ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

POLITICAS Y PROCEDIMIENTOS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA ENTIDAD FINANCIERA

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

MARITZA SORAYA RUIZ CONSTANTE
Maritza.Ruiz@tcs.ec

DIRECTOR: ING. JUAN HERRERA
Juan.Herrera@leveltech.com.ec

Quito, Abril 2010

DECLARACIÓN

Yo, Maritza Soraya Ruiz Constante declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Maritza Ruiz Constante

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Maritza Soraya Ruiz Constante, bajo mi supervisión.

Ing. Juan Herrera S.
DIRECTOR DE PROYECTO

AGRADECIMIENTO

Agradezco a mis padres por su apoyo en todo momento.

DEDICATORIA

Dedicado a mi madre, de quien he aprendido que con valor, paciencia y sabiduría, todo se puede vencer y sobrellevar los momentos más difíciles que se nos presenta en nuestra vida.

Maritza

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

1. CAPITULO 1 ANALISIS DE RIESGOS

1.1. Situación Actual de la Entidad Financiera

Ante el esquema de globalización que las tecnologías de la información han originado principalmente por el uso masivo y universal de la Internet y sus tecnologías, la Entidad Financiera se ve inmersa en ambientes agresivos donde el delinquir, sabotear, robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crackers, etc., es decir en transgresores.

Conforme las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un continuo riesgo, que obliga a la Entidad Financiera a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

En nuestro país no existe una sola institución que no se haya visto sujeta a los ataques en sus instalaciones, tanto desde el interior como del exterior, basta decir que cuando en el centro estamos sujetos a un ataque un grupo de gente se involucran y están pendientes de éste, tratando de contrarrestar y anular estas amenazas reales.

La carencia de recursos humanos involucrados en seguridad, la escasa concientización, la falta de visión y las limitantes económicas han retrasado el plan rector de seguridad que se requiere.
La seguridad de las instituciones en muchos de los países se ha convertido en cuestión de seguridad nacional, por ello contar con un documento de políticas de seguridad es imprescindible, y debe de plasmar mecanismos confiables que con base en la política institucional proteja los activos del Centro.

Por lo tanto se debe establecer en la Entidad Financiera, una organización de seguridad visible, sólida y flexible que esté apoyada por la Alta Gerencia para proveer el marco necesario que permita minimizar los riesgos de seguridad de información viabilizando la implementación y soporte de soluciones automáticas de seguridad.

Para todas las unidades de negocios de una Entidad Financiera, la información es un activo esencial. Es crucial que toda la información sensible sea mantenida de manera confidencial, sea precisa y esté disponible, de la manera apropiada para cubrir las necesidades de los negocios. Será responsabilidad de cada individuo proteger adecuadamente la información que maneje durante el desempeño de sus actividades.

Esta política regulará el comportamiento que deberá ser observado y cumplido por todos los funcionarios (regulares, terciarizados, temporales, pasantes, etc.) de una Entidad Financiera, para lograr la seguridad de la información.

Los terceros involucrados (proveedores, clientes, etc.) serán incluidos en los requerimientos de esta política de manera contractual y obligatoria.

Esta política provee un marco de trabajo para todos los procesos estándares y sus mecanismos de seguridad. Define los objetivos de seguridad, clasifica la información, responsabilidades y principios fundamentales para asegurarla de acuerdo con los objetivos del negocio. Cuando la política se vea afectada por leyes y/o regulaciones nacionales y/o internacionales deberá ser actualizada a fin de cumplir con las exigencias de la Entidad Financiera.

1.1.1. Clasificación de la Información

La información debe ser clasificada para señalar la necesidad, la prioridad y el grado de protección.
La información tiene diversos grados de sensibilidad y criticidad. Algunos ítems pueden requerir un nivel de protección adicional o un tratamiento especial. Se debe utilizar un sistema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de tratamiento especial.

1.1.1.1. Pautas de la clasificación

Las clasificaciones y controles de protección asociados de la información, deben tomar cuenta de las necesidades de la empresa con respecto a la distribución (uso compartido) o restricción de la información, y de la incidencia de dichas necesidades en las actividades de la organización, por ejemplo: acceso no autorizado o daño a la información. En general, la clasificación asignada a la información es una forma sencilla de señalar cómo ha de ser tratada y protegida. La información y las salidas de los sistemas que administran datos clasificados deben ser rotuladas según su valor y grado de sensibilidad para la organización. Asimismo, podría resultar conveniente rotular la información según su grado de criticidad, por ejemplo: en términos de integridad y disponibilidad.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, verbigracia, cuando la información se ha hecho pública.
Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso ("over- classification") puede traducirse en gastos adicionales innecesarios para la organización.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente, debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una política predeterminada. Se debe considerar el número de categorías de clasificación y los beneficios que se obtendrán con su uso.

Los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos. Deben interpretarse cuidadosamente los rótulos de clasificación de los documentos de otras organizaciones que podrían tener distintas definiciones para rótulos iguales o similares.

La responsabilidad por la definición de la clasificación de un ítem de información, por ejemplo: un documento, registro de datos, archivo de datos y por la revisión periódica de dicha clasificación, debe ser asignada al creador o propietario designado de la información.

1.1.1.2. Rotulado y manejo de la información

Es importante que se defina un conjunto de procedimientos adecuados para el rotulado y manejo de la información, según el esquema de clasificación adoptado por la organización. Estos procedimientos deben incluir los recursos de información en formatos físicos y electrónicos. Para cada clasificación, se deben definir procedimientos de manejo que incluyan los siguientes tipos de actividades de procesamiento de la información: Copia, Almacenamiento, Transmisión por correo, fax y correo electrónico, Transmisión oral, incluyendo telefonía móvil, correo de voz, contestadores automáticos.

1.1.2. Segregación de funciones y definición de roles de trabajo

Estructura Organizacional

La estructura organizacional que soportará la función de Seguridad de la Información, es la siguiente:

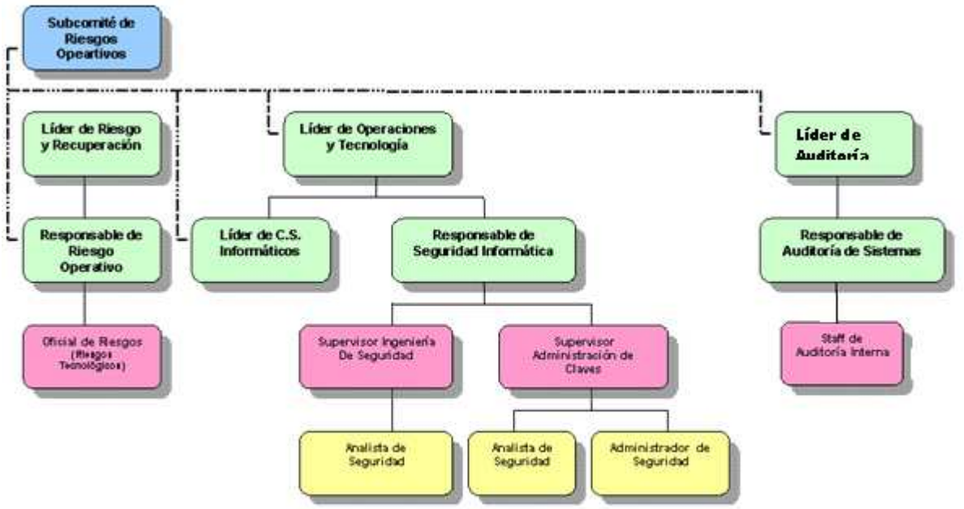

Figura 1.1: Estructura Organizacional

Existen funciones altamente privilegiadas o sensibles al interior de la Entidad Financiera, las que serán separadas de otras similares, para minimizar el riesgo de abuso de privilegio y para maximizar la habilidad de quienes tienen la responsabilidad de controlar las funciones de los demás.

Respetando el principio de segregación de funciones, algunos roles serán ejercidos por distintos funcionarios o perfiles, como por ejemplo: administración del control de acceso a sistemas operativos, aplicaciones de negocio, uso normal de los sistemas y aplicaciones, auditoría y administración de la seguridad de la información.

Subcomité de Riesgos Operativos

Es su responsabilidad la aprobación de las políticas de Seguridad de la Información, evaluar el comportamiento de los riesgos identificados e instruir se tomen acciones para mantener bajo control dicho comportamiento.

Responsable de Riesgo Operativo

Bajo su responsabilidad se encuentran la identificación, clasificación y valoración de eventos de riesgo operativo relacionados a los procesos de Seguridad de Información, así como por la definición de políticas tendientes a mitigarlos y del seguimiento a la ejecución de los planes de acción correspondientes.

El Responsable de Riesgo Operativo tiene como objetivo contar con un procedimiento y metodología de administración de riesgo operativo, que en función de la estrategia Institucional, la normativa legal vigente y lo determinado por el Comité Integral de Riesgo, permita identificar las posibles fuentes de pérdidas generadas en los procesos de Seguridad de Información, entre otros.

Es su responsabilidad, además, la determinación de provisiones que cubran a la Entidad Financiera de eventuales pérdidas provocadas por la materialización de los riesgos en mención.

Oficial de Riesgos (Riesgos Tecnológicos)

Elaborar las políticas tendientes a mitigar los riesgos de los procesos de Seguridad de Información, revisarlas con las otras áreas involucradas y someterlas a la aprobación del Subcomité de Riesgos Operativos.

Responsable de Seguridad Informática

Bajo su responsabilidad está la implementación de las políticas de Riesgo Operativo Aplicación Seguridad de la Información, así como de la definición y puesta en marcha de planes de acción tendientes a cumplir con las mismas.

Es además su responsabilidad, reportar a Riesgo Operativo la conclusión de los mencionados planes de acción y, por tanto, de la mitigación de los riesgo identificados.

Unidades Ejecutoras

En su ámbito de acción sus responsabilidades son:

- Conocer y cumplir las políticas de Riesgo Operativo Aplicación Seguridad de la Información.
- Definir y ejecutar los planes de acción para implementar las Políticas.
- Reportar la conclusión de los planes de acción a Riesgo Operativo.

Responsable de Auditoría de Sistemas

Es su responsabilidad la verificación del cumplimientos de políticas de Riesgo Operativo Aplicación: Seguridad de la Información, en las diferentes áreas de Negocio y Soporte, así como también de informar a Riesgos Operativos sobre las observaciones encontradas en los exámenes de auditoria aplicados.

Además también deberá evaluar si la consistencia de los mecanismos de seguridad implementados concuerdan con los requerimientos y el diseño de seguridad.

Recursos Humanos

Es su responsabilidad que el nuevo personal que se incorpore a la Entidad Financiera será instruido respecto de la sensibilidad de los sistemas de información y la información bajo su control.

Como una parte integral de la operación diaria de los sistemas de negocios, será creada y mantenida una concientización de la necesidad de la seguridad de la información en todo el personal.

Administrador de Sistemas

Para cada red de área extendida (WAN) y red corporativa (MAN) del Grupo, será designado un Administrador de Sistemas que garantice las prestaciones de acuerdo con las políticas, normas, procedimientos y estándares establecidos.

Propietario de la Información

Es responsable por la integridad y confidencialidad de la información nueva o transformada que ha sido generada por un sistema de información automático o manual a su cargo. Es también responsable de controlar el correcto almacenamiento, el proceso, la distribución y comunicación de esta información.

Los propietarios de la información son los responsables de clasificarla. Esta clasificación mantendrá el principio de “Necesidad de Conocer”.

Un propietario de la información no tiene que ser necesariamente un Líder o Responsable de la Organización, podrá ser también un Comité o una Unidad.

Los propietarios de la información son responsables en última instancia de la clasificación y la seguridad de todas las transacciones asociadas con sus activos, así como de asegurar la información específica de la Institución y de los clientes.

Usuario Final

Los usuarios finales son los custodios de la información que crean o almacenan y cumplirán con esta Política en lo que respecta a su uso y administración. Los empleados serán informados regularmente sobre las políticas y estándares existentes, y recibirán capacitación cuando sea necesario.

Terceros involucrados

Los terceros involucrados se atendrán a los lineamientos establecidos por esta Política.

1.1.3. Definición y creación de procesos de control

1.1.3.1. Clasificación de la Información

Objetivo

Determinar los niveles de Clasificación de la Información de la Entidad Financiera para su protección frente a pérdida, divulgación no autorizada o cualquier forma de uso indebido, ya sea de modo accidental o intencionado.

La información adopta muchas formas, al interior de los sistemas, como fuera de ellos. Es decir puede ser:

- Almacenada, en los sistemas o medios portables.
- Transmitida, a través de redes o entre sistemas.
- Impresa o escrita, en papel y/o hablada en conversaciones.

Bajo el punto de vista de seguridad, la protección adecuada debe ser aplicada a todas y cada una de las formas de presentación de la información: documentos, programas, archivos de datos, pantallas de consulta, reportes, impresiones, correo electrónico, etc.

Alcance

Límites del proceso

Se deberá clasificar toda la información generada por y para la Entidad Financiera.

Aplicabilidad

Rige en el ámbito nacional para todo el personal de la Entidad Financiera, debiendo ser cumplida por todos sus funcionarios (regulares, temporales, pasantes, etc.), así como también para las empresas y su personal que presten servicios de asesoría o consultoría a la Institución.

Las empresas relacionadas deberán aplicar esta política sobre la información enviada por la Entidad Financiera.

Áreas y usuarios involucrados

- Propietario de la Información, Líder o Responsable de Área.
- Usuario Final.
- Proveedor de Servicio de Tecnología

Definiciones

Información Estratégica

Aquella que proporciona a la Entidad Financiera una ventaja competitiva en el mercado, de manera que su uso indebido o la divulgación no autorizada lo perjudicaría. Algunos ejemplos de información estratégica pueden ser: Datos técnicos, científicos o financieros, Planes o proyecciones de negocios o de comercialización, listas de clientes, Datos del Personal, Formularios prenumerados/preimpresos con información completa, Informes financieros trimestrales antes de ser conocidos oficialmente, etc.

Información de Clientes

Información generada por los empleados encargados de dar servicio al cliente. Como ejemplo se cita: Documentación soporte para apertura de cuentas, papeletas de transacciones en cuentas con información completa, cheques depositados y/o pagados, pólizas de acumulación, certificados de inversión, comprobantes de cheques certificados, de pensiones, de transacciones contables, estados de cuenta por entregar, y toda la documentación generada por el área de Atención al Cliente.

Transmisión Electrónica

Constituye intercambio de información, voz o datos mediante medios electrónicos, incluso teléfonos, sistemas de conferencia por vídeo, redes locales o de áreas ampliadas.

Copia

Reproducción de la información en cualquier formato: fotocopia, impresión o duplicación electrónica.

1.1.3.2. Clasificación de Riesgos de Proyectos

Objetivo

Definir los criterios objetivos con los que se obtendrá la calificación del riesgo de un Proyecto de Aplicación, la misma que determinará si el Proyecto deberá ser certificado para pasar a producción.

Alcance

Límites del proceso

El proceso se inicia con la notificación del Proveedor de Servicio de Tecnología - Líder de Proyecto al Proveedor de Servicio de Seguridad Informática sobre un nuevo Proyecto de Aplicación que ha finalizado su fase de Visión y Alcance, a continuación se realiza la Calificación de Riesgo por el personal del Proveedor de Servicio de Seguridad Informática y se informa su resultado a Auditoría, Riesgo Operativo y al Proveedor de Servicio de Tecnología - Líder de Proyecto.

Aplicabilidad

Se aplicará para todos los Proyectos de Aplicación (Son todas las aplicaciones nuevas (desarrolladas, adquiridas o contratadas su desarrollo) o los cambios mayores/significativos que involucren un esfuerzo de 80 horas o más.

Áreas y usuarios involucrados

1 Riesgo Operativo.
2 Proveedor de Servicio de Tecnología.
3 Proveedor de Servicio de Seguridad Informática.

Definiciones

Proyecto de Aplicación
Son todas las aplicaciones nuevas (desarrolladas, adquiridas o contratadas su desarrollo) o los cambios mayores/significativos que involucren un esfuerzo de 80 horas o más.

1.1.3.3. Acceso por parte de Terceros

Objetivo

Establecer en la Entidad Financiera el marco regulatorio que norme el acceso de Terceros a la información de la Institución.

Alcance

Límites del proceso
Todas aquellas actividades de la Entidad Financiera, en las que participen terceros.

Aplicabilidad
Se aplicará para determinar tanto el acceso físico como lógico a todos los terceros que sin tener relación de dependencia con la Entidad Financiera usan o dan soporte a la Organización, los sistemas de información, la infraestructura o la información de la Entidad Financiera.

Áreas y usuarios involucrados

1. Propietario de la Información
2. Gerente de Área
3. C.S. Jurídicos
4. Usuario Final

5. Proveedor de Servicio de Seguridad Informática
6. Proveedor de Servicio de Tecnología

Definiciones

Terceros

Denominación otorgada a los individuos que sin tener una relación de dependencia con la Entidad Financiera, deben acceder a su información por motivos de negocio.

Información Clasificada

Se denominará Información Clasificada exclusivamente a aquella que pertenece a los niveles 3 Confidencial y 4 Estrictamente Confidencial.

1.1.3.4. Seguridad Física y Ambiental

Objetivo

Minimizar los riesgos potenciales creados por amenazas accidentales y/o deliberadas (ataque, pérdida, robo o daño a los sistemas de información), a los que se encuentran expuestos los recursos informáticos físicos, que puedan ocasionar la interrupción total o parcial de las actividades del negocio, a través de la definición de controles, procedimientos y/o mecanismos que permitan una máxima protección a un costo razonable.

Alcance

Límites del proceso

La seguridad física incluye las normas y procedimientos utilizados para asegurar los equipos, periféricos y líneas de comunicación y por consiguiente los edificios, áreas de trabajo en las oficinas y escritorios en los cuales están ubicados, para protegerlos de violaciones deliberadas y de interrupciones accidentales que provoquen la disminución de la disponibilidad de los mismos.

Aplicabilidad

Deberá ser considerada para todos los equipos, periféricos y líneas de comunicación de de todas las plataformas computacionales de la Entidad Financiera, que residan en sus instalaciones o la de terceros.

Áreas y usuarios involucrados

1. Seguridad Física.
2. Compras, Logística y Mantenimiento.
3. Gerentes – Responsables de Área.
4. Usuario Final.
5. Proveedor de Servicio de Seguridad Informática.

1.1.3.5. Actualizaciones Directas a la Base de Datos

Objetivo

Minimizar el riesgo de que la información de la Entidad Financiera en producción pierda su integridad y confidencialidad debido a las actualizaciones directas a la Base de Datos.

Alcance

Límites del proceso

El procedimiento inicia con el requerimiento del usuario final, luego la autorización del Propietario de Información, y termina con la actualización por parte del Administrador de la Base de Datos.

Aplicabilidad

Se aplicará en todos los modificaciones directas que se realicen a la Base de Datos del ambiente de producción de la Entidad Financiera.

Áreas y usuarios involucrados

1. Propietario de la Información
2. Proveedor de Servicio de Tecnología

Definiciones

Incidencia

Requerimiento o solicitud de modificación directa a la base de datos.

1.1.3.6. Protección contra software malicioso

Objetivo

Minimizar los riesgos operativos inherentes a la utilización de los sistemas informáticos y protegerlos de los efectos/daños causados por Software Malicioso

Alcance

Límites del proceso

Se debe considerar en todos los procesos relacionados con la utilización de sistemas de información automáticos de la Entidad Financiera.

Aplicabilidad

Se aplicará en la actividad diaria de los funcionarios autorizados a utilizar los sistemas de información automáticos de la Institución.

Áreas y usuarios involucrados

1. Entidad Financiera
2. Proveedor de Servicio de Tecnología
3. Proveedor de Servicio de Seguridad Informática

Definiciones

Sistema de Información Automático

Un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio.

Sistema informático

El hardware o equipo computacional conformado por cada una de las partes físicas que forman un computador, incluidos sus periféricos, maquinaria y equipos.

El software o conjunto de programas (Sistemas operativos, aplicaciones) que permiten Operar el equipo computacional.

Sistemas Informáticos Críticos

Aquellos que automaticen los procesos críticos para el negocio de la Entidad Financiera.

Software Malicioso

Ciertos programas, denominados en su conjunto como malware o software malicioso, creados con la intención principal de atacar a la seguridad de los sistemas informáticos.

Virus Informático

Programa diseñado para copiarse dentro de otro programa. Es diseñado para causar la pérdida o alteración de datos en una estación de trabajo y en casos extremos en el sistema al cual está conectada.

Antivirus

Software que detecta y elimina los virus informáticos. En su mayoría contiene dos partes la primera se activa al inicializar el equipo y la segunda se puede ejecutar en cualquier momento a voluntad expresa del usuario.

1.1.3.7. Acceso a Recursos Tecnológicos

Objetivo

Minimizar los riesgos operativos del proceso de Administración de Acceso a Recursos Tecnológicos, que consiste en la administración de control de acceso a las diferentes plataformas de producción de la Entidad Financiera.

Alcance

Límites del proceso

El proceso de Administración de Acceso a Recursos Tecnológicos inicia con la solicitud de acceso a una plataforma de producción de la Institución, siguiendo luego, con la creación, modificación o eliminación del(os) usuario(s) en la misma.

Aplicabilidad

Se aplicará a todos los accesos que se generen a nivel de los sistemas operativos, bases de datos, utilitarios de plataforma, en el ambiente de Producción de la Entidad Financiera.

Áreas y usuarios involucrados

1. Auditoría
2. Proveedor del Servicio de Administración de Claves.
3. Proveedor del Servicio de Tecnología

Definiciones

Usuarios del Sistema

Usuarios que vienen predefinidos en un utilitario, base de datos o sistema operativo.

Formato Encriptado

Formato en el que se almacena la información a través de un tratamiento a fin de impedir que nadie excepto el destinatario de los mismos pueda leerla.

1.1.3.8. Administración de Perfiles

Objetivo

Minimizar las vulnerabilidades de seguridad informática del proceso de Administración de Perfiles, el mismo que permite implementar en los recursos de Tecnología de Información la definición formal de un perfil establecida por su propietario y autorizada por los correspondientes propietarios de información.

Alcance

Límites del proceso

El proceso de Administración de Perfiles inicia con la solicitud de implementación de perfiles por parte de su propietario, siguiendo luego, con la configuración de acceso en el/los recursos de Tecnología de Información solicitados.

Aplicabilidad

Se aplicará a todas las implementaciones de perfiles que accedan a los recursos de Tecnología de Información de la Entidad Financiera en el ambiente de Producción, como son:

- Opciones, recursos, transacciones y/o servicios de aplicativos informáticos
- Herramientas de Ofimática como correo electrónico, Internet, etc.
- Accesos a recursos adicionales como USB, lector de diskette, impresoras locales, firmas digitales, entre otros.

Áreas y usuarios involucrados

1. Propietario de Perfiles.
2. Proveedor del Servicio de Administración de Claves.
3. Proveedor del Servicio de Tecnología.

Definiciones

Formato Encriptado

Formato en el que se almacena la información a través de un tratamiento a fin de impedir que nadie excepto el destinatario de los mismos pueda leerla.

1.1.3.9. Administración de Accesos Usuarios

Objetivo

Minimizar los riesgos operativos del proceso de Administración de Usuarios que consiste en atender los requerimientos de asignación, cambio, modificación o eliminación de usuarios, de acuerdo a las políticas y procedimientos definidos para la administración de seguridades en cada uno de los aplicativos de la Organización.

Alcance

Límites del proceso

El proceso analizado inicia con el requerimiento de acceso a la información del usuario final, a continuación la generación de la Orden de Trabajo (ODT), la validación e implementación del requerimiento y respectiva respuesta al solicitante.

Aplicabilidad

Se aplicará a todos los requerimientos de administración de usuarios en todos los aplicativos del ambiente de Producción de la Entidad Financiera, Áreas y usuarios involucrados.

Áreas y usuarios involucrados

1. Punto de Contacto
2. Usuario Final
3. Proveedor de Servicio de Administración de Claves
4. Proveedor de Servicio de Tecnología

Definiciones

Punto de Contacto

Representante definido por el Gerente de cada área o departamento que tiene bajo su responsabilidad la administración de las necesidades de información de los usuarios finales de dicha área o departamento.

Usuario Final

Los funcionarios que tienen acceso privilegiado a la información a través de un sistema de información automático, concedido por medio de un proceso formal de definición, aprobación e implantación de estos accesos.

Formato Encriptado

Formato en el que se almacena la información a través de un tratamiento a fin de impedir que nadie excepto el destinatario de los mismos pueda leerla.

1.1.3.10. Definición de Perfiles

Objetivo

Establecer la definición de perfiles en los recursos de Tecnología de Información de la Entidad Financiera.

Alcance

Se considerará en el proceso de definición de perfiles, a fin de garantizar una adecuada implementación de los mismos.

Áreas Involucradas

1. Todas las Áreas de la Entidad Financiera.

Definiciones

Perfil

Inventario de accesos a los recursos de Tecnología de Información que permiten al personal cumplir con sus funciones de negocio formalmente definidas, pudiendo ser:

- Opciones, recursos, transacciones y/o servicios de aplicativos informáticos
- Herramientas de Ofimática como correo electrónico, Internet, etc.
- Accesos a recursos adicionales como USB, lector de diskette, impresoras locales, firmas digitales, entre otros.

1.1.3.11. Reseteo de Claves de Usuarios

Objetivo

Minimizar los riesgos operativos identificados en el análisis de riesgo del proceso de Reseteo de Claves de Usuario el mismo que consiste en inicializar la clave de un usuario con un valor predefinido debido a su olvido o confusión por parte del funcionario solicitante.

Alcance

Límites del proceso

El proceso analizado inicia con el requerimiento de reseteo por parte del usuario final, a continuación su registro, la validación e implementación del requerimiento y respectiva respuesta al solicitante.

Aplicabilidad

Se aplicará a todos los requerimientos de administración de usuarios en todos los aplicativos de los ambientes de Producción de la Entidad Financiera.

Áreas y usuarios involucrados.

1. Usuario Final
2. Proveedor del Servicio de Administración de Claves.
3. Proveedor del Servicio de Reseteo de Claves de Usuarios.
4. Proveedor del Servicio de Tecnología.

Definiciones

Usuario Final

Los funcionarios que tienen acceso privilegiado a la información a través de un sistema de información automático, concedido por medio de un proceso formal de definición, aprobación e implantación de estos accesos.

1.1.3.12. Clasificación de Riesgos de Proyectos

Objetivo

Definir los criterios objetivos con los que se obtendrá la calificación del riesgo de un Proyecto de Aplicación, la misma que determinará si el Proyecto deberá ser certificado para pasar a producción.

Alcance

Límites del proceso

El proceso se inicia con la notificación del Proveedor de Servicio de Tecnología - Líder de Proyecto al Proveedor de Servicio de Seguridad Informática sobre un nuevo Proyecto de Aplicación que ha finalizado su fase de Visión y Alcance, a continuación se realiza la Calificación de Riesgo por el personal del Proveedor de Servicio de Seguridad Informática y se informa su resultado a Auditoría, Riesgo Operativo y al Proveedor de Servicio de Tecnología - Líder de Proyecto.

Aplicabilidad

Se aplicará para todos los Proyectos de Aplicación.

Áreas y usuarios involucrados

1. Riesgo Operativo
2. Proveedor de Servicio de Tecnología
3. Proveedor de Servicio de Seguridad Informática

Definiciones

Proyecto de Aplicación

Son todas las aplicaciones nuevas (desarrolladas, adquiridas o contratadas su desarrollo) o los cambios mayores/significativos que involucren un esfuerzo de 80 horas o más.

1.1.3.13. Desarrollo y Mantenimiento de Sistemas

Objetivo

Minimizar los riesgos operativos inherentes al proceso de Gestión de Proyectos Informáticos.

Alcance

Límites *del proceso*

El proceso inicia con la presentación del Anteproyecto para su aprobación al Comité de Costos y finaliza una vez que la solución automática esté lista para presentarse a la Certificación.

Aplicabilidad

Debe ser considerada para todas las soluciones automáticas que se instalen en el ambiente de producción de la Entidad Financiera.

Áreas y usuarios involucrados

1. Proveedor de Servicio de Tecnología
2. Líder de Producto

1.1.3.14. Administración de la Continuidad

Objetivo

Minimizar el riesgo y su consecuente impacto en la Entidad Financiera si alguna o todas las unidades de Negocio enfrentarían una interrupción no planificada en sus operaciones, ocasionada por una falla en los servicios informáticos y/o telecomunicaciones o por una contingencia.

Alcance

Límites del proceso

Están considerados dentro de los límites todos los procesos del Negocio que han sido definidos como críticos.

Áreas y usuarios involucrados

1. Entidad Financiera

Definiciones

Proceso Crítico

Es el indispensable para la continuidad del negocio y las operaciones de la Entidad Financiera y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo.[1]

Aplicaciones/Servicios/ Activos Críticos

Aquellos que permiten automatizar los procesos críticos del Negocio.

Modelo de Respaldo y Recuperación

Modelo que considera para la información procesada en un determinado sistema:

1 Modo de procesamiento alterno.
2 Almacenamiento fuera de sitio.
3 Nombre de los archivos o tablas a respaldar.
4 Frecuencia de ciclos de obtención, retención y actualización de los respaldos.

- Número de Respaldos – Medios, Número de respaldos a obtenerse por Tabla/Archivo y especificación del medio magnético al cual se direccionarán.
- Revisión periódica de software y hardware para la compatibilidad con los recursos de respaldos.
- Prueba periódica de los respaldos para garantizar la eficacia de la restauración.
- Normas de rotulación, listado, transporte y almacenamiento de los respaldos.

[1] Adaptado de la Resolución No. JB-2005-834 emitida por la Junta Bancaria del Ecuador

Propietario de la Información

Son todos los niveles superiores y/o intermedios de las diferentes áreas de la Entidad Financiera. Un propietario no tiene que ser necesariamente un Líder o Responsable de la Organización, podrá ser también un Comité o una Unidad.

1.1.3.15. Plan de Continuidad del Negocio (BCP – Business Continuity Plan)

Conjunto de tareas que permite a las organizaciones continuar su actividad en la situación de que un evento afecte sus operaciones. Un plan de continuidad afecta tanto a los sistemas informáticos como al resto de procesos de una organización y tiene en cuenta la situación antes, durante y después de un incidente.

De acuerdo a la Resolución No. JB-2005-834 de la Junta Bancaria del Ecuador, el Plan de continuidad está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos tanto en la información como en la operación. Un plan de continuidad incluye un plan de contingencia, un plan de reanudación y un plan de recuperación.

Plan de Contingencia

Conjunto de procedimientos a aplicar en el caso que ocurra un evento particular que pueda afectar a la organización.

La resolución No. JB-2005-834 de la Junta Bancaria del Ecuador, lo define como el conjunto de procedimientos alternativos a la operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto financiero que pueda ocasionar cualquier evento inesperado específico. El plan de contingencia se ejecuta el momento en que se produce dicho evento.

Plan de Reanudación

En la resolución No. JB-2005-834 de la Junta Bancaria del Ecuador, se cita: Especifica los procesos y recursos para mantener la continuidad de las operaciones en la misma ubicación del problema.

Recuperación frente a Desastres (DRP – Disater Recovery Plan)

Procedimientos a aplicar en el caso de que ocurra un incidente de tal magnitud que afecte a la totalidad de los sistemas informáticos de una organización.

La resolución No. JB-2005-834 de la Junta Bancaria del Ecuador, define así al Plan de Recuperación: Especifica los procesos y recursos para recuperar las funciones del negocio en una ubicación alterna o fuera de la Institución.

Análisis de Impacto en el Negocio (BIA –Business Impact Análisis)

El procedimiento de analizar las pérdidas sufridas por una entidad si las actividades críticas del negocio no están disponibles.

1.2. Identificación de Vulnerabilidades – Penetration Testing

Vulnerabilidad

Es una falla de Seguridad en un Sistema, debido a malos diseños, malos desarrollos, malas implementaciones, malas instalaciones y hasta a descuidos humanos. En resumen es una debilidad o una falta de control.

Exploit

Es la herramienta o táctica utilizada de manera tal que permita a un atacante aprovechar una vulnerabilidad dada.

1.2.1. Metodología de Análisis de Seguridad

Consiste en realizar un intento de intrusión controlado a los sistemas de información de la compañía, con el objetivo de identificar las vulnerabilidades a las que están expuestas las redes y definir los planes de acción para mitigarlas

Se busca emular:

- Un intruso fortuito.
- Un intruso motivado.
- Actos intencionales de un empleado insatisfecho.
- Actos accidentales de empleados.
- Otros.

1.2.2. El Mapa de la Seguridad

Las secciones del mapa son:

1. Seguridad Física.
2. Seguridad en Comunicaciones.
3. Seguridad en Internet.
4. Factor Humano.
5. Seguridad de la Información.

1.2.3. Enfoque de Posicionamiento frente al objetivo

Externo:

Se busca emular los diferentes perfiles de atacantes externos y sus motivaciones.

Interno:

Se busca emular los diferentes perfiles de atacantes internos y sus motivaciones.

Dicho enfoque suele ser desde las siguientes ópticas:

- Usuario Final sin privilegios.
- Usuario Administrativo con privilegios.
- Tercero ajeno a la empresa con acceso físico.

1.2.4. Análisis de Vulnerabilidades

Los Análisis de Vulnerabilidades incluyen:

- Escaneo de Red para detectar puertos abiertos, usando las mismas herramientas que utilizan los intrusos.
- Escaneo de Vulnerabilidades de Aplicaciones y de Infraestructura.
- Análisis de cada dirección IP en la red.
- Validación manual del estado del escaneo para eliminar los resultados que son “Falsos Positivos”.

Las herramientas de evaluación de la vulnerabilidad son un método efectivo para identificar las vulnerabilidades que se pueden explotar y tomar medidas proactivas y preventivas para proteger las redes y los sistemas.

1.2.5. Resultado de las Vulnerabilidades encontradas

Vulnerabilidades	Porcentaje
Software defectuoso	60%
Equipo configurado en forma inapropiada	50%
Cumplimiento forzoso inadecuado	50%
Diseño deficiente de redes	70%
Procesos defectuosos o incontrolados	70%
Administración inadecuada	80%
Personal insuficiente	90%
Falta de conocimiento para brindar soporte a usuarios o ejecutar procesos	60%
Falta de funcionalidad en la seguridad	80%
Falta de mantenimiento apropiado	70%
Elección deficiente de contraseñas	80%
Tecnología no probada	80%
Transmisión de comunicaciones no protegidas	80%
Fuga de información	70%
Comunicaciones gerenciales deficientes	90%
Controles de seguridad configurados en forma ineficiente	70%
Políticas y normas de seguridad deficientes	90%
Analizar el cumplimiento de los estándares de seguridad en las Estaciones de Trabajo de la Entidad Financiera.	El 80% de los recursos exponen información sin los controles restrictivos de usuarios (recursos compartidos)
Permisos a usuarios no autorizados sobre carpetas compartidas.	70%
Puertos abiertos innecesarios.	70%
Usuarios locales no autorizados.	80%

Tabla 1.1: Resultados de las Vulnerabilidades encontradas en la Entidad Financiera

1.3. Identificación de Amenazas

Amenazas
Son circunstancias o incidentes que tienen la probabilidad de ocasionar daño a un recurso de información al explotar vulnerabilidades en el sistema.

1.3.1. Clasificación de las amenazas

Las amenazas por lo general se clasifican del siguiente modo:

Naturales
Amenazas tales como: inundaciones, incendios, ciclones, lluvia/granizo plagas y terremotos.

Accidentales
Amenazas físicas tales como: agua, daño/derrumbe de edificios, pérdida de servicios públicos y falla en los equipos.

Físicas Premeditadas
Amenazas como: bombas, incendios y robo.

Intangibles Premeditadas
Fraude, espionaje, hackeo, robo de identidad, código malicioso, ingeniería social, ataques por phishing y negación de ataques de servicio.

1.4. Métricas de Seguridad Informática

Un requerimiento de una gerencia de seguridad efectiva es garantizar que exista una retroalimentación continua sobre una variedad de elementos relacionados con la seguridad.

Se pueden utilizar las métricas técnicas para proporcionar un monitoreo cuantitativo y pueden incluir entre otros, los siguientes elementos:

- Número de vulnerabilidades no corregidas.
- Número de observaciones cerradas de auditoría.
- Número o porcentaje de cuentas de usuario que cumplen con las normas.

Las métricas cualitativas se pueden aplicar para determinar tendencias y puede incluir Indicadores de Calidad.
Otras medidas relevantes de importancia aplicables incluyen la rentabilidad de los controles y el grado de fallas de controles.

Muchas otras métricas son posibles y podrían incluir tanto medidas técnicas como conductuales, por ejemplo: estado del parche, infecciones por virus, reinicio de le contraseñas. Al diseñar las métricas es recomendable establecer un límite para cada medición. Las buenas métricas deben tener atributos SMART, es decir; deben ser específicas, mesurables, alcanzables, repetibles y dependientes del tiempo. Las métricas pueden utilizarse entonces para dar seguimiento al progreso.

1.5. Tabla de Riesgos Identificados

El gerente de seguridad de información debe entender el perfil de riesgo de negocio de una organización. Ningún modelo brinda un panorama completo; sin embargo categorizar lógicamente las áreas de riesgo de una organización facilita centrar la atención en las decisiones y las estrategias clave para la administración de riesgos. Así mismo permite a la organización desarrollar e implementar medidas para la mitigación de riesgos que sean relevantes para el negocio y rentables.

1.5.1. Categorías de riesgo determinadas

Áreas de Riesgo Operativo	Descripción	Mapeo de Información o TI
Riesgo ambiental operativo y de instalaciones	Pérdida o daño a las capacidades operativas ocasionados por problemas en instalaciones, utilerías servicios o equipos	Manejo de la continuidad de negocio para las instalaciones/equipos de TI.
Riesgo de salud e integridad física	Amenazas a la salud o integridad del personal, clientes y público en general	Confidencialidad de domicilios particulares, calendarios de viajes, etc.
Riesgo de seguridad de información	Divulgación o modificación no autorizada de información, pérdida de la disponibilidad de la información o uso inapropiado de la información.	Todos los aspectos de la seguridad de la información y de TI.
Riesgo de marcos de control	Diseño o desempeño inadecuado de la infraestructura de administración de riesgos existente	Análisis del proceso de negocio para identificar flujos de información y puntos de control críticos.
Riesgo legal y de cumplimiento regulatorio	Incumplimiento de las leyes de los países en los que se opera, incumplimiento de cualquier norma fiscal, regulatoria o de presentación de información, incumplimiento de contratos o no celebrar contratos para proteger los intereses del negocio	Cumplimiento con la legislación para la protección de datos, regulaciones para el control criptográfico, etc. la exactitud, oportunidad y calidad de la información presentada a las entidades y el manejo del contenido de toda la información que se envía a terceros.
Riesgo de gobierno corporativo	Incumplimiento de los directores con sus obligaciones regulatorias personales en el manejo y el control de la compañía.	Elaboración de políticas sobre seguridad de información, medición e informes sobre el desempeño.

Áreas de Riesgo Operativo	**Descripción**	**Mapeo de Información o TI**
Riesgo reputacional	Los efectos negativos de la opinión pública y la opinión de los clientes, la reputación del mercado y el daño ocasionado a la marca por fallas en el manejo de las relaciones públicas.	Controlar la divulgación de información confidencial; presentar la imagen pública de una empresa bien administrada.
Riesgo estratégico	No cumplir con las metas estratégicas a largo plazo del negocio, entre ellas, depender de resultados calculados o planeados que puedan estar bajo el control de terceros.	Administrar la calidad y la consistencia de la información sobre la cual se basen las decisiones de negocio estratégicas tales como: fusiones, adquisiciones y ventas.
Riesgo de procesamiento y desempeño	Problemas con la entrega del servicio o producto ocasionados por fallas en los controles internos, sistemas de información o integridad de los empleados, errores, o deficiencias en los procedimientos operativos.	Todos los aspectos de la seguridad de los sistemas de información y la aplicación de la seguridad por parte de los empleados al llevar a cabo sus funciones.
Riesgo Tecnológico	Falla en la planeación, el manejo y monitoreo del desempeño de los proyectos, productos, servicios, procesos, personal y canales de distribución relacionados con la tecnología	Falla en los sistemas de tecnología de información y comunicaciones y la necesidad de una administración de la continuidad del negocio.
Riesgo de administración de proyectos	Falla en la planeación y administración de los recursos requeridos para alcanzar metas tácticas de proyectos, que conducen a excesos de presupuesto, de tiempo, una combinación de ambos o una falla para concluir el proyecto, la falla técnica	Administración de todos los proyectos relacionados con seguridad de información.

Áreas de Riesgo Operativo	Descripción	Mapeo de Información o TI
	de proyecto o no administrar los aspectos de integración con las partes involucradas del negocio y el impacto que pueden tener los cambios en las operaciones de negocio.	
Riesgo de actos ilícitos o delictivos	Pérdida o daño ocasionado por fraude, robo, negligencia voluntaria, faltas graves, vandalismo, sabotaje, extorsión.	Proporcionar servicios y mecanismos de seguridad para prevenir todo tipo de delito cibernético.
Riesgo de recursos humanos	No reclutar, desarrollar o retener a los empleados que cuenten con habilidades o conocimientos apropiados, falla para manejar las relaciones laborales.	Necesidad de políticas que protejan a los empleados de acoso sexual, racismo, etc. mediante sistemas de correo electrónico corporativo, etc.
Riesgo de proveedores	No evaluar adecuadamente las capacidades de los proveedores, que resulte en interrupciones en el proceso de abastecimiento o calidad deficiente en la entrega de los bienes y servicios proporcionados; no entender o administrar los temas de la cadena de abastecimiento.	Contratación externa de actividades de procesamiento de información de TI u otra información de negocio.
Riesgo de información gerencial	Presentación de información inadecuada, imprecisa, incompleta o inoportuna para sustentar el proceso de toma de decisiones de la gerencia.	Administrar la precisión, integridad, vigencia, oportunidad y calidad de la información utilizada para sustentar las decisiones gerenciales.
Riesgo de ética	Daño ocasionado por prácticas de negocio no éticas, entre ellas,	Recopilación, almacenamiento y uso ético de la información;

Áreas de Riesgo Operativo	Descripción	Mapeo de Información o TI
	aquellas de socios comerciales. Los temas incluyen discriminación racial o religiosa, explotación de mano de obra infantil, contaminación, temas ambientales, conducta ante grupos en desventaja, etc.	manejo del contenido informativo de sitios Web, Intranets y correos electrónicos corporativos, así como sistemas corporativos de mensajería instantánea.
Riesgo geopolítico	Pérdida o daño en algunos países ocasionado por inestabilidad política, calidad deficiente de infraestructura en regiones en desarrollo o diferencias culturales y malos entendidos.	Manejar todos los aspectos de la seguridad de información y de seguridad de sistemas de TI en regiones en las que la empresa opera pero donde existen riesgos geopolíticos particulares.
Riesgo climático	Pérdida o daño ocasionado por condiciones climáticas inusuales entre ellas: sequía, calor inundación, frío, tormenta, vientos, etc.	Manejo de la continuidad del negocio para los equipos de TI.

Tabla 1.2: Categorías de Riesgo

1.6. Determinación del Impacto

Impacto

Es el elemento fundamental para la administración de riesgos. En última instancia, todas las actividades para la administración de riesgos están diseñadas para reducir el impacto a niveles aceptables.

El análisis de impacto determinará la criticidad y sensibilidad de los activos de información.

Al resultado de cualquier vulnerabilidad que sea explotada por una amenaza que ocasione una pérdida se llama **impacto.**

El impacto se **cuantifica** como una pérdida financiera directa a corto plazo o una pérdida financiera fina (**indirecta)** a largo plazo.

Es toda pérdida ocasionada por una vulnerabilidad que sea explotada por una amenaza.

1.6.1. Resultado de los posibles impactos

El impacto se determina mediante una evaluación de impacto al negocio y el análisis posterior. Este análisis determinará la criticidad y sensibilidad de los activos de información. Brindará la base para establecer facultades de control de acceso, así como para los planes de continuidad de negocio.

Impactos	Porcentajes
Pérdida directa de dinero (efectivo o crédito)	80%
Responsabilidad penal o civil	80%
Pérdida de reputación, buen nombre/imagen	70%
Reducción en el valor de las acciones	70%
Conflicto de intereses para el personal, clientes o accionistas	70%
Violaciones a la confidencialidad/privacidad.	80%
Pérdida de oportunidades de negocio/competencia.	80%
Pérdida de participación en el mercado.	70%
Interrupción en las actividades de negocio.	70%
Reducción en el desempeño/eficiencia operativos	80%

Tabla 1.3: Resultados de los posibles Impactos en la Entidad Financiera

1.7. Determinación del Nivel de Riesgo

El estado de riesgo actual se debe determinar mediante una evaluación integral de riesgos. Así como deben establecerse los objetivos de riesgo como parte del estado deseado, así debe determinarse el estado actual del riesgo para establecer la base para realizar un análisis diferencial de los riesgos que deba incluirse en la estrategia y hasta qué grado.

Una evaluación completa de riesgos incluye un análisis de amenazas y vulnerabilidad que de manera individual proporcionen información útil para desarrollar una estrategia.

Puesto que los riesgos pueden tratarse de distintas formas: por ejemplo: modificando la conducta riesgosa, desarrollando contramedidas para las amenazas, reduciendo las vulnerabilidades o desarrollando controles, esta información dará el fundamento para determinar la estrategia más rentable para tratar los riesgos. De igual forma llevar a cabo evaluaciones periódicas adicionales permitirá obtener las métricas necesarias determinar los avances.

El riesgo es parte inherente del negocio y, dado que resulta impráctico y costoso eliminar todos los riesgos, cada organización tiene un nivel de riesgo que acepta. Para determinar el nivel razonable de riesgo aceptable, el administrador de riesgos debe determinar el punto óptimo en el cual el costo de las pérdidas se interfecta el costo de mitigar el riesgo.

Determinar medidas del Riesgo

- Es la probabilidad de que una amenaza ocurra.
- Es la facilidad con que un ataque se implementa (Amenaza x Vulnerabilidad).

- Un riesgo resulta de la existencia de una amenaza explotando una vulnerabilidad.

- Una amenaza sin vulnerabilidad no presenta riesgo, y una vulnerabilidad sin amenaza tampoco.

- Si la combinación de amenaza y vulnerabilidad no produce impacto, tampoco han de implantarse las medidas de protección necesarias.

- Un riesgo puede estar compuesto por varias amenazas.

Una vez que hemos identificado las amenazas, será necesario determinar que tan probable es que esa amenaza pueda ocurrir. Al examinar la amenaza existen dos formas claves de evaluar la probabilidad e impacto. El primer método es establecer la probabilidad sin la consideración de los controles existentes. El otro método es examinar el nivel de riesgo tomando en cuenta los controles existentes. Esto permitirá examinar los controles existentes y establecer un nivel de riesgo basado en que tan eficaces son los controles existentes. La probabilidad a la que es susceptible una organización respecto a una amenaza específica se describe típicamente como alta, media o baja.

Una vez que la probabilidad de que las amenazas ha sido determinada, entonces el Impacto de las amenazas tendrá que evaluarse. Antes de determinar el nivel del impacto, es necesario asegurar que el alcance del análisis y evaluación de riesgos se ha definido claramente.

Nivel de Impacto	Definición
Alto	La perdida de confidencialidad, integridad o disponibilidad podría ser esperada o tener efectos severos en las operaciones organizacionales, activos o individuos. • Degradación severa o perdida de la capacidad de la misión en una extensión y duración que la organización no es capaz de realizar

	sus funciones primarias. • Resulta en un daño mayor para los activos de la organización. • Resulta en pérdidas financieras mayores. • Resulta en daños severos o catastróficos para los individuos involucrando la perdida de la vida o serias amenazas a la vida.
Medio	La perdida de confidencialidad, integridad o disponibilidad podría ser esperada o tener efectos serios en las operaciones organizacionales, activos o individuos. • Degradación significativa en la capacidad de la misión en una extensión y duración que la organización es capaz de realizar sus funciones primarias, pero la efectividad es reducida. • Resulta en un daño significativo para los activos de la organización. • Resulta en pérdidas financieras significativas. • Resulta en daños significativos para los individuos pero no en la perdida de la vida o serias amenazas a esta.
Bajo	La perdida de confidencialidad, integridad o disponibilidad podría ser esperada o tener efectos limitados en las operaciones organizacionales, activos o individuos. • Degradación en la capacidad de la misión en una extensión y duración que la organización es capaz de realizar sus

	funciones primarias, pero la efectividad es reducida. • Resulta en un daño menor para los activos de la organización. • Resulta en pérdidas financieras menores. • Resulta en una exposición menor al daño.

Tabla 1.4: Definición del nivel de impacto

Una vez se ha establecido el nivel de probabilidad y el nivel de impacto, se podrá asignar un nivel de riesgo. Esto puede hacerse creando la siguiente matriz:

Alto : Una acción correctiva debe ser implementada
Moderado Alto : Una acción correctiva debería ser implementada
Moderado Bajo : Se requiere acciones de monitoreo.
Bajo : No se requiere ninguna acción en este momento

Resultado de la Determinación del Nivel de Riesgo

Amenazas vs. Impacto	Nivel de Riesgo
Pérdida directa de dinero (efectivo o crédito)	Alto
Violaciones a la confidencialidad/privacidad	Alto
Interrupción en las actividades de negocio	Alto
Interrupción en las actividades de negocio	Alto
Responsabilidad penal o civil	Alto
Reducción en el valor de las acciones	Alto
Pérdida de oportunidades de negocio/competencia	Alto

Tabla 1.5: Resultado de la Determinación del Nivel de Riesgo

Después de que el nivel de riesgo ha sido evaluado, el siguiente paso es preguntarse ¿qué se va a hacer con los riesgos? esta etapa es conocida como el manejo o la administración del riesgo y básicamente hay 3 alternativas, una es tolerar el riesgo (no se implementan controles), otra es transferir el riesgo (se transfiere el riesgo a un tercero) y la ultima es mitigar el riesgo (se implementan controles), esta alternativa es la que tiene un peso mayor en el proceso ya que en esta se buscará que la organización tenga un nivel aceptable de riesgos. Por consiguiente, será importante identificar tantos controles como sea posible. En esta etapa se requiere la participación de especialistas de seguridad.

Al seleccionar cualquier tipo de control será necesario medir el impacto operacional para la organización. Cada control tendrá un impacto de alguna manera.

El costo de los controles debe ser analizado y evaluado detalladamente, Una buena regla de dedo es evaluar si el control es más caro que el activo que va a proteger no se debe implementar.

Durante esta etapa se podrá determinar si se requieren controles de seguridad basados en algún estándar.

Análisis Costo-Beneficio

Después de identificar todos los controles posibles y evaluar su viabilidad y efectividad se debe realizar un análisis costo-beneficio.

Este proceso debe ser realizado para cada control, para determinar si el control recomendado es apropiado para la organización. Un análisis de costo- beneficio debe determinar el impacto de implementar y después determinar el impacto de no implementarlo.

Uno de los costos a largo plazo de cualquier control es el requerimiento de mantener su efectividad. Al realizar un análisis de costo-beneficio es necesario considerar el costo de implementación basado en los siguientes factores:

• Costo de implementación incluyendo la inversión inicial para el software y hardware, como mantenimientos soporte etc. etc.
• Reducción de efectividad operacional.
• Implementación de políticas adicionales y procedimientos para apoyar a los controles.
• El costo de la capacitación que apoye al personal a mantener la efectividad del control.

Prácticamente ningún activo o actividad está libre de riesgo, y no todos los controles implementados pueden eliminar el riesgo, el propósito de manejar los riesgos es tener a la organización con el nivel de seguridad que realmente requiere para tener un nivel aceptable de riesgo y que la operación, la capacidad de servicio no se vean afectadas por la implementación de controles además de que la inversión sea razonable y que no se hagan inversiones cuantiosas e innecesarias. Un programa de seguridad que tiene como su meta el 100% de seguridad causará que la organización tenga 0% de productividad, teniendo en cuenta que ningún control mitigara el 100% del riesgo en ninguna situación.

2. CAPÍTULO 2 MARCO DE GESTIÓN PARA LA SEGURIDAD DE INFORMACIÓN

Introducción Normas ISO 27001 e ISO 27002

ISO 27001

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

1979 Publicación BS 5750 - ahora ISO 9001
1992 Publicación BS 7750 - ahora ISO 14001
1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.
En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar **ISO 27001.**

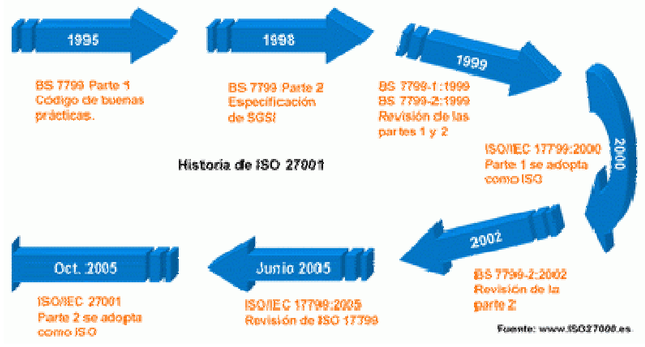

Figura 2.1: Historia de ISO 27001

Este Estándar Internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este Estándar Internacional fomenta que sus usuarios enfaticen la importancia de:

1. Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
2. Implementar y operar controles para manejar los riesgos de la seguridad de la información.
3. Monitorear y revisar el desempeño y la efectividad del SGSI y
4. Mejoramiento continuo en base a la medición del objetivo.

Este estándar internacional adopta el modelo del proceso: Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI.

Modelo del Proceso: Planear-Hacer-Chequear-Actuar

Planear (Establecer el SGSI)	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
Hacer (Implementar y Operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos SGSI
Chequear (Monitorear y Revisar el SGSI)	Evaluar, y donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
Actuar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante para lograr el mejoramiento continuo del SGSI.

Tabla 2.1: Modelo del Proceso (PDCA)

Existen cinco CLAVES que se plantea en ISO-27001

1. Orientar la seguridad con sus procesos de negocio.
2. Gestionar su seguridad (no solo medidas técnicas).
3. Continuar su proceso de calidad.
4. Obtener una validación sólida sobre la situación.
5. Entrar en el proceso que se está gestando.

1. Orientar la seguridad con sus procesos de negocio

El primer paso para la implementación de ISO-27001, es el análisis de riesgo (AR)
Esta actividad, puede hacerse siguiendo cualquier metodología, siempre y cuando demuestre coherencia.

El resultado final del mismo, será a través del análisis de activos, impacto, salvaguardas, etc, llegar a determinar los niveles de riesgo (fundamentalmente residuales) al que cada activo quedará expuesto, con la intención de "trabajar" de aquí en más sobre los mismos, en un ciclo continuo (Plan-Do-Check-Act).

2. **Gestionar su seguridad (no solo medidas técnicas):** El holismo enfatiza la importancia del todo, el cual, es más grande que la suma de las partes y da importancia a la interdependencia de estas. Holismo, eso es gestionar la seguridad.
La experiencia, es que la seguridad hasta ahora no dejaba de ser un conjunto de partes, conformadas por mayor o menor cantidad de medidas técnicas, según la empresa. ISO-27001, reúne la totalidad de ellas y al integrarlas a través de un Sistema de Gestión de la Seguridad de la Información (SGSI) y llevado como un ciclo continuo (PDCA) genera holismo, un resultado superior a la suma de sus partes.

3. Continuar su proceso de calidad. Todo proceso tecnológico se encuentra en una situación de necesidad de demostrar, garantizar y justificar su "Calidad".
Calidad, esa es la palabra clave de la Industria competitiva. Hoy en día, en casi todos los productos, el usuario final tiene una clara visión de lo que está comprando, y sabe casi con certeza, si se trata de un producto de buena, de dudosa, y/o de escasa calidad. Todo ello se debe a una serie de medidas, acciones, denominaciones, controles, garantías, certificaciones, y por supuesto la gran mayoría de ellos pasa por organismos reguladores, a los cuales ciertas industrias se esfuerzan por "escuchar y seguir" y otras no.

Al usuario final le llega esta imagen, gracias a toda una cadena industrial, que va desde la materia prima hasta el producto final. En el siglo XXI, uno de los pilares de esta cadena es la informática, por lo tanto si se está hablando de una cadena de eslabones compuestos por calidad, no queda más que volver al viejo dicho "una cadena se corta por el eslabón más fino".
De esto se trata ISO 27001. Si tuviera que reducirse toda la norma en una frase sería: ISO 27701 "Pone calidad a la seguridad"

4**. Obtener una validación sólida sobre su situación:** ISO-27001, puede ser el puente de unión entre las orillas de la seguridad y las regulaciones legales. Esta consideración no puede dejar dudas, pues el último grupo de controles de ISO-27001, se refiere a "Marco legal y buenas prácticas".

5. Entrar en el proceso que se está gestando: Uno de los principales motores que están incrementando las certificaciones ISO 27001 son la aparición en contratos, de sugerencias al proveedor respecto a estar certificado en esta norma. Cada vez más contratos, estipulan que el proveedor apropiado debería tener la certificación en ISO-27001.

Dominios de la ISO 27001

Dominios	Descripción
Dominio 1: Política de Seguridad	Proporcionar dirección y apoyo gerencial para brindar seguridad de la información.
Dominio 2: Organización de la Seguridad	Administrar la seguridad de la información dentro de la organización**.**

Dominio 3: Clasificación de la Información	Determinar los niveles de clasificación de la información para su protección frente a pérdida, divulgación o cualquier forma de uso indebido.
Dominio 4: Seguridad en los Recursos Humanos	Reducir los riesgos de error humano, robo, fraude o uso inadecuado de instalaciones.
Dominio 5: Seguridad Física y Ambiental	Impedir accesos no autorizados, daños e interferencia a las sedes e información de la empresa
Dominio 6: Administración de las Comunicaciones y Operaciones	Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
Dominio 7: Control de Accesos	El acceso a la información y los procesos de negocio deben ser controlados sobre la base de los requerimientos la seguridad y de los negocios.
Dominio 8: Adquisición, desarrollo y mantenimiento de Sistemas de Información	Asegurar que la seguridad es incorporada a los sistemas de información.
Dominio 9: Administración de Incidentes.	Objetivos. Identificación, Registro, Análisis, Solución y Reporte.
Dominio 10: Administración de la Continuidad de los Negocios	Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos de los negocios de los

	efectos de fallas significativas o desastres.
Dominio 11 Cumplimiento de Leyes y Regulaciones.	Impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

Tabla 2.2: Dominios de la ISO 27001

ISO27002

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Este estándar contiene 11 cláusulas de control de seguridad, conteniendo colectivamente un total de 39 categorías de seguridad principales y una cláusula introductoria que presenta la evaluación y tratamiento del riesgo.

Cada cláusula contiene un número de categorías de seguridad principales. Las 11 cláusulas (acompañadas por el número de categorías de seguridad principales incluidas dentro de cada cláusula) son:

a) Política de Seguridad (1);
b) Organización de la Seguridad de la Información (2);
c) Gestión de Activos(2);
d) Seguridad de Recursos Humanos (3);
e) Seguridad Física y Ambiental (2);
f) Gestión de Comunicaciones y Operaciones (10);
g) Control de Acceso (7);

h) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información (6);
i) Gestión de Incidentes de Seguridad de la Información (2):
j) Gestión de la Continuidad Comercial (1);
k) Conformidad (3)

Nota: El orden de las cláusulas en este estándar no implica su importancia. Dependiendo de las circunstancias todas las cláusulas pueden ser importantes, por lo tanto, cada organización que aplica este estándar debiera identificar las cláusulas aplicables, cuán importante son y su aplicación a los procesos comerciales/individuales. También, las listas en este estándar no están por orden de prioridad a no ser que así se especifique.

2.1. Requerimientos mínimos obligatorios

Todos los programas de seguridad de información tienen que informarse y orientarse por los requerimientos legales y regulatorios de la organización. El cumplimiento con las normas de gobierno obligatorias, la debida diligencia y un apoyo tecnológico apropiado de las políticas legales son áreas que dependen, en parte, del programa de seguridad de información.

Además se podría requerir al gerente de seguridad de información que apoye las normas legales relacionadas con la privacidad de la información y las transacciones, la recopilación y el manejo de registros de auditoría, las políticas de retención de correos electrónicos, los procedimientos de investigación de incidentes, así como la cooperación con las autoridades legales. Los temas legales también deben tenerse en consideración cuando se investigue o se monitoree a un empleado de la organización, o bien, cuando se vayan a tomar medidas disciplinarias por comportamiento inadecuado.

2.1.1. Factores físicos y ambientales

La confidencialidad, la integridad y la disponibilidad de la información podrían verse afectadas por el acceso físico o el daño o la destrucción de componentes físicos. El nivel de seguridad que rodea a cualquier hardware o software de información debe depender de la sensibilidad de los datos a los que se pueda acceder, la importancia de las aplicaciones procesadas, el costo del equipo y la disponibilidad del equipo de respaldo.

Existe una amplia variedad de controles de seguridad físicos tales como: candados electrónicos, detectores de movimientos, cámaras, dispositivos de bloqueo, que se encuentran disponibles para que el gerente de seguridad de información implemente la seguridad física.

Es preciso establecer políticas de seguridad física como complemento de los dispositivos de control. El control físico para los recursos informáticos debe aplicarse con base en la sensibilidad de la información que en ellos se procesa y almacena. Se debe proporcionar acceso solo cuando sea necesario. Los ambientes informáticos tienen que implementar sistemas para monitorear y controlar los factores ambientales tales como: la temperatura, la humedad y la calidad de la energía eléctrica.

Los computadores personales suelen utilizarse en áreas menos seguras, y por ello, requieren de consideraciones especiales. Si una estación de trabajo tiene una función particularmente sensible o se requiere que almacene información sensible, sería conveniente aislar dicha estación de trabajo.

Las laptops y los dispositivos portátiles también pueden requerir consideraciones especiales, en particular dados los riesgos significativos de robo o pérdida durante el viaje.

El gerente de seguridad de información tiene que proporcionar controles de confidencialidad sólidos y persistentes para proteger la información sensible en caso de captura de la laptop o el dispositivo portátil.

2.1.2. Ética

Es importante que el programa de la gerencia de la seguridad de información implemente un código de ética que oriente las decisiones y las actividades.
El programa suele requerir que las personas se involucren en actividades en las que sea importante un ejercicio sólido de la ética, por ejemplo: monitorear actividades del usuario, pruebas de penetración, acceso a datos personales sensibles.

Las actividades deben limitarse de manera explícita a responsabilidades definidas y deben llevarse a cabo con profesionalismo y de acuerdo con las leyes y políticas aplicables.

2.1.3. Diferencias culturales/regionales

El gerente de seguridad de información debe conocer las diferencias que existen en las percepciones, costumbres y comportamientos apropiados en las diferentes regiones y culturas. Deben desarrollarse e implementarse políticas, controles y procedimientos. Deben evitarse algunos elementos que podrían ser ofensivos culturalmente para otros.

El gerente de seguridad de información debe coordinarse con el departamento de recursos humanos para desarrollar estrategias adecuadas para tratar las diferencias que existen en las diferentes regiones y culturas que se encuentran representadas dentro de la organización.

2.1.4. Logística

El gerente de seguridad de información debe tratar los temas logísticos en forma efectiva, sobre todo considerando el volumen significativo de interacción con otras unidades de negocio y personas que requiere un programa efectivo de la gerencia de la seguridad de información.

A continuación se enlistan algunos temas logísticos que el gerente de seguridad de información necesita ser capaza de manejar.

- Planeación y ejecución estratégica e interinstitucional.
- Administración de proyectos y tareas.
- Coordinación de reuniones y actividades del comité.
- Desarrollo de programas de procedimientos que se ejecutan regularmente.
- Priorización de recursos y administración de cargas de trabajo.

2.2. Protección de la Información Financiera

La Información Corporativa (información relativa a los productos, servicios, clientes, proveedores, personal, método de trabajo, organización, estrategias empresariales, información económica y financiera, etc...) se considera como uno de los principales activos de negocio de cualquier empresa, y como tal, debe ser protegida adecuadamente con medios técnicos y legales, de forma que se evite, en la medida de lo posible, que cualquier persona física o jurídica pueda acceder/obtener/tratar/difundir la misma fraudulenta o ilícitamente, causando perjuicios más o menos graves a su titular.

A continuación se abordan determinados medios legales a tener en cuenta por cualquier empresa para la protección de la Información Corporativa Confidencial, tanto a nivel interno (con respecto al personal que accede/trata esa información con motivo de su relación laboral), como a nivel externo (cuando es una tercera empresa o persona la que accede y trata la información); así como las acciones legales que permiten la defensa y reparación de los derechos e intereses del titular.

2.2.1. ¿Qué entendemos por Información Confidencial?

La Real Academia de la Lengua Española define “Confidencial” como “que se hace o se dice en confianza o con seguridad reciproca entre dos o más personas”, y “Confidencialidad” como “la cualidad de confidencial”.

Así, el empresario tiene la libertad de calificar como Confidencial, cualquier documento o información, que a su juicio, influya directa o indirectamente en el desarrollo del negocio: estrategias empresariales, métodos de negocio, documentos contractuales, propiedad intelectual, patentes, desarrollo de nuevos productos, etc.

Esta Información Confidencial ha de gozar de una protección especial, tendente a evitar su filtración, divulgación o difusión a terceros, acciones que pueden causar graves perjuicios a su empresa (imaginemos por ejemplo, que una determinada estrategia empresarial tendente a posicionar en el mercado una determinada empresa, es filtrada y difundida previa y fraudulentamente a la competencia, lo que impide al empresario el posicionamiento deseado).

2.2.2. Protección interna de la Información Confidencial de la empresa.

A) ¿Qué establecen las normas laborales?

Respecto a la Protección de la Información Confidencial dentro de la propia empresa hay que distinguir entre los trabajadores y el personal de alta dirección, que por razón de su puesto y funciones, accede o trata dicha Información.

En cuanto a los Trabajadores, se entiende que existe una obligación de confidencialidad y secreto intrínseca a la relación laboral, incluso cuando no exista una referencia expresa a la misma en el Contrato de Trabajo o no se hayan firmado Acuerdos de Confidencialidad específicos.

A pesar que existan Estatutos de los Trabajadores es recomendable incluir en los Contratos Laborales o adicionalmente a los mismos, Acuerdos o Pactos de Confidencialidad, que establezcan claramente las obligaciones de los trabajadores en este sentido.

Con la firma de estos Acuerdos o Pactos de Confidencialidad, informaremos a los trabajadores de las pautas a seguir en el tratamiento de la Información Confidencial, sus obligaciones y los límites establecidos, pudiendo, con esta medida, reducir algunas prácticas que se dan en el mundo empresarial (por ejemplo: llevarse las bases de datos o información confidencial o reservada, desarrollos de nuevos productos, etc... en el momento de abandonar el puesto laboral) o, en caso contrario, tener un documento que pueda servir como prueba en juicio en el que se manifiesta expresamente la obligación de confidencialidad y secreto, y el conocimiento del trabajador de tal obligación.

En cuanto al Personal de Alta Dirección, y dado que por razón de su cargo acceden a información especialmente sensible y/o confidencial, existe la obligación expresa de mantener la confidencialidad y secreto de las informaciones a las que tiene acceso por razón de su cargo, siendo práctica habitual el firmar

Acuerdos específicos de confidencialidad junto con los Contratos de Trabajo, bien a través de una cláusula específica de confidencialidad en los Contratos, o bien incluyendo un Pacto o Acuerdo de Confidencialidad como Anexo al contrato principal de trabajo.

Además de la obligación de confidencialidad específica que tiene el personal de alta dirección de las empresas, hay que hacer referencia al pacto de no concurrencia, es decir, aquel por el que un personal de alta dirección no podrá celebrar contratos de trabajo con otras empresas.

B) Otros medios de protección interna de la Información Corporativa o Confidencial.

Además del establecimiento de Acuerdos o Pactos de Confidencialidad, la empresa deberá tener establecidos medios técnicos u organizativos que permitan la protección de la información confidencial independientemente del soporte en el que sea tratada o almacenada.

Así es recomendable establecer las siguientes medidas de protección:

- Limitar el acceso a la información confidencial. Es decir, permitir el acceso a dicha información sólo al personal que por razón de su cargo o funciones es necesario que acceda a dicha información, no permitiendo tal acceso al resto del personal.

- Establecer medidas técnicas que permitan la visualización o tratamiento de información confidencial (por ejemplo: uso de contraseñas para el acceso a los documentos, criptografía, etc...).

- Mantener/Almacenar los documentos confidenciales en soporte papel, en armarios que se encuentren cerrados bajo llave o cajas fuertes, a las que sólo tengan acceso las personas autorizadas.

- Realizar copias de seguridad que eviten la perdida de información confidencial o sensible en caso de catástrofe, guardando una copia fuera de las instalaciones principales de la empresa (recordemos lo sucedido en el edificio Windsor de Madrid para comprender la importancia de esta medida).

Por último, y en relación a la protección de la información confidencial dentro del ámbito interno de la empresa, hay que señalar que en la prestación de determinados servicios se accede a información confidencial de terceros, existiendo de este modo, una obligación especifica de confidencialidad con respecto a esa tercera empresa, obligación de confidencialidad que se extiende a los trabajadores que tratan dicha información, y que por tanto, debe quedar expresamente regulada a nivel interno, a fin de evitar posibles responsabilidades derivadas de la negligencia de algún trabajador de la empresa.

2.2.3. Protección de la Información Confidencial de la empresa cuando es tratada por terceros. Los contratos de outsourcing.

Cuando una empresa vaya a encargar la prestación de un determinado servicio, que implique el tratamiento o acceso a información confidencial por parte de terceras empresas, es recomendable incluir en el Contrato de Prestación de Servicios, una cláusula específica de confidencialidad, o bien, firmar directamente con cada una de las personas que accedan a dicha Información, Pactos o Acuerdos de Confidencialidad específicos.

2.2.4. Contenido básico de un Acuerdo o Pacto de Confidencialidad.

- Establecer claramente qué se entiende por Información Confidencial. En este sentido, se puede establecer el deber de guardar secreto respecto de toda o determinada información tratada, siendo recomendable huir de referencias genéricas a la confidencialidad.

- Establecer claramente los medios, recursos o información que se pone a disposición del trabajador o tercera empresa, determinando la titularidad de la misma.

- Establecer específicamente la obligación de secreto y confidencialidad, el deber de actuar diligentemente en cuanto al tratamiento, conservación, almacenamiento, transporte, etc., estableciendo que en todos los casos deberán adoptarse los medios que aseguren y garanticen dicho secreto, y se evite su pérdida o el acceso a la misma de terceros no autorizados.

- Establecer la obligación de devolver la información confidencial a la que se ha tenido acceso en el momento que termine la relación contractual, estableciendo, igualmente, que a pesar de dicha terminación, la obligación de confidencialidad y secreto permanecerá vigente durante el plazo que sea establecido por las partes (la práctica habitual en este sentido, es establecer un plazo de 2 años después de finalizada la relación contractual).

- Es conveniente, igualmente, informar de las consecuencias que pueden derivarse del incumplimiento de dicha obligación de confidencialidad y secreto. Así puede establecerse que la sustracción o revelación de dicha información puede ser constitutivo de un ilícito de naturaleza penal (art. 197 CP del descubrimiento y revelación de secretos), puede ser objeto de acciones disciplinarias (despido disciplinario en caso de que el incumplimiento venga por parte de un trabajador), reclamación de indemnizaciones por daños y perjuicios, etc...

- Por último, en los Acuerdos o Pactos de Confidencialidad pueden establecerse todas las especialidades, que por razón de la relación contractual que se establece, sean establecidas por las partes.

2.2.5. Límites de la Obligación de Confidencialidad y Secreto.

Hay que señalar que la Obligación de Confidencialidad y Secreto queda limitada en aquellos casos en los que, por imperativo legal, la parte obligada sea requerida por un organismo jurisdiccional o administrativo para facilitar determinada información.

En estos casos, deberán ser atendidas aquellas órdenes en las que:

- La obligación de entrega venga determinada de manera concreta en la orden.

- Sea dictada por una administración o juzgado competente.

- Sea firme.

En estos casos, se informará a la otra parte de inmediato sobre el requerimiento recibido, siempre que no exista obligación de guardar secreto sobre el mismo por mandato legal, administrativo o judicial.

2.3. Marco de Gestión de Seguridad de Información

Al igual que los trazos arquitectónicos de alto nivel, el marco de la gerencia define los componentes, la forma y las funciones del programa de la gerencia de la seguridad de información. Por otro lado, los procedimientos, las normas y la arquitectura de seguridad técnica son como los anteproyectos que definen la implementación a detalle.

El marco de la gerencia de la seguridad de información es una representación conceptual de un programa de gerencia de seguridad de información que describe la combinación de controles técnicos, operativos, gerenciales y de seguridad física en relación con los ambientes técnico y operativo de una organización.

2.3.1. Revisión y modificación de políticas y normas

Conforme se implementa el programa será necesario actualizar políticas, y mayor plazo, a medida que evoluciona la organización. El gerente de seguridad de información tendrá que implementar procedimientos para agregar, modificar y en algunos casos retirar políticas de seguridad de información.

Será necesario conformar un comité de revisores/aprobadores de políticas para cada nivel de jerarquía de la política. Por ejemplo: podría ser necesario que el equipo de la alta dirección o incluso los miembros del consejo, revisen las políticas del programa de más alto nivel; por su parte, podría ser necesaria la aprobación de los representantes de la gerencia de tecnología de las políticas operativas técnicas de nivel más bajo. Estas entidades deberán revisar las políticas regularmente, ya sea en conjunto (por lo general, cada año) o a medida que se incrementen (por lo general, cada trimestre).

Las propuestas de cambio se hacen con base en las revisiones de la política o a medida que tienen un interés en la organización reconocen la necesidad de un cambio en la política. El gerente de seguridad de información debe dar seguimiento a los cambios que se propongan a las políticas y procedimientos, y revisarlas en los foros apropiados. Las revisiones de las propuestas de cambios deben llevarse a cabo cada trimestre, cada semestre o cada año, dependiendo de la cantidad de cambios propuestos. Durante las primeras etapas de la implementación del programa, el gerente de seguridad de información esperaría ver más cambios propuestos en la misma medida en que se adoptan políticas y se adaptan a las necesidades y las limitaciones específicas de la organización.

A medida que evoluciona el programa, es probable que las revisiones a la política impulsen propuestas de cambio.

El gerente de seguridad de información también debe dar seguimiento a los cambios hechos a las políticas. Estos registros deben incluir la política original, el cambio propuesto, la razón para dicho cambio, el análisis de riesgo y los impactos en el cumplimiento, el estado del cambio (aprobado/rechazado/suspendido), así como las aprobaciones gerenciales efectivas del cambio.

Asimismo deben elaborarse minutas de las reuniones que traten los cambios a las políticas a fin de mantener un registro transparente de la administración cooperativa de la política para auditores y revisores.

La modificación de las normas probablemente tendrá lugar con mayor frecuencia que la modificación de las políticas. Estos cambios suele ser motivados por cambios en la tecnología, tales como: disponibilidad de nuevas capacidades de seguridad, la introducción o eliminación de la funcionalidad de la aplicación, la evolución de la infraestructura técnica y los requerimientos de nuevas iniciativas de negocio. Cada norma debe tener asignada un dueño y/o equipo de revisión para revisar la norma en forma periódica o cuando lo justifiquen los cambios ambientales.
Los cambios a las normas deben administrarse de un modo similar a los cambios en la política y deben incluir también un análisis de riesgo.

2.3.2. Métricas y monitoreo de la Seguridad

Un requerimiento de una gerencia de seguridad efectiva es garantizar que exista una retroalimentación continua sobre una variedad de elementos relacionados con la seguridad. Los procesos de monitoreo se requieren para garantizar el cumplimiento con las leyes y las regulaciones aplicables a las cuales está sujeta la organización.

En años recientes varias industrias se han sujetado a reglamentaciones específicas para garantizar la seguridad y la privacidad de la información sensible, sobre todo en organizaciones del sector financiero.

Al fin de evaluar la efectividad de un programa de seguridad de una organización, el gerente de seguridad de información tiene que tener un vasto entendimiento de cómo monitorear los programas y los controles de seguridad de manera continua.

Es importante que el gerente de seguridad desarrolle un método congruente y confiable para determinar la efectividad continua del programa. Una forma es llevar a cabo evaluaciones de riesgo de manera regular e identificar las mejoras al paso del tiempo.

Otra herramienta tradicional es aplicar pruebas de penetración externas para determinar la vulnerabilidad del perímetro. Las pruebas de penetración internas también resultan valiosas para determinar la configuración y otras deficiencias.
Llevar a cabo pruebas de penetración internas periódicamente al mismo tiempo que se da seguimiento a los resultados puede ser un indicador útil de tendencias. La mayoría de las organizaciones llevan a cabo escaneos periódicos de la vulnerabilidad para determinar si se corrigen las vulnerabilidades abiertas y ver si surgen otras nuevas.

2.3.3. Monitoreo de las actividades relacionadas con la seguridad en la infraestructura y las aplicaciones de negocio

Dado que las 24 horas del día, los 7 días de la semana, es probable que exista una vulnerabilidad de la organización a violaciones en la seguridad, el monitoreo continuo de las actividades de seguridad es un proceso de negocio prudente que debe implementar el gerente de seguridad de información.

El monitoreo continuo de los sistemas de detección de intrusos (IDSs) y los firewalls pueden proporcionar información en tiempo real sobre intentos de violación a las defensas perimetrales. Capacitar al personal del Help Desk para escalar informes sospechosos que puedan indicar una violación o un ataque. Esta información puede ser crucial para tomar acciones correctivas en forma oportuna.

Los sistemas de detección de intrusos son cada vez más inteligentes, ya que pueden detectar intentos directos de acceso no autorizado, así como proporcionar un análisis inteligente para indicar tendencias. Esto podría facilitar que se tomen medidas proactivas para evitar ataques exitosos contra los sistemas de información de la organización. Otras técnicas de monitoreo posterior al hecho son el registro de incidentes, las revisiones de bitácoras (logs).

2.3.4. Determinar el éxito de las inversiones en la seguridad de información

Es importante que el gerente de seguridad cuente con procesos para determinar la efectividad en general de las inversiones en la seguridad y hasta qué grado se han cumplido los objetivos. Siempre hay una competencia por los recursos dentro de las organizaciones, por lo que la alta dirección debe obtener los mejores réditos sobre inversión a fin de justificar los costos.

Durante el diseño y la implementación del programa de seguridad, el gerente de seguridad de información debe asegurarse de que se hayan definido y acordado los indicadores clave de desempeño, y que se encuentre implementado un mecanismo para medir el avance con base en dichos indicadores. De esta manera el gerente de seguridad de información puede determinar el éxito o el fracaso de diversos componentes del programa de seguridad y si su costo está justificado o no.

2.3.5. Pruebas y modificaciones de controles

Los cambios al ambiente técnico u operativo a menudo pueden modificar el efecto de protección que tienen los controles o generar nuevas deficiencias que los controles existentes no están diseñados para mitigar.
Las pruebas periódicas a los controles deben implementarse para garantizar que los mecanismos exijan de manera continua el cumplimiento de las políticas y que los controles de procedimientos se ejecuten de manera consistente y efectiva.

Los cambios a los controles técnicos u operativos tienen que ejecutarse con precaución. Los cambios a los controles técnicos deben ejecutarse bajo procedimientos de control de cambios y con la aprobación de las partes interesadas. El gerente de seguridad de información debe analizar el ambiente de control propuesto a fin de determinar si existen vulnerabilidades nuevas o recurrentes en el diseño y para asegurarse de que el control esté debidamente diseñado es decir, que sea auto protector, que contenga una política en caso de falla). Una vez implementados, deberán llevarse a cabo pruebas de aceptación para verificar que los mecanismos exijan el cumplimiento de las políticas preescitas.

2.3.6. Proveedores externos de servicios

A menudo las empresas cuentan con servicios que prestan proveedores externos además de llevar a cabo el negocio con proveedores, distribuidores y otros socios de manera electrónica. Esto no implica una renuncia de la responsabilidad de la seguridad de la organización ni una delegación de responsabilidades.

El gerente de seguridad de información debe hacer lo necesario para garantizar que las partes externas cumplan con las políticas de seguridad de información establecidas en la organización. Algunos temas comunes que se deben tener en cuenta se enlistan a continuación:

- Aislamiento del acceso de la parte externa a los recursos.
- Integridad y autenticidad de los datos y las transacciones.
- Protección contra código o contenido malicioso.
- Acuerdos y procedimientos de privacidad/confidencialidad.
- Normas de seguridad para los sistemas de transacciones.
- Confidencialidad en la transmisión de datos.
- Administración de identidad y accesos de terceros.
- Procedimientos de contacto y escalación de incidentes.

2.3.7. Integración en los procesos del ciclo de vida

Alcanzar una seguridad efectiva de los sistemas de información es más fácil cuando las cuestiones de riesgo y protección se encuentran incluidas en el ciclo vital del desarrollo de sistema. Este proceso por lo general consiste en establecer requerimientos, arquitectura y diseño de soluciones, prueba de concepto, desarrollo y codificación completos, pruebas de integración, utilización, pruebas de calidad y aceptación, mantenimiento y fin de la vida de los sistemas.

Los controles definidos de seguridad básica deben ser un requerimiento permanente para todos los desarrollos de nuevos sistemas. Algunos ejemplos incluyen las funciones de autenticación, registro en bitácoras, control de acceso basado en roles y mecanismos de confidencialidad en la transmisión de datos. El gerente de seguridad de información debe consultar fuentes tanto regionales como de la industria para determinar el conjunto básico de funciones de seguridad que es apropiado para sus políticas organizacionales y otras necesidades. Podrían justificarse los controles complementarios con base en el análisis de vulnerabilidad, riesgo y amenaza.

2.3.8. Monitoreo y Comunicación

El monitoreo de la seguridad de los sistemas de información es un componente crucial de cualquier programa de gerencia de la seguridad de información.

El gerente de seguridad debe considerar el desarrollo de un ambiente de monitoreo central que proporcione a los analistas la visión de todos los recursos de información de la empresa.

Existe una amplia gama de incidentes relacionados con la seguridad que se registran en bitácoras y que se podrían monitorear, por lo que la organización necesitará determinar cuáles incidentes serían más pertinentes en términos de recursos afectados y tipo de incidente.

Es crucial desarrollar procedimientos para analizar incidentes y tomar medidas de respuesta apropiadas. Los analistas de monitoreo de seguridad deben recibir capacitación sobre estos procedimientos, en tanto que los supervisores de monitoreo deberán contar con procedimientos para resolver anomalías desconocidas. Por lo general, los procedimientos de respuesta implican analizar incidentes relacionados y estados del sistema, recopilar información adicional relacionada con el incidente, investigar cualquier actividad sospechosa o turnar el asunto a analistas de nivel superior o a la gerencia. Asimismo, deben llevarse a cabo pruebas periódicas a la ruta para escalar los incidentes de seguridad.

2.3.9. Documentación

La elaboración y el mantenimiento de documentación relacionada con la seguridad es un componente operativo importante de un programa efectivo de gerencia de la seguridad de información. Algunos documentos que comúnmente guardan relación son:

- Políticas, procedimientos operativos tradicionales.
- Diagramas técnicos de infraestructura, aplicaciones y flujos de datos.

- Análisis de riesgos, recomendaciones y documentación relacionada.
- Diseño de sistemas de seguridad, políticas de configuraciones y documentación de mantenimiento.
- Registros operativos, tales como: informes de turnos y de monitoreo de incidentes.

Se deberá asignar un dueño para cada documento, quien será responsable de actualizar la documentación. Los cambios deberán efectuarse con las recomendaciones de la gerencia o del comité directivo de seguridad.
El dueño tendrá también la responsabilidad de garantizar que el acceso a la documentación sea apropiado, esté controlado y se pueda auditar.

2.3.10. Integración de las actividades de aseguramiento

Un objetivo principal de las actividades de seguridad es brindar la certeza a las operaciones de negocio de que los incidentes adversos no tendrán un impacto significativo en la capacidad para alcanzar los objetivos. Sin embargo, otro objetivo de la gerencia de seguridad es proporcionar un nivel aceptable de previsibilidad de las operaciones en términos de confidencialidad, integridad y disponibilidad de los activos de información.

Por lo general, existen dos formas de intentar alcanzar la integración de estas actividades. Un enfoque es mediante la conformación de un comité directivo de seguridad que consta de representantes de estas áreas además de los miembros de las unidades de negocio y/u operaciones. El comité directivo debe tener un estatuto claro de sus responsabilidades, autoridad y obligaciones, y reunirse de manera consistente.

El otro enfoque es a través de políticas y normas completas y bien elaboradas que integren las funciones de seguridad y aseguramiento de la organización.

2.3.11. Reglas generales de uso/Política de uso aceptable

Mientras que los procedimientos específicos proporcionan los pasos detallados que se requieren para muchas funciones en el nivel operativo, existe también un grupo extenso de usuarios que pueden beneficiarse de un resumen fácil de utilizar de lo que deben y no deben cumplir con la política.

Una forma eficaz de ayudar a estos usuarios generales a entender sus responsabilidades relacionadas con la seguridad es desarrollando una política de uso aceptable. Está política puede especificar en términos cotidianos las obligaciones y las responsabilidades de todos los usuarios en forma directa y concisa. Sin duda, es necesario comunicar de manera efectiva la política de uso a todos los usuarios y asegurarse de que la hayan leído y entendido. La política de uso difundirse a todo el personal que tendrá acceso a los activos de información, sin importar su estado laboral.

Por lo general, estas reglas de uso para todo el personal incluyen la política y las normas para el control de acceso, la clasificación, el etiquetado y manejo de documentos e información, los requerimientos para la presentación de información y las limitaciones en cuanto a divulgación. Pueden incluir también reglas sobre el uso del correo electrónico, así como otros recursos y activos de información. Estas reglas de uso proporcionan un límite de seguridad general para toda la organización.

2.3.12. Asignación de roles y responsabilidades

Con el fin de manejar la seguridad, debe quedar claro quién hace qué y quién es responsable. No hacerlo conducirá invariablemente a fallas en la seguridad y las piezas no encajarán.

El gerente de seguridad de información debe considerar que algunas actividades relacionadas con la seguridad son esporádicas e intermitentes, en tanto que otras son constantes y continuas. Por ejemplo: el trabajo de diseño como lo es la arquitectura, sólo será necesario que se realice de manera periódica, en tanto que la administración del sistema y las iniciativas de cumplimiento serán constantes. Para ser efectivo, el gerente de seguridad de información debe considerar estos elementos cuando se contrate personal para una organización de seguridad.

2.3.13. Proveedores Externos de Seguridad

Servicios prestados por otras empresas alineados con las políticas establecidas

Los proveedores de seguridad subcontratados son una estrategia viable de la que puede hacer uso el gerente de seguridad de información para contribuir al diseño y la operación del programa de seguridad de información de la organización. No obstante el gerente de seguridad de información necesita asegurar, hasta donde sea posible, que el proveedor subcontratado cumpla con las políticas de seguridad de información establecidas.

Se deberá discutir los requerimientos y parámetros de las políticas de seguridad de información de la organización. El cumplimiento del proveedor con estas políticas de seguridad debe estar en los primeros lugares en la lista de factores de decisión cuando se elija a un proveedor. El gerente de seguridad de información debe entender las diferencias que pueden existir y si el proveedor de servicio puede o no cumplir con dichas políticas de seguridad.

El gerente de seguridad de información debe asegurarse de que los factores de cumplimiento estén claramente definidos en el acuerdo de nivel de servicio (SLA) que formalice con el proveedor de seguridad (interno o externo).
Esto ayudará al gerente de seguridad de información a administrar el desempeño del proveedor de seguridad y garantizar que está cumpliendo con su compromiso de apegarse a las políticas de seguridad de la organización.

2.3.14. El proceso de administración de cambios

Casi todas las organizaciones utilizan algún tipo de proceso de administración de cambios. En algunos casos esto puede no hacerse de manera formal. El gerente de seguridad de información debe identificar todos los procesos de administración de cambios que utiliza la organización a fin de obtener de ellos información que permita notificar que se están realizando cambios que puedan tener impacto en la seguridad.

Es necesario que el gerente de seguridad de información implemente procesos mediante los cuales las implicaciones en la seguridad estén incluidas en cada proceso de administración de cambios que la organización pudiera implementar.

Si se desarrolla una aplicación internamente, es importante que se introduzcan los elementos de seguridad en una etapa temprana del ciclo de desarrollo con el fin de minimizar las vulnerabilidades y garantizar el cumplimiento con las normas de seguridad de la organización. Será importante asegurarse de que las especificaciones técnicas incluyan los requerimientos de la seguridad que establecen las normas de la organización para cumplir con la política. Además los planes de prueba y aseguramiento de calidad (QA) tienen que sujetarse a una revisión por parte del gerente de seguridad a fin de garantizar que se han probado y certificado en forma adecuada los elementos de la seguridad.

2.3.15. Evaluaciones de la vulnerabilidad

Las evaluaciones de la vulnerabilidad son una de las herramientas clave con las que cuenta el gerente de seguridad de información para evaluar la efectividad del programa de seguridad de información para administrar el riesgo.

Las evaluaciones de vulnerabilidad ayudan a determinar deficiencias en los sistemas pero son sólo un componente de una evaluación de riesgo. Es importante tener en consideración que seguramente existe una amenaza que explote una vulnerabilidad la cual, a su vez, ocasione un impacto.

2.3.16. Debida diligencia

La debida diligencia es un término que en esencia está relacionado con la noción de la norma de debido cuidado. Es la idea de que existen pasos que debe seguir una persona razonable de competencia similar en circunstancias similares. En el caso del gerente de seguridad de información, esto significa garantizar que se cuente con todos los componentes básicos de un programa razonable de seguridad. Algunos de estos componentes básicos son:

- Apoyo de la alta dirección.
- Políticas, normas y procedimientos integrales.
- Formación, capacitación y concienciación apropiadas sobre seguridad a lo largo de la organización.
- Evaluación periódica de riesgos.
- Procesos efectivos de respaldo y recuperación.
- Esfuerzos apropiados de cumplimiento.

Asimismo, es importante tener en cuenta que aquellos terceros que prestan servicios a la organización y en los que ésta confía también pueden representar un riesgo para los recursos de información, y es necesario contar con una debida diligencia en lo referente a contratos y acuerdos.

2.3.17. Resolución de temas relacionados con el incumplimiento

Los temas relacionados con el incumplimiento por lo general resultan en riesgos para la organización, por lo cual es importante desarrollar procesos específicos para resolverlos en una forma efectiva y oportuna.

Por lo general, se desarrolla un programa para documentar cada tema de incumplimiento, y se asigna y registra la responsabilidad de resolverlo. El seguimiento periódico también es clave para garantizar que cualquier tema de incumplimiento y otras desviaciones se traten en forma oportuna y satisfactoria. Es posible identificar los temas de incumplimiento y otras diferencias a través de una serie de mecanismos, entre otros:

- Monitoreo normal.
- Informes de auditoría.
- Revisiones a la seguridad.

3. CAPITULO 3 POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

ISO 27001: Es una norma generalizada que establece requerimientos detallados para los programas de gerencia de seguridad de información, incluye 11 áreas generales de control:

- **Política de seguridad:** Proporciona dirección gerencial y apoyo sobre seguridad de información de acuerdo con los requerimientos de negocio y las leyes y regulaciones aplicables.
- **Organización de activos y recursos:** Ayuda a administrar la seguridad de la información dentro de la organización.
- **Clasificación de activos y controles:** Medidas que identifican los activos y establece medidas adecuadas para su protección y manejo.
- **Seguridad del Personal:** Se asegura de que el personal, contratistas y terceros usuarios conozcan sus responsabilidades.
- **Seguridad física y ambiental:** Medidas que previenen accesos no autorizados, daño e interferencia a las instalaciones, equipos, información y otros activos de la organización.
- **Administración de comunicaciones y operaciones:** Medidas que garantizan la operación correcta y segura de los equipos de procesamiento de información.
- **Control de Acceso:** Medidas que garantizan el acceso autorizado de usuarios.
- **Adquisición, desarrollo y mantenimiento de sistemas de información:** Garantiza que la seguridad de software de sistemas de aplicación e información esté incorporada a los sistemas de información.

- **Administración de la continuidad del negocio:** Medidas que previenen, mitigan y minimizan el impacto que tienen las interrupciones a las actividades de negocio.
- **Administración de comunicaciones y operaciones:** Medidas que garantizan la operación correcta y segura de los equipos de procesamiento de información.
- **Cumplimiento:** Medidas que evitan violaciones de cualquier ley penal o civil y cualquier requerimiento de seguridad.

ISO 27002: (ISO 17799): Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Los beneficios incluyen:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.

- Proporciona confianza y reglas claras a las personas de la organización.
- Reduce costos y mejora los procesos y servicio.
- Aumenta la motivación y satisfacción del personal.

3.1. Definición de Políticas de seguridad de información utilizando las normas ISO27001 e ISO27002

3.1.1. Políticas para la Clasificación de la Información

Entidad Financiera

1. Toda la información generada por y para la Entidad Financiera deberá ser clasificada.

Propietario de la Información

2. Deberá proceder a la clasificación de la información bajo su responsabilidad considerando los siguientes factores: su contenido, naturaleza y valor, por lo tanto deberá analizar su información para proceder a clasificarla, basándose principalmente en los perjuicios que pudiera ocasionarle a la Entidad Financiera y/o su personal. Dichos perjuicios pueden ser económicos, financieros, políticos, sociales, de imagen, legales y/o gremiales. Complementariamente deberá tener en cuenta las definiciones de la Alta Dirección de la Entidad Financiera y las leyes y regulaciones vigentes en el país, así su información deberá ser ubicada en uno de los siguientes niveles:

NIVEL	CLASIFICACIÓN	DESCRIPCIÓN
Nivel 1	Público	Información que podría ser conocida y utilizada sin previa autorización por cualquier persona, sea o no funcionario de la Entidad Financiera. Puede ser comunicada y utilizada como parte del dominio público, por ejemplo: estados financieros de ejercicios anteriores.
Nivel 2	Interno	Información que, sin poder ser publicada, puede ser conocida y utilizada por todos los funcionarios y algunos colaboradores externos autorizados, y cuya divulgación o uso no autorizados podría ocasionar pérdidas leves y asumibles por la Entidad Financiera. Información relacionada con procedimientos internos de operación como por ejemplo los procedimientos de Cuadre, de Caja, Caja Chica, etc.
Nivel 3	Confidencial	Información que sólo puede ser conocida y utilizada por un grupo de funcionarios, que la necesiten para cumplir con sus funciones y colaboradores externos autorizados y que hayan firmado el compromiso de confidencialidad, su divulgación o uso no autorizados podría ocasionar pérdidas significativas materiales o de imagen. Se trata de información sensible, como lo es la información de clientes, índices financieros del período en curso, base de datos de RRHH, los algoritmos, mecanismos y procedimientos de

NIVEL	CLASIFICACIÓN	DESCRIPCIÓN
		seguridad de información etc.
Nivel 4	Estrictamente Confidencial	Información que sólo puede ser conocida y utilizada por el Directorio, Gerencia General y Vicepresidencias relacionada directamente con las decisiones estratégicas de la Institución o en su defecto es conocida únicamente por su Propietario, su divulgación o su uso no autorizado podría ocasionar graves pérdidas materiales o de imagen a la Institución, los Accionistas o los Clientes, como por ejemplo Informes de Organismos de Control, claves de acceso a los sistemas de clientes y/o usuarios, decisiones de estrategias de crecimiento, ventas, inversiones, fusiones, etc.

Tabla 3.1: Clasificación de la Información

Se denominará Información Clasificada exclusivamente a los niveles 2 Confidencial y 3 Estrictamente Confidencial.

3. Es su exclusiva responsabilidad asignar o cambiar el nivel de clasificación de la información a su cargo, cumpliendo con los siguientes requisitos:

- Asignarle una fecha de efectividad.
- Comunicárselo al Custodio de la Información.
- Ejecutar los procedimientos necesarios para que los usuarios conozcan la nueva clasificación.

4. Garantizar que toda la información bajo su responsabilidad se encuentre correctamente clasificada.

5. En caso de existir información generada por entidades externas (por ejemplo la SIB) referente a la Entidad Financiera al momento de su recepción deberá ser considerada en el nivel 3 Estrictamente Confidencial, hasta que su Propietario realice la clasificación correspondiente y la comunique a todas las áreas relacionadas para mantener la validez de la información y garantizar su manejo adecuado.

6. Ante la ausencia del funcionario autorizado para realizar la clasificación su reemplazo deberá ser quien tome esta responsabilidad.

3.1.2. Políticas para el tratamiento de Información Clasificada

Generales

Entidad Financiera

1. La Información clasificada deberá ser conocida o utilizada, sólo por funcionarios autorizados y siempre por aquel personal que tenga la “necesidad de Negocio de conocerla”

2. Todos los funcionarios que accedan a información clasificada por motivos de trabajo, deberán firmar un Compromiso de Confidencialidad y no Divulgación de la misma.

3. La información clasificada deberá permanecer en todo momento, lejos del alcance de los funcionarios y personas que no tengan la necesidad de conocerla.

4. La información clasificada deberá almacenarse en los equipos de procesamiento centralizado, en caso de almacenarse en estaciones de trabajo deberá seguir el estándar de seguridad establecido.

5. La información clasificada contenida en medios físicos deberá guardarse bajo llave permanentemente, y durante su uso deberá evitarse que pueda ser leída por personas no autorizadas.

6. La información clasificada deberá permanecer siempre protegida y su utilización deberá restringirse a los momentos en los que nadie, que no esté autorizado, pueda verla o leerla.

7. Se deberá implementar la política de “escritorios vacíos” que implica conservar todo documento impreso bajo llave cuando no esté en uso.

8. Se garantizará la implementación de controles de integridad, exactitud, confidencialidad e inviolabilidad de la información clasificada que se transmita electrónicamente, que permitan la correcta recepción del envío por parte del destinatario.

9. Siempre que la información clasificada sea enviada a través de redes de comunicaciones, propias o ajenas deberá viajar encriptada y la clave de descifrado deberá ser enviada por otro medio.

Propietario de la Información, Líder o Responsable de Área

10. Verificar que los funcionarios a su cargo que reciben esta información, cumplan con las obligaciones descritas en esta Política.

Rotulado

Propietario de la Información

11. Si la información no puede ser rotulada el Propietario tiene la obligación de informar a todas las áreas que la reciben su clasificación.

Usuario Final

12. El nivel de clasificación, tiene que estar rotulado en todos y cada uno de los medios que contengan información clasificada, considerando lo siguiente, según corresponda los rótulos:

- Entidad Financiera - Confidencial
- Entidad Financiera – Estrictamente Confidencial

Deberán ser colocados en lugares de fácil detección y su ubicación dependerá del entorno:
Físico o electrónico.

• **Físico,** debe aparecer en cada página del documento o del medio físico que la contengan.

O

En la primera página del documento clasificado, a más del rótulo, se debe colocar la siguiente leyenda "La información descrita en el presente documento es de uso

reservado y exclusivo de la Entidad Financiera. Está prohibida su reproducción sin previa autorización o su utilización en otros fines distintos para el cual fue entregada".

• **Electrónico**, la clasificación debe aparecer al comienzo de cada archivo o conjunto de datos que estén destinados a la lectura.

En todas las pantallas de acceso a esta Información así como en los reportes que la contengan deberá desplegarse la etiqueta Entidad Financiera – Confidencial o Entidad Financiera – Estrictamente Confidencial según corresponda.

13. Los documentos destinados a transmisión, (por ejemplo, hojas de portada de medios, fax símil o magnético) que acompañan a la información clasificada, también deben llevar el respectivo rótulo.

14. Los rótulos de Información Entidad Financiera - Confidencial o Entidad Financiera – Estrictamente Confidencial no deberán abreviarse.

15. Los contenedores externos de los documentos no deben estar etiquetados como documentos clasificados.

16. Los medios magnéticos desmontables que contenga información clasificada deben rotularse con la siguiente leyenda: "Propiedad de Entidad Financiera - Contiene información Entidad Financiera – Confidencial / Entidad Financiera – Estrictamente Confidencial y debe ser protegida de usos o acceso no autorizados. No debe ser retirado del control de la Entidad Financiera sin la adecuada autorización y sin tener colocado el rótulo Entidad Financiera – Confidencial/ Entidad Financiera – Estrictamente Confidencial".

Protección

Propietario de la Información

17. Para el almacenamiento de la información clasificada en cualquier sistema o medio de almacenamiento, deberán garantizar:

- Tener los medios físicos y lógicos adecuados para protegerla
- No permitir su acceso público
- Implementar mecanismos que limiten el acceso a esta información

18. Recuperar toda la información, en forma física o electrónica, cuando el depositario o custodio de la misma es transferido, se le asignen tareas diferentes o cese en sus funciones.

Usuario Final

19. La creación de salidas impresas de información clasificada estará siempre bajo la Responsabilidad y control del usuario que genera la impresión.

20. El uso de cualquier dispositivo para generar salidas impresas que contengan información clasificada deberá limitarse a aquellos que:

- Estén situados en áreas de acceso limitado o restringido, o
- Tengan algún tipo de control de borrado de listados, o

Sean de uso exclusivo del usuario (impresora local)

21. Si ninguna de las opciones anteriores está disponible, se puede imprimir en cualquier otro dispositivo siempre y cuando los listados sean recogidos personal e inmediatamente por el usuario.

22. Proteger la información de terceros bajo su poder, de acuerdo con los términos de los convenios realizados para el efecto.

Divulgación

Propietario de la Información

23. La información clasificada deberá ser copiada y distribuida solo a las personas con “necesidad de Negocio de conocerla”. El copiado y la distribución deberán ser realizados por personal autorizado por el Propietario de Información.

24. El Propietario de la información se reservará el derecho de aprobar personalmente toda copia de la información, y deberá añadir a la información la leyenda “No Reproducir”.

25. Deberá enumerar todas las copias aprobadas con el objeto de hacer seguimiento de las mismas y designar un coordinador para administrar este control.

26. La copia generada deberá ser entregada conjuntamente con una certificación del Propietario de Información acerca de la veracidad de su contenido.

Usuario Final

27. La divulgación a otros funcionarios o a terceros con necesidad de Negocio de conocer la información (por ejemplo, clientes, proveedores, socios comerciales, consultores, empresas asociadas en participación, empresas que prestan servicios de outsourcing, etc.) solo se puede efectuar cuando se cumplan las siguientes condiciones:

- Que el Propietario de Información lo apruebe.
- Cuando antes de su divulgación, el tercero firme un compromiso de confidencialidad que ha sido aprobado por el Departamento Legal de la Entidad Financiera.

28. La divulgación no autorizada de información clasificada deberá ser comunicada inmediatamente al Responsable del área y a su Propietario.

Transporte

Usuario Final
Todos
Proveedor de Servicios de Tecnología

29. Siempre que la información clasificada sea transportada dentro del ámbito de la Institución, deberá estar contenida en un sobre o contenedor cerrado y rotulado con la clasificación más alta del contenido.

30. Si la información clasificada es enviada al exterior o por un medio de correo ajeno a la Institución, el sobre o contenedor cerrado y rotulado deberá ser introducido en otro sobre o contenedor cerrado y NO rotulado. Deberá incluirse el acuse de recibo por parte del destinatario.

Transmisiones Electrónicas

Usuario Final

31. La Información Clasificada podrá ser transmitida por redes inalámbricas sólo en el perímetro de la Entidad Financiera y utilizando el canal de la Entidad Financiera.

32. Evitar discutir Información Clasificada en llamadas telefónicas fuera de la institución. Si usted está autorizado para discutir información confidencial con alguien que no pertenezca a la institución, deberá hacerlo en persona.

33. Nunca deje mensajes confidenciales en correo telefónico fuera de la institución.

34. Evite enviar documentos que contengan Información Clasificada vía fax. Si el material clasificado tiene que ser enviado vía fax, procure verificar que el número de teléfono del fax sea el correcto y la persona receptora se encuentre en disposición de recibir el documento.

Viajes

Usuario Final

35. Los funcionarios de la Entidad Financiera no deberían llevar información clasificada en sus viajes, pero de ser estrictamente necesario deberían cumplir lo siguiente:

- Conservar la información en su poder en todo momento.
- Al llegar a su destino, dejar en resguardo la información en alguna dependencia de la Institución, si es posible.

36. La información clasificada no deberá dejarse dentro del equipaje que se verifica en los aeropuertos, ni en cuartos de hotel, ni vehículos, que estén o no cerrados con llave.

Destrucción

Usuario Final

Proveedor de Servicios de Tecnología

37. Cuando ya no sea útil la información clasificada deberá ser destruida en la forma más adecuada al soporte que la contenga:

- Impresos y papel: Mediante trituradoras que permitan destruirla totalmente bajo control.

• Medios de almacenamiento: Antes de deshacerse de disquetes u de otros medios de almacenamiento, los funcionarios deberán asegurarse de borrar o volver ilegible toda información clasificada contenida en ellos.

3.1.3. Políticas para el tratamiento de Información Estrictamente Confidencial

Generales

Entidad Financiera

1 A más de cumplir con las Políticas para el tratamiento de Información Clasificada, deberá cumplir con las siguientes consideraciones:

Encriptación

Proveedor de Servicio de Tecnología

2. Deberá encriptar todos los archivos que contengan Información Estrictamente Confidencial del ambiente de producción como de cualquier otro ambiente en las siguientes situaciones:

- Procesamiento diario
- Almacenamiento en los sistemas
- Transmisión electrónica a través de las redes
- Generación de copias de respaldo
- Almacenamiento en logs de eventos

Propietario de la Información

3. Deberá guardar como información Estrictamente Confidencial las claves utilizadas en los procesos de encripción y desencripción.

Utilización

Todos

Proveedor de Servicios de Tecnología

4. No está permitido su uso para propósitos de prueba en los desarrollos y/o implementaciones de sistemas.

3.1.4. Políticas para la Segregación de Funciones y definición de roles de trabajo

El Responsable de Riesgo Operativo es el encargado de liderar la definición y mantenimiento de la misma. Esta Política estará sujeta a una revisión regular anualmente.

El Responsable de Seguridad Informática, liderará la implementación de esta Política.

El Responsable de Auditoría de Sistemas, liderará la verificación del cabal cumplimiento de la Política en la Entidad Financiera.

Dentro del alcance de esta Política, se implementará un adecuado monitoreo para garantizar que todos los eventos relacionados con la seguridad sean identificados y corregidos. Todas estas actividades de monitoreo serán consistentes con las regulaciones y legislación de privacidad vigentes.

Esta Política determina requerimientos mínimos para el gerenciamiento de la Información, Control de Accesos, Seguridad Física, Comunicaciones, Operaciones y Desarrollo de Sistemas.

Cada empleado de una Entidad Financiera será, consecuentemente, consciente de la responsabilidad de asegurar la información bajo su cargo y actuará para preservar la misma.

El presente es una propuesta de las políticas de seguridad para normar a la Entidad Financiera. Se mencionan los aspectos que representan un riesgo o las acciones donde se ve involucrada la Entidad Financiera y que compete a las tecnologías de la información; se han contemplado también las políticas que reflejan la visión de la actual administración respecto a la problemática de seguridad informática.

La propuesta ha sido detenidamente planteada, analizada y revisada a fin de no contravenir con las garantías básicas de la Entidad Financiera, y no pretende ser una camisa de fuerza, y más bien muestra una buena forma de operar el sistema con seguridad.

3.1.5. Políticas de Riesgo

Clasificación de Riesgos de Proyectos

Proyecto de Aplicación

Son todas las aplicaciones nuevas (desarrolladas, adquiridas o contratadas su desarrollo) o los cambios mayores/significativos que involucren un esfuerzo de 80 horas o más.

Entidad Financiera

1. Todo Proyecto de Aplicación que tenga calificación de riesgo ALTO para pasar a producción deberá obtener:

- La certificación funcional por parte del Usuario.
- La certificación técnica por parte de QA (Quality Assurance) del Proveedor de Servicio de Tecnología, y
- La certificación de seguridad por parte del Proveedor de Servicio de Seguridad Informática.

3.1.6. Políticas accesos parte de Terceros

1. Toda entrega de información de la Entidad Financiera a Terceros se hará a través de la firma del CONTRATO DE CONFIDENCIALIDAD – ANEXO 1 Normas de Seguridad, que describe las condiciones para el manejo de la información que será entregada.

3.1.7. Propietario de la Información

2. Establecer, justificado en el cumplimiento de los objetivos de negocio, el acceso a terceros considerando al menos las mismas restricciones de acceso a la información definidas para un funcionario interno. Deberá autorizar este acceso, definir la vigencia del mismo y asumir la responsabilidad por las acciones que se puedan realizar con su utilización.

3. Limitar el acceso a la información a lo mínimo indispensable para cumplir con el trabajo asignado.

Gerente de Área

4. Notificar a Recursos Humanos para que proceda con el registro en la base de datos de personal, indicando al menos los siguientes datos:

- Nombre completo del Tercero
- Cédula de Identidad
- Empresa a la que pertenece
- Relación con la Entidad Financiera

5. Reportar inmediatamente a Recursos Humanos y al Proveedor de Servicio de Seguridad Informática cada modificación en la condición contractual con Terceros.

6. Definir el acceso a Terceros a los sistemas informáticos y solicitar la autorización al Propietario de Información correspondiente, únicamente cuando sea necesario y de acuerdo a las Políticas y procedimientos establecidos respecto a Definición y Administración de Perfiles y Usuarios.

C.S. Jurídicos

7. Establecer conjuntamente con Riesgo Operativo el formato del CONTRATO DE CONFIDENCIALIDAD que se establecerá con Terceros. El mismo deberá incluir al menos cláusulas que especifiquen:

• Los requerimientos de seguridad de la información de la Entidad Financiera y las acciones a tomar en caso de violación del contrato.

• La no utilización del nombre de la Entidad Financiera por terceros en sus materiales de propaganda o mercadeo, a menos que reciba autorización escrita de la institución.

La prohibición de hacer pública la naturaleza y/o la existencia de la relación de Negocio con la Entidad Financiera, sin la autorización escrita de la Institución

• La destrucción o devolución inmediata de toda la información recibida por el tercero, una vez que se finalice el contrato de prestación de servicios relacionado.

8. Revisar, una vez que han sido completados, todos los contratos de confidencialidad firmados con Terceros.

Usuario Final

9. No deberá divulgar ninguna información relacionada a acuerdos o transacciones de Negocio relacionadas con clientes o terceros sin previa autorización del Vicepresidente de su Área.

10. En el caso de que un funcionario de la Entidad Financiera firmar un acuerdo de confidencialidad para un Tercero, este deberá ser revisado y aprobado por el C.S. Jurídicos.
11. Informar de violaciones a la seguridad de la información por parte de terceros al Proveedor de Servicio de Seguridad Informática.

Proveedor de Servicio de Seguridad Informática

12. Actualizar inmediatamente las modificaciones en la condición contractual de terceros.

Proveedor de Servicio de Tecnología

13. No deberá conceder a terceros la entrada a la red o a Internet vía telefónica, ni privilegios a las redes privadas virtuales, a menos que esté autorizada normalmente por el Propietario de la Información correspondiente y el medio haya sido certificado por el Proveedor de Servicio de Seguridad Informática y sólo por el tiempo requerido para cumplir las tareas autorizadas.

Sanciones

El incumplimiento de estos puntos será sujeto a sanciones determinadas por el nivel de supervisión de acuerdo a lo estipulado por el Reglamento Interno.

3.1.8. Políticas Seguridad Física y ambiental

1. Diseñar e implementar un programa de control de entrada y salida de equipos en horarios no regulares a nivel institucional, el mismo que deberá ser registrado, verificado y auditado.

2. Para el caso de áreas controladas, deberá dar énfasis a los siguientes puntos:

a. Desarrollar e implementar, de acuerdo a la Ley y Reglamentos vigentes, un Plan de Emergencia y evacuación de los(as) edificios/instalaciones, que permita:

- Evitar, o al menos minimizar, las causas de las emergencias.
- Garantizar la fiabilidad de los medios de protección.
- Tener informados de las medidas de protección a todos los ocupantes de las instalaciones.
- Disponer de personal organizado y adiestrado para las situaciones de emergencia.
- Hacer cumplir la normativa vigente de seguridad.
- Preparar la posible intervención de recursos externos (Policía, Bomberos, Ambulancias, etc.)

b. Implementar un único punto o puerta de acceso y los controles de acceso físico efectivos en proporción de los recursos humanos y el valor de los activos a proteger a través de mecanismos como llaves, guardias de seguridad, sistemas electrónicos de control de acceso (cierres con clave, lectura de banda magnética, lectores ópticos, biométricos), que cumplan al menos los siguientes requisitos:

- Permitir el acceso únicamente a las personas autorizadas por el responsable o propietario del área.
- Registrar quién, dónde y cuándo se realizó una entrada y/o salida.

c. Implementar sistemas de detección de situaciones anómalas y previsibles como puertas abiertas, acceso de intrusos, inundación, incendio o humo, etc. que permitan conocer inmediatamente la ocurrencia de un hecho de este tipo y su localización, así como definir e implementar los procedimientos de revisión de funcionamiento, riguroso mantenimiento preventivo, tratamiento de notificaciones y paso a los estados de Alerta y Alarma. Estos medios de detección deben integrarse en un único sistema, preferentemente automático que los gestione y al menos:

- Reporte la anomalía y su gravedad.
- Inicie acciones de corrección automáticas.
- Proponga acciones manuales a realizar por el personal entrenado para ello.
- Registre las actuaciones (qué, quién, cómo, dónde y cuándo).

Este sistema deberá funcionar incluso con el suministro eléctrico de emergencia.

d. Implementar medios automáticos y/o manuales de extinción de incendios, considerando el elemento extintor (agua, CO2, compuestos halogenados) apropiado para el previsible tipo de incendio en el área.

e. Revisar y documentar que las salidas de emergencia tengan alarmas y sean audibles y/o visibles, en la propia área y en la consola de control de seguridad. Realizar esta revisión al menos, anualmente e incluir la verificación del correcto funcionamiento incluso del alumbrado de emergencia en caso de pérdida de suministro eléctrico. La documentación de las revisiones del funcionamiento de las alarmas deberá guardarse como documento auditable por el período de un año.

f. Garantizar que todos los empleados, y las personas ajenas a la empresa con autorización para acceder por razones de negocio, porten permanentemente y en un lugar visible un identificador:

- Los empleados, al menos con fotografía y nombre legible a corta distancia.
- Las restantes personas, al menos, nombre y distintivo de la función que cumple.

g. Coordinar con el departamento de Bomberos un programa de inspecciones periódicas.

C.S. Compras, Logística y Mantenimiento

3 Para el caso de áreas controladas (Anexo No. 1), deberá dar énfasis a los siguientes puntos:

a. Implementar una adecuada protección para el suministro de energía eléctrica, Considerando:

- Que la calidad y continuidad son los requerimientos básicos del suministro de energía eléctrica.

- Las variaciones de frecuencia deberán ser corregidas con equipos estabilizadores que la mantengan en los rangos establecidos por los fabricantes de los recursos informáticos.

- Las variaciones de tensión deben ser manejadas por un sistema de alimentación interrumpida (UPS) de modo que se pueda prevenir efectos de posibles micros cortes por tiempo limitado y no como única alternativa.

b. Implementar una adecuada protección para el suministro de aire acondicionado, considerando:

- Incorporar el mecanismo de corte automático tras producirse una detección de incendio.

- Mantener el ambiente con la temperatura y la humedad adecuada, dentro de los límites indicados por los fabricantes de los recursos informáticos.

c. Conjuntamente con Seguridad Física implementar medios automáticos y/o manuales de extinción de incendios.

Gerentes – Responsables de áreas

4. Garantizar que la ubicación de los computadores personales de su área cumpla con las siguientes consideraciones:

- Que estén ubicados físicamente separados de las áreas de atención al público, en el caso de que necesariamente deban instalarse áreas sin restricción deberán al menos estar protegidas por una barrera física tal como un mostrador o un divisor que prevenga un acceso fácil a los clientes.

- El área en la que se encuentren los computadores personales deberá estar protegido contra contaminante ordinario o factores ambientales tales como humo, polvo, calor, humedad, partículas alimenticias y líquidos.

- Se deberá incorporar protección contra sobrecargas eléctricas y electricidad estática.

5.Definir e implantar las reglas de utilización de cada computador personal, portátil, dispositivos adicionales (CD, DVD, USB) y otros instalados en su área, que garanticen la protección de la información que almacenen o transmitan contra accesos no autorizados, considerando:

- Que la autorización del acceso a los empleados bajo su responsabilidad a los equipos o dispositivos está basada exclusivamente para realizar trabajos concernientes con las funciones de negocio.

- Que deberá definir e implementar un nivel de seguridad para cada equipo de su área en función de:

a. La clasificación de la información almacenada.
b. Los riesgos de la organización.
c. El costo del equipo, y
d. La disponibilidad de un equipo de respaldo

- Por cada riesgo para la seguridad de la información almacenada en los equipos o dispositivos de su área, deberá tomar una decisión específica acerca de:

a. Aceptar el riesgo.
b. Buscar cobertura externa o ajustar los controles para reducir las pérdidas.
c. Documentar formalmente esta decisión.
d. Para el caso de aceptar el riesgo, serán de su total responsabilidad los incidentes de seguridad que podría surgir, así como todos los efectos relacionados.

e. Para el caso de buscar cobertura externa se deberá contratar una póliza de seguro cuya cobertura sea adecuada y vigente para cada amenaza significativa a la confidencialidad, integridad y disponibilidad de la información almacenada.

f. Para el caso de ajustar los controles para reducir las pérdidas, será su exclusiva responsabilidad implementar los planes de acción necesarios para minimizar los riesgos de fuga de información.

6. Definir e implantar las reglas de utilización de cada impresora instalada en su área, que garanticen la protección de las salidas impresas de información clasificada contra accesos no autorizados. Para el caso de las impresoras remotas deberá considerar que:

- No estén situadas en áreas públicas.
- Las impresoras remotas situadas en áreas internas deberán tener uno o más de los controles siguientes:

a. Tener asignado un responsable de entregar las salidas impresas al Usuario final que las envió, o

b. Estar directamente atendidas por el usuario final, o

c. Recoger los listados personal e inmediatamente después de terminar la impresión, o tener la posibilidad de borrar los listados pendientes de Impresión.

Usuario Final

7. Todo identificador, especialmente los que permitan el acceso a áreas controladas, es de uso personal, intransferible y debe ser considerado como una contraseña de acceso físico y no compartirlo con nadie, la responsabilidad de los incidentes de seguridad en los que esté relacionado un identificador será de su propietario.

8. Si está autorizado a ingresar a Áreas Controladas no deberá permitir que otras personas no autorizadas ingresen al mismo tiempo. Si las otras personas están autorizadas deben registrar su acceso.

9. Está terminantemente prohibido el consumo en áreas controladas de alimentos, cigarrillo, bebidas alcohólicas o cualquier tipo de drogas.

10. Garantizar que su equipo de trabajo no esté conectado en la misma fuente de poder que los equipos que ocasionen interferencia electromagnética.

11. Cuidar el computador personal/portátil que tiene a su cargo y evitar robo de la información que contiene.

12. Proteger los medios magnéticos bajo su responsabilidad de accesos no autorizados.

13. Al salir temporalmente de su área de trabajo, deberá considerar:

- Implementar las medidas de seguridad necesarias (candados físicos, claves de protección de pantalla, teclado, etc.) que no permitan que otra persona pueda acceder a la información de su computador.

- Salir totalmente de las aplicaciones que esté utilizando, y con mayor razón cuando maneje información confidencial.

14. Al finalizar su trabajo, deberá considerar:

- Si el computador personal/portátil contiene información confidencial, deberá utilizar mecanismos de bloqueo físico o automático para deshabilitar su acceso.
- Si trabaja en una oficina que puede ser cerrada, deberá cerrarla.

15. Si trabaja con un computador portátil deberá:

- Considerar las mismas medidas de seguridad que para un computador personal.

- Garantizar el acceso a través de clave a los archivos de su producción.

- Garantizar que, cuando el acceso físico o lógico a información de su equipo portátil no pueda ser controlado o, por su nivel de clasificación, requiera medidas adicionales de seguridad, esta deberá ser cifrada de forma que quede ilegible y no pueda ser procesada por ningún usuario o persona no autorizada.

- Al finalizar su trabajo guardarlo bajo llave en un escritorio o anaquel seguro.

- Al viajar, deberá utilizar claves de control para el bloqueo de disco y configuración, protección de teclado y pantalla. Mantener el computador en su posesión y no exponerlo en automóviles o cuartos de hotel. No dejar el computador al alcance de terceros.
- No deberá añadir un ruteador, puente, módem o dispositivo de entrada a su computador sin previa autorización del área de Tecnología.

16. Al compartir la información de su equipo, deberá:
    - Al viajar, verificar los directorios e información que está compartiendo.
    - Habilitar claves de acceso a los mismos.
    - El usuario que recibe la solicitud deberá hacer su propia evaluación de conceder o no el acceso a su recurso y por lo tanto la respectiva clave y un tiempo definido de compartimiento.
    - El solicitante deberá desactivar el acceso compartido, una vez que haya finalizado su actividad.

17. Utilizar los computadores personales, portátiles y los dispositivos de almacenamiento adicionales como unidades de diskette, cd, dvd, usb y otros a los que ha sido previamente autorizado y en funciones de negocio.

18. Mantener el control de las salidas impresas que han sido enviadas a impresoras remotas.

19 Definir un modelo de respaldo/recuperación y almacenamiento fuera de sitio para la información que estime conveniente, con la frecuencia que garantice la supervivencia de la información por la cual responde a la Entidad Financiera.

20. El incumplimiento de estos puntos será sujeto de sanciones que podrán ir desde un llamado de atención al empleado hasta la aplicación de una multa o visto bueno.

Proveedor de Servicio de Seguridad Informática

21. Generar el procedimiento para la custodia de claves de manejo de archivos de equipos portátiles en caso de separación del empleado o pérdida del equipo.

Anexo 1. Distribución y Valoración de áreas

Un edificio o las instalaciones de la Entidad Financiera pueden estar distribuidos en varias áreas o zonas que dependiendo de su utilización y los bienes contenidos, tienen que estar sometidas a una serie de controles de acceso.

Se utilizará los siguientes criterios de distribución:

- **Áreas Públicas:** Espacios en los que no hay ningún tipo de restricción de acceso a empleados o personas ajenas a la empresa.
- **Áreas Internas**: Espacios reservados habitualmente a los empleados y personas ajenas a la empresa con autorización por motivos de negocio. En estos lugares pueden existir recursos informáticos con un valor bajo.

- **Áreas de acceso limitado:** Espacios cuyo acceso está reservado a un grupo reducido de empleados y personas ajenas a la empresa autorizadas por un acuerdo escrito. En estos lugares pueden concentrarse recursos informáticos que, en conjunto tienen un valor medio.

- **Áreas de acceso restringido:** Espacios cuyo acceso está reservado a un grupo muy reducido de empleados y personas ajenas a la empresa autorizadas por un acuerdo escrito, que tengan necesidad de acceder por razones de negocio. En estos lugares se encuentran recursos informáticos que, en conjunto tienen un alto valor o contienen activos de información críticos para las actividades de negocio.

- Las áreas de acceso limitado y restringido se denominarán Áreas Controladas, permanecerán cerradas, incluso cuando estén atendidas y sus accesos controlados.

Valoración

Los requisitos de control de acceso físico deberán basarse en el valor de los Sistemas de Información contenidos en cada área y en la importancia de las actividades de negocio suministradas por ellos.

Así, el valor de un sistema de información se deberá obtener de acuerdo a los siguientes criterios:

- Alto valor: Sistemas corporativos grandes y medios
- Medio valor: Pequeños sistemas corporativos y redes de área local (LAN)

- Bajo valor: pequeños sistemas (PC) y terminales

Para cada caso deberá considerarse adicionalmente los siguientes aspectos

Sistemas Críticos:
Aquellos que automaticen procesos críticos para el negocio de la empresa, y mantengan en una categoría Alto:

a. El costo y la necesidad de sustitución de los equipos en los cuales operan.
b. El impacto que podría ocasionarse en caso de una carencia prolongada de operación y la no disponibilidad de la información que suministran

Sistemas no Críticos:
Aquellos que automaticen procesos no críticos para el negocio de la empresa, y mantengan en una categoría Medio/Bajo:

a. El costo y la necesidad de sustitución de los equipos en los cuales operan.
b. El impacto que podría ocasionarse en caso de una carencia prolongada de operación y la no disponibilidad de la información que suministran.

La valoración final deberá ser realizada teniendo en cuenta todos los aspectos descritos, de acuerdo a la siguiente tabla:

SERVICIO	VALOR DEL SISTEMA	ÀREA
Sistemas Críticos	Alto	Área de Acceso Restringido
Sistemas No Críticos	Medio	Área de Acceso Limitado
	Bajo	
Unidades de Centro de Cómputo		Área de Acceso Restringido

SERVICIO	VALOR DEL SISTEMA	ÀREA
independientemente del sistema que soporten. Servidores, elementos de comunicación (Bridges, Gateway, routers, switch), herramientas que permitan visualizar el tráfico de las líneas/redes (sniffer, spoofers, trace tools)		
Las áreas que albergan los suministros auxiliares (energía Área de Acceso Restringido eléctrica, aire acondicionado) que dan servicio a los sistemas de información		Área de Acceso Restringido

Tabla 3.2: Valoración de áreas

Estos controles no son aplicables a sistemas temporales dedicados a pruebas o demostraciones.

3.1.9. Políticas Actualizaciones Directas a la Base de Datos

Entidad Financiera

Requerimiento o solicitud de modificación directa a la base de datos.

1. El proceso de modificación a las bases de datos deberá ser estrictamente considerado como una excepción, cuya ejecución deberá ser aprobada por el Propietario de la Información, o sus delegados[2] formalmente establecidos, de tal forma que cada incidencia ocurrida deberá generar la correspondiente modificación en la base de datos y la orden de mantenimiento que permita corregirla definitivamente.

[2] Los delegados deberán tener el cargo de Gerente o Responsable de Área, o mínimo el nivel inferior siguiente al Gerente o Responsable de Área. Los delegados no podrán ser los ejecutores de las afectaciones a la Base de Datos

Propietarios de la información

Autorizar la ejecución de scripts para solucionar incidencias reiterativas en el ambiente de producción o la solución a incidencias eventuales.

Proveedor de Servicio de Tecnología

2. Cuando se realicen modificaciones directas a las bases de datos del ambiente de producción de la Entidad Financiera, se deberá considerar en el proceso de Control de Cambios:

• La identificación y registro del requerimiento de la modificación.

• Evaluación del impacto del cambio en relación a la confidencialidad, integridad y disponibilidad de la base a ser actualizada.

• El procedimiento formal de aprobación del cambio por el Propietario de la Información.

• El procedimiento formal que identifique las responsabilidades de abortar y recuperar los cambios sin éxito y la correspondiente comunicación a las áreas y funcionarios involucrados.

• Conservar un registro auditable de la modificación realizada al menos por 5 años.

3. Deberá tipificar todas y cada una de las incidencias que dan paso a las modificaciones a las bases de datos y clasificarlas como reiterativas o eventuales de acuerdo a las tablas y campos que deben ser afectados.

4. Deberá administrar el registro de excepciones y remitirá mensualmente a riesgo Operativo el listado de las mismas.

5. Para el caso de incidencias reiterativas el Líder de Mantenimiento o el Líder de Proyecto deberá analizar y documentar el script general que deba realizarse, en el que se incluya todas las instrucciones que permitan garantizar la consistencia de la base de datos, es decir tanto las modificaciones a las tablas de datos como a las tablas de log's o las que fueren necesarias.

6. El Líder de Mantenimiento o el Líder de Proyecto en el caso de que se presenten incidencias eventuales deberá realizar el análisis, documentación y solicitar la aprobación para cada una de ellas.

7. El Líder de Mantenimiento o el Líder de Proyecto deberá desarrollar la solución definitiva para las incidencias reportadas.

Sanciones

El incumplimiento de estos puntos será sujeto a sanciones según lo estipulado en el Reglamento Interno de Personal.

3.1.10. Políticas Protección contra software malicioso

Usuario Final

1. Verificar con el antivirus instalado:

• Los respaldos de información antes ser restaurados

• Todos los dispositivos de almacenamiento que se ingrese en las estaciones de trabajo y protegerlos contra escritura, utilizar únicamente dispositivos de datos nunca de programas.

2. Apagar su equipo de trabajo, desconectarlo de la red y reportar tan pronto como sea posible al Help Desk todo funcionamiento no adecuado del software, ante la sospecha de presencia de virus o al identificar las siguientes anomalías:

• Cambios inesperados en la fecha.

• Cambios de longitud de los archivos, especialmente los ejecutables.

• Programas que tardan más tiempo del adecuado en arrancar o que se ejecutan con mayor lentitud de lo normal.

• Disminución de memoria de la estación de trabajo.
• Programas que intentan grabar en medios protegidos sin razón aparente.

• Cambios imprevistos de nombres de discos duros y unidades de cd, etc.

• Mensajes extraños en la pantalla.

• Y cualquier otra situación que se considere anómala.

3. No abrir ni ejecutar programas que no hayan sido solicitados por usted y sean recibidos por cualquier medio electrónico, aún si proceden de una fuente confiable.

4. Está prohibido terminantemente:

• Instalar computadores, dispositivos o software de propiedad de los empleados en la red de la Entidad Financiera o sus oficinas.

• Intentar reemplazar programas infectados o recuperar información, esta tarea debe ser cumplida por personal calificado.

• Ejecutar o copiar archivos de juegos en la estación de trabajo.

• Acceder a programas de origen público como anuncios, promociones, etc.

• Obtener software desconocido del Internet.

• Propagar de manera deliberada archivos o software infectados por virus que puedan ocasionar daños o entorpecer el funcionamiento de los sistemas informáticos.

Proveedor de Servicio de Seguridad Informática

5. Proponer a la Entidad Financiera las alternativas de adquisición de herramientas automáticas necesarias para controlar software malicioso.

6. Proponer a la Entidad Financiera las alternativas de adquisición de un antivirus a través de una base técnica de requerimientos.

7. Definir los parámetros de configuración de los sistemas de protección contra software malicioso instalados en la Entidad Financiera y realizar el control y seguimiento de los mismos.

8. Deberá organizar y mantener un equipo propio de respuesta ante emergencias que suministre la identificación acelerada de los problemas, el control de los daños y servicios de solución en caso de emergencias informáticas producidas por infección de virus.

9.Diseñar, implementar y difundir los procedimientos para realizar escaneo de puertos TCP y UDP que podrían ser utilizados por programas troyanos o gusanos sobre todos los rangos de direcciones de los equipos de la Entidad Financiera con el fin de detectar la existencia de software malicioso.

10. Informar a todos los usuarios sobre los virus informáticos y las medidas preventivas y cómo evitar la activación de los mismos a través de los canales de difusión establecidos por la Entidad Financiera.

Proveedor de Servicio de Tecnología

11. Es la única responsable de ejecutar el proceso de instalación, administración y monitoreo de los sistemas de protección contra software malicioso, en todos los equipos computacionales de la Entidad Financiera.

12. Garantizar que en todos los equipos de la Entidad Financiera se encuentre instalado un antivirus con definiciones actualizadas, que permita detectar y eliminar los virus que puedan contagiarse a la red, cortafuegos, servidores FTP, servidores de correo, servidores de la intranet y/o estaciones de trabajo a través de dispositivos, correo electrónico o transmisión de información infectada.

13. Diseñar, implementar y difundir los procedimientos para verificar la integridad de los sistemas informáticos críticos con el fin de detectar cambios no autorizados en los archivos de configuración, en los archivos de software base, software aplicativo y en los demás recursos del sistema.

14. Desconectar de la red de la Entidad Financiera los equipos que no posean los parches de software adecuados o que estén contaminados con software malicioso.

15. Reportar inmediatamente al Proveedor de Servicio de Seguridad Informática los incidentes evidenciados de seguridad relacionados con software malicioso.

Sanciones

El incumplimiento de estos puntos será sujeto a sanciones que podrán ir desde un llamado de atención al empleado hasta la aplicación de visto bueno.

Si el incumplimiento de esta política por parte del usuario final ocasionará una infección por software malicioso en los equipos de la Entidad Financiera, la Institución en su esfuerzo por proteger la confidencialidad, integridad y disponibilidad de la información que resida en los sistemas informáticos o de comunicación, no será responsable por la pérdida o daño de datos, información o
Software contaminado del usuario final.

3.1.11. Políticas Acceso a Recursos Tecnológicos

Auditoría

1. El Vicepresidente del Área es responsable de autorizar el acceso propio y al personal de su área a los recursos tecnológicos de la Entidad Financiera siguiendo el procedimiento establecido para el efecto. En caso de requerir acceso a las tablas o archivos que guardan la información de la Entidad Financiera, este deberá ser exclusivamente en modo de consulta.

2. Es responsabilidad del Vicepresidente del Área al momento de conocer la separación de su personal regular y no regular, ya sea por renuncia voluntaria y/o visto bueno, notificar al proveedor del Servicio de Administración de Claves se proceda con la desactivación de sus accesos.

Proveedor del Servicio de Administración de Claves

3. Es la única área responsable de centralizar la administración del control de acceso a recursos tecnológicos a las diferentes plataformas en el ambiente de Producción de la Entidad Financiera.

4. Deberá generar las normas, estándares y procedimientos específicos de seguridad para la administración de usuarios en Sistemas Operativos, Base de Datos u otros utilitarios propios de cada plataforma.

5. Deberá contar como parte del procedimiento interno con un mecanismo, que permita la validación de lo definido vs. lo ejecutado.

6. Deberá contar un procedimiento de optimización que incluya la depuración de la información almacenada y la actualización de los manuales de procedimientos.

7. Deberá ser el custodio de los usuarios del sistema y generar el procedimiento de seguridad para el caso en que se requiera su utilización. Para la operación diaria se generarán usuarios personalizados con similares atributos y privilegios de acceso a los originales.

8. El Gerente del Área de Administración de Claves del Proveedor es responsable de autorizar el acceso al personal de su área a los recursos tecnológicos de la Entidad Financiera siguiendo el procedimiento establecido para el efecto. En caso de requerir acceso a las tablas o archivos que guardan la información de la Entidad Financiera deberá ser exclusivamente en modo de consulta.

9. Es responsabilidad del Gerente del Área al momento de conocer la separación de su personal regular y no regular, ya sea por renuncia voluntaria y/o visto bueno, autorizar se proceda con la desactivación de sus accesos.

10. En caso de que el Gerente de Área personalmente requiera acceso a los recursos tecnológico de las plataformas de la Entidad Financiera, este deberá ser autorizado directamente por el Gerente General del Proveedor.

11. La información utilizada y producida en este proceso está clasificada como información confidencial, su distribución debe contar con la aprobación del Gerente de Riesgo Operativo de la Entidad Financiera. Cada transacción de control de acceso deberá generar registros auditables, los mismos que podrán ser revisados en el momento y por el personal que la Entidad Financiera estime conveniente.

12. De igual manera deberá definir formalmente un modelo de respaldo y recuperación de esta información, el mismo que deberá ser implementado conjuntamente con el proveedor del servicio de Tecnología, considerando al menos:

- Modo de procesamiento alterno
- Almacenamiento fuera de sitio
- Nombre de los archivos o tablas a respaldar
- Frecuencia de ciclos de obtención, retención y actualización de los respaldos.

- Número de Respaldos – Medios, Número de respaldos a obtenerse por Tabla/Archivo y especificación del medio magnético al cual se direccionarán.

- Prueba periódica de los respaldos para garantizar la eficacia de la restauración.

- Normas de rotulación, listado, transporte y almacenamiento de los respaldos.

Proveedor del Servicio de Tecnología

13. En el desarrollo de proyectos o adquisición de software para la Administración de Accesos a Recursos Tecnológicos se deberá implementar pistas de auditoría, las que deberán tener al menos la siguiente estructura:

- Fecha/Hora de modificación
- Estación de trabajo desde la que se realizó la modificación.
- Usuario
- Datos básicos que fueron afectados.

Así como también la característica de que la información relacionada a la Administración de Seguridad deberá almacenarse en formato encriptado.

14 La información de claves o de sus criptogramas no deberá ser visualizada en ningún aplicativo de Producción.

15 Todas las claves de operación de equipos o dispositivos electrónicos (por ejemplo: los ATM´S) deberán ser generadas por una caja de seguridad criptográfica y bajo ningún concepto deberán almacenarse en el código de un programa, y en el caso de archivos siempre y cuando estos estén encriptados.

16. El Gerente del Área de Tecnología del Proveedor es responsable de autorizar el acceso al personal de su área a los recursos tecnológicos de la Entidad Financiera siguiendo el procedimiento establecido para el efecto. Estos accesos corresponderán exclusivamente a las funciones que su personal deba ejecutar.

17. Es responsabilidad del Gerente del Área al momento de conocer la separación de su personal regular y no regular, ya sea por renuncia voluntaria y/o visto bueno, notificar al proveedor del Servicio de Administración de Claves se proceda con la desactivación de sus accesos.

18. En caso de que el Gerente de Área personalmente requiera acceso a los recursos tecnológico de las plataformas de la Entidad Financiera, este deberá ser autorizado directamente por el Gerente General del Proveedor.

3.1.12. Políticas Administración de Perfiles

Proveedor del Servicio de Administración de Claves

1. Es la única área responsable del proceso de Administración de Perfiles en el ambiente de Producción de la Entidad Financiera.

2. Será responsable de considerar como habilitantes de la ejecución de este proceso la solicitud del Propietario de Perfiles debidamente autorizada por los correspondientes Propietarios de Información y deberá mantener un registro histórico de todas las actualizaciones realizadas de forma individual o masiva, formal o emergente.

3. En el ambiente de producción no generará:

- Perfiles que no hayan sido definidos a través del proceso formal de Definición de Perfiles vigente en la Entidad Financiera.

- Perfiles con acceso total a las opciones, recursos, transacciones y/o servicios de un aplicativo.

- Perfiles con acceso a opciones, recursos, transacciones y/o servicios de aplicativos de negocio para el personal de Tecnología. En este caso específico si existiera una excepción deberá ser formalmente documentada, aprobada por el Propietario de Información correspondiente y por el Gerente de Tecnología y tener una vigencia determinada. Esta autorización deberá ser guardada como documento auditable por el período de 5 años.

4. Deberá generar el procedimiento que permita implementar este proceso. Deberá contar en el procedimiento interno un mecanismo que permita verificar razonabilidad de lo definido vs. lo ejecutado.

5. Deberá contar un procedimiento de optimización semestral que incluya la depuración de la información almacenada y la actualización de los manuales de procedimientos.

6. El proveedor del servicio de Administración de Claves deberá tratar la información generada en este proceso como información confidencial, su distribución deberá contar con la aprobación del Propietario de Perfil correspondiente.
De igual manera deberá definir formalmente un modelo de respaldo y recuperación de esta información, considerando al menos:

- Almacenamiento fuera de sitio.
- Nombre de los archivos o tablas a respaldar.
- Frecuencia de ciclos de obtención, retención y actualización de los respaldos.
- Número De Respaldos – Medios, Número de respaldos a obtenerse por Tabla/Archivo y especificación del medio magnético al cual se direccionarán.
- Prueba periódica de los respaldos para garantizar la eficacia de la restauración.
- Normas de rotulación, listado, transporte y almacenamiento de los respaldos.

Proveedor del Servicio de Tecnología

8. En el proceso de Gestión de Proyectos Tecnológicos para la Administración de Perfiles se deberá implementar pistas de auditoría, las que deberán tener al menos la siguiente estructura:

- Fecha/Hora de modificación.

- Estación de trabajo desde la que se realizó la modificación.
- Usuario.
- Acción ejecutada.
- Datos básicos que fueron afectados.

Así como también la característica de que toda la información relacionada a la Administración de Seguridad deberá almacenarse en formato encriptado.

9. En el proceso de Gestión de Proyectos Tecnológicos los requerimientos de control de acceso deberán tener la más alta prioridad a fin de minimizar la ocurrencia de incidentes de seguridad, eliminar las tareas manuales y la potencialidad de error en su ejecución.

10. En caso de existir el requerimiento de distribuir la información relacionada con la administración de seguridad (por ejemplo: perfiles, usuarios, contraseñas, etc.) se deberá garantizar que la información del repositorio central sea exactamente igual a la distribuida.

3.1.13. Políticas Administración de Usuarios

Entidad Financiera

1. Todos los usuarios que afecten la información de producción (on line/batch) deberán estar registrados en los sistemas de control de acceso de la Entidad Financiera.

Proveedor del Servicio de Administración de Claves

2. Es responsable de ejecutar el proceso de Administración de Usuarios, por lo tanto deberá identificar formalmente un Punto de Contacto y su correspondiente backup que realice la solicitud para la ejecución de este proceso con las áreas o departamentos de la Entidad Financiera.

3. Procesará únicamente los requerimientos para el caso de personal externo a la Entidad Financiera, siempre y cuando entre la Entidad Financiera y la correspondiente Empresa para la cual labora este personal se haya firmado el CONTRATO DE CONFIDENCIALIDAD – ANEXO A Normas de Seguridad.

4. Deberá ejecutar el proceso de Administración de Usuarios, considerando al menos los siguientes requisitos:
En el ambiente de producción no se generarán:

- Usuarios para el personal de Tecnología.
- Usuarios no personalizados.
- Usuarios para realizar pruebas funcionales o de impacto de las aplicaciones.

Se generarán usuarios genéricos únicamente para identificar a los componentes o programas que realizan transacciones de batch, convivencia, etc. y no para ser usados bajo responsabilidad de los funcionarios de la Entidad Financiera.

- Cada funcionario debe tener un usuario único e intransferible en todos y cada uno de los aplicativos definidos en producción, al que le corresponderá un perfil de acuerdo a la función que desempeña.

- En el ambiente de Producción ningún usuario mantendrá el estado de activo, cuando el empleado propietario del mismo se encuentre definitivamente separado de la Entidad Financiera.

Las excepciones a este punto deberán ser formalmente autorizadas por el Propietario de la Información y el Gerente de Tecnología. Esta autorización deberá ser guardada como un registro auditable por el período de 5 años.

5. Deberá determinar formalmente los niveles de servicio para cada tipo de requerimiento.

6. Deberá garantizar que el proceso de Administración de Usuarios esté soportado documentalmente por la solicitud realizada por el Punto de Contacto, debidamente autorizada por el Gerente de Área y deberá mantener un registro histórico de todas las actualizaciones realizadas de forma individual o masiva, formal o emergente.

7. Para los casos en los que los Gerentes de Área realicen un requerimiento para sí mismos, este deberá ser autorizado por el Vicepresidente de la División correspondiente. En el caso de un Vicepresidente, éste podrá proceder con la autorización para su propio requerimiento.

8. Para la eliminación de usuarios en el servicio de Red, deberá soportarse en la información publicada en el aplicativo de Manejo de Habilitantes de RRHH.

9. Deberá contar con una base de datos que contenga al menos:

- Datos generales del Usuario (Cédula, Nombre completo, oficina, empresa).
- Accesos (código de usuario y perfil en cada uno de los aplicativos a los que ingresa).

- Trazabilidad del Usuario (Fecha de última actualización, Histórico de las actualizaciones realizadas).

10. Debido al volumen de procesamiento que involucra este proceso deberá contar en el procedimiento interno un mecanismo, que permita verificar la razonabilidad de lo solicitado vs. lo ejecutado.

11. Deberá contar un procedimiento de optimización semestral que incluya la depuración de la información almacenada y la actualización de los manuales de procedimientos.

12.La información utilizada y producida en este proceso está clasificada como información confidencial su distribución debe contar con la aprobación del Gerente de Riesgo Operativo de la Entidad Financiera. Cada transacción de administración de usuarios deberá generar registros auditables, los mismos que podrán ser revisados en el momento y por el personal que la Entidad Financiera estime conveniente.

13. De igual manera deberá definir formalmente un modelo de respaldo y recuperación de esta información, el mismo que deberá ser implementado conjuntamente con el proveedor del servicio de Tecnología, considerando al menos:

- Modo de procesamiento alterno
- Almacenamiento fuera de sitio
- Nombre de los archivos o tablas a respaldar
- Frecuencia de ciclos de obtención, retención y actualización de los Respaldos.
- No. De Respaldos – Medios, Número de respaldos a obtenerse por

Tabla/Archivo y especificación del medio magnético al cual se direccionarán.

- Prueba periódica de los respaldos para garantizar la eficacia de la restauración.
- Normas de rotulación, listado, transporte y almacenamiento de los Respaldos.

Punto de Contacto

14. Es responsabilidad del Punto de Contacto realizar la solicitud para la creación, modificación y eliminación de usuarios para su área en los diferentes aplicativos, considerando los SLA´s establecidos con el proveedor del Servicio de Administración de Claves.

Proveedor de Servicio de Tecnología

15. En el desarrollo de proyectos o adquisición de software para la Administración de Perfiles y Usuarios se deberá implementar pistas de auditoría, las que deberán tener al menos la siguiente estructura:

- Fecha/Hora de modificación
- Estación de trabajo desde la que se realizó la modificación
- Usuario
- Acción ejecutada
- Datos básicos que fueron afectados

Así como también la característica de que la información relacionada a la Administración de Seguridad deberá almacenarse en formato encriptado.

3.1.14. Políticas Definición de Perfiles

Propietario de Perfiles

1. Definir los perfiles para el personal de su área considerando:

- Salvaguardar la información de la Entidad Financiera a través de los tres principios básicos de seguridad:

  Confidencialidad
  La información debe ser vista y manejada únicamente por quienes tienen derecho o la autoridad de hacerlo.

  Integridad
  La información debe ser consistente, fiable y no susceptible a alteraciones no deseadas.

  Disponibilidad
  La información debe ser accedida en el momento en que el usuario requiera de ella.

- Adecuada separación de funciones respecto a la generación de información sobre:

  - La descripción, funcionalidad, características, riesgo, control y consideraciones adicionales de las opciones, recursos, transacciones y/o servicios de todos los aplicativos del ambiente de producción, herramientas de ofimática o recursos adicionales.

  - Necesidades de información de un área, departamento u oficina.

2. Una vez definidos los perfiles de su área deberá solicitar la autorización al Propietario de Información correspondiente y remitir los perfiles autorizados al proveedor del servicio de Administración de Claves para su implementación.

3. Deberá actualizar la definición de sus perfiles en caso de presentarse los siguientes eventos:

- Generación de nuevos procesos, rediseño de procesos existentes.
- Generación de nuevas funcionalidades, cambio de funcionalidades existentes.
- Salida a producción de nuevos aplicativos, mantenimientos de opciones, recursos y/o transacciones de aplicativos existentes

4. El propietario de perfiles es el propietario de información de los perfiles implementados en su área, deberá tratarlos como información confidencial.

5. De igual manera deberá definir formalmente un modelo de respaldo y recuperación de esta información.

6. Para el caso de la Red de Oficinas:

• El propietario de perfiles del Front Operativo será el Gerente de esta área o su delegado formalmente establecido.

• El propietario de perfiles de Negocios serán los Vicepresidentes de Personas, Empresas, Consumo y Micro crédito según su competencia, o sus delegados formalmente establecidos.

7. Deberá depurar los usuarios de su área al menos una vez al año.

Proveedor del servicio de Administración de Claves

8. Implementar en los recursos de Tecnología de Información exclusivamente los perfiles solicitados por un Propietario de Perfiles y debidamente autorizados por los correspondientes Propietarios de Información.

3.1.15. Políticas Reseteo de Claves de Usuarios

Proveedor del Servicio de Administración de Claves

1. Es responsable de ejecutar el proceso de Reseteo de Claves de Usuarios, podrá delegar esta función y compartir su responsabilidad con una Unidad ejecutora, siempre y cuando se cumplan los siguientes requisitos:

- El procedimiento de Reseteo, deberá estar formalmente establecido, aprobado y difundido.

- Las herramienta(s) automática(s) que soporte(n) este proceso debe(n) implementarse totalmente, de acuerdo a los requerimientos solicitados por Seguridad Informática.

- De igual manera dicha(s) herramienta(s) deberá(n) implementar pistas de auditoría, en el caso de que el aplicativo no lo permita, existirá una excepción que deberá ser formalmente documentada, aprobada por el Vicepresidente de Operaciones y Tecnología quien asumirá el riesgo consecuente y además se implementará un mecanismo administrativo de control.

- Al implementar un esquema descentralizado el alcance de la función de reseteo deberá estar limitado exclusivamente al ámbito de acción de los funcionarios a quienes se ha dado esta responsabilidad.

Usuario Final

2. La función de reseteo no deberá ser considerada dentro del flujo normal de trabajo, es una actividad de excepción y en el 80% de los casos generada por el incumplimiento de la Política de Uso de Claves por parte del usuario final, por esta razón si la causa de generación del requerimiento de reseteo está bajo la responsabilidad del usuario final, este estará sujeto a las sanciones definidas a discreción de su línea de supervisión.

Proveedor del Servicio de Administración de Claves

3. Deberá establecer formalmente los niveles de servicio para este tipo de requerimiento. Así como también el número de veces permitido de reseteo por usuario dentro de un período de tiempo determinado.

4. Deberá garantizar que cada transacción efectuada de Reseteo esté soportada por el requerimiento realizado por el Usuario Final y deberá mantener un registro histórico de todos los reseteos ejecutados.

5. El proceso de reseteo deberá contar en el procedimiento interno un mecanismo, que permita la validación diaria de lo solicitado vs. lo ejecutado.

6. Deberá contar un procedimiento de optimización semestral que incluya la actualización de los manuales de procedimientos.

7. Deberá implementar un procedimiento de Manejo de Alertas que permita detectar incidentes de seguridad en este proceso, el mismo que deberá estar formalmente establecido, aprobado y difundido.

8. La información utilizada y producida en este proceso está clasificada como información confidencial, su distribución debe contar con la aprobación del Gerente de Riesgo Operativo de la Entidad Financiera.

9. De igual manera deberá definir formalmente un modelo de respaldo y recuperación de esta información, el mismo que deberá ser implementado conjuntamente con el proveedor del servicio de Tecnología, considerando al menos:

- Modo de procesamiento alterno
- Almacenamiento fuera de sitio
- Nombre de los archivos o tablas a respaldar
- Frecuencia de ciclos de obtención, retención y actualización de los Respaldos.
- No. De Respaldos – Medios, Número de respaldos a obtenerse por Tabla/Archivo y especificación del medio magnético al cual se direccionarán.

Proveedor del Servicio de Reseteo de Claves de Usuarios

10. Deberá proceder con un requerimiento de reseteo siempre y cuando:

- El solicitante del requerimiento sea el usuario final directamente afectado. Para lo cual deberá implementar el procedimiento y los mecanismos necesarios que le permitan esta verificación. Una vez realizado el requerimiento de reseteo se contestará exclusivamente al usuario final.

- La excepción a este punto estará dada exclusivamente en el caso de que el usuario final no se encuentre y el acceso a su información sea de vital importancia para el cumplimiento de las funciones de una Unidad. En este caso, el reseteo se lo hará únicamente con la aprobación de la línea de supervisión a nivel de Responsable o Gerente, que lo deberá solicitar formalmente vía mail al Proveedor del Servicio de Reseteo de Claves de Usuarios, Unidad que direccionará el requerimiento al proveedor del Servicio de Administración de Claves, quienes procederán con el mismo bajo las siguientes consideraciones:

  - La responsabilidad de las acciones realizadas a través de la utilización de la nueva clave serán de la línea de supervisión solicitante.

  - Una vez realizado el requerimiento se contestará al usuario final y al funcionario designado por la línea de supervisión para utilizarla.

Proveedor de Servicio de Tecnología

10. En el desarrollo de proyectos o adquisición de software que implemente la función de Reseteo de Claves de Usuario, los Líderes de Proyecto / Analistas Funcionales deberán considerar:

- La información correspondiente a claves de acceso deberá almacenarse en formato encriptado y no deberá ser parte de programas, comandos de inicio de sesión o macros de software.

- La operación de reseteo deberá inicializar la clave de un usuario final con un número calculado randómicamente.

- Una vez que la clave de un usuario final haya sido inicializada, el usuario no podrá acceder al aplicativo mientras no personalice su clave.

- Se deberá implementar pistas de auditoría para la ejecución de este procedimiento, las que deberán tener al menos la siguiente estructura:

  - Fecha/Hora de modificación.
  - Estación de trabajo desde la que se realizó la modificación.
  - Usuario.
  - Acción ejecutada.
  - Datos básicos que fueron afectados.

3.1.16. Políticas Clasificación de Riesgo de Proyectos

Entidad Financiera

1. Todo Proyecto de Aplicación que tenga calificación de riesgo ALTO para pasar a producción deberá obtener:

- La certificación funcional por parte del Usuario.
- La certificación técnica por parte de QA (Quality Assurance) del Proveedor de Servicio de Tecnología y
- La certificación de seguridad por parte del Proveedor de Servicio de Seguridad Informática.

Riesgo Operativo

2. Identificará y valorará los riesgos consecuentes de una excepción a la Certificación de los Proyectos de Aplicación, los mismos que serán minimizados una vez que la excepción esté regularizada.

Proveedor de Servicio de Tecnología

3. Utilizar los estándares de los requerimientos de las certificaciones Funcional, Técnica y de Seguridad e incorporarlos como parte de la Metodología de Desarrollo de Proyectos de Aplicación.

4. Incluir en la Metodología en la fase de "Visión y Alcance" la actividad de Calificación de Riego y en la fase de “Estabilización” la actividad de Certificación.

5. El Área de Control de Cambios deberá cumplir con lo siguiente:

- El procedimiento de Control de Cambios incluirá entre los documentos a ser presentados para un paso a producción, el Formulario para evaluar el riesgo debidamente completado.

- El área de Control de Cambios validará la existencia de dicho Formulario y verificará que existan los documentos de las certificaciones funcional y técnica. En caso de que el riesgo del Proyecto de Aplicación sea ALTO, verificará también la existencia de la certificación de seguridad o en su defecto la correspondiente excepción debidamente documentada.

- Será la unidad responsable de la administración de las excepciones a la Certificación y control de su regularización.

- Deberá diseñar, implementar y difundir los procedimientos para la Administración y Regularización de Excepciones, considerando como uno de sus resultados el reporte mensual de excepciones vencidas a las áreas de Riesgo Global y Auditoría.

Proveedor de Servicio de Seguridad Informática

6. Será la responsable de realizar la Calificación de Riesgo del Proyecto.

7. Deberá diseñar, implementar y difundir los procedimientos para Calificación de Riesgo de los Proyectos de Aplicación y Certificación de Seguridad.

8. Informará mensualmente a las áreas de Auditoría y Riesgo Operativo la calificación de los Nuevos Proyectos de Aplicación.

3.1.17. Políticas Desarrollo y Mantenimiento de Sistemas

Entidad Financiera

1. El diseño de la infraestructura de IT, las aplicaciones de negocio y las aplicaciones de usuario final, deberán implementar los requerimientos de seguridad documentados en esta política. Los mismos que deberán ser incorporados en cada paso del ciclo de desarrollo/adquisición de software (Visión y Alcance aprobado, Planes del Proyecto aprobados, Alcance completado, Entrega Aprobada, Instalación Completa y en uso).

2. Las aplicaciones que se instalen en el ambiente de producción deberán ser diseñadas e implementadas bajo un entorno seguro, que incluya la validación de datos de entrada, el procesamiento interno, la autenticación de mensajes, la salida de datos y pistas de auditoría.

Proveedor de Servicio de Tecnología

3. Los datos de entrada deberán ser validados para asegurar que son correctos y apropiados. Deberá incorporar controles en la captura de:

- Transacciones de negocios.
- Datos permanentes (nombres y direcciones, límites de crédito, números de referencia al cliente), y
- Tablas de parámetros (precios de venta, tasa de impuestos, índice de conversión de dinero).

4. Los controles a implementarse deberán evitar:

- Valores fuera de rango.
- Caracteres inválidos en campos de datos.
- Datos faltantes o incompletos.
- Volúmenes de datos que exceden los limites inferior y superior.
- Controles de datos no autorizados o inconsistentes;

5. Deberá garantizar que los controles implementados dependerán de la naturaleza de la aplicación y del impacto de eventuales alteraciones de datos en el negocio, así deberá considerar los siguientes controles mínimos:

- Garantizar la confiabilidad de las tablas y/o archivos lo que permitirá detectar la corrupción que podrían sufrir los datos que han sido correctamente ingresados debido a errores de procesamiento o a través de actos deliberados.

- Garantizar que el diseño de los aplicativos implemente las restricciones para minimizar los riesgos de fallas de procesamiento que conducen a una pérdida de la integridad de la información.

- Implementar procedimientos para recuperación ante fallas, a fin de garantizar el procesamiento correcto de los datos.

- Verificación de la integridad de los datos entre computadoras centrales y remotas.

Controles de procesamiento interno batch

Proveedor de Servicio de Tecnología

Deberá garantizar que los siguientes controles mínimos:

- Garantizar que los Aplicativos calendarizados se ejecuten en la fecha definida.

- Garantizar que los programas se ejecuten en la secuencia correcta y si se interrumpen en caso de producirse una falla, que se detenga todo el procesamiento posterior, relacionado a la interrupción, hasta que se resuelva el problema.

- Implementar procedimientos de manejo de excepciones que interpreten las respuestas del sistema operativo y permitan ejecutar las acciones necesarias en caso de fallas o interrupciones.

Controles de procesos de migración

Proveedor de Servicio de Tecnología

7. Deberá garantizar que los siguientes controles mínimos:

• Implementar procedimientos de validación automática que garanticen la migración oportuna y correcta de la información de un aplicativo anterior a uno nuevo.

Validación de los datos de salida

Proveedor de Servicio de Tecnología

8. Deberá garantizar la salida de datos de un aplicativo, al menos en los siguientes puntos:

- Provisión de información suficiente, para que el Propietario de la Información determine la exactitud, totalidad, precisión y clasificación de la información.

Protección de los datos de prueba

Proveedor de Servicio de Tecnología

9. La información confidencial o estrictamente confidencial no deberá ser utilizada para Propósitos de prueba. Si se utiliza información de esta índole, esta debe ser sometida a un proceso de despersonalización antes de su uso. Este proceso deberá ser certificado por el proveedor de Servicio de Ingeniería de Seguridad.

Desarrollo de Software

Proveedor del Servicio de Tecnología

10. Deberá incluir en la metodología de desarrollo lo siguiente:

- En la etapa de Anteproyecto, el Líder de Producto deberá conceptualizar el Plan de Contingencia en caso de la pérdida de disponibilidad del nuevo aplicativo, así como también deberá generar el entregable de Definición de Propietarios del Proceso y de Información.

- En la etapa de Planes del Proyecto aprobados, el Líder de Producto deberá generar el entregable Requerimientos de Control de acuerdo a la Política de Clasificación de Información.

- En la etapa de Alcance Aprobado, el Líder de Proyecto deberá generar los entregables: Listado de opciones y su descripción; Modelo de Respaldo y Recuperación, y Autorizadores de modificaciones directas a las BDD.

- En la etapa de Alcance Aprobado, el Líder de Producto deberá generar el entregable de Perfiles autorizados por el Propietario de Información.

- En la etapa de Entrega Aprobada, el Líder de Producto deberá generar los entregables Manual de Usuario; Plan de Contingencia para la falta de disponibilidad del nuevo aplicativo, y Definición de los SLA´s del nuevo aplicativo.

Desarrollo de Software Externo

Líder de Producto

11. Si el desarrollo de software está bajo la responsabilidad de Proveedores externos deberá considerar en la definición del Alcance del Proyecto al Proveedor de Servicio de Tecnología y al Proveedor de Servicio de Seguridad Informática.

12. Entregar información a los proveedores externos siempre y cuando el formato vigente del Contrato de Confidencialidad haya sido completado y firmado.

Proveedor del Servicio de Seguridad Informática

13. Participará de las reuniones de definición del alcance del proyecto estableciendo los Lineamientos de seguridad de la aplicación en los siguientes niveles:

- Seguridad del sistema operativo donde se ejecutará la aplicación.
- Seguridad de la aplicación.
- Seguridad en el almacenamiento de la información confidencial y estrictamente confidencial.
- Seguridad en el proceso de comunicación.
- Análisis de vulnerabilidades de la aplicación.

Proveedor del Servicio de Tecnología

14. Entregar a los Proveedores externos el Estándar de Programación Segura de la Entidad Financiera para su conocimiento y cumplimiento.

Proveedor Externo del Servicio de Tecnología

15. Cumplir con todos y cada uno de los requerimientos de la metodología de desarrollo de proyectos informáticos vigente para el desarrollo interno de la Entidad Financiera.

Preliminar a la Certificación

Líder de Producto

16. Coordinar con el Líder del Proyecto y el Proveedor de Servicio de Seguridad Informática la calificación de riesgo de proyectos de aplicación para Certificación.

Propietario de Perfiles

17. Actualizar los perfiles existentes y/o definir nuevos perfiles que consideren al nuevo aplicativo y solicitar su aprobación a los Propietarios de Información correspondiente.

Propietario de Información

18. Para la información a su cargo del nuevo aplicativo deberá:

- Aprobar solicitudes de actualización o generación de perfiles de usuarios para los aplicativos bajo su responsabilidad.

- Aprobar el modelo de respaldo y recuperación de su información.

- Seleccionar un período de retención de su información, en base a lo estipulado en la Ley y Políticas vigentes.

Proveedor del Servicio de Tecnología

19. Solicitar para proceder al paso a producción del aplicativo al menos la siguiente documentación:

- La calificación de riesgo de proyectos de aplicación para Certificación. Si la aplicación ha sido calificada como de Riesgo Alto adicionalmente deberá solicitar la Certificación de Seguridad.

- El listado del (os) Propietario(s) de Proceso y Propietario(s) de Información del nuevo aplicativo.

- La conformidad del Proveedor del servicio de Seguridad Informática respecto a la adecuada autorización de los Propietarios de Información sobre el listado de los perfiles que consideren la funcionalidad del nuevo aplicativo.

- El Plan de Contingencia para la falta de disponibilidad del nuevo aplicativo.

- Los SLA’s el nuevo aplicativo.

- Todos los requisitos especificados en la metodología vigente de trabajo.

3.1.18. Políticas Administración de la Continuidad

Entidad Financiera

1. Deberá designar un Equipo de continuidad de Negocio, integrado por las áreas de: Auditoría, Riesgos, Legal, Administrativa y las correspondientes áreas de Negocio y los Proveedores de los Servicios de Seguridad Informática, Tecnología y Operaciones, este equipo implementará un proceso de Administración de Continuidad de Negocios para crear una respuesta consistente y disponer de una planificación ordenada que permita a la Entidad Financiera minimizar el impacto y consecuencias de un suceso inesperado, a la vez que le asista durante las etapas de recuperación de su normal operación.

2. El Directorio de la Entidad Financiera establecerá su delegación en el Comité de Continuidad de Negocios a fin de cumplir con las responsabilidades establecidas en la Resolución No. JB-2005-834 Sección V Artículo 1 Numeral 1.5. Este Comité estará formado por los Líderes de Auditoría, Riesgos y Recuperación, Administrativo y Recursos Humanos, Personas, Empresas, Tesorería, Legal, Control Financiero y Marketing; a nivel consultivo el Responsable de Riesgo Operativo y por parte de los Proveedores de Servicios de Seguridad Informática, Tecnología y Operaciones el Vicepresidente de Operaciones y Tecnología y los Responsables de Seguridad Informática y Tecnología. Este Comité deberá ser el responsable de la toma de decisiones estratégicas que permitan implementar en la Entidad Financiera el proceso de Administración de la Continuidad de Negocios.

3. La administración de Continuidad de Negocios deberá incluir controles destinados a:

- Identificar y reducir riesgos.
- Atenuar las consecuencias de los incidentes perjudiciales, y
- Asegurar la reanudación oportuna de los Procesos Críticos.

Equipo de Continuidad de Negocios

4. Implementar un proceso controlado para el desarrollo y mantenimiento de la Continuidad de Negocios de la Entidad Financiera. Este proceso deberá al menos contemplar lo siguiente:

- Análisis de Riesgo, identificación de los riesgos en términos de probabilidad de ocurrencia e impacto.
- Análisis de Impacto.
- Estrategias de Continuidad.
- Elaboración y documentación del BCP de conformidad con la estrategia de continuidad acordada.
- Política de Comunicación

CONTINUIDAD DEL NEGOCIO Y ANÁLISIS DE IMPACTO

Equipo de Continuidad de Negocios

5. Desarrollar el Análisis de Riesgo, que permita identificar eventos que puedan ocasionar interrupciones en los procesos críticos de negocios, cuyo objetivo sea medir el grado de exposición de la organización a hechos potencialmente disruptivos. El análisis deberá incluir las exposiciones físicas, las medidas de protección existentes y un análisis de la relación costo/beneficio de la reducción de la exposición.

6. Ejecutar el Análisis de Impacto del Negocio, conjuntamente con los Propietarios de la Información.

7. De acuerdo a los resultados de los análisis de riesgo e impacto al negocio, deberá Desarrollar el Plan Estratégico de Continuidad de Negocio.

8. Aprobar formalmente los procesos, aplicativos, servicios y activos de información críticos, incluyendo sus correspondientes modelos de respaldos y recuperación.

9. Aprobar el plan estratégico para determinar el enfoque global con el que se implementará la Administración de la Continuidad del Negocio.

ELABORACIÓN E IMPLEMENTACIÓN DE PLANES DE CONTINUIDAD DEL NEGOCIO

Equipo de Continuidad de Negocios

10. Una vez establecidos el nivel de riesgo y el impacto al negocio deberá plantear diversas estrategias de continuidad. Estas estrategias deberán permitir ejecutar los procesos críticos en el plazo previsto por el análisis de impacto de negocio y con un costo paralelo de acuerdo al análisis de riesgos.

11. Implantar la estrategia de continuidad aprobada por el Comité de Continuidad de Negocios.

Líder y Responsable de Área

12. Difundir y hacer cumplir las responsabilidades de su personal en el proceso de Continuidad de Negocio.

Comité de Continuidad de Negocios

13. Aprobar la alternativa más eficaz con el menor costo posible que permita implementar un Plan de Continuidad del Negocio.

C.S. Jurídicos

14. En el caso de que la alternativa seleccionada sea arrendar un Centro Alternativo, deberá garantizar que el contrato detalle al menos los siguientes servicios:

- Reserva de Recursos (capacidad, almacenamiento, etc.).
- Prueba realizada y/o planificada.
- Desastre real, tiempo de ocupación.
- Soporte técnico y asesoría.
- Posibilidad de que el centro sea auditado por el personal que la Entidad Financiera Designe.

El contrato deberá garantizar, en cualquier caso, la disponibilidad del centro alternativo y la realización de las pruebas periódicas de recuperación en las fechas predeterminadas.

3.1.19. Políticas PARA EL INTERCAMBIO DE INFORMACIÓN

Correo Electrónico Uso para Negocios

- Los sistemas de correo electrónico de la Entidad Financiera serán principalmente utilizados para fines de negocios.

- Está prohibido a los empleados el uso de cualquier sistema de correo electrónico que no sea de la Entidad Financiera, para enviar o recibir información.

- El uso de sistemas de mensajería instantánea no aprobados, no está permitido.

- Todos los mensajes enviados desde la Entidad Financiera cumplirán con la normativa legal vigente y los estándares de la Institución en cuanto a su contenido.

- Los mensajes de correo electrónico, incluyendo los archivos adjuntos serán clasificados de acuerdo a esta Política, basados en la sensibilidad de la información contenida. Consecuentemente, serán asegurados de acuerdo a esta clasificación.

- No está permitido utilizar los recursos informáticos con el fin de difundir cadenas, mensajes, información, publicar comentarios políticos de carácter impropio que atenten contra las buenas costumbres, ofendan la dignidad de personas y/o instituciones con fines de propaganda y/o difusión de información no autorizada. El incumplimiento de esta disposición conlleva sanciones.

Transmisión por correo electrónico

La información confidencial o estrictamente confidencial no será enviada por correo electrónico, a menos que se encuentre protegida de acuerdo a los estándares de la Entidad Financiera.

Monitoreo de las Comunicaciones

La Entidad Financiera se reserva el derecho de monitorear cualquier tráfico electrónico como parte de sus actividades operacionales normales, dentro del marco de la legislación vigente.

Internet

- Los funcionarios de la Entidad Financiera podrán acceder a Internet si su funcionalidad de Negocio así lo amerita.

- El uso personal de Internet será permitido dentro de límites razonables y siempre que los web sites accedidos no sean ilegales o inapropiados para un ambiente de trabajo bien controlado.

- Internet no será utilizada para violar derechos de propiedad intelectual de ninguna clase.

- El acceso a otros recursos que no sean páginas de Internet, está reservado a usuarios autorizados.

- La Entidad Financiera se reserva el derecho de bloquear el acceso a sitios de Internet considerados inapropiados.

- La descarga de archivos electrónicos desde Internet – por parte de los usuarios finales – no está permitida.

- Está estrictamente prohibido intentar vulnerar o violar cualquier sistema informático o redes en Internet.

Transferencia de Archivos

- La información clasificada como confidencial no será enviada a través de ningún mecanismo de transferencia de archivos, a menos que sea encriptada de acuerdo a los estándares de la Entidad Financiera.

MARCO PARA LA PLANIFICACIÓN DE LA CONTINUIDAD DEL NEGOCIO

Equipo de Continuidad de Negocios

15. Deberá mantener un solo marco para los planes de continuidad del negocio, a fin de garantizar su uniformidad e identificar prioridades de prueba y mantenimiento.

Deberá tener en cuenta los siguientes puntos:

- Condiciones de implementación de los planes que describan el proceso a seguir antes de poner en marcha los mismos.
- Procedimientos de emergencia.
- Procedimientos de recuperación.
- Procedimientos de reanudación.
- Cronogramas de mantenimiento y pruebas.
- Cada plan debe tener un propietario específico. Los procedimientos de emergencia, los planes de reanudación y los planes de recuperación deberán ser parte de las responsabilidades de los Propietarios de Información correspondientes.

PRUEBA, MANTENIMIENTO Y REEVALUACIÓN DE LOS PLANES DE CONTINUIDAD DEL NEGOCIO.

Equipo de Continuidad de Negocios

16. Probar periódicamente los BCP, para garantizar su actualización y efectividad, así como también asegurar que el personal involucrado, conozca y cumpla a cabalidad sus responsabilidades.

17. Evaluar cada prueba que se realice a fin de retroalimentar el BCP, emitir un informe al Comité de Continuidad de Negocios, este documento deberá guardarse como registro auditable al menos por cinco años.

18. Diseñar un plan de mantenimiento continuo para garantizar la efectividad del BCP.

19. Garantizar la distribución del BCP actualizado. Así, el BCP (Plan de Continuidad del Negocio) deberá estar accesible de manera continua en Internet, por lo menos en dos sitios diferentes soportados por proveedores diferentes de servicios.

Sanciones

El incumplimiento de estos puntos será sujeto a sanciones que podrán ir desde un llamado de atención al empleado hasta la aplicación de visto bueno.

La no participación de una determinada área en el proceso de Continuidad de Negocios, generará para la misma, una provisión determinada de acuerdo a las tareas no cumplidas y a sus respectivas consecuencias.

3.2. Definición de los procedimientos de seguridad de información utilizando las normas ISO27001 e ISO27002

3.2.1. Procedimiento para la Clasificación de la Información

1. Cada jefe de departamento dará importancia a la información en base al nivel de clasificación que demande el activo.

2. La información pública puede ser visualizada por cualquier persona dentro o fuera de la institución.

3. La información interna, es propiedad de la institución, en ningún momento intervendrán personas ajenas a su proceso o manipulación.

4. La información confidencial es propiedad absoluta de la organización, el acceso a ésta es permitido únicamente a personal administrativo.

5. Los niveles de seguridad se detallan como nivel de seguridad bajo, nivel de seguridad medio y nivel de seguridad alto.

3.2.2. Procedimientos accesos por parte de Terceros

1. Al ser contratado como empleados de la Organización, se les entregará la documentación necesaria para cubrir todas las necesidades inherentes a su cargo.

2. Los requisitos mínimos de seguridad se expresan, en cuestión del monitoreo y adecuación de un servicio con respecto a su entorno o medio de operación.

3. El administrador de sistemas tomará las medidas necesarias para asignar los servicios a los usuarios externos.

4. El no cumplimiento de las disposiciones de seguridad y responsabilidad sobre sus acciones por parte de los usuarios de la red institucional, se obliga a la suspensión de su cuenta de usuario de los servicios.

3.2.3. Procedimiento Seguridad Física y Ambiental

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

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

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

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

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

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

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

8. Toda visita a las oficinas de tratamiento de datos críticos e información (unidad de informática, sala de servidores entre otros) deberá ser registrada mediante el formulario de accesos a las salas de procesamiento crítico, para posteriores análisis del mismo.

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

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

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

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

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

3.2.4. Procedimiento Desarrollo y Mantenimiento de Sistemas

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

2. Las configuraciones y puesta en marcha de servicios, son normadas por el departamento de informática, y el comité de seguridad.

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

4. La unidad de informática, o personal de la misma dedicado o asignado en el área de programación o planificación y desarrollo de sistemas, efectuará todo el proceso propio de la planificación, desarrollo, adquisición, comparación y adaptación del software necesario para la Entidad Financiera.

5. La aceptación del software se hará efectiva por la Gerencia de la institución, previo análisis y pruebas efectuadas por el personal involucrado en el tema.

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

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

8. El software diseñado localmente o llámese de otra manera desarrolladas por programadores internos, deberán ser analizados y aprobados, por el gestor de seguridad, antes de su implementación.

9. Es tarea de programadores el realizar pruebas de validación de entradas, en cuanto a:
   Valores fuera de rango.
   Caracteres inválidos, en los campos de datos.
   Datos incompletos.
   Datos con longitud excedente o valor fuera de rango.
   Datos no autorizados o inconsistentes.
   Procedimientos operativos de validación de errores
   Procedimientos operativos para validación de caracteres.

Procedimientos operativos para validación de la integridad de los datos.
Procedimientos operativos para validación e integridad de las salidas.

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

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

3.2.5. Procedimientos para Intercambio de Información

Control de Salida al Internet

Seguridad Informática

1. Realizar controles sobre el tráfico Web desde estaciones de la red.
2. Definir los sitios de navegación que serán restringidos a los usuarios.
3. Emitir reportes periódicos sobre navegación Web.
4. Definir perfiles con permisos de navegación para usuarios de la red.

Plataforma Distribuida (Administrador de servicio de Internet)

5. Implementar los controles solicitados por Seguridad Informática sobre los servidores de navegación Web.

Control de Uso del Correo

Seguridad Informática

6. Realizar controles sobre el tráfico de mensajes electrónicos desde estaciones de la red hacia Internet.
7. Realizar el control de tráfico.
8. Emitir reportes periódicos sobre uso del servicio de correo electrónico.

3.2.6. Procedimiento Manejo Incidentes Seguridad código malicioso

Objetivo

Disponer los lineamientos para el manejo de incidentes relacionados a código malicioso en la red de la Entidad Financiera.

Alcance

Este procedimiento cubre los incidentes generados por la acción de código malicioso dentro de la red de la Entidad Financiera.

Áreas que intervienen

Las áreas de la Entidad Financiera que intervienen en el manejo de incidentes de código malicioso son:

- Seguridad Informática.
- Plataforma Distribuida.
- Soporte en Sitio.
- Help Desk

Roles y Responsabilidades

Las responsabilidades dentro del proceso de manejo incidentes de código malicioso son:

Seguridad Informática

- Ejecutar controles preventivos sobre la infraestructura tecnológica de la Entidad Financiera.
- Mantener actualizada las bases de conocimiento utilizadas para la revisión de código malicioso.
- Mantener actualizados los procedimientos de monitoreo y control, utilizados para mitigar el riesgo de pérdida de confidencialidad, integridad, autenticidad o disponibilidad de la información.
- Analizar e identificar código malicioso que genere incidentes de seguridad.
- Determinar el impacto de código malicioso.
- Decidir las acciones que mitiguen el impacto de la acción de código malicioso.
- Realizar pruebas de concepto de procedimientos para mitigar acción de código malicioso.
- Coordinar con el proveedor la entrega de firmas o definiciones en caso de ser necesario.
- Coordinar con el Help Desk las acciones o comunicaciones que se remiten a los usuarios durante y posterior al incidente.
- Proponer medidas de mitigación o eliminación.
- Realizar informe de incidente.
- Monitorear la erradicación de código malicioso.
- Registrar estadísticas y acciones en base de conocimiento.

Plataforma Distribuida

- Revisar informes de Seguridad Informática sobre controles preventivos e implementar o justificar las novedades reportadas.
- Identificar código malicioso que genere incidentes de seguridad y reportar a Seguridad Informática.
- Implementar controles sobre los servicios de red o aplicaciones que sean sugeridos por Seguridad Informática.
- Monitorear comportamiento de enlaces de comunicación y reportar novedades a Seguridad Informática.
- Ejecutar las acciones que Seguridad Informática establezca como medidas de mitigación sobre los servicios.
- Reportar a fabricante muestras de archivos para estudio de virus.
- Coordinar con el soporte local y entregar al fabricante la información necesaria.
- Obtener firmas de antivirus que mitiguen la acción de código malicioso.
- Ejecutar pruebas de firmas de antivirus y verificar su efectividad en ambiente de producción.
- Distribuir la firma de antivirus en la infraestructura de la Entidad Financiera.
- Monitorear la erradicación del código malicioso.
- Reportar avances de distribución de firma de antivirus.
- Monitorear servicios, aplicaciones, enlaces, equipos afectados.

Soporte en Sitio

- Coordinar y ejecutar las medidas de mitigación propuestas por Seguridad Informática.
- Reportar anomalías en la ejecución de los servicios o funcionamiento de aplicaciones.

Help Desk

- Distribuir comunicados generados por Seguridad Informática durante y posterior al incidente.

- Enrutar los requerimientos generados por causa del código malicioso que genere el incidente.
- Difundir y dar soporte en caso de que Seguridad Informática genere un procedimiento de mitigación o eliminación del código malicioso.

DIFUSION

Métodos de difusión de código malicioso

Ingeniería Social

Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el 'ingeniero social'.

Spam

Correo enviado de forma masiva y que no ha sido solicitado por el receptor. Este es el método más barato y efectivo de difusión de intentos de fraude.

Uso de múltiples vectores de propagación

Código malicioso que utiliza diferentes mecanismos de difusión, correo electrónico, programas de mensajería instantánea como Internet Relay, MSN Messenger, AOL Instant Messenger, Yahoo Messenger, ICQ; uso de vulnerabilidades conocidas, evasión de mecanismos de detección.

Información de contactos

Proveedores:

Se debe incluir:

Código, Nombre, Compañía, Teléfono, Móvil, Email, Organización, Empresa, Dirección, Ciudad, Teléfono, Soporte Contratado, Contactos, Número de contacto.

Mecanismos de reporte

Usuario, Soporte en Sitio

Llamada telefónica o correo electrónico dirigido a Help Desk reportando comportamiento anómalo de aplicaciones en equipo.

Help Desk

Generar un requerimiento para Seguridad Informática con datos del incidente reportado por el Usuario o Soporte en Sitio.

Seguridad Informática o Plataforma Distribuida

- Reportar el incidente, remitiendo un correo electrónico a los contactos técnicos de Soporte Local con copia a Soporte Comercial.

- Confirmar la revisión del correo por vía telefónica a los contactos técnicos de Soporte Local.

- Generar un documento del incidente reportado a fin de dar seguimiento.

Soporte Local

Los servicios contratados por la Entidad Financiera comprenden una asistencia prepagada, que incluye 50 horas de soporte así como llamadas telefónicas de soporte.
Estas 50 horas de servicio serán cubiertas en un esquema de 5x8, es decir 5 días a la semana, 8 horas al día. Se podrá realizar soporte fuera de horario previa coordinación entre el cliente y el proveedor.
El soporte se realizará bajo las siguientes consideraciones:

- El soporte está destinado únicamente para la Entidad Financiera y no se podrán transferir las horas de soporte a ninguna empresa afiliada o independiente del mismo.

- Si la Entidad Financiera solicita una visita por parte de un técnico para revisar un determinado problema este es descontado de las horas contratadas siempre y cuando se haya dado solución al problema.

- El control de consumo de horas de soporte se las realizará a través de las Tarjetas de Asistencia, y debe contar con la firma del técnico y de la persona responsable de la Entidad Financiera.

- Por cada una de las horas consumidas y que se encuentran marcadas en la tarjeta de asistencia existe un reporte asociado al incidente donde se detalla el problema reportado. Este reporte es enviado vía correo electrónico a las personas involucradas.

- Estas horas pueden ser utilizadas para soporte.

- Las consultas planteadas por el cliente no tienen la misma prioridad que un incidente de soporte o problema reportado, los tiempos de respuestas tendrán como mínimo 24 horas.

- Los trabajos fuera de horario laboral deberán ser coordinados con al menos 48 horas de anticipación.

- El soporte después de las 18:00 horas de lunes a viernes equivaldrá a 1.5 horas por cada hora de trabajo, el soporte en fines de semana y feriados equivaldrá a 2 horas por cada hora de trabajo según lo estipulado en el código de trabajo.

- El tiempo máximo de respuesta a una llamada de servicio para que un técnico se comunique con el cliente es de 3 (Tres) horas.

- El tiempo se contabilizará como hora o fracción de hora con un soporte mínimo de 1 hora por visitas efectivas que serán controladas por el cliente.

RECURSOS DISPONIBLES PARA EL ANALISIS

Computador

Para el análisis de software malicioso se utilizará un equipo asignad para la tarea perteneciente a Seguridad Informática.

Diskette Externo

La unidad de diskette externo con conectividad al puerto USB.

Diagramas de principales servicios

Por la naturaleza del negocio estos pueden variar por lo que Seguridad Informática debe realizar la actualización periódica de la información y almacenarla en un repositorio centralizado.

Direccionamiento de la red

Por la naturaleza del negocio estos pueden variar por lo que Seguridad Informática debe realizar la actualización periódica de la información y almacenarla en un repositorio centralizado.

Listado de puertos utilizados por troyanos

La lista de puertos utilizados por troyanos son datos dinámicos, la información debe mantenerse actualizada diariamente.

Recursos de Mitigación

Parches Sistema Operativo

Realizar una revisión del equipo para definir el estado, de existir novedades reportarlas al administrador para su corrección.

Software Antivirus

En caso de requerir la actualización de definiciones o versión se deberá definir el procedimiento por Plataforma Distribuida.

Sistema Operativo

Los procedimientos para instalación del Sistema Operativo en equipos de la red de datos deben ser distribuidos a todo el personal de Soporte en Sitio, al igual que los procedimientos de seguridad para ingreso de estaciones de trabajo, servidores y certificación de servidores.

Herramientas de revisión

Las herramientas que se utilizarán para el análisis del código malicioso son:

- Autoruns
- ProcessExplorer
- ProcessMonitor
- GFIScanner

PREVENCION

REVISION DE VULNERABILIDADES

Seguridad Informática

Realizar de manera periódica la revisión de las vulnerabilidades de Sistema Operativo. La revisión se realizará sobre los siguientes aspectos:

- Parches Sistema Operativo
- Carpetas Compartidas
- Políticas implementadas
- Aplicaciones instaladas
- Puertos abiertos
- Servicios implementados
- CGI Abuse
- Backdoors
- Usuarios definidos
- Usuarios logeados
- Estado de usuarios
- Registros SNMP

Reportar al Administrador los equipos desactualizados
Dar seguimiento a la corrección de vulnerabilidades reportadas

Plataforma Distribuida (Administrador de Servicio)

- Revisar vulnerabilidades reportadas por Seguridad Informática.
- Corregir o justificar vulnerabilidades reportadas.
- Reportar corrección a Seguridad Informática.

CONTROL DE SOFTWARE DE ANTIVIRUS

La Entidad Financiera determinará el software antivirus que utilizará.

Distribución de versiones

Seguridad Informática

- Realizar un control sobre la distribución de la versión de forma mensual.
- Reportar al Administrador los equipos desactualizados.
- Dar seguimiento a la actualización de la versión en equipos reportados.
- Generar indicadores sobre estado de versiones de antivirus.

Plataforma Distribuida (Administrador de Antivirus)

- Revisar equipos reportados por Seguridad Informática.
- Coordinar con Soporte en Sitio la actualización de versión.
- Reportar actualización a Seguridad Informática

Soporte en Sitio

- Actualizar la versión de Antivirus en equipos reportados de acuerdo a procedimiento entregado por Plataforma distribuida.

- Reportar actualización a Administrador de Antivirus.

Distribución de definiciones

Seguridad Informática

Antivirus

- Realizar un control sobre la distribución de definición de forma mensual o por demanda en caso de incidentes de virus.
- Reportar al Administrador los equipos con definiciones desactualizados.
- Dar seguimiento a la actualización de la definición en equipos reportados.
- Generar indicadores sobre estado de definiciones de antivirus.

IPS:

- Monitorear los eventos en la consola de IPS.
- Mantener actualizada la base de conocimientos en la cual se registran los eventos que han sido analizados y que están bloqueados por los dispositivos IPS.
- Mantener actualizada la base de datos de equipos monitoreados a través de alertas de IPS.
- Analizar las firmas que se registran en las actualizaciones de los IPS.

Plataforma Distribuida (Administrador de Antivirus)

- Revisar equipos reportados por Seguridad Informática.
- Coordinar con Soporte en Sitio la actualización de definición.

- Reportar actualización a Seguridad Informática.

Soporte en Sitio

- Actualizar la definición de Antivirus en equipos reportados.
- Reportar actualización a Administrador de Antivirus.

Control de configuración antivirus

Seguridad Informática

- Generar las políticas de configuración de plataforma antivirus.
- Realizar un control sobre la configuración de las políticas de antivirus de forma semestral o por demanda en caso de incidentes de virus.
- Reportar al Administrador los equipos con definiciones desactualizados.
- Dar seguimiento a la actualización de la definición en equipos reportados.
- Generar indicadores sobre estado de definiciones de antivirus.
- Suscribirse a los boletines de productos para conocer el estado de parches y actualizaciones.

Plataforma Distribuida (Administrador de Antivirus)

- Revisar novedades en reporte sobre control de configuración de antivirus.
- Corregir y modificar la configuración del Software antivirus.
- Reportar actualización a Seguridad Informática.
- Aplicar parches de productos.

Control de listas negras

Seguridad Informática

- Realizar la búsqueda de los dominios.
- Realizar controles del tráfico de salida de correo electrónico hacia Internet a fin de detectar envíos masivos de correo.
- Coordinar acciones con Plataforma Distribuida y Soporte en sitio para revisión de equipos con comportamiento anómalo en envíos masivos de correo electrónico.

Plataforma Distribuida (Administrador de Antivirus)

- Realizar un análisis de las configuraciones y revisiones del software antivirus en estaciones reportadas como alto tráfico.
- Coordinar con Seguridad Informática las acciones para corrección de comportamiento anómalo en envíos masivos de correo electrónico.

Soporte en Sitio

- Realizar un análisis de las configuraciones de sistemas operativos y ejecutar las tareas de mantenimiento recomendadas en estaciones reportadas como alto tráfico.

- Coordinar con Seguridad Informática las acciones para corrección de comportamiento anómalo en envíos masivos de correo electrónico.

POLITICAS Y CAPACITACION

Seguridad Informática

- Apoyar al cumplimiento de las políticas de uso de Correo Electrónico y Navegación Web, mediante controles periódicos.

- Remitir reportes de funcionarios TOP en el uso de los servicios a Recursos Humanos.

- Notificar a funcionarios TOP en cantidad de mensajes y cantidad de tráfico en MB con copia a su línea de supervisión para la justificación respectiva.

- Mantener una base de datos de cuentas justificadas.

- Apoyar a la capacitación de los funcionarios en el tema de Seguridad Informática.
- Revisar periódicamente las políticas de uso de servicios y notificar a Riesgo Operativo, actualizaciones modificaciones sugeridas.

DETECCION Y ANALISIS

IDENTIFICAR CODIGO MALICIOSO

Help Desk

- Remitir reporte de usuario o Soporte en Sitio sobre incidente de virus a Seguridad Informática.

Seguridad Informática

- Analizar notificación de Help Desk, buscar patrones en código malicioso como: dirección URL, remitente o mensaje en sistemas de correo electrónico, navegación Web o Messenger.

- Buscar información en base de conocimiento.

- Identificar a equipo, usuario, rol dentro de la red de la estación reportada.

- Ejecutar un escaneo en equipo reportado para análisis de vulnerabilidad de acuerdo a procedimiento de escaneo de equipos.

- Solicitar a Plataforma Distribuida y Soporte en Sitio análisis de estación de usuario, en relación al estado de definiciones y versión de Antivirus, configuraciones de sistema operativo, parches.

Soporte en sitio

- Ejecutar las herramientas de revisión y remitir resultados a Seguridad Informática.
- De ser necesario retirar de la red el equipo que reporte comportamiento anómalo y entregar a Seguridad Informática para su análisis.

Plataforma Distribuida

- Realizar una revisión de configuración de software antivirus, tareas de búsqueda y corrección de software malicioso y remitir información de comportamiento anómalo proveedor de solución de Antivirus.

ANALISIS

Seguridad Informática

- Analizar comportamiento del tráfico.

Logs Antivirus

Seguridad Informática – Plataforma Distribuida

- Determinar estado en cuanto a versión y definición de antivirus en la red de datos.
- Analizar logs de acciones de antivirus en estación reportada.
- Investigar firma de antivirus que mitigue acción de código malicioso.
- Reportar información comportamiento anómalo a Proveedor.
- Reportar en caso de ser necesario muestra de virus para análisis de fabricante.

Logs Correo Electrónico

Seguridad Informática

- Buscar patrón de referencia en logs de correo electrónico.
- Coordinar con Plataforma Distribuida revisiones en dispositivos de protección de código malicioso en correo electrónico.

Plataforma Distribuida

- Analizar acción tomada por software antispam de Correo Electrónico.
- Investigar direcciones fuente de mensajes con patrón de código malicioso en Internet.
- Coordinar con Seguridad Informática acciones de revisión de código malicioso.

Información Pública

Seguridad Informática

- Investigar en Internet sobre patrón encontrado, a fin de identificar firma de antivirus de cualquier fabricante creada para mitigar el riesgo de código malicioso.
- Determinar las fuentes de propagación del código malicioso.
- Investigar métodos de propagación de código malicioso.

Plataforma Distribuida

- Colaborar con Seguridad Informática para determinar las fuentes de propagación del código malicioso.

Monitoreo de enlaces

Plataforma Distribuida

- Monitorear los enlaces de comunicación e identificar tráfico anómalo en la red de datos.
- Notificar a Seguridad Informática en caso de encontrar anomalías en el análisis del tráfico de la red de datos.

Almacenamiento de evidencias

Seguridad Informática

- Abrir una carpeta con la fecha del incidente (año/mes/día) dentro del
- Almacenar toda la documentación y reportes notificados por las áreas involucradas.
- En caso de muestras de archivo infectados, estos deberán ser empaquetados antes de su almacenamiento.

PRIORIZACION

Identificar recursos afectados

Seguridad Informática

- Determinar el número de incidentes en IPS que mantienen el patrón de código malicioso.
- Determinar en segmentos de red afectados. Utilizar análisis de tráfico en IPS.
- Determinar equipos sin firma de antivirus publicada para mitigar código malicioso.
- Determinar número de mensajes y destinatarios en caso de que el código malicioso sea transmitido por correo electrónico.
- Determinar equipos y usuarios que acceden a sitio Web en caso de que el código malicioso sea transmitido por navegación Web.

Plataforma Distribuida

- Colaborar con Seguridad Informática en el cálculo de equipos sin firma de antivirus publicada para mitigar código malicioso, número de mensajes y destinatarios en caso de que el código malicioso sea transmitido por correo electrónico, y usuarios que acceden a sitio Web en caso de que el código malicioso sea transmitido por navegación Web.

Help Desk

- Llevar estadística de reportes de incidentes de código malicioso y reportar a Seguridad Informática.

Medir Impacto

Seguridad Informática

- Determinar las fuentes de propagación del código malicioso. Investigar en Internet.
- Determinar segmentos vulnerables a contagio de código malicioso. Utilizar reportes de estado de versiones, Correo Electrónico y Navegación Web.

Reporte incidente

Seguridad Informática

- Notificar incidente y propuestas de medidas de mitigación a Plataforma Distribuida, Soporte en Sitio, Líneas de supervisión y Líderes de área.
- Enviar notificación de acciones tomadas para mitigar incidente a Help Desk para su revisión y distribución.
- Enviar recomendaciones de Seguridad Informática para usuarios finales a Help Desk.
- Revisar, personalizar y difundir comunicaciones solicitadas por Seguridad Informática.

ERRADICACION

CONTROL DE PROPAGACION

Seguridad Informática

- Solicitar la suspensión de servicios de red, retiro de equipos de la red, bloqueo de direcciones de navegación Web, bloqueo de remitentes de correo electrónico como resultado del análisis realizado.
- Recolectar muestra de código malicioso en equipos reportados como infectados.

Plataforma Distribuida

- Ejecutar procedimientos para suspensión de servicios, retiro de equipos de la red, bloqueo de direcciones de navegación Web, bloqueo de remitentes de correo electrónico solicitados por Seguridad Informática como medidas de control de propagación de código malicioso.
- Recolectar muestra de código malicioso en equipos reportados como infectados.
- Remitir muestra de código malicioso a Proveedor.
- Obtención de definición con firma para corrección y prevención de software malicioso.
- Actualización de definición forzada en equipos reportados como infectados.
- Configuración y monitoreo de actualización de definición automática en estaciones de la red de datos.
- Implementar las reglas de bloqueo en servicios de red propuestas por Seguridad Informática – Correo Electrónico, Navegación Web.

Soporte en Sitio

- Desconectar de la red de datos equipos con comportamiento anómalo por código malicioso, en caso de que Seguridad Informática lo determine.
- Reemplazar equipo a funcionario y entregar equipo a Seguridad Informática para revisión de incidente

ELIMINACION

Seguridad Informática

- Ejecutar pruebas de concepto sobre virus reportado en equipos no infectados con firma antivirus activa.
- Verificar distribución de firma de antivirus actualizada a equipos infectados.
- Solicitar la reactivación de servicios de red suspendidos por incidente.
- Monitoreo de actividad en IPS, Correo Electrónico, Navegación Web.

Plataforma Distribuida

- Monitoreo de distribución de firma de antivirus en equipos de la red de la Entidad Financiera.
- Monitoreo de enlaces de comunicaciones, correo electrónico, navegación Web.
- Revisión de acciones tomadas por antivirus en equipos reportados como infectados.
- Revisión del comportamiento de equipos infectados por código malicioso.
- Documentación de acciones tomadas y reportes a Seguridad Informática.

Soporte en Sitio

- Conexión a la red de datos equipos con comportamiento anómalo por código malicioso, en caso de que el comportamiento se corrija con la aplicación de la firma antivirus.
- Monitoreo de comportamiento de equipo reconectado en la red de datos.

DOCUMENTACION

Seguridad Informática

- Documentar el incidente en un Informe Gerencial de código malicioso que contenga las siguientes secciones:

  - Antecedentes
  - Sistemas Afectados
  - Diagnóstico
  - Impacto
  - Solución

- Situación Actual
- Conclusiones
- Recomendaciones

- Almacenar informe en directorios previamente establecidos
- Remitir informe al Responsable de Seguridad Informática.

Plataforma Distribuida - Soporte en Sitio

- Remitir la información que Seguridad Informática considere necesaria para documentar el incidente de código malicioso.

RECUPERACION

VERIFICAR FUNCIONALIDAD

Seguridad Informática

- Monitorear tráfico de red en sistema IPS.
- Monitorear logs de sistema antivirus
- Monitorear logs de tráfico de correo electrónico.

Plataforma Distribuida

- Monitoreo de distribución de firma de antivirus en equipos de la red de la Entidad Financiera.
- Monitoreo de correo electrónico, navegación en Web.
- Monitoreo de servicios afectados.

Soporte en Sitio

- Monitoreo de funcionamiento de estaciones reportadas.

LECCIONES APRENDIDAS

Seguridad Informática

- Registrar incidente en base de conocimientos.
- Verificar procedimientos en manejo de incidentes y sugerir modificaciones en caso de ser necesarias.
- Crear procedimientos de monitoreo adicionales en caso de ser requeridos.

Plataforma Distribuida - Soporte en Sitio

- Revisar documentación de Incidente de Código Malicioso, y sugerir a Seguridad Informática cambios o ampliaciones en procedimientos.

ESTADISTICAS INCIDENTES

Seguridad Informática

- Obtener datos estadísticos del incidente y documentarlos.
- Equipos afectados
- Tiempo tomado en resolver incidente
- Evaluación Incidente
- Repositorio de Evidencias

Plataforma Distribuida - Soporte en Sitio – Help Desk

- Remitir la información que Seguridad Informática considere necesaria para la obtención de estadísticas de incidente de código malicioso.

3.3 Procedimiento de Concienciación a los usuarios

El mejor plan de seguridad[3] se vería seriamente hipotecado sin una colaboración activa de las personas involucradas en el sistema de información, especialmente si la actitud es negativa, contraria o de “luchar contra las medidas de seguridad”. Es por ello que se requiere la creación de una “cultura de seguridad” que, emanando de la alta dirección, conciencie a todos los involucrados de su necesidad y pertinencia.

Son dos los pilares fundamentales para la creación de esta cultura:

- Una política de seguridad corporativa que se entienda (escrita para los que no son expertos en la materia), que se difunda y que se mantenga al día.

- Una formación continua a todos los niveles, recordando las cautelas rutinarias y las actividades especializadas, según la responsabilidad adscrita a cada puesto de trabajo.

A fin de que estas actividades cuajen en la organización, es imprescindible que la seguridad sea:

- Mínimamente intrusiva: que no dificulte innecesariamente la actividad diaria ni hipoteque alcanzar los objetivos de productividad propuestos,

- Sea **“natural”**: que no de pie a errores gratuitos, que facilite el cumplimiento de las buenas prácticas propuestas y **practicada por la Dirección:** que brinde ejemplo en la actividad diaria y reaccione con presteza a los cambios e incidencias.

---

[3] El Plan de Seguridad está constituido por el detalle de la definición de los requerimientos mínimos y la descripción de los controles, mecanismos, procedimientos ha implementarse para que un sistema mantenga un nivel básico de seguridad.

Resultado Dominios ISO vs. Cobertura en el Proyecto de Titulación

Número	Dominio	Cobertura	Referencia
1	**Dominio1: Polìtica de Seguridad** - **Documentación de la política de seguridad de la información.**	**Mediana**	**Secciones:** 1.1.2 2.3.1; 2.3.12 3.1.10; 3.3
2	**Dominio 2: Organización de la Seguridad** - **Infraestructura de seguridad de la información.** - **Seguridad frente al acceso por parte de terceros.** - **Tercerización.**	**Mediana**	**Secciones:** 1.1.3.3; 1.1.3.2; 1.5.1 2.3.3 3.1.6; 3.2.2
3	**Dominio 3: Clasificación de la Información** - **Pautas de clasificación.** - **Rotulado y manejo de la información**	**Mediana**	**Secciones:** 1.1.1.1; 1.1.1.2 3.1.1; 3.1.2
4	**Dominio 4: Seguridad en los Recursos Humanos** - **Seguridad en la definición de puestos de trabajo y la asignación de recursos.** - **Capacitación del usuario.** - **Respuesta a incidentes y anomalías en materia de seguridad.**	**Mediana**	**Secciones** 1.1.2; 1.5.1;1.7 2.1.3;2.3.8; 2.3.16 3.1.8; 3.1.10 4.1

5	**Dominio 5: Seguridad Física y Ambiental** - **Áreas seguras.** - **Seguridad del equipamiento.** - **Controles Generales.**	**Mediana**	**Secciones:** 1.1.3.4 3.1.8; 3.2.3
6	**Dominio 6:Administración de las Comunicaciones** - **Protección contra software malicioso.** - **Mantenimiento.** - **Administración y seguridad de los medios de almacenamiento.**	**Parcial**	**Secciones:** 1.1.3.6 3.1.9;3.1.2;3.1.10;3.1.2; 3.2.3; 3.2.6;3.1.19
7	**Dominio 7: Control de Accesos** - **Requerimientos de negocio para el control de accesos.** - **Administración de accesos de usuarios** - **Responsabilidades del usuario.** - **Control de acceso a la red.** - **Control de acceso al sistema operativo** - **Control de acceso a las aplicaciones.** - **Monitoreo del acceso y uso de los sistemas.** - **Computación móvil y trabajo remoto.**	**Mediana**	**Secciones:** 3.1.11;3.1.12;3.1.13;3.1.14

8	**Dominio 8: Adquisición, desarrollo y mantenimiento de Sistemas de Información** - **Requerimientos de seguridad de los sistemas.** - **Seguridad en los sistemas de aplicación.** - **Controles criptográficos.** - **Seguridad de los archivos del sistema.** - **Seguridad de los procesos de desarrollo y soporte.**	**Mediana**	Secciones: 3.1.16; 3.1.17;3.1.10
9	**Dominio 9: Administración de Incidentes.**	**Mediana**	Secciones:2.3.8;2.3.9;3.1.11 3.2.6;3.1.15
10	**Dominio 10: Administración de la Continuidad de los Negocios.** - **Aspectos de la administración de la continuidad de los negocios.** - **Proceso de administración de la continuidad de los negocios.** - **Continuidad del negocio y análisis del impacto.** - **Elaboración e implementación de planes de continuidad de los negocios.**	**Mediana**	**Secciones:** 1.1.3.15 3.1.17; 3.1.18

11	**Dominio 11: Cumplimiento de Leyes y Regulaciones.** - **Cumplimiento de requisitos legales.** - **Consideraciones de auditoria de sistemas**	**Parcial**	Secciones: 2.1; 2.3.2 3.1.1;

Tabla 3.3: Resultados Dominios ISO vs. Cobertura en el Proyecto de Titulación

4. CAPITULO 4.CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- El comportamiento humano puede representar el mayor riesgo relacionado con la información para cualquier organización. A fin de administrar la seguridad en una organización, es importante que el gerente de seguridad de información tenga en cuenta la cultura y el comportamiento del personal.

- Mayormente los controles de seguridad, se siguen implementando de manera reactiva.

- Las vulnerabilidades tienen otras dimensiones además de la tecnológica, por ejemplo: una organización que no tenga un programa formal de capacitación y concientización sobre la seguridad. La vulnerabilidad en este caso se derivaría de la falta de conocimiento por parte del usuario respecto de las políticas, normas y lineamientos de seguridad.

- Puesto que los recursos de información cambian con el paso del tiempo, es importante saber que tanto el límite de seguridad, como los recursos se deben adaptar a las amenazas cambiantes y nuevas vulnerabilidades. Es importante que todos los que tengan un interés en la organización conozcan los cambios y que se alcance un consenso apropiado.

- Las métricas son importantes pero de poco uso si no se resuelven las tendencias adversas a tiempo. El gerente de seguridad de información debe contar con un proceso mediante el cual se revisen las métricas en forma regular y se informe cualquier actividad inusual.

- ISO/IEC 27001 es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo. La norma es particularmente interesante si la protección de la información es crítica, como en finanzas, sanidad sector público y tecnología de la información (TI).

- ISO/IEC 27001 también es muy eficaz para organizaciones que gestionan la información por encargo de otros, por ejemplo, empresas de subcontratación de TI. Puede utilizarse para garantizar a los clientes que su información está protegida

- Cuando se habla de informática, la seguridad es uno de los pilares fundamentales que le da sustento, pues de nada sirve el mejor sistema, si este no está Disponible, No es Confiable, Su información es errónea o imprecisa, compromete a otras empresas o permite borrar hechos o transacciones, etc.

4.2. Recomendaciones:

- Es imperativo realizar un análisis integral de riesgo físicos (eléctricos, fuego, inundación) para elaborar un plan de mejoras en la seguridad física del edificio de una Entidad Financiera, en donde entre otros se contemple: detectores de humo, detectores de inundación, detectores de calor, cámaras de video, y el respectivo monitoreo desde un centro de atención 24 por 7, ya que pueden darse impactos de eventos extremadamente altos.

- Aplicar estándares de seguridad vigentes para el sistema operativo y recomendaciones de seguridad para servidores Web.

- Activar políticas del directorio activo ya que actualmente el sistema de autenticación es vulnerable a ataques de fuerza bruta**.**

- Generar estadísticas (indicadores de gestión) para la Alta Gerencia, los mismos que brindarán una visión real de la situación de la Organización, tales como:
  a. Correo Electrónico / Mensajes Recibidos (Total de mensajes recibidos cada mes).
  b. Correo Electrónico / Mensajes Enviados / Cuentas Top.
  c. Correo Electrónico / Cantidad de Mensajes enviados por dominio.
  d. Correo Electrónico / Cantidad de Megabytes enviados por usuario.
  e. Antivirus / Número de equipos / Versión de Antivirus.
  f. Credenciales de Red /Valores Consolidados Mensual Bloqueo – Reseteos.
  g. Evaluaciones para certificaciones de servidores.
  h. Aplicaciones / Evaluación de Aplicaciones con Riesgo Alto y no Alto.
  i. Aplicaciones / Certificación de Aplicaciones.
  j. Aplicaciones / Acumulado de Vulnerabilidades.
  k. Tráfico por categoría de sitio WEB.
  l. Tráfico porcentual por hora del día.
  m. Monitoreo de actividad de usuarios / Varias plataformas.

- Actualizar de forma constante, transparente y de acuerdo a las necesidades existentes al momento, el manual de normas y políticas de seguridad.

- Asignar presupuesto para la gestión de seguridad de la información.

- Asignar personal al área de seguridad de la información.

- Concienciar los usuarios, en temas de seguridad, hacerles sentirse responsables y parte de la institución.

- Dar seguimiento a estándares internacionales sobre temas de seguridad de la información.

- Contratar los servicios de terceros (Hacking ético), para ejecutar pruebas completas de intrusión a los sistemas de la red institucional.

- Capacitar a los empleados de la institución, en temas de seguridad, adoptando un estricto control de las técnicas más comunes de persuasión de personal (Ingeniería Social).

- El Gerente de Seguridad de Información debe desarrollar capacidades de administración de logística ya sea a través de capacitación, auto estudio o tutela.

GLOSARIO

Área Crítica

Es el área física donde se encuentra instalado el equipo de cómputo y telecomunicaciones que requiere de cuidados especiales y son indispensables para el funcionamiento continuo de los sistemas de comunicación.

Auditoría

Llevar a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.

Bases de Datos

Es un conjunto de datos interrelacionados y un conjunto de programas para accesarlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápida.

Cracker

Se refiere a una persona que utiliza sus conocimientos de hacking con fines ofensivos o maliciosos.

Hacker

Se refiere a una persona que disfruta aprendiendo los detalles de los sistemas con el fin de extender la capacidad y/o alcance para lo cual fueron creados.

Holismo

En teoría de sistemas, el **holismo** es la idea de que las propiedades de un sistema, no pueden determinarse con la simple suma de sus partes (o analizando sus partes de forma individual); sino que las partes o componentes deben verse como un todo.

El holismo se resume en la frase: "El todo es más importante que la suma de sus partes", de Aristóteles.

Ingeniería Social

Es el aprovechamiento de los conocimientos de las personas para convencerlas de que ejecuten acciones o actos que puedan revelar información sensible.

Integridad

Cuán precisa, completa y válida es la información.

Métricas de Seguridad

Un forma de medición que se utiliza para determinar cualquier aspecto de la operación de .cualquier actividad relacionada con la seguridad.

Mitigación de riesgo

La administración de un riesgo mediante el uso de controles y contramedidas.

Políticas

Declaraciones de alto nivel sobre el propósito y la dirección de la gerencia.

Procedimientos

Una descripción detallada de los pasos necesarios para realizar operaciones específicas conforme a las normas aplicables.

TI

Tecnología de Información.

Vulnerabilidades

Una deficiencia en el diseño, la implementación, la operación o los controles internos en un proceso que podría explotarse para violar la seguridad del sistema.

WWW (World Wide Web)

Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de Internet en una forma fácilmente accesible. Sistema avanzado para navegar a través de Internet.

Anexos

ENTIDAD FINANCIERA CONFIDENCIAL
COMPROMISO DE FIDELIDAD (Empresa)

Yo, _____, a nombre y en representación de _____, en mi calidad de _____, libre y voluntariamente declaro lo siguiente:

Hemos recibido de _____, la debida autorización para acceder mediante _____ a determinada información CONFIDENCIAL con el objeto de_____ _____.

Con este antecedente, en la calidad en la que comparezco, me obligo a nombre propio y de las personas que trabajan para mi representada, aguardar absoluta reserva de la información confidencial a la que tendremos acceso en el futuro como consecuencia de la autorización recibida; a no divulgar esta información en todo o en parte, ni permitir que persona alguna pueda utilizarla con cualquier fin extraño de aquel por el que nos fue entregada.

Para el caso de incumplimiento del presente compromiso de fidelidad, responderemos por daños y perjuicios que se produzcan.

Para el caso de controversia renuncio domicilio y me someto a los jueces competentes de la ciudad de _____.

Acepto y me ratifico en el compromiso adquirido y para constancia firmo en la ciudad de _____, a los _____, días del mes de _____, de _____.

_____
Firma
Nombre de la empresa:
Nombre del Representante Legal que comparece:
R.U.C.:

Anexo 1: Compromiso Fidelidad Empresa

CONFIDENCIAL

COMPROMISO DE FIDELIDAD (Usuario)

Yo, _____ , en mi calidad de funcionario de la empresa _____libre y voluntariamente declaro lo siguiente:

He recibido autorización para acceder a determinada información CONFIDENCIAL perteneciente a ---------- con el exclusivo objeto de cumplir con las tareas que se me han asignado.

Con este antecedente, me obligo a guardar absoluta reserva de la Información Confidencial a la que tengo y tendré acceso en el futuro; a no divulgar esta información en todo o en parte, ni permitir que persona alguna pueda utilizarla con cualquier fin extraño de aquel por el que me fue entregada.

Para el caso de incumplimiento del presente compromiso de fidelidad, responderé por daños y perjuicios que se produzcan.

Para el caso de controversia renuncio domicilio y me someto a los jueces competentes de la ciudad de QUITO_____.

Acepto y me ratifico en el compromiso adquirido y para constancia firmo en la ciudad de XXXX, a los XX , días del mes de XXXXXXXXXXe del XXXX.

_____

Firma

Cargo:
Nombre:
C.I.:

Anexo 2: Compromiso Fidelidad Usuario

Bibliografía

1. Manual de Preparación al Examen CISM 2007. Impreso en los Estados Unidos de Norteamérica. Alejandro Vasquez Nava. Francisco Salvador Garcia Dayo.
2. Root Secure. Security Makers. Ethical Hacking Teoría y Práctica. www.root-secure.com
3. Texto traducido y adaptado de “The Security Policy Life Circle: Functions and Responsibilities” de Patrick D. Howard, Information Security Management Hadnbook, Edited by Tipton & Krause. CRC Press LLC, 2008.
4. Cano, Heimy J.Pautas y Recomendaciones para Elaborar Políticas de Seguridad Informática (PSI). Universidad de los Andes, Colombia.2007.
5. Organization for Economic Cooperation and Development (OEDC) Guidelines for Security of Information Systems. 2007.
6. Swanson, et al. (2008) National Institute of Standard and Technology (NIST).
7. General Principles for Information Systems Security Policies.
8. ISO/IEC 17799:2005, “Information technology – Security techniques – Code of practice for
9. information security management”, Junio 2005.
10. Alberts and A. Dorofee, “Managing information Security Risks. The OCTAVE Approach”,Addison Wesley, 2003.
11. UNE-ISO/IEC 17799:2002, “Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información”, 2002.
12. United States General Accounting Office, Accounting and Information Management Division,
13. Information Security Risk Assessment -- GAO Practices of Leading Organizations. Ministerio de Administraciones Públicas, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997.

14. Magerit versión 2 Glosario “Risk Management: Multiservice Tactics, Techniques, and Procedures for Risk Management”,Air Land Sea Application Center, FM 3-100.12, MCRP 5-12.1C, NTTP 5-03.5,AFTTP(I) 3-2.30. February 2001.
15. Air Force Pamphlet 90-902, “Operational Risk Management (ORM) Guidelines and Tools”,December 2000.
16. KPMG Peat Marwick LLP, “Vulnerability Assessment Framework 1.1“, October 1998.
17. Magerit, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”,MAP, versión 1.0, 1997
18. GMITS, ISO/IEC TR 13335-2:1997, “Information technology - Security techniques Guidelines for the management of IT security - Part 2: Managing and planning IT security”.
19. Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades”, MAP, 2004.C.

Direcciones Electrónicas

- http://sco-world.de/category/viren-wurmer-trojaner/. 2007.
- http://www-secure.symantec.com/enterprise/support/news_bulletins/ teschsupp_bulletin_form.js.2007.
- http://www.symantec.com/enterprise/support/all_products.jsp. 2008
- http://www.rediris.es/mail/abuso/ln.es.html.2008
- Red Temática Iberoamericana de Criptografía y Seguridad de la Información http://www.criptored.upm.es/
- Seguridad y Protección de la Información (José Luis Morant, Arturo Ribagorda y Justo Sancho; Primera reimpresión Agosto 2006, Editorial Centro de Estudios Ramón Areces). Libro de texto de varias Universidades de Madrid. Muy buena introducción a la Seguridad, cubriendo Criptografía, Políticas de Seguridad y Seguridad en Bases de Datos y Redes.http://www.cerasa.es/cgi-bin/inflibro.exe?
- http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf
- http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf
- http://www.iso27000.es/iso27000.html

- http://blog.segu-info.com.ar/2007/09/diferencias-entre-iso-27001-e-iso-27002.html.
- http://www.microsoft.com/spain/empresas/legal/informacion_confidencial.mspx María González Moreno de Manaca Consulting, S.L.2009
- Defensa contra hackers. Protección de información privada (Richard Mansfield. 2000 Anaya Multimedia, Serie Guía Práctica para Usuarios) Sobre cómo instalar ZoneAlarm y un poco de criptografía básica para Visual Basic.