SEGURIDAD EN REDES Y SISTEMAS INFORMÁTICOS

Ana González (Kao)

UNIDAD 3. POLÍTICAS DE SEGURIDAD.

BY NC SA

ÍNDICE UNIDAD 3

1. TIPOS DE POLÍTICAS, CÓMO DEFINIR UNA POLÍTICA APROPIADA, PLANIFICACIÓN DE LA SEGURIDAD.
1.1 INTRODUCCIÓN
2. ¿QUÉ SON LAS POLÍTICAS DE SEGURIDAD?
3. ¿CÓMO DEBEN DE SER LAS POLÍTICAS?
4. PRINCIPIOS FUNDAMENTALES
5. ¿CÓMO DEBEN ELABORARSE LAS POLÍTICAS?
6. EJEMPLO DE POLÍTICA

BY NC SA

1. TIPOS DE POLÍTICAS, CÓMO DEFINIR UNA POLÍTICA APROPIADA, PLANIFICACIÓN DE LA SEGURIDAD.

1. Introducción

La falta de políticas y procedimientos en seguridad es uno de los problemas más graves que confrontan las empresas hoy día en lo que se refiere a la protección de sus activos de información frente a peligros externos e internos.

¿Por qué son importantes las políticas?

Porque aseguran la elección, implantación y aplicación correcta de las medidas de seguridad necesarias para esa organización específica.

Muchas empresas en su desconocimiento de que la seguridad no es un producto si no un proceso, compran productos de seguridad pensando que son la panacea de resolución de todos sus problemas, por supuesto esto no es así lo cual conlleva la consecuente desilusión al respecto, sin hablar de la supérfula inversión realizada.

En un número grande de casos, esta situación puede atribuirse al hecho que no se ha creado una infraestructura organizativa adecuada para la seguridad informática.

Un estudio y creación de unas buenas políticas acordes a la estructura de la organización ayuda a elegir los productos de seguridad adecuados aunque estos hayan de ser externalizados ya que la mayoría de las organizaciones no tiene los recursos para diseñar e implantar medidas de control desde cero.

Las políticas pueden proporcionar la comprensión y la guía adicional que el personal necesita para actuar como desearía la gerencia en lo que a seguridad se refiere. De manera que tales políticas pueden ser una manera de garantizar de que se está apropiadamente seleccionando, desarrollando e implantando los sistemas de seguridad.

Por que demuestran el apoyo de la Presidencia y de la Junta Directiva.
La mayoría de las personas no es consciente de la gravedad de los riesgos relativos a la

BY NC SA

seguridad y por eso no se toma el tiempo para analizar estos riesgos a fondo. Además, como no tiene la experiencia suficiente, no es capaz de evaluar la necesidad de ciertas medidas de seguridad.

Las políticas son una manera clara y definitiva para que la alta gerencia pueda mostrar que:

- La seguridad de los activos de información es importante
- El personal debe prestar la atención debida a la seguridad.

2. ¿Que son las políticas de Seguridad Informática?

Las políticas son un documento redactado y pensado por profesionales de la seguridad donde se indican una serie de instrucciones documentadas, que definen la forma en que se llevan a cabo determinados procesos dentro de una organización, también describen cómo se debe tratar un determinado problema o situación.

Este documento está dirigido principalmente al personal interno de la organización, aunque hay casos en que también personas externas quedan sujetas al alcance de las políticas.

Por simples que parezcan, las políticas de seguridad pueden evitar desastres mayores

Entrando al tema de seguridad informática, una política de seguridad es un conjunto de reglas y prácticas que regulan la manera en que se deben dirigir, proteger y distribuir los

BY NC SA

recursos en una organización para llevar a cabo los objetivos de seguridad informática de la misma.

Las políticas adoptadas han de ser comunicadas a los usuarios ya que como hemos visto anteriormente son una parte crucial de la seguridad, siempre hay que tener en cuenta que la seguridad comienza y termina con personas, y debe:

- Ser holística (cubrir todos los aspectos relacionados con la misma).
- Adecuarse a las necesidades y recursos.
- Ser atemporal. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia, esto no implica que deban ser eternas, ya que están sometidas a control de versiones según va variando la organización, si no que han de poder aplicarse en cualquier momento y circunstancia.
- Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.
- Deben ser redactadas en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos al alcance de cualquier miembro de la organización, claro está sin sacrificar su precisión.
- Deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

Objetivo de una política de seguridad

El objetivo de una política de seguridad informática es la de implantar una serie de leyes, normas, estándares y prácticas que garanticen la seguridad, confidencialidad y disponibilidad de la información, y a su vez puedan ser entendidas y ejecutadas por todos aquellos miembros de la organización a las que van dirigidos.

Misión, visión y objetivos de la organización

La misión, visión y objetivos varían mucho de una organización a otra, esto es normal si se considera que una organización es diferente de otra en sus actividades y en el conjunto de elementos que la conforman (Elementos humanos, recursos materiales, infraestructura).

BY NC SA

De manera rápida se definirán los conceptos de misión, visión y organización.

Misión

Una misma organización puede tener varias misiones, que son las actividades objetivas y concretas que realiza. Las misiones también pretenden cubrir las necesidades de la organización.
La misión es influenciada en momentos concretos por algunos elementos como: la historia de la organización, las preferencias de la gerencia y/o de los propietarios, los factores externos o del entorno, los recursos disponibles, y sus capacidades distintivas

Visión

Es la imagen idealizada de lo que se quiere crear. Tal idea debe estar bien definida, pues todas las actividades de la organización estarán enfocadas a alcanzar esta visión.

Objetivos

Son actividades específicas enfocadas a cumplir metas reales, alcanzables y accesibles. Se puede decir que un objetivo es el resultado que se espera logra al final de cada operación.

Así, se vuelve importante considerar la misión, la visión y el objetivo de ser de la empresa, a fin de realizar un estudio que con base en éstas permita identificar el conjunto de políticas de seguridad informática que garantice la seguridad, confidencialidad y disponibilidad de la información.

3. ¿Cómo deben ser las políticas de seguridad?

Debe:

- ✓ Definir la postura de la dirección y de la gerencia con respecto a la necesidad de proteger la información corporativa.
- ✓ Definir el uso de los recursos de información.
- ✓ Definir la base para la estructura de seguridad de la organización.
- ✓ Ser un documento de apoyo a la gestión de seguridad informática.
- ✓ Tener larga vigencia, manteniéndose sin grandes cambios en el tiempo
- ✓ Ser general, sin comprometerse con tecnologías específicas.
- ✓ Debe abarcar toda la organización
- ✓ Debe ser clara y evitar confusiones

BY NC SA

- ✓ No debe generar nuevos problemas
- ✓ Debe permitir clasificar la información en confidencial, uso interno o pública.
- ✓ Debe identificar claramente funciones específicas de los empleados como: responsables, directivos, administradores o usuarios, que permitan proteger la información.

3.1 Elementos de una política:

- Políticas específicas
- Procedimientos
- Estándares o prácticas
- Estructura organizacional

Políticas Específicas

Definen en detalle aspectos específicos que regulan el uso de los recursos de información y están más afectadas a cambios en el tiempo que la política general.

Procedimiento

Define los pasos para realizar una actividad
Evita que se aplique criterio personal.

Ejemplo:

Procedimiento de Alta de Usuarios:

1.- Cada vez que se contrate a una persona, su jefe directo debe enviar al administrador de acreditaciones o de sistemas, una solicitud formal de creación de cuenta, identificando claramente los sistemas a los cuales tendrá accesos y tipos de privilegios.
2.-El administrador de sistemas debe validar que la solicitud formal recibida indique: fecha de ingreso, perfil del usuario, nombre, privilegios asociados a la cuenta, sección o unidad a la que pertenece.
3.- El administrador de sistemas creará la cuenta del usuario a través del sistema implantado para tal fin y le asignará una clave inicial para que el usuario acceda.

Estándar

En muchos casos depende de la tecnología
Se debe actualizar periódicamente

Ejemplo:
Estándar de Instalación de PC:
Tipo de máquina:

BY NC SA

Para plataforma de Caja debe utilizarse máquinas Lanix
Para otras plataformas debe utilizarse máquinas Compaq o HP.

Registro:
Cada máquina instalada debe ser registrada en la base de datos de la organización identificada por mac y por los números de serie de componente, identificando así mismo a qué unidad o departamento pertenece y llenar formulario de traslado de activo fijo

Condiciones eléctricas:
Todo equipo computacional debe conectarse a la red eléctrica computacional y estar provisto de una regleta sais.

¿Que se debe tener en cuenta?

Objetivo: qué se desea lograr
Alcance: qué es lo que protegerá y qué áreas serán afectadas
Definiciones: aclarar términos utilizados
Responsabilidades: Qué debe y no debe hacer cada persona
Revisión: cómo será monitoreado el cumplimiento
Aplicabilidad: En qué casos será aplicable
Referencias: documentos complementarios
Sanciones e incentivos

Políticas de seguridad y Controles

Los controles son mecanismos que ayudan a cumplir con lo definido en las políticas
Si no se tienen políticas claras, no se sabrá qué controlar.

Orientación de los controles:

PREVENIR que ocurra la amenaza
DETECTAR poder detectar la amenaza en caso de que ocurra
RECUPERAR las condiciones ideales de funcionamiento una vez que se ha producido un evento indeseado.

4. Principios fundamentales de las políticas de seguridad

Son las ideas principales a partir de las cuales son diseñadas las políticas de seguridad.

Los principios fundamentales son: responsabilidad individual, autorización, mínimo privilegio, separación de obligaciones, auditoría y redundancia.

BY NC SA

Responsabilidad individual

Este principio dice que cada elemento humano dentro de la organización es responsable de cada uno de sus actos, aun si tiene o no conciencia de las consecuencias.

Autorización

Son las reglas explícitas acerca de quién y de qué manera puede utilizar los recursos.

Mínimo privilegio

Este principio indica que cada miembro debe estar autorizado a utilizar únicamente los recursos necesarios para llevar a cabo su trabajo. Además de ser una medida de seguridad, también facilita el soporte y mantenimiento de los sistemas.

Separación de obligaciones

Las funciones deben estar divididas entre las diferentes personas relacionadas a la misma actividad o función, con el fin de que ninguna persona cometa un fraude o ataque sin ser detectado. Este principio junto con el de mínimo privilegio reducen la posibilidad de ataques a la seguridad, pues los usuarios sólo pueden hacer uso de los recursos relacionados con sus actividades, además de que facilita el monitoreo y vigilancia de usuarios, permitiendo registrar y examinar sus acciones.

Auditoría

Todas las actividades, sus resultados, gente involucrada en ellos y los recursos requeridos, deben ser monitoreados desde el inicio y hasta después de ser terminado el proceso.

Además es importante considerar que una auditoría informática busca verificar que las actividades que se realizan así como las herramientas instaladas y su configuración son acordes al esquema de seguridad informática realizado y si éste es conveniente a la seguridad requerida por la empresa.

Redundancia

Trata entre otros aspectos sobre las copias de seguridad de la información, las cuales deben ser creadas múltiples veces en lapsos de tiempos frecuentes y almacenados en lugares distintos.

Sin embargo, la redundancia como su nombre lo indica, busca “duplicar” y en este sentido se puede decir que a través de los respaldos se duplica información, y lo mismo se puede realizar en diferentes aspectos, como por ejemplo: en cuanto a energía eléctrica, una planta de luz para garantizar que opere en casos de emergencia, servidores de datos que entren en operación cuando el primario sufra una avería, etcétera, de manera tal que la redundancia se considera en aquellos casos o servicios que se vuelven imprescindibles para la empresa y que no pueden suprimirse pase lo que pase.

BY NC SA

Múltiples respaldos de la misma información es un ejemplo de cómo la redundancia es benéfica

Políticas para la confidencialidad

Desde el primer capítulo, se ha mencionado la necesidad de mantener el control sobre quién puede tener acceso a la información (ya sea a los documentos escritos o a los medios electrónicos) pues no siempre queremos que la información esté disponible para todo aquel que quiera obtenerla.
Por ello existen las políticas de confidencialidad, encargadas de establecer la relación entre la clasificación del documento y el cargo (nivel jerárquico dentro de la organización) que una persona requiere para poder acceder a tal información.

Políticas para la integridad

La política de integridad está orientada principalmente a preservar la integridad antes que la confidencialidad, esto se ha dado principalmente porque en muchas de las aplicaciones comerciales del mundo real es más importante mantener la integridad de los datos pues se usan para la aplicación de actividades automatizadas aún cuando en otros ambientes no es así, como en los ámbitos gubernamental o militar.

Modelos de Seguridad: abstracto, concreto, de control de acceso y de flujo de información

BY NC SA

Un modelo de seguridad es la presentación formal de una política de seguridad ejecutada por el sistema. El modelo debe identificar el conjunto de reglas y prácticas que regulan cómo un sistema maneja, protege y distribuye la información.

Los modelos de seguridad pueden ser de dos tipos, abstracto y concreto:

Modelo Abstracto

Se ocupa de las entidades abstractas como sujetos y objetos.

Modelo Concreto

Traduce las entidades abstractas a entidades de un sistema real como procesos y archivos.

También pueden clasificarse como modelos de control de acceso y modelos de flujo de información.

Modelos de control de acceso

Identifican las reglas necesarias para que un sistema lleve a cabo el proceso que asegura que todo acceso a los recursos, sea un acceso autorizado, en otras palabras, se enfoca a la protección, administración y monitoreo de los procedimientos de acceso a la información. Estos modelos refuerzan el principio fundamental de seguridad de autorización, ya que éste protege tanto a la confidencialidad como a la integridad.

Modelos de flujo de información

Una meta de las políticas de seguridad es proteger la información. Los modelos de control de acceso se aproximan a dicha meta indirectamente, sin relacionarse con la información pero sí con objetos (tales como archivos) que contienen información. Estos modelos se enfocan a proteger los objetos con los que se trabajan en el sistema una vez que se han superado los procesos de control de acceso.

Desarrollo de políticas orientadas a servicios de seguridad

Como llevamos repitiendo a lo largo de toda la unidad las políticas de seguridad son un conjunto de normas y procedimientos que tienen por objetivo garantizar la seguridad en cada proceso en los que estén involucrados. Esto es aplicable a todos los procesos llevados a cabo en una organización, incluso los servicios de seguridad (Confidencialidad,

BY NC SA

autenticación, integridad, no repudio, control de acceso, disponibilidad) son diseñados con base en estos documentos.

Publicación y Difusión de las Políticas de Seguridad

Como todos los documentos creados por una organización, se debe decidir correctamente hacia qué grupos van dirigidas las políticas de seguridad, por qué medios se van a dar a conocer, si se desea que otros grupos puedan conocer su contenido.
El objetivo principal de la publicación y difusión es que el grupo objetivo entienda en qué consisten las políticas y se cree conciencia sobre su importancia a través de pláticas y talleres para tal fin.

Procedimientos y Planes de Contingencia

Solo cuando una organización toma conciencia de lo importante que es la seguridad de sus recursos incluyendo sus tecnologías de la información, es cuando empieza a diseñar y establecer medidas de seguridad que tienen por objetivo protegerla de diversas situaciones perjudiciales.
Aunque prevenir éstos desastres es de vital importancia, tampoco se puede descuidar la casi inevitable eventualidad de que sucedan, para ello también se necesita formular y establecer una serie de procedimientos que permitan enfrentar los problemas y posteriormente restaurar las condiciones normales de operación del área afectada.

Procedimientos Preventivos

Contempla todos los procedimientos antes de que se materialice una amenaza, su finalidad es evitar dicha materialización.
Los procedimientos preventivos pueden variar dependiendo del tipo de actividades que realiza la organización, los recursos que tiene disponibles, que es lo que quiere proteger, las instalaciones en que labore y la tecnología que use.

Las actividades que se realizan en este punto son las siguientes:

-Copias de seguridad de las bases de datos y otros tipos de documentos con información indispensable para la organización

BY NC SA

-Instalación de dispositivos de seguridad tales como cerraduras, alarmas, puertas electrónicas, cámaras de seguridad, software de protección para los equipos de cómputo, entre otros.

-Inspeccionar y llevar un registro constante del funcionamiento y estado de los recursos informáticos, la infraestructura y las condiciones del edificio.

-Instauración de servicios de seguridad, como líneas telefónicas de emergencia, extintores, construcción de rutas de emergencia (Entrada y salida), plantas eléctricas de emergencia, etc.

-Establecer un centro de servicio alternativo que cuente con los recursos necesarios para continuar las operaciones de la organización hasta el momento en que el centro de trabajo normal pueda ser usado en condiciones normales.

-Capacitación del personal en el uso adecuado de las tecnologías informáticas, en le ejecución correcta de sus labores y en la ejecución de los procedimientos de emergencia.

Procedimientos Correctivos

Los procedimientos correctivos son acciones enfocadas a contrarrestar en lo posible los daños producidos por un desastre, ataque u otra situación desfavorable y restaurar el funcionamiento normal del centro de operación afectado.
Al igual que los procedimientos preventivos, pueden variar según los recursos disponibles, pero también varía dependiendo el daño que se quiere contrarrestar pues no todas las emergencias requieren el uso de todos los procedimientos correctivos definidos por la organización.

Planes de Contingencia

El Plan de Contingencias es el instrumento de gestión para el manejo de las Tecnologías de la Información y las Comunicaciones.
Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de una institución en caso de desastres y situaciones catastróficas como incendios, terremotos, inundaciones, etc. pero también contiene las medidas para enfrentar los daños producidos por robo, sabotaje e incluso ataques terroristas.
El plan de contingencia es un requisito indispensable para que una respuesta de emergencia sea rápida y efectiva. Sin una previa planificación de contingencia se perderá mucho tiempo en los primeros días de una emergencia.

BY NC SA

Objetivos y Características de un Plan de Contingencias

Los principales puntos que debe cumplir un plan de contingencia son:

-Reducir la probabilidad de que ocurra un desastre.

-Establecer los procedimientos necesarios para enfrentar y solucionar los eventos negativos que se presenten.

-Aminorar los efectos negativos de un desastre una vez ocurrido.

-Asegurar la continuidad de las operaciones de la organización.

-Restablecer el funcionamiento normal de las áreas afectadas por el desastre.

-Dar a conocer el plan de contingencia al personal involucrado.

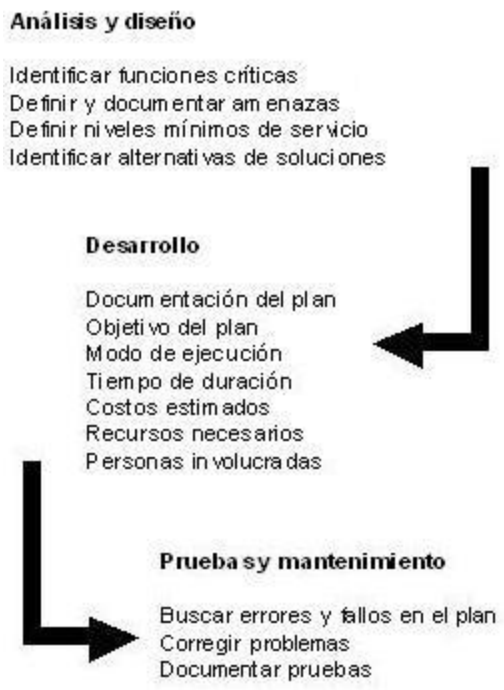
Para lograr tales objetivos, se debe diseñar e implantar una serie de procedimientos acorde a las necesidades y recursos disponibles que permitan responder de manera oportuna y precisa a todos los eventos negativos a los que se enfrente la organización. Estos procedimientos deben estar basados en los resultados obtenidos de un análisis previo de riesgos y un establecimiento de prioridades.

Fases del Plan de Contingencia

Un plan de contingencias está dividido en fases, esto facilita el monitoreo del desempeño de dicho plan así como también ayuda a la detección de fallos e implementación de mejoras, pues cada fase está enfocado a una serie de aspectos específicos y cualquier posible cambio se aplicará a partir de la fase apropiada sin necesidad de modificar todo el plan completo.

Las fases se pueden dividir en análisis y diseño, desarrollo, pruebas y mantenimiento.

BY NC SA



En cada fase se realizan diferentes actividades, esto facilita posibles modificaciones futuras

Análisis y Diseño

En esta fase se identifican las funciones de la organización que pueden considerarse como críticas y se les da un orden jerárquico de prioridad.
Se define y se documentan las amenazas a las que están expuestas las funciones críticas y se analiza el impacto que tendrá un desastre en las funciones en caso de materializarse.
También se definen los niveles mínimos de servicio aceptable para cada problema planteado.
Se identifican las posibles alternativas de solución así como evaluar una relación de costo/beneficio para cada alternativa propuesta

Desarrollo de un plan de contingencias

- En esta fase se creará la documentación del plan, cuyo contenido mínimo será:
- Objetivo del plan.
- Modo de ejecución.
- Tiempo de duración.

BY NC SA

- Costes estimados.
- Recursos necesarios.
- Evento a partir del cual se pondrá en marcha el plan.
- Personas encargadas de llevar a cabo el plan y sus respectivas responsabilidades.
- Es necesario que el plan sea validado por los responsables de las áreas involucradas. De igual manera hay que tener en cuenta las posibles consecuencias jurídicas que pudiesen derivarse de las actuaciones contempladas en él.

Pruebas y Mantenimiento

Consiste en realizar las pruebas pertinentes para intentar valorar el impacto real de un posible problema dentro de los escenarios establecidos en la etapa de diseño. Las pruebas no deben buscar comprobar si un plan funciona, mas bien debe enfocarse a buscar problemas y fallos en el plan para así poder corregirlos. Es necesario documentar las pruebas para su aprobación por parte de las áreas implicadas

En la fase de mantenimiento se corrigen los errores encontrados durante las pruebas, pero también se revisa que los elementos preparados para poner en acción el plan de contingencia estén en condiciones óptimas para ser usados de un momento a otro para contrarrestar un desastre. En caso contrario, se les debe reparar o sustituir.

Algunas de las actividades realizadas en esta fase son:

- Verificar la disponibilidad de los colaboradores incluidos en la lista del plan de contingencia.
- Verificar los procedimientos que se emplearan para almacenar y recuperar los datos (backup).
- Comprobar el correcto funcionamiento del disco extraíble, y del software encargado de realizar dicho backup.
- Realizar simulacros, capacitando al personal en el uso de los procedimientos indicados en el plan de contingencia para la medición de su efectividad.

5. ¿Cómo deben elaborarse las políticas?

1. Recopilar material de apoyo

Para elaborar eficazmente un conjunto de políticas de seguridad informática, debe haberse efectuado previamente un análisis de riesgo que indique claramente las necesidades de seguridad actuales de la organización. Antecedentes de fallas en la seguridad, fraudes, demandas judiciales y otros casos pueden proporcionar una orientación sobre las áreas que necesitan particular atención.

BY NC SA

Para afinar aun más el proceso, se debe tener copia de todas las otras políticas de organización (o de otras organizaciones similares) relativas a compra de equipos informáticos, recursos humanos y seguridad física.

2. Definir un marco de referencia

Después de recopilar el material de apoyo, debe elaborarse una lista de todos los tópicos a ser cubiertos dentro de un conjunto de políticas de seguridad. La lista debe incluir políticas que se piensa aplicar de inmediato así como aquellas que se piensa aplicar en el futuro.

3. Redactar la documentación

Después de preparar una lista de las áreas que necesitan la atención y después de estar familiarizados con la manera en que la organización expresa y usa las políticas, se estará ahora listos redactar las políticas, para lo cual pueden servir de ayuda el ejemplo que se encuentra más adelante.
Las políticas van dirigidas a audiencias significativamente distintas, en cuyo caso es aconsejable redactar documentos diferentes de acuerdo al tipo de audiencia.

Por ejemplo, los empleados podrían recibir un pequeño folleto que contiene las políticas de seguridad más importantes que ellos necesitan tener presente. En cambio, el personal que trabaja en informática y en telecomunicaciones podría recibir un documento considerablemente más largo que proporciona mucho más detalles.

Una vez que se hayan elaborado los documentos sobre las políticas, deben ser revisados por un comité de seguridad informática antes de ser sometido a consideración de la Presidencia y Junta Directiva para su aprobación. Este comité debería tener representantes de los distintos departamentos de la organización y una de sus funciones más importantes es evaluar la viabilidad de las políticas en materia de análisis costo/beneficio y sus implicaciones.

Las preguntas que debe contestar son, por ejemplo: ¿Son estas políticas prácticas y fácilmente aplicables?, ¿Son estas políticas claras e inequívocas?

Es muy importante que la Junta Directiva apruebe las políticas, ya que estas implican nuevas costumbres y reglas en el ámbito laboral que no siempre son bien acogidas por los empleados.

Además es fundamental de que luego de la entrada en vigor, las políticas se apliquen estrictamente, ya que de otra forma se puede fomentar la hipocresía entre los empleados y la tolerancia por conductas inapropiadas. El tener políticas que no se aplican puede ser peor que no tener políticas en absoluto.

BY NC SA

La aplicación de nuevas políticas es a menudo más eficaz si los empleados han sido informados de exactamente qué actividades representan trasgresiones de la seguridad y qué penalización recibirían si fueran encontrados culpables.
Un curso o taller de sensibilización es una forma muy efectiva para dar a conocer las nuevas políticas. Es una buena forma de hacer entender a los trabajadores que la información interna es la propiedad de organización, y el riesgo que supone tanto para ellos como para la organización que esta información llegue a ser copiada o divulgada.

Veámoslo en 10 pasos:

01. Estudio de la 27001

Comience por familiarizarse con la norma y su propósito. No es raro que las organizaciones introduzcan un sistema de gestión de seguridad de la información antes de que tengan una comprensión completa de qué se trata la norma y sus requisitos. De esta manera se puede utilizar la norma como una simple lista de verificación de requisitos que deben ser enumerados y no ocupar demasiado tiempo en la preparación de documentos desnecesarios para la ISO 27001. Además, se arriesga a cumplir parcialmente con los requisitos de la norma y que el trabajo se convierta en algo sistemático. Los preparativos son esenciales para obtener éxito en la certificación

02. Garantizar que la Dirección está involucrada y aprueba el proyecto

El éxito requiere compromiso de la alta dirección, es necesario que esta esté involucrada al implementar, supervisar, revisar, mantener y mejorar continuamente el sistema de gestión.

También debe garantizar que los recursos necesarios para trabajar con el sistema de gestión de seguridad de la información estén disponibles, bien como verificar que los empleados encargados de la elaboración, aplicación y mantenimiento del sistema tienen la competencia adecuada y brindar la capacitación necesaria. Con estos prerrequisitos es posible:

- Desarrollar una política de seguridad de la información
- Determinar los objetivos y planes relativos a la seguridad de la información
- Asignar papeles y responsabilidades dentro del sistema de seguridad de la información

03. Determinar la política y el alcance de la seguridad de la información

BY NC SA

A partir del momento en que la dirección demuestre estar involucrada y comprometida, es posible comenzar a trabajar con el sistema de gestión de seguridad de la información. En este paso la organización debe determinar el alcance del sistema de gestión y definir:

- Política de seguridad de la información
- Objetivos para la seguridad de la información
- Responsabilidades y reglas claras con respecto a seguridad de la información.

Cuando se definan estos puntos es necesario decidir qué partes de la organización serán incluidas en el sistema de gestión - áreas, recursos, técnicas, etc.

04. Elegir un método para la evaluación de riesgos

La evaluación de riesgos le ayudará a identificar el potencial de la seguridad de la información y cómo los riesgos pueden afectar a su información confidencial y la probabilidad de que se conviertan en una realidad. La elección del modelo de evaluación de riesgo es uno de los elementos más importantes al implementar un sistema de gestión de seguridad de información. La norma no determina el modelo que se debe utilizar. En su lugar, la norma requiere que el modelo elegido:

- Evalúe los riesgos relacionados con confidencialidad, integridad y disponibilidad
- Establezca metas para mantener los riesgos en un nivel aceptable
- Determine criterios que definan cuando el riesgo es aceptable.

5. Identificar, analizar y evaluar los riesgos

Al identificar los riesgos que deben ser analizados y evaluados:

- Evalúe cómo se vería perjudicada la organización si los riesgos de seguridad identificados se convirtieran en una realidad. Evalúe las consecuencias si la confidencialidad, integridad o
- disponibilidad de sus activos (recursos de información) se vieran comprometidos o damnificados.
- Realice una estimación de los diferentes niveles de riesgo.
- Determine si los riesgos son aceptables o si requieren una acción siguiendo criterios de aceptabilidad previamente definidos.
- Después, elija una de las siguientes acciones:

BY NC SA

- Aceptar el riesgo. Por ejemplo, si las acciones requieren demasiados costos o si
- no es posible que la organización tome las medidas necesarias (por ejemplo, en caso de desastres naturales o revoluciones políticas).
- Transfiera la responsabilidad del riesgo a otra persona. Por ejemplo, un proveedor externo o una compañía de seguros.
- Permita a los mecanismos de control mantener el riesgo en un nivel aceptable.

6. Definir acciones y objetivos para gestionar los riesgos

Para cumplir los requisitos señalados durante el proceso de evaluación de riesgos, acciones y objetivos deben ser identificados e implementados.

Esta identificación debe tener en cuenta los criterios de riesgos aceptables e inaceptables, así como obligaciones legales y regulatorias y contractuales.

7. Implementación de la ISO 27001

Implementar un plan que incluya:

- Una descripción de la gestión de riesgos donde se proporcione la gestión de acciones, recursos, responsabilidades y el orden de prioridad de las acciones con respecto a la seguridad de la información.
- Un plan de gestión de riesgos para alcanzar los objetivos. Esto incluye la financiación y la asignación de funciones y responsabilidades.
- Las medidas necesarias para alcanzar los objetivos.
- Capacitación
- Implementación del sistema y gestión de los recursos.

8. Educar a los empleados y asignar recursos

Recursos suficientes (personal, tiempo y dinero) deben ser asignados para implementar un sistema de gestión de seguridad de la información, bien como las medidas de seguridad. También es importante que los empleados que trabajan con el sistema de gestión de seguridad de la información (por ejemplo, con el mantenimiento del sistema, la documentación y la seguridad) sean entrenados correctamente.

BY NC SA

9. Auditoría interna, revisión gerencial y mejoras

Para garantizar que el sistema de gestión de seguridad de la información es y continuará siendo efectivo, la norma incluye los siguientes requisitos:

- Ejecutar auditorías internas
- La gerencia debe ejecutar evaluaciones periódicas del sistema de gestión de seguridad la información para asegurar que el sistema permanece completo y facilitar los procedimientos para encontrar mejoras para el sistema de gestión de seguridad de la información.

10. Comience su camino hacia la certificación y considere a pre-evaluación

Es común dedicar mucha energía para perfeccionar las cosas que ya funcionan bien, mientras que otros elementos esenciales no reciben la atención necesaria. Planee una pre-evaluación externa algunos meses antes de la auditoría de certificación, aunque su sistema gestión no esté completamente implementado. La identificación de áreas de no conformidad en la fase inicial le permitirá corregir posibles fallas antes de pasar a la auditoría de certificación.

5. Ejemplo de una política:

1. Justificación

Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra Compañía. Sin ellos nos quedaríamos rápidamente fuera del negocio y por tal razón la Presidencia y la Junta Directiva tienen el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, interrupción de servicio, accidentes y desastres naturales.

La información perteneciente a la Compañía debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se procesa (PCs, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Las distintas gerencias de la Compañía están en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna

BY NC SA

debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos. En todo caso cada año el Comité de Seguridad Informática llevará a cabo un análisis de riesgos y se revisarán las políticas de seguridad. Así mismo, se preparará cada año un informe para la Junta Directiva que muestre el estado actual de la Compañía en cuanto a seguridad informática y los progresos que se han logrado.
A todos los empleados, consultores y contratistas debe proporcionárseles adiestramiento, información, y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la Compañía. Debe hacerse hincapié en que la seguridad informática es una actividad tan vital para la Compañía como lo son la contabilidad y la nómina.
La finalidad de las políticas de seguridad que se describen más adelante es proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los computadores de la Compañía (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

2. Responsabilidades

Los siguientes entes son responsables, en distintos grados, de la seguridad en la Compañía:

El Comité de Seguridad Informática está compuesto por los representantes de los distintos departamentos de la Compañía, así como por el Gerente de Informática, el Gerente de Telecomunicaciones (cuando exista), y el abogado o representante legal de la Compañía. Este Comité está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad en informática y telecomunicaciones. También es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones trimestrales o ad hoc, el Comité efectuará la evaluación y revisión de la situación de la Compañía en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad.

La Gerencia de Informática es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Junta Directiva y la Gerencia de Telecomunicaciones (cuando exista). También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

El Jefe de Seguridad es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

El Administrador de Sistemas es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las

BY NC SA

bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como por ejemplo, aplicar inmediatamente los parches correctivos cuando le llegue la notificación del fabricante del producto o de un ente como el CERT (Computer Emergency Response Team). El Administrador de Sistemas también es responsable de informar al Jefe de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un Jefe de Seguridad, el Administrador de Sistemas realizará sus funciones.

Los usuarios son responsables de cumplir con todas las políticas de la Compañía relativas a la seguridad informática y en particular:

Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.

No divulgar información confidencial de la Compañía a personas no autorizadas.

No permitir y no facilitar el uso de los sistemas informáticos de la Compañía a personas no autorizadas.

No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Compañía.

Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.

Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.

Reportar inmediatamente a su jefe inmediato a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la Compañía y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

3. Políticas de seguridad para computadores

Los computadores de la Compañía sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

Los equipos de la Compañía sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

BY NC SA

Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática

No se permite fumar, comer o beber mientras se está usando un PC.

Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder no interrumpibles (UPS).

Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.

Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Compañía se requiere una autorización escrita.

La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.

Si un PCs tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

BY NC SA

No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente.

Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Compañía.

A menos que se indique lo contrario, los usuarios deben asumir que todo el software la Compañía está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

Los usuarios no deben copiar a un medio removible (como un diskette), el software o los datos residentes en las computadoras de la Compañía, sin la aprobación previa de la gerencia.

No pueden extraerse datos fuera de la sede de la Compañía sin la aprobación previa de la gerencia. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.

Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.

Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la Compañía.

No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.

Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el Departamento de Informática.

Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

BY NC SA

No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la Compañía a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

Periódicamente debe hacerse el respaldo de los datos guardados en PCs y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de Compañía debe guardarse en otra sede, lejos del edificio.

Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los gerentes de los distintos departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).

La información de la Compañía clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por la Gerencia de Informática.

No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.

El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

Siempre que sea posible, deba eliminarse información confidencial de de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de una representante de la Compañía.

No deben salirse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la Compañía.

El personal que utiliza un computador portátil que contenga información confidencial de la Compañía, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información debe estar cifrada.

4. Políticas de seguridad para las comunicaciones

Propiedad de la información

Con el fin de mejorar la productividad, la Compañía promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados

BY NC SA

por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la Compañía y no propiedad de los usuarios de los servicios de comunicación.
Uso de los sistemas de comunicación

Los sistemas de comunicación de la Compañía generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la Compañía.

Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Compañía y en tal sentido deben usarse las horas no laborables.

Confidencialidad y privacidad

Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que estén cifrados. Para tal fin debe utilizarse PGP (Pretty Good Privacy), Outolook, Outlook Express u otros productos previamente aprobados por la Gerencia de Informática.

Los empleados y funcionarios de la Compañía no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La Compañía se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.

Es política de la Compañía no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoría. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.

De manera consistente con prácticas generalmente aceptadas, la Compañía procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica (PABX) contienen detalles sobre el número llamado, la duración de la llamada, y la hora en que se efectuó la llamada.

Reenvío de mensajes
Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la Compañía, se debe ejercer cierta cautela al remitir

BY NC SA

los mensajes. En todo caso no debe remitirse información confidencial de la Compañía sin la debida aprobación.

Borrado de mensajes

Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

5. Políticas de seguridad para redes

Propósito

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la Compañía al estar conectada a redes de computadoras.

Alcance

Esta política se aplica a todos los empleados, contratistas, consultores y personal temporal de la Compañía.

Aspectos generales

Es política de la Compañía prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

Modificaciones

Todos los cambios en la central telefónica (PABX) y en los servidores y equipos de red de la Compañía, incluyendo la instalación de el nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

Cuentas de los usuarios

Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.

BY NC SA

No debe concederse una cuenta a personas que no sean empleados de la Compañía a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

Privilegios especiales, tal como la posibilidad de modificar o barrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Gerente de Informática determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas Unix no deben entrar inicialmente como "root", sino primero empleando su propio ID y luego mediante "set userid" para obtener el acceso como "root". En cualquier caso debe registrarse en la bitácora todos los cambios de ID.

Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

Cuando un empleado es despedido o renuncia a la Compañía, debe desactivarse su cuenta antes de que deje el cargo.

Contraseñas y el control de acceso

El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

BY NC SA

Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

Para el acceso remoto a los recursos informáticos de la Compañía, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña (o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad).

Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Compañía, pudiendo ser causal de despido.

Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

Los archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

BY NC SA

Los servidores de red y los equipos de comunicación (PABX, routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo, tarjetas de proximidad).

BY NC SA