coordinar con el responsable los cambios que haya que realizar en las comunicaciones que no sean internas del Centro de Cómputos para que los usuarios puedan seguir utilizando las prestaciones ;

- Verificar el correcto funcionamiento de los elementos de comunicaciones y la conectividad.

- **Equipo de comunicaciones a usuarios:** Las responsabilidades de este equipo son:

  - Participar en la generación de las comunicaciones oficiales a usuarios ante contingencias, recuperación de prestaciones, demoras incurridas que invaliden o modifiquen lo comunicado anteriormente y el restablecimiento de las condiciones normales;

  - Realizar las comunicaciones a los usuarios internos.

3.5. ESTABILIZACIÓN

En el capitulo anterior se describieron las medidas a implantar para asegurar el entorno, a partir del estudio del mismo y de la elaboración del Plan de Aseguramiento. En esta fase se realiza un estudio con el objeto de verificar la obtención de los resultados esperados de la implantación anterior, y la realización de los ajustes necesarios para estabilizar el entorno.

Todo cambio genera más cambios, y en particular esta metodología, al abarcar todos los niveles de estudio del entorno (físico, lógico y organizacional) hace que todos los ámbitos de la empresa objetivo se vean afectados por el proyecto en mayor o menor medida. Es por eso que en esta etapa uno de los objetivos es verificar la evolución del entorno a partir de los cambios propuestos, y realizar los ajustes necesarios para corregir errores, adecuar los controles y minimizar las diferencias entre el Plan y la Implantación de la solución.

3.5.1 Análisis de resultados.

Dentro del proyecto de Aseguramiento del entorno informatizado, el Experto en Seguridad debe considerar un tiempo para realizar el balance respecto de la

efectividad y adecuación de los cambios implantados en el entorno y evaluar la necesidad de realizar ajustes.

Todo Plan sufre cambios continuos a través del tiempo, que deben acompañar la transformación del entorno. Estos cambios deben ser considerados dentro del Plan de Aseguramiento, en los distintos modelos propuestos para cada etapa.

En particular los modelos que deberán revisarse al menos una vez por año para su adaptación a los cambios son:

- Informe de Riesgos;
- Mapa de Usuarios;
- Mapa de Red, PRED.

Requiriendo los demás modelos presentados en esta Tesis pero no mencionados en este apartado una continúa adaptación a través de la vida del Entorno.

3.5.2 Ajuste

La etapa de ajuste está dedicada a realizar ajustes sobre el Plan de Aseguramiento según los resultados obtenidos y analizados en la etapa anterior de esta misma fase y los inconvenientes o nuevos requerimientos que pudieran surgir en la etapa de implantación.

Un proyecto como el que aquí se presenta puede tomar gran envergadura y desarrollarse en un tiempo prolongado durante el cual el entorno sufrirá modificaciones inherentes a la vida de los sistemas, por lo que puede surgir la necesidad de ajustes en ciertos aspectos de seguridad.

Se debe considerar siempre en esta disciplina que los avances científicos son muy rápidos, y se deben considerar las nuevas soluciones tecnológicas ofrecidas en el mercado, que pueden traducirse, muchas veces, en cambios funcionales y en las técnicas procedimentales de implantación.

Los puntos de control que necesiten cambios, mejoras o los que surjan durante el proyecto se tomarán en cuenta para completar y adaptar el Plan de aseguramiento para una segunda implementación, delimitando nuevamente su Alcance, que podrá reducirse a aplicar solamente los cambios surgidos en esta etapa para lograr un completo aseguramiento del entorno.

3.5.3 Cierre de la implantación.

El cierre de la implantación se debe realizar cuando se concluyeron los últimos controles que constituyen el Plan de Aseguramiento y concluidas las etapas de concientización y capacitación de usuarios. Como todo cierre de proyectos, es recomendable realizar un balance del trabajo y presentar los resultados al sector responsables de la empresa objetivo. Un informe ejecutivo es un informe resumido los objetivos fijados al comienzo del proyecto y los objetivos logrados, de los conceptos manejados y la forma en que se obtuvieron los resultados.

3.5.4 Capacitación de usuarios.

Se deberá capacitar a los usuarios para la correcta interpretación y su natural adaptación a los cambios implementados en el entorno, para su inserción en el sistema y su normal desarrollo de actividades, y por sobre todo para que comprenda la importancia de los cambios realizados y de su mantenimiento. Se debe convencer al usuario de la importancia de su colaboración en el esfuerzo de mantener el entorno seguro. Asimismo, se le debe informar de las nuevas reglas y/o políticas de la organización, la forma de trabajar para que su labor no interfiera ni perjudique el esfuerzo implicado en el proyecto de aseguramiento, los procedimientos a usar para revertir situaciones o manejar catástrofes, etc.

Se deberá dejar constancia de que el usuario fue informado respecto de las Políticas de Seguridad, y su completa comprensión y su conformidad respecto de su cumplimiento.

3.5.4.1 Técnicas para la capacitación de usuarios:

- Presentaciones grupales;
- Manuales y folletos;
- Cursos;
- Coaching (un usuario experimentado capacita a un usuario inexperto);
- Teleconferencias;
- Comunicados.

Se recomienda generar confianza de los usuarios en la persona encargada de la capacitación. Se sugiere encargar esta tarea a un empleado carismático y emprendedor, predispuesto y que tenga una buena relación interpersonal con sus pares. Para todas las técnicas de capacitación aquí presentadas, y las que se escapan a este trabajo, se sugiere contar con una fuerte documentación que pueda ser consultada por los usuarios, acompañada por gráficos y todo tipo de material que colabore al rápido aprendizaje e incorporación de los conceptos de seguridad.

Temario

A continuación se presenta un temario básico de capacitación general que deberá ser analizado para aplicar en detalle los temas que correspondan según las Políticas aplicadas en la empresa objetivo:

1. ¿Qué es la información? Explicar que se entiende por información, sus diferentes formas, como se genera, donde y como se puede guardar y a su valor para la empresa. Esto último se relaciona directamente con el nivel de confidencialidad de información que se maneje en el negocio dependiendo de sus características.

2. ¿Qué es la seguridad? Presentar el concepto de Seguridad sus implicancias y sus consecuencias.

3. Intrusos y amenazas: Definir los intrusos externos e internos, sus amenazas y formas de presentación.

3.6 MANTENIMIENTO

Esta es la última fase de la metodología MSEI. Comienza posteriormente a la implantación del Plan de Aseguramiento, luego de la estabilización del entorno y se mantiene durante toda su vida.

Durante la vida del entorno ocurren incidencias y cambios que deben ser analizados y documentados, así como también se deben llevar a cabo controles periódicos y aplicar las correspondientes actualizaciones para mantener un nivel confiable de seguridad en el entorno.

3.6.1 Control de incidencias.

El control de incidencias es una técnica que permite controlar y registrar los eventos ocurridos que atentan contra la seguridad del entorno. Consiste en llevar un registro y un seguimiento de los eventos anormales que ocurran en el entorno objetivo en particular, y en la compañía en general.

Se debe definir el alcance de los eventos o incidencias a registrar. El control de incidencias permite:

- Registrar cambios o pérdida de información;
- Registrar y dar solución a los requerimientos de los usuarios;
- Administrar los usuarios (dar de alta, baja y modificar permisos);
- Registrar nuevas vulnerabilidades manifiestas en el sistema y tomar medidas preventivas para el futuro;
- Dar informe del incidente a quien corresponda;
- Justificar posibles cambios;

- Crear una fuente de información para capacitar a los usuarios.

3.6.1.1 Incidencias de seguridad

Los siguientes eventos son considerados incidencias de seguridad, entre otros:

- Violaciones a la confidencialidad de los datos;
- Violaciones a la integridad de los datos;
- Bloqueo de cuentas de usuarios;
- Anomalías en la disponibilidad de recursos;
- Negación de los servicios;
- Fallas en los sistemas de información;
- Anomalías en el funcionamiento de los sistemas de software;
- Desaparición de información;
- Aparición de datos no creados por el usuario.

3.6.1.2 Notificación de incidencias

El usuario que protagonice un evento que pueda poner en riesgo la seguridad del entorno deberá informar de lo ocurrido.

El Procedimiento de Manejo de Incidencias del Manual de Seguridad de la empresa indicará los pasos a seguir o el circuito para el registro de incidencias.

El ES debe analizar la forma de establecer un circuito de administración de incidencias. Para esto deberá pensar en:

- Un ente **denunciante** que presente el incidente e informa de la ocurrencia y efectos observados (por lo general son los usuarios);
- Un ente **receptor-derivador** de incidencias encargado del asiento en registros apropiados;
- Un ente **responsable** encargado de la resolución del incidente, entendiéndose por resolución el manejo de la incidencia, su tratamiento y, si es posible, su solución (personal técnico especializado, el administrador de la red, etc.);
- Un ente **informante** que entregue el resultado del manejo del incidente al ente denunciante.

En estructuras medianas y grandes suele dar soporte a este esquema el Servicio de Atención al Cliente (SAC), o Help Desk. Toda persona que detecte un incidente de seguridad deberá informarlo de inmediato al ente receptor-derivador.

El área de Recursos Humanos debe intervenir en los casos en que se produzcan eventos que requieran medidas disciplinarias o correctivas.

El Oficial de Seguridad debe mantener una lista de contactos actualizada sobre las personas que deberán ser notificadas ante la ocurrencia de incidencias de seguridad.

3.6.1.3 Documentación

Se deberá conservar de manera segura un resumen de todas las incidencias y acciones realizadas. El acceso y conservación de la información referente a incidencias que han afectado a información clasificada deberá ser controlado cuidadosamente a fin de proteger la confidencialidad de los individuos y minimizar la exposición de la compañía y las obligaciones relacionadas con la privacidad.

3.6.1.4 Reporte de Incidencias

Es un informe detallado que elabora el ente receptor-derivador del incidente inmediatamente de ocurrido éste, en el que debe especificar con el mayor detalle posible lo ocurrido, y enviárselo al responsable asignado, junto al mail de notificación.

El *Reporte de Incidencias* contiene:

- Número de incidente (asignado por el responsable);
- Fecha del incidente;
- Hora del incidente;
- Nombre de la persona que reporta el incidente;
- Sector donde trabaja;
- Ubicación física;
- PC afectada por el incidente;
- Activo (software o hardware) afectado con path completo y/o nombre de la aplicación;
- Nombre del responsable;
- Descripción del incidente;
- Archivos adjuntos (imágenes, logs, etc.);
- Acción/reacción del usuario frente al incidente (por ejemplo: "apagué la máquina", "cierre la aplicación", etc.).

Todos estos datos deben ser completados con el mayor detalle posible por el usuario afectado, salvo el campo correspondiente al número de incidente, que deberá ser completado por el responsable.

Los Reportes de Incidencias deberán ser conservados con fines de análisis y reportes.

Manual de Procedimientos sobre Reporte de Incidencias

El *Manual de Procedimientos sobre Reporte de Incidencias* es un documento que deberá confeccionarse para capacitar a los usuarios en el proceso de reporte de incidencias de seguridad en el entorno.

Este documento debe explicar en forma sencilla y concisa el procedimiento de reporte de incidencias para ser utilizado como guía por los usuarios al momento de declarar un incidente.

Este Manual, como toda la documentación referente a procedimientos de usuarios y Normas deben estar al alcance de todos los empleados, y se debe asegurar que los usuarios tengan conocimiento de la existencia del mismo, su fin y aplicación.

3.6.1.5 Respuesta a incidencias

El ente responsable encargado de analizar y resolver el incidente debe dar respuesta al usuario afectado por el evento, intentando dar indicaciones para que éste comprenda el origen del incidente y tome medidas correctivas cuando sea posible.

Asimismo, el responsable deberá informar al Oficial de Seguridad cuando ocurran incidencias graves de seguridad. Es su responsabilidad desarrollar soluciones en respuesta a las incidencias de seguridad críticos que hayan afectado a los servicios informáticos o aquellos que tengan efectos globales, tales como ataques de virus informáticos, vulnerabilidades de parches de software.

3.6.1.6 Recolección de incidencias

Todas las evidencias deberán ser recolectadas en una manera consistente utilizando técnicas apropiadas que garanticen la autenticidad, integridad, exactitud y veracidad de las mismas. Las evidencias físicas deben ser conservadas en una forma segura, tal como guardarlas en una caja fuerte.

Se debe preservar la cadena de custodia de las evidencias recolectadas. El acceso se debe limitar al mínimo de personas necesarias para responder e investigar incidencias de seguridad. Para las evidencias lógicas se ha desarrollado un documento llamado Registro de Incidencias, que recompila la información obtenida en cada incidente por el Reporte de Incidencias.

3.6.1.7 Registro de incidencias

Es un documento donde se centraliza el registro de las incidencias, para fines estadísticos, educativos y de control.

Es administrado por una persona responsable de la administración de las incidencias, que suele ser el Oficial de seguridad.

Al recibir un Reporte de Incidencias de un usuario, el responsable en cuestión agrega una fila en el registro de incidencias correspondiente al reporte recién recibido y guarda el reporte de Incidencias en una carpeta determinada para tal fin. Se mantiene un solo documento a fin de simplificar el mantenimiento, pero, en organizaciones que por su tamaño lo necesiten, se podrá llevar un documento por sector, cuyos responsables se encargarán de centralizar finalizado el período especificado en la Política de Seguridad.

3.6.1.8 Investigación

Todas las áreas de sistemas deberán colaborar en la investigación de las incidencias de seguridad ocurridas a fin de asegurar que todas las posibles consecuencias del mismo han sido consideradas.

3.6.1.9 Seguimiento de incidencias

El Oficial de Seguridad debe garantizar que todas las incidencias de seguridad sean analizadas en función de la causa de origen, a fin de prevenir la ocurrencia de incidencias similares en el futuro y de mejorar la metodología de respuesta ante incidencias en función de lo aprendido durante la resolución de los mismos.

3.6.1.10 Prevención de incidencias

Se deberá contar con un plan de respuesta ante incidencias con un equipo de personas responsables, que puede estar considerado dentro del PRED (Plan de Recuperación del Entorno ante Desastres).

El Oficial de Seguridad deberá asegurar que las técnicas de prevención incluyan la utilización de software antivirus, filtrado de contenido, y mecanismos de control de acceso de los usuarios y recursos que sean razonables y apropiados, mediante la utilización de firewalls y routers, que son administrados por la organización.

3.6.2 Control de cambios

En la fase de Mantenimiento, y durante toda la vida del entorno, se recomienda llevar un estricto control de cambios en el sistema y las instalaciones. Se deben considerar cambios que afecten cualquier elemento del entorno, como:

- Sistemas operativos de servidores;
- Sistemas operativos de estaciones de trabajo;
- Configuraciones de equipos;
- Sistemas aplicativos en general;
- Aplicaciones de escritorio;
- Motores de base de datos;

- Servicios de correo electrónico;
- Sistemas de protección contra virus informáticos;
- Elementos de comunicaciones (routers, switches, etc.,);
- Entre otros.

Los cambios deben pasar por un circuito de autorizaciones desde que nace el requerimiento hasta que se implanta el cambio. Desde un punto de vista macroscópico, se podría decir que un cambio pasa por cuatro estados durante su vida:

1. Inicialmente surge como un requerimiento solicitado por un usuario.
2. Luego del análisis de los responsables, se convierte en un requerimiento aprobado.
3. El siguiente estado en el desarrollo de la solución.
4. Finalmente, se concreta el cambio en la implantación del cambio.

Las siguientes son las responsabilidades de las personas que forman el comité de cambios:

Usuario solicitante: Detectar mejoras a implantar en el entorno, ya sean cambios de configuraciones, mejoras de performance, mejoras de operatoria, mejoras de estética, etc.;

Administrador de la infraestructura técnica: Analizar que los cambios a realizar en el entorno no afecten la funcionalidad del mismo, evaluando no solo el impacto sino también la criticidad.

Administrador de bases de datos: Analizar que los cambios a realizar en el entorno no afecten la funcionalidad del mismo, evaluando no solo el impacto sino

también la criticidad; Mantener actualizada la documentación de configuración de los sistemas;

Analista de aplicaciones: Analizar que los cambios a realizar en el entorno no afecten la funcionalidad del mismo, evaluando no solo el impacto sino también la criticidad.

Oficial de Seguridad: Evaluar el impacto de los cambios para que no se realicen cambios en configuraciones que estén en contra de la normativa de seguridad.

3.6.2.1 Procedimiento de Control de Cambios

Es en una Tabla de procedimiento de control de cambios de cumplimiento obligatorio.

3.6.2.2 Diagrama de flujo

Es un esquema de procedimientos.

3.6.2.3 Formulario de Control de cambios

Para realizar un efectivo control de cambios, a continuación se pretenda un formulario para documentar el seguimiento de los cambios, desde que surgen como un requerimiento de usuario hasta su implementación en producción.

El objetivo de este registro es dejar asentados los datos de la persona que realizo el requerimiento (usuario solicitante), las autorizaciones correspondientes, los requisitos para su implantación en el entorno productivo y la aceptación del responsable del sitio vivo y el personal del área usaría.

CAPITULO IV

MARCO FINAL

4.1 CONCLUSIONES

1. Utilizando el método científico y como base en varias normas de seguridad y calidad para construir la presente metodología la hipótesis cero planteada es verdadera, con lo cual se demuestra la veracidad de la afirmación, dejando sin efecto la hipótesis 1.

2. Con relación a los objetivos con la construcción de una metodología de seguridad para entornos informatizados aplicando la norma ISO – 17799 de fases integradas se cumple con el objetivo general de tesis planteada el cual fue el de diseñar un método para la seguridad de entornos informáticos.

3. En la introducción de este trabajo mencionamos la necesidad de una herramienta que le permita a los profesionales de Informática descubrir y analizar las vulnerabilidades de los entornos informatizados e implantar técnicas para asegurarlos a lo largo de esta tesis hemos analizado objetivos de control que llevan al Experto en Seguridad a lograr el aseguramiento del entorno objetivo basados en los principales estándares internacionales de seguridad, la normativa Boliviana vigente y las mejores practica profesionales del mundo.

4. Con este análisis logramos formalizar una metodología práctica, y factible para convertir entornos informatizados inseguros en entornos protegidos, y lograr una clara evaluación de los mismos.

5. El Ingeniero de Sistemas o Licenciado en Informática que utilicé esta metodología, podrá evaluar el contenido y alcance de las distintas fases y aplicar los controles que considere necesario para el objeto de su trabajo.

6. Independientemente del tamaño del entorno objetivo y de la clase de negocio que apoye, esta metodología permitirá conocer el entorno e implantar medidas para asegurarlo.

7. De acuerdo a la investigación realizada, la legislación Boliviana no comprende una regulación específica para las metodologías de seguridad.

4.2 RECOMENDACIONES

1. Por efectos de la investigación y los riesgos en los cuales se puede incurrir, se recomienda incluir en la metodología de seguridad la materia de un derecho informático, para los futuros profesionales tengan un conocimiento solido sobre la parte jurídica, contrataciones responsabilidades civiles penales, administrativas, tributación en bienes intangibles, derechos de autor, derechos intelectuales que en la medida que la ciencia de la informática, con su avance vertiginoso, abra nuevas fuentes del conocimiento que tienen que ser regulados por el hombre en sociedad y que brindan al nuevo profesional informático una educación integral en temas referentes a este campo.

2. El trabajo de investigación que se realizo abre nuevas perspectivas de investigación en otras aéreas del conocimiento legal informático, como el perito informático, firma digital, etc. Que tienen que ser estudiadas en base al alcance de la doctrina comprada y adaptación a la realidad nacional.

3. Proteger al profesional informático dotándole de un documento robusto y con base en las normas internacionales (ISO) ante posibles problemas.

ANEXOS

BIBLIOGRAFIA

- [IRAM/ISO/IEC 17799] Julio 2005. Proyecto 1 de norma Argentina. Código de práctica para la gestión de la seguridad de la información. Basada en ISO/IEC Estándar 17799: Information Technology – Code of Practice for Information Security.
- [Antonio Villalon Huerta] Julio 2002 Seguridad en Unix y Redes, Versión 2.1.
- [Cobit] Cobit Standard – Objetivos de Control para la información y Tecnologias – 2000, emitido por el Comité directivo del Cobit y la Information Systems Audit. And Control Fundation.
- [ISECOM] ISECOM – Institute for Security and Open Methodologies.
    - http://www.isecom.org
- [iss.net] ISS- Internet Security Systems.
    - http://www.isecom.org
- [MMC] Conjunto de herramientas de configuración de seguridad de Microsoft- MMC. 2003.
    - http://microsoft.com

GLOSARIO DE TÉRMINOS

Los siguientes son términos utilizados en este trabajo, obtenidos de [ISO – 17799, 2005], [Antonio Villalón Huerta2000] , [Stallings1999], [Technet]:

Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

Análisis de riesgos: Evaluación de las amenazas, impactos y vulnerabilidades relativos a la información y a las instalaciones de procesamiento de la misma, y a la probabilidad de que ocurran.

Autenticación: procedimiento de comprobación de la identidad de un usuario.

Autorización: Garantizar que todos los accesos a datos y/o transacciones que los utilicen, cumplan con los niveles de autorización correspondientes para su utilización y divulgación.

Backup: copia de los datos de un archivo automatizado en un soporte que posibilite su recuperación.

Basurero: La información de los desperdicios dejados alrededor de un sistema puede ser aprovechada por intrusos provocar un hurto o daño.

Bombas lógicas: Programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o un estilo técnico Bombas Lógicas), etc. Si no se produce la condición permanece oculto al usuario.

Backdors y trapdors: Son instrucciones que permiten a un usuario acceder a otros procesos o a una línea de comandos, y suelen ser aprovechados por intrusos malintencionados para tomar control sobre las computadoras.

Challenge-response: Metodología utilizada para la autenticación de usuarios denominada usualmente desafío-respuesta. Se realiza un interrogante o una serie de ellos que sólo el usuario autorizado puede conocer la respuesta.

Chip-cards: Tarjetas que poseen integrado un circuito impreso, en el cual se almacenan datos que posibilitan la autenticación del usuario.

Cliente: toda entidad, empresa, organismo o persona que presente su entorno informatizado con el fin de que el ES lo analice y lo asegure.

Conejos: Programas que no dañan directamente al sistema por alguna acción destructiva, sino que tienen la facilidad de reproducirse exponencialmente de manera de provocar en poco tiempo una negación de servicio al consumir los recursos (memoria, disco, procesador, etc).

Confiabilidad: Garantizar que los sistemas informáticos brinden información correcta para ser utilizada en la operatoria de cada uno de los procesos.

Confidencialidad: Garantizar que toda la información está protegida del uso no autorizado, revelaciones accidentales, espionaje industrial, violación de la privacidad y otras acciones similares de accesos de terceros no permitidos.

Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Copia del respaldo o resguardo: ver backup.

Courier: Mensajero, correo. Persona o dispositivo mediante el cual se envían mensajes o elementos.

Desktop environments: Configuraciones de escritorio.

Dial-back: Metodología de rellamado ante la recepción de petición para establecer una comunicación con un servidor. Al recibir este dicho requerimiento produce el corte de la llamada y luego se comunica mediante una dirección preestablecida.

Disponibilidad: Garantizar que la información y la capacidad de su tratamiento manual y automático, sean resguardados y recuperados eventualmente cuando sea necesario, de manera tal que no se interrumpa significativamente la marcha de las actividades.

Download: (descargar, bajar, bajarse) En Internet proceso de transferir información desde un servidor de información al propio ordenador personal.

Eaves dropping: Es la escucha no autorizada de conversaciones, claves, datos, etc.

Eficacia: Garantizar que toda información que sea utilizada es necesaria y entregada de forma oportuna, correcta, consistente y útil para el desarrollo de las actividades.

Eficiencia: Asegurar que el tratamiento de la información se realice mediante una óptima utilización de los recursos humanos y materiales.

Entorno: Se considera entorno un amplio espectro de ambientes, desde empresas multinacionales distribuidas físicamente en el mundo hasta datos individuales, una empresa informatizada, puede definirse como el edificio que alberga a la empresa objetivo o como el Centro de Cómputos (CC) o Centro de Procesamiento de Datos (CPD) donde se encuentran los servidores, un sector informatizado de un negocio, una red de telecomunicaciones, un equipo de cómputos, una aplicación, archivos lógicos o cualquier elemento susceptible a ataques informáticos.

ES: Experto en Seguridad. En este trabajo se lo considera el principal actor, que utiliza la metodología AEI para asegurar un entorno informatizado.

Exactitud: Asegurar que toda la información se encuentre libre de errores y/o irregularidades de cualquier tipo.

Fallback: Metodología de emergencia ante fallas que posibilitan la recuperación de información perdida.

Firewall (cortafuegos): Dispositivo que se coloca entre una red local e Internet y cuyo objetivo es asegurar que todas las comunicaciones entre los usuarios de dicha red e Internet se realicen conforme a las normas de seguridad de la organización que lo instala.

Gateway (pasarela): Punto de una red que actúa como punto de entrada a otra red.

Gusanos (Worms): Son programas independientes (no necesitan insertarse en otros archivos) que se expanden a través de la red realizando distintas acciones como instalar virus, o atacar una PC como un intruso.

Hacker (pirata): Una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores.

Hacking (pirateo): Acción de piratear sistemas informáticos y redes de telecomunicación.

Herramientas de seguridad: Son utilitarios que sirven para identificar vulnerabilidades en un sistema. Pueden ser una amenaza si un intruso las utiliza en el sistema y detecta fallas en la seguridad de las que el administrador no está enterado.

Hoax: (camelo, bulo) Término utilizado para denominar a rumores falsos, especialmente sobre virus inexistentes, que se difunden por la red, a veces con mucho éxito causando al final casi tanto daño como si se tratase de un virus real.

Host system: (sistema anfitrión, sistema principal) Ordenador que, mediante la utilización de los protocolos TCP/IP, permite a los usuarios comunicarse con otros sistemas anfitriones de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet, WWW y FTP. La acepción verbal (to host) describe el hecho de almacenar algún tipo de información en un servidor ajeno.

Identificación: procedimiento de reconocimiento de la identidad de un usuario.

ID: Nombre o identificación de usuario.

Incidencia o incidente: cualquier anomalía que afecte o pudiera afectar a la seguridad del entorno.

Ingeniería social: Consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían, como revelar su contraseña o cambiarla.

Integridad: Asegurar que sea procesada toda la información necesaria y suficiente para la marcha de las actividades en cada uno de los sistemas informatizados y procesos transaccionales.

Laptop: (computador portátil, ordenador portátil) Ordenador de tamaño pequeño-medio, que se puede transportar como un maletín y apoyar en el regazo (lap).

Legalidad: Asegurar que toda la información y los medios físicos que la contienen, procesen y/o transporten, cumplan con las regulaciones legales vigentes en cada ámbito.

Logged in: Conexión del equipamiento.

Logged out: Desconexión de equipamiento.

Logging: Registro de actividades en un archivo informático, de diferentes situaciones, se utiliza normalmente como evidencia de auditoria.

Login: Conexión. Entrada en una red.

Logon: Procedimiento de conexión o entrada al sistema por parte de un usuario.

Logs: Registros de situaciones en un sistema informático, tales como actividades de usuarios, control de contraseñas, etc. Es el resultado de puesta en marcha del logging.

Mainframe: Estructura principal. Computadora de gran tamaño de tipo multiusuario, utilizada en empresas.

Masquerading: Un intruso puede usar la identidad de un usuario autorizado que no le pertenece simplemente apoderándose de un nombre de usuario y contraseña válidos.

No Repudio: Garantizar los medios necesarios para que el receptor de una comunicación pueda corroborar fehacientemente la autenticidad del emisor.

Notebook: Computador u ordenador portátil.

Normativa de Seguridad: Conjunto de reglas, normas, procedimientos, estándares e instructivos que regulan los aspectos funcionales y técnicos de la seguridad informática en una organización.

Outputs: Salida. Se refiere al producto del proceso de datos, con relación a su presentación, bien puede ser impresa o por pantalla u otro medio idóneo.

Over-classification: Clasificación en exceso. Se refiere al proceso de clasificación de la información con relación a la categorización respecto a su publicidad o no.

PABXs: Centralita privada automática (Private Automatic Branch eXchange) (ramal de intercomunicación telefónica privada). Son ramales de intercomunicación digital interno que permiten manejar tanto la circulación de voz como la de los datos, utiliza conmutación de circuitos.

Palmtop: Ordenador de pequeño tamaño, algo mayor que un paquete de cigarrillos, que se puede llevar en la palma de la mano (palm) y que, además de otras funciones, permite la conexión con Internet.

Password: (palabra de paso, contraseña) Conjunto de caracteres alfanuméricos que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.

PC: Personal Computer. Computadora Personal.

PIN: Personal Identification Number. Número de identificación personal, clave utilizada para el acceso a cajeros automáticos, asociada con una tarjeta de débito o de credito.

Protección Física: Garantizar que todos los medios de procesamiento y/o conservación de información cuenten con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado.

Propiedad: (derecho a propiedad) Asegurar que todos los derechos de propiedad sobre la información utilizada en el desarrollo de las tareas, estén adecuadamente establecidos a favor de sus propietarios.

Recurso: cualquier parte componente de un entorno informatizado.

Router: Sistema constituido por hardware y software para la transmisión de datos en una red. El emisor y el receptor deben utilizar el mismo protocolo de comunicaciones.

Scanners: Software, a veces asociado a equipamiento que permite realizar la inspección de comunicaciones, usualmente mediante el barrido de frecuencias.

Schedulling: Planificación, se utiliza como requerimiento para el desarrollo de tareas, programación, ejecución de procesos, etc.

Shoulder Surfing: Consiste en espiar físicamente a los usuarios para obtener claves de acceso al sistema, números válidos de tarjetas de crédito, etc.

Spooled data: Datos en cola de espera. Los mismos pueden hallarse en dicha situación para su ingreso o su salida, impresión.

Stop: Cierre del sistema. Tanto de software, programa o aplicación, como de hardware, equipamiento.

Seguridad de la información: La preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistemas de información: conjunto de archivos automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos.

Software malicioso: (malware) Es un término común que se utiliza al referirse a cualquier programa malicioso o inesperado o a códigos móviles como virus, troyanos, gusanos o programas de broma.

Soporte: objeto físico susceptible de ser tratado en un entorno informatizado y sobre el cual se pueden grabar o recuperar datos.

Teleworking site: Sitio de trabajo remoto o a distancia.

Timeouts: Son programas que se pueden utilizar durante un período de tiempo determinado;

Tokens: Dispositivos de hardware que posibilitan la generación aleatoria de claves de acceso.

Troyanos: Similar al famoso Caballo de Troya, estos programas maliciosos ocultan sus intenciones reales bajo la apariencia de un juego, una animación, etc. Algunos troyanos permiten el acceso al equipo infectado, otros borran archivos, introducen un virus o comprometen la seguridad del sistema atacado de diferentes maneras.

Upgrading: Ascender de nivel, actualizar, modernizar.

UPS: Usage Parameter Control. Parámetros de control de uso.

Usuario: sujeto o proceso autorizado para acceder a datos o recursos.

Web: World Wide Web, o simplemente Web, es el universo de información accesible a través de Internet, una fuente inagotable del conocimiento humano.

Worms: (Gusanos) Son programas que tratan de reproducirse a si mismo, no produciendo efectos destructivos sino el fin de dicho programa es el de colapsar el sistema o ancho de banda, replicándose a si mismo.

PREGUNTAS

Nivel Físico

1- ¿El espacio es compartido (oficina propia, box del sector, común)?

La pregunta apunta a ver si la Workstation en estudio está aislada físicamente de otras, o está ubicada en un sector compartido, como un box de trabajo o un lugar abierto.

2- ¿Hay otros sectores de la empresa en el mismo piso?

La pregunta apunta a si el espacio físico es ocupado por personas de distintos sectores.

3- ¿Se accede a esta Workstation con llave propia del sector?

Se refiere a si la Workstation en estudio está ubicada en un lugar físico al que se accede con llave u otro mecanismo de seguridad propio del sector de trabajo, y no da acceso a otros sectores.

4- ¿Existe algún circuito de circulación abierto hasta esta Workstation?

Se apunta a verificar si existe un camino inseguro a la Workstation como podría ser un pasillo que da a una salida no asegurada. Un ejemplo típico es la PC de trabajo de una recepcionista que está al alcance del público.

5- ¿Está cerca de alguna puerta?

Con CERCA se hace referencia a “pocos metros”.

6- ¿Está cerca de algún pasillo?

Con CERCA se hace referencia a “pocos metros”.

7- ¿Está cerca de alguna ventana?

Con CERCA se hace referencia a “pocos metros”.

8- ¿Guarda la documentación impresa o magnética bajo llave propia?

Por ejemplo en un armario de uso particular.

9- ¿Guarda la documentación impresa o magnética bajo llave común al sector?

Por ejemplo en un armario de uso común de todo el sector.

10- ¿Maneja algún tipo de codificación para la rotulación de cintas, CDs, etc.?

La pregunta apunta a verificar si se utiliza alguna técnica preestablecida para nomenclar dispositivos de almacenamiento, o simplemente se rotulan con nombres legítimos.

Un ejemplo de nombre legítimo podría ser: back05122002.tar que indica claramente que ese dispositivo contiene un archivo de backup del día 5 de diciembre del 2002.

11- ¿Posee conexión a una LAN?

Se le debe preguntar al usuario si está conectado a la red local.

12- ¿Posee conexión a una WAN?

Se le pregunta al usuario si en su red existen equipos ubicados físicamente en otro edificio.

13- ¿Tiene acceso a Internet?

La pregunta apunta a verificar si el usuario tiene acceso a Internet.

14- ¿Hay cables al descubierto?

La pregunta apunta a verificar si el cableado está protegido, por ejemplo, con tubos cobertores e se encuentran subterráneos, o simplemente se expanden a la vista.

15- ¿Usa esta Workstation otro usuario regularmente?

Esta pregunta apunta a verificar si la Workstation es compartida por distintos usuarios. Esto suele darse en situaciones donde los empleados trabajen part-time o simplemente se requiera de monitorización continua durante las 24 hs.

16- ¿Trabaja con servidores de uso exclusivo de su sector o son compartidos por más de un sector?

Por ejemplo, si trabajan los sectores de Desarrollo y Prueba con un mismo servidor.

Nivel Lógico

17- ¿Posee conexión permanente a Internet?

Por ejemplo ADSL, Cable módem, etc.

18- ¿Posee IP fija?

Esta pregunta apunta a conocer cómo se hace la administración de las direcciones de red, que afectará en la definición de un blanco identificable o no.

19- ¿Se puede acceder en forma remota a esta Workstation?

Por ejemplo a través de conexiones TELNET.

20- ¿Tiene acceso solamente a los recursos que necesita para trabajar?

La pregunta apunta a verificar si desde la Workstation se puede acceder a sectores de la LAN que no son necesarios para realizar el trabajo, apuntando al principio de "otorgar solo los privilegios mínimos y necesarios para la realización del trabajo"

21- ¿Lo ven desde la LAN sólo los que lo necesitan ver?

Para verificar si sectores no autorizados tienen acceso a esta terminal.

22- ¿Posee documentación de las aplicaciones que utiliza?

Esta pregunta apunta a chequear si los usuarios poseen documentación suficiente para el uso de los aplicativos de trabajo.

23- ¿Hay más usuarios configurados de los que realmente usan la workstation?

Esta pregunta apunta a verificar si existen configurados usuarios que no son estrictamente necesarios.

24- ¿Usa un SO monousuario?

Por ejemplo Windows 98, Windows Millenium, etc.

25- ¿Es usuario experto de su SO?

Apunta a verificar si el usuario es capaz de realizar tareas de administración del sistema, por ejemplo, configurar un firewall, verificar opciones de seguridad, y manejar el file system en forma adecuada.

26- ¿Usa la misma contraseña para más de un sistema?

Por ejemplo, si el usuario utiliza la misma contraseña para ingresar al sistema operativo y para el programa de correo.

27- ¿Cambia las contraseñas con regularidad?

REGULARIDAD se podría llegar a considerar hasta un mes.

28- ¿Realiza copias de respaldo de su información personal sensible?

La realización de las copias de respaldo o backup es responsabilidad del administrador de la red y del operador responsable.

29- ¿Posee carpetas compartidas en esta PC?

Se refiere a las carpetas que pueden ser accedidas por otros usuarios desde otras workstations.

30- ¿Usa el antivirus regularmente para revisar archivos peligrosos?

Se consideran ARCHIVOS PELIGROSOS los de origen incierto, o los transportados en memorias flash, discos y cintas de gran capacidad, etc.

Nivel De La Organización

31- ¿Existe una persona encargada de administrar la seguridad?

32- ¿Existen Normas o procedimientos de seguridad?

La pregunta apunta a descubrir si el usuario está informado de la existencia de un marco normativo de seguridad.

33- ¿Existe algún procedimiento para solicitar nuevos requerimientos?

Esta pregunta apunta a verificar si el usuario conoce los procedimientos formales de solicitud de nuevos requerimientos, y si efectivamente estos procedimientos existen.

34- ¿Procesa información que es confidencial para gente del mismo piso?

Esta pregunta pretende verificar si en esta Workstation se procesa información que es confidencial para personas que comparten el mismo espacio físico.

35- ¿Intercambia datos/información con otros departamentos?

Esta pregunta pretende descubrir la interrelación entre departamentos, y la existencia de flujo de información entre ellos.

36- ¿Intercambia datos/información con otras empresas?

Esta pregunta pretende descubrir la interrelación entre los empleados de la empresa con externos, y la existencia de flujo de información entre ellos.

37- ¿Trabajan terceros en su piso?

Se refiere a si trabajan personas subcontratadas o externas a la empresa en el mismo sector físico.

38- ¿Cuando ocurre un incidente, informa a alguien o trata de manejarlo solo?

Por ejemplo: cuando sucede una anomalía en el software el usuario llama a un técnico de sistemas para que vea lo sucedido.

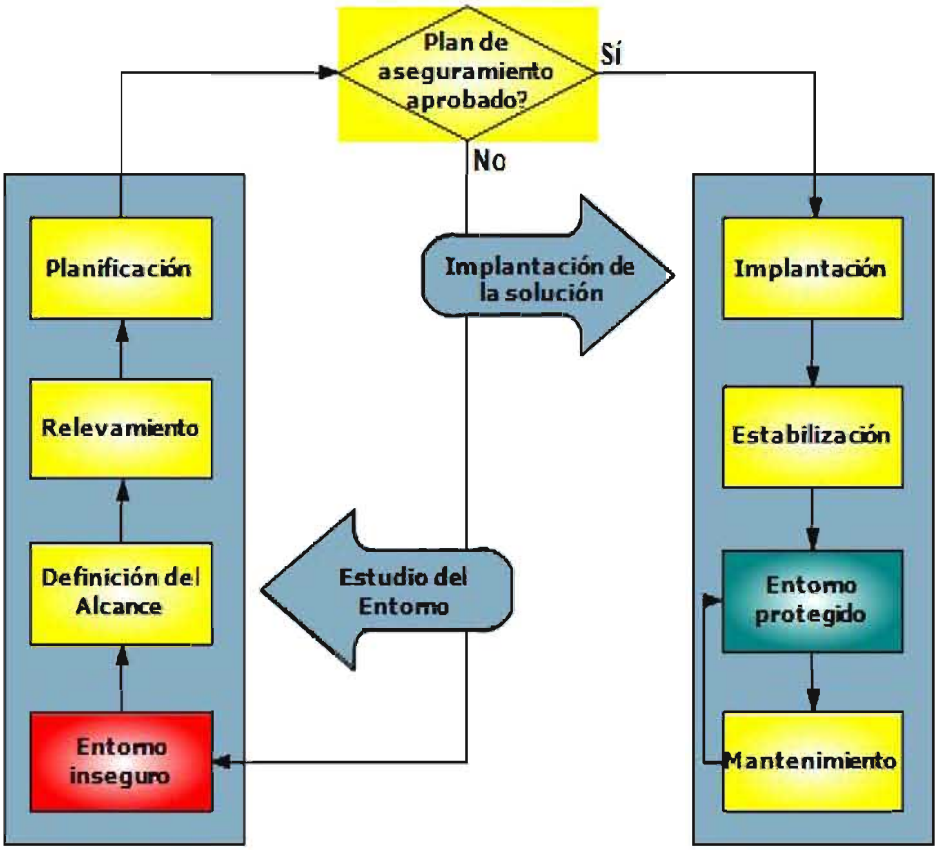
39- ¿Cómo informa los nuevos requerimientos?

La pregunta apunta a descubrir si existe un procedimiento de control de cambios y reporte de requerimientos de usuario.

40- ¿Ha firmado algún acuerdo de confidencialidad?

La pregunta apunta a determinar si el usuario tiene conciencia de la criticidad de la información que maneja.

DIAGRAMA DE FASES


Plan de aseguramiento aprobado?
Sí
No
Planificación
Relevamiento
Definición del Alcance
Entorno inseguro
Implantación de la solución
Estudio del Entorno
Implantación
Estabilización
Entorno protegido
Mantenimiento

FASE / ETAPA	ACTOR	ENTREGABLE
1 Definición del Alcance		
1.1 Análisis de requerimientos de usuario	ES, cliente	**Documento de Requerimientos de Usuario**
1.2 Elaboración del Alcance	ES, cliente	**Alcance**
1.3 Aprobación del Alcance	cliente	
1.4 Estimación de tiempos y costos	ES	
1.4.1 Costos capitales		
1.4.2 Costos recurrentes		
1.4.3 Costos no recurrentes		
1.5 Elaboración del Plan de Trabajo	ES	**Plan de Trabajo**
2 Relevamiento		
2.1 Elaboración del Relevamiento General	ES, usuarios	**Relevamiento General**
2.2 Elaboración del Relevamiento de Usuario	ES	**Relevamiento de Usuario**
2.3 Análisis de vulnerabilidades	ES	**Mapa de Vulnerabilidades**
2.4 Análisis de riesgos	ES	**Informe de Riesgos**
3 Planificación	ES	
3.1 Elaboración del Plan de Aseguramiento	ES	**Plan de Aseguramiento**
3.1.1 Protección física	ES	**Plan de Aseguramiento, Mapa de Elementos de Red**
3.1.1.1 Protección de las instalaciones	ES	**Plan de Aseguramiento**
3.1.1.2 Protección de los equipos	ES	**Plan de Aseguramiento, Mapa de Elementos de Red**
3.1.2 Protección lógica	ES	**Plan de Aseguramiento, Mapa de Usuarios, Inventario de Backups, Documento de Actualización de Software, Tabla de Permisos sobre Activos Lógicos**
3.1.2.1 Protección de la información	ES	**Plan de Aseguramiento**
3.1.2.2 Protección de los Sistemas Operativos		**Plan de Aseguramiento, Mapa de Usuarios, Registros y archivos de Log**
3.1.2.3 Protección de los datos	ES	**Plan de Aseguramiento, Tabla de Permisos sobre Activos Lógicos, Documento de actualización de Software, Inventario de backups,**
3.1.2.4 Protección a nivel de la organización	ES	**Plan de Aseguramiento**
3.2 Aprobación del Plan de aseguramiento	cliente	
4 Implantación		
4.1 Elaboración del Relevamiento de Activos	ES	**Inventario de Activos, ABM Activos**
4.1.1 Inventario de activos		**Inventario de Activos Físicos, Inventario de Activos Lógicos**
4.1.2 Rotulación de activos	ES	**Inventario de Activos**
4.1.3 Análisis de criticidades	ES	**Inventario de Activos**

FASE / ETAPA	ACTOR	ENTREGABLE
4.2 Clasificación de la información	ES	
4.3 Elaboración/adaptación de la Normativa de Seguridad	ES	**Manual de Seguridad**
4.3.1 Interiorización del experto con la política y negocio de la organización	cliente	**Organigrama, documentación del proceso comercial, etc.**
4.3.2 Elaboración/adaptación de la Normativa de Seguridad	ES	**Manual de Seguridad**
4.3.3 Aprobación de la Política de Seguridad		
4.4 Publicación de la Normativa de Seguridad		
4.4.1 Implantación de una campaña de concientización		**Comunicados, Presentaciones, Documentación,**
4.4.2 Capacitación de usuarios		**Presentaciones, Documentación, Manual de Seguridad**
4.5 Implantación del Plan de Aseguramiento		
4.5.1 Implantación a nivel físico	ES	**Inventario de Activos, ABM Activos**
4.5.2 Implantación a nivel lógico	ES	**Inventario de Activos, ABM Activos**
4.5.3 Implantación a nivel de la Organización		
4.6 Elaboración del Plan de Recuperación del Entorno ante Desastres		**Tabla de Criticidades por Equipo, Tabla de Criticidades por Servicio, Tabla de Criticidades por Aplicación, PRED, Procedimiento de Declaración de la emergencia, Procedimiento de Recuperación de las prestaciones, Procedimiento de Reestablecimiento de las Condiciones Normales**
5 Estabilización		
5.1 Analisis de resultados	ES	**Informe de Implantación**
5.2 Ajuste		
5.3 Cierre de la implantación	ES	**Informe de Cierre de la Implantación**
5.4 Capacitación de usuarios	ES	**Manual de Seguridad, Manual de Procedimientos sobre Reporte de Incidencias, presentaciones, Manuales, Folletos, Cursos, Comunicados**
6 Mantenimiento		
6.1 Control de incidencias	ES, cliente	**Reportes de Incidencias, Registro de Incidencias**
6.2 Control de cambios	ES, cliente	**Formulario de Control de Cambios, ABM Activos, Documento de Actualizaciones de software**

DOCUMENTOS