Guía para la Implementación de Seguridad de la Información en una MIPYME.

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía Técnica

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.2	6/11/2016	Actualización CCP - MINTIC

1. INTRODUCCIÓN

En un entorno empresarial globalizado y competitivo como el existente en la actualidad, las empresas dependen cada vez más de sus sistemas de información y de la información que estos administran, pues se ha demostrado que tienen una enorme influencia en la toma de dediciones estratégicas para aumentar su nivel de competitividad.

El problema de la seguridad de la información se caracteriza por la complejidad y la interdependencia. La gestión de la seguridad contiene un número importante de factores y elementos que se interrelacionan entre sí. Las MIPYMES suelen tener una débil comprensión de la seguridad de la información, tecnologías de seguridad y medidas de control, y suelen dejar el análisis de riesgos o el desarrollo de las políticas de seguridades olvidadas. De ahí la gran importancia de divulgar esta guía al interior de las empresas de nuestro país

2. TERMINOS Y DEFINICIONES

Activo

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Amenazas

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Adware

Adware es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.

Advertencia

Mensaje que comunica al usuario que una acción puede ocasionar u ocasionara la pérdida de datos del sistema del usuario.

Alarma

Sonido o señal visual que se activa cuando se produce una condición de error.

Alerta

Notificación automática de un suceso o un error.

Amenaza

Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Amenazas polimorfas

Las amenazas polimorfas son aquellas que tienen la capacidad de mutar y en las cuales cada instancia del malware es ligeramente diferente al anterior a este. Los cambios automatizados en el código realizados a cada instancia no alteran la funcionalidad del malware, sino que prácticamente inutilizan las tecnologías tradicionales de detección antivirus contra estos ataques.

Amenaza Externa

Amenaza que se origina fuera de una organización.

Amenaza Interna

Amenaza que se origina en una organización.

Analizador

Herramienta de configuración automatizada que analiza una red en busca de sistemas activos y actúa como guía durante el proceso de definición de los sistemas que desea supervisar y de las firmas de ataques que desea asociar con cada sistema.

Antispam

Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

Antivirus

Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Aplicaciones engañosas

Las aplicaciones engañosas son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.

Arquitectura de Seguridad

Conjunto de principios que describe los servicios de seguridad que debe proporcionar un sistema para ajustarse a las necesidades de sus usuarios, los elementos de sistema necesarios para implementar tales servicios y los niveles de rendimiento que se necesitan en los elementos para hacer frente a las posibles amenazas.

Ataques multi-etapas

Un ataque en múltiples etapas es una infección que normalmente implica un ataque inicial, seguido por la instalación de una parte adicional de códigos maliciosos. Un ejemplo es un troyano que descarga e instala adware.

Ataques Web

Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Autenticación

Garantía de que una parte de una transacción informática no es falsa. La autenticación normalmente lleva consigo el uso de una contraseña, un certificado,

un número de identificación personal u otra información que se pueda utilizar para validar la identidad en una red de equipos.

Blacklisting o Lista Negra

La lista negra es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.

Bot

Un bot es una computadora individual infectada con malware, la cual forma parte de una red de bots (botnet).

Botnet

Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección.

Caballo de Troya

Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

Certificado

Los sistemas criptográficos utilizan este archivo como prueba de identidad. Contiene el nombre del usuario y la clave pública.

Crimeware

Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidor del software.

Ciberdelito

El ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.

Contraseña

Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña.

Cuarentena

Aislar archivos sospechosos de contener algún virus, de modo que no se pueden abrir ni ejecutar.

Encriptación

La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.

Exploits o Programas intrusos

Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

Filtración de datos

Una filtración de datos sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados

Firewall

Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Grooming

Es una nueva forma de acoso y abuso hacia niños y jóvenes que se ha venido popularizando con el auge de las TIC, principalmente los chats y redes sociales. Inicia con una simple conversación virtual, en la que el adulto se hace pasar por otra persona, normalmente, por una de la misma edad de víctima con el fin de

Gusanos

Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, a diferencia de un Virus.

Ingeniería Social

Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

Keystroke Logger o Programa de captura de teclado (Keylogger)

Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

Malware

El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo

electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas.

Mecanismo de propagación

Un mecanismo de propagación es el método que utiliza una amenaza para infectar un sistema.

Negación de servicio (DoS)

La negación de servicio es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o red para los usuarios. Un ataque distribuido de negación de servicio (DDoS) es aquel en que el atacante aprovecha una red de computadoras distribuidas, como por ejemplo una botnet, para perpetrar el ataque.

Pharming

Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del re-direccionamiento e ingresen información personal, como la información bancaria en línea, en el sitio fraudulento.

Phishing

Método más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Redes punto a punto (P2P)

Red virtual distribuida de participantes que hacen que una parte de sus recursos informáticos estén a disposición de otros participantes de la red, todo sin necesidad de servidores centralizados. Las redes puntos a punto son utilizadas para compartir música, películas, juegos y otros archivos. Sin embargo, también son un mecanismo muy común para la distribución de virus, bots, spyware, adware, troyanos, rootkits, gusanos y otro tipo de malware.

Riesgo

El riesgo es el efecto de la incertidumbre sobre los objetivos.

Rootkits

Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final.

Los rootkits no infectan las máquinas por sí mismos como lo hacen los virus o gusanos, sino que tratan de proporcionar un entorno indetectable para ejecutar códigos maliciosos. Los atacantes normalmente aprovechan las vulnerabilidades en el equipo seleccionado o utilizan técnicas de ingeniería social para instalar manualmente los rootkits. O, en algunos casos, los rootkits pueden instalarse automáticamente al ejecutarse un virus o gusano o incluso simplemente al navegar en un sitio Web malicioso.

Sistema de detección de intrusos

Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Sistema de prevención de intrusos

Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Spam

También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común

de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing

Spyware o Software Espía

El software espía consta de un paquete de software que realiza un seguimiento y envía información confidencial o personal a terceros. La información personal es información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de las personas no desearía compartir con otras, como detalles bancarios, números de tarjetas de créditos y contraseñas. Terceros puede hacer referencia a sistemas remotos o partes con acceso local.

Virus

Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.

Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales.

Vulnerabilidad

Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

- Permitir que un atacante ejecute comandos como otro usuario
- Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
- Permitir a un atacante hacerse pasar por otra entidad
- Permitir a un atacante realizar una negación de servicio

3. PANORAMA DE INSEGURIDAD Y AMENAZAS EN COLOMBIA

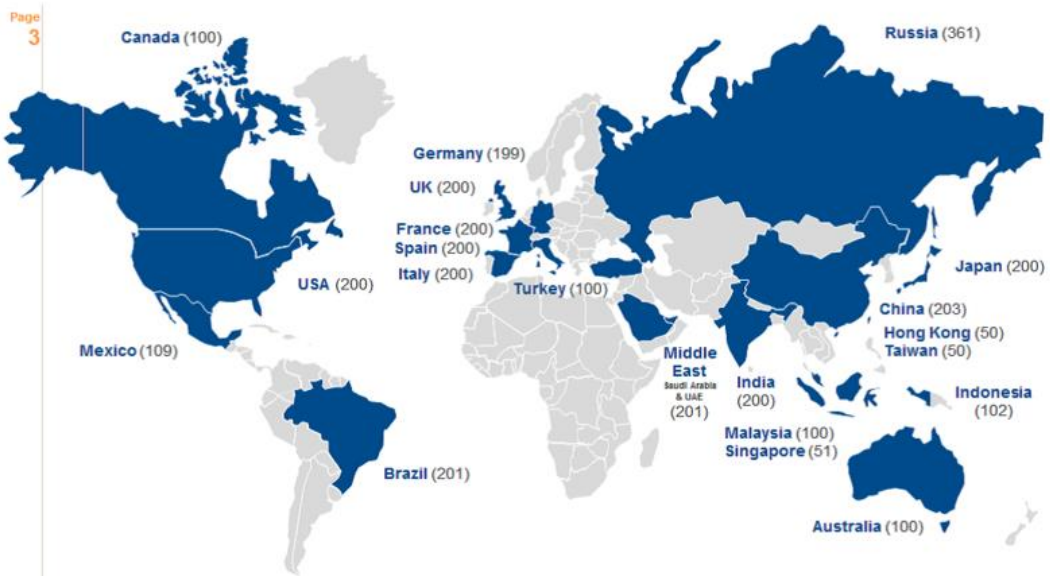
El contexto del cibercrimen aborda todo tipo de esferas; en ese sentido firmas de auditoría y el Centro Cibernético Policial argumenta que el 46 % de los crímenes informáticos se dan por la carencia de elementos de seguridad, asimismo existen cuatro tipos de crimen que afecta el sector económico: malversación de activos, fraude financiero, corrupción y Cibercrimen como se observa en la siguiente gráfica:

Gráfica 1. Sectores representados en el estudio

Tomado de encuesta realizada por KPMG

La mayoría de incidentes ocasionaron un impacto significativo en los sectores indicados, sin mencionar que muchos de ellos se dieron por causa de la ausencia de políticas implementadas de seguridad en la información, el Cibercrimen, de acuerdo a estas cifras han perdido utilidades de un 55% por cada semestre computarizado desde el 2012 a 2014; una de cada 15 empresas afectadas NO posee ninguna clase de política de seguridad en la información, y 10 de cada 100 no gestiona ninguna clase de activo en la que se permita evaluar los elementos críticos de la organización.

Este panorama aumenta por la ausencia de sensibilización de las personas encargadas de la custodia y manipulación de la información; de la misma manera incrementa la participación de los empleados en la comisión de una conducta tipificada en la ley penal, 6.5 de cada 10 empresas han padecido algún tipo de fraude en los últimos dos años, en ese sentido ven como la implementación de tecnología es proporcional al riesgo y vulnerabilidad de sus sistemas. Kaspersky, una de las firmas más prestigiosas de antivirus y protección de amenazas informáticas manifiesta que el 68% de empresas de américa latina han sufrido algún ataque de malware durante estos últimos 12 meses, este estudio revela que las empresas se ven afectadas por virus, gusanos, spyware y otros programas maliciosos que se aprovechan de la ingeniería social para obtener información confidencial para poder instalar o inyectar estas ciberamenazas en los equipos de cómputo de las empresas.



Tomado de http://latam.kaspersky.com/mx/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/kaspersky-lab-68-de-empresas-en-am%C3%A9rica-latin

El Centro Cibernético Policial ha recibido cerca de 34 denuncias cada semana en donde se atienden distintos tipos de ataques contra los sectores, económico, financiero, social y gubernamental; razón que involucra en la construcción del primer portal de ciberseguridad del país en donde se dispone de atención de las modalidades de delito informático que afectan el sector empresarial en Colombia.

Actualmente el CCP atiende cerca de 172.576 ciudadanos en línea, cifra que durante el 2015 ha venido en aumento, cuyos principales elementos de reporte se evidencian a partir de la denuncia de las conductas que más afectan a la Pymes con distintas modalidades que han afectado la ciberseguridad en el interior de estas organizaciones, el mayor índice de conductas detectadas por el Centro Cibernético Policial son:

Email Spoofing Financiero: Es una técnica de ingeniería social que es aprovechada por el ciberdelincuente para crear un mensaje aparentemente verídico autorizando determinada acción en la nómina o contable, desconociendo los preceptos de autenticidad del origen; asimismo se plantea desde la posibilidad que se afecte a las oficinas de nómina o tesorería en los días cercanos al pago de obligaciones de parafiscales en cada una de las Empresas.

Indebida clasificación de la información financiera: El atacante puede vulnerar el sistema informático, sin embargo la ausencia de una clasificación de los datos confidenciales, privados, semi-privados y personales, son los criterios que busca el ciberdelincuente para generar la capacidad para acceder al operador de las transacciones; en este sentido el ciberdelincuente intentará acceder al ambiente informático y robar datos dentro del contexto transaccional de la víctima.

Mensaje engañoso "Hoax" y Spam: Una de las características de los mensajes falsos, son aquellos que generalmente puede llegar a la bandeja de entrada desde una dirección electrónica desconocida; en efecto el mensaje fraudulento siempre indicará la acción inmediata para realizar una actividad por parte de la víctima, por otro lado el "Spam" o correo basura pretende enviar al usuario a publicidad engañosa o muchas veces re-direccionarlo a sitios web con contenido malicioso o dañino.

Robo de Información: Es la apropiación indebida de información confidencial por parte del ciberdelincuente para poder asegurar la comisión de otras conductas delictivas.

Vishing: Actividad delincuencial de ingeniería social que se produce mediante una llamada telefónica a algún miembro de la empresa haciéndose pasar por un proveedor para tener acceso algún elemento confidencial o generar alguna actividad de pago frente alguna deuda (pago de mercancía, facturas pendientes, etc.), este tipo de técnica se presenta en la mayoría de los casos con anuncios pregrabados mediante teléfono VoIP.

Ingeniería Social: Actividad delictiva que se usa generalmente para ganar provecho del eslabón más débil de la empresa para la obtención de información confidencial.

Pishing: Es la suplantación de sitios web de manera fraudulenta para capturar datos financieros, privados, personales o confidenciales, para sacar provecho de estos mediante el apoderamiento de grandes bases de datos financieras de la empresa.

Pharming: Es una variación del Pishing que tiene como finalidad cambiar la dirección de ingreso a los portales bancarios dentro del equipo de cómputo afectado, generando a partir de este una conexión a la página del delincuente.

Robo de identidad: Es una actividad delictiva asociada a la suplantación de clientes financieros de la empresa, empleando tarjetas de crédito o cupos de endeudamiento que permiten por parte de la empresa brindar fuga de información y hacer ataques de ingeniería social.

Malware Financiero: La carencia de políticas de antivirus y mala percepción de las técnicas de los ciberdelincuentes permite que los ataques de malware sean más permitidos, estos programas son diseñados con el fin de apoderarse de información confidencial y privada de la empresa u organización para que un tercero pueda realizar modificaciones en los sistemas informáticos y así generar fraudes de mayor cuantía.

APT – Amenazas Avanzadas Persistentes: Es muchas empresas la infección mediante la ejecución de programas publicitarios, avisos engañosos, correos indeseados, archivos descomprimidos, pueden facilitar el acceso a información clasificada como privada o confidencial; estas amenazas que constantemente se presentan pero que permanecen ejecutándose en el sistema son amenazas informáticas que debe tener en cuenta el administrador de tecnología de la Empresa.

Secuestro de Datos: La descarga de objetos adjuntos en correos electrónicos, propuestas de pago, spam, correo publicitario, archivos comprimidos, documentos de atracción por el usuario pueden ser elementos que pueden afectar los datos confidenciales del equipo de cómputo, estos programas permiten realizar el secuestro de información financiera.

4. QUE DEBO TENER EN CUENTA PARA IMPLEMENTAR SEGURIDAD AL INTERIOR DE MI EMPRESA

¿QUÉ ES SEGURIDAD?

Si nos remitimos al diccionario, nos encontramos con algunas definiciones:

- Sustantivo femenino). Certeza, firmeza, confianza. Sin riesgo
- Dícese de las cosas ciertas, firmes y/o libres de peligro o riesgo. Estado de las cosas bajo protección
- Confianza, tranquilidad de una persona procedente de la idea de que no hay ningún peligro que temer

4.1. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad de la información se encarga de garantizar la integridad, confidencialidad, disponibilidad de nuestra información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006].

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006].

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. [NTC5411-1:2006].

4.2. ORGANICE LA SEGURIDAD DE LA INFORMACIÓN AL INTERIOR DE LA EMPRESA

La alta dirección de la empresa debe apoyar activamente la seguridad al interior de ella, mediante un compromiso demostrado definiendo roles y responsabilidades dentro de la empresa tendientes a garantizar el la seguridad de la información.

ES IMPORTANTE, iniciar la implementación de seguridad de la información en los procesos misionales de su empresa o a los procesos que son considerados el núcleo del negocio.

4.3. CREE UNA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

4.3.1. QUE ES UNA POLITICA?

Conjunto de orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

4.3.2. QUE ES UNA POLITICA DE SEGURIDAD DE LA INFORMACION?

Conjunto de Directrices que permiten resguardar los activos de información

4.3.3. COMO DEBE SER UNA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

- Debe definir la postura de la dirección o la gerencia con respecto a la necesidad de proteger la información corporativa
- Orientar a los funcionarios con respecto al 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 TI y Seguridad Informática
- Ser general sin comprometerse con tecnologías especificas (Principio de Neutralidad Tecnológica)
- Debe abarcar toda la organización
- Debe ser de larga vigencia, manteniéndose sin grandes cambios en el tiempo.
- Debe ser clara y evitar confusiones o interpretaciones
- No debe generar nuevos problemas
- Debe permitir clasificar la información en confidencial, uso interno, publica

- Debe identificar claramente funciones específicas de los empleados como: Responsables, Custodio, o Usuario.

4.3.4. QUE DEBE CONTENER UNA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

- Políticas especificas
- Procedimientos
- Estándares o practicas
- Controles
- Estructura organizacional

4.3.5. QUE SON LAS POLITICAS ESPECÍFICAS

Definen en detalle los aspectos específicos que regulan el uso de los recursos tecnológicos y recursos de información y suelen ser más susceptibles al cambio, a diferencia de la política general de la organización.

4.3.6. QUE SON LOS PROCEDIMIENTOS

- Define los pasos para realizar una actividad especifica
- Evita que se aplique el criterio personal

4.3.7. QUE SON LOS ESTANDARES

Es un documento establecido por consenso que sirve de patrón, modelo o guía que se usa de manera repetitiva. Los estándares de seguridad suelen ser actualizados periódicamente ya que dependen directamente de la tecnología.

4.3.8. QUE SE DEBE TENER EN CUENTA EN LA CREACION DE UNA POLITICA

- Objetivo: Que se desea lograr.
- Alcance: Que es lo que se protege y quienes deben cumplirla.
- Definiciones: Aclaración de términos utilizados.
- Responsabilidades: Que debe y no debe hacer cada persona
- Revisión: Como será monitoreado el cumplimiento (Seguimiento, Indicadores, Resultados)
- Aplicabilidad: En qué casos será aplicable.
- Referencias: Documentos complementarios (Anexos).

5. SENSIBILICE A LOS EMPLEADOS

Realice periódicamente capacitaciones sobre las políticas de seguridad de la información de la empresa y las actualizaciones de las mismas. Además de esto sensibilizar a los empleados sobre las amenazas a las que están expuestos.

Para ello es recomendable crear un plan de comunicaciones que como mínimo contenga lo siguiente:

Introducción

Objetivo

Alcance

Divulgación y sensibilización

Mostrar la problemática que genera el cambio

Beneficios de la seguridad de la información

Un plan de gestión de la cultura de seguridad de la información en su empresa

Validación de la situación actual de la empresa

Situaciones evidenciadas de casos registrados

Una encuesta

Presentación de resultados

Plan de comunicaciones

¿Cuál es el objetivo de comunicación de la campaña?

¿A qué público se va a dirigir el mensaje?

¿Qué acción queremos que el público objeto realice?

¿Cuáles son las barreras para la acción deseada?

¿Qué esperamos lograr?

¿Qué valores distintivos tendrá la campaña?

¿Cuáles son los medios para comunicar los mensajes?

¿Cuáles mensajes se van a reforzar?

Conformación del equipo de sensibilización

Caracterización para la definición de los grupos objetivo

Definición de los grupos objetivo

Ejecutar el plan de sensibilización

Acompañamiento a la implementación

Controlar el proceso

Indicadores - cubrimiento del plan de capacitación

Indicadores – efectividad del plan de capacitación y sensibilización

Indicadores – cumplimiento del despliegue

Indicadores – efectividad de la capacitación

Indicadores – hábitos de cultura de seguridad

Glosario

6. IDENTIFIQUE LOS ACTIVOS DE INFORMACIÓN DE SU EMPRESA

Activo, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización.

Activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información.

Descripción de los activos de información:

- Datos: Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización.
- Aplicaciones: El software que se utiliza para la gestión de la información.
- Personal: En esta categoría se encuentra tanto la plantilla propia de la organización, como el personal subcontratado, los clientes, usuarios y, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización.
- Servicios: Aquí se consideran tanto los servicios internos, aquellos que una parte de la organización suministra a otra (por ejemplo la gestión administrativa), como los externos, aquellos que la organización suministra a clientes y usuarios (por ejemplo la comercialización de productos).
- Tecnología: Los equipos utilizados para gestionar la información y las comunicaciones (servidores, PCs, teléfonos, impresoras, routers, cableado, etc.)
- Instalaciones: Lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, etc.)
- Equipamiento auxiliar: En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos (equipos de destrucción de datos, equipos de climatización, etc.)

6.1. COMO REALIZAR UN INVENTARIO DE ACTIVOS DE INFORAMACIÓN

El inventario de activos que se va a utilizar para la gestión de la seguridad no debería duplicar otros inventarios, pero sí que debe recoger los activos más importantes e identificarlos de manera clara y sin ambigüedades.

El inventario de activos es la base para la gestión de los mismos, ya que tiene que incluir toda la información necesaria para mantenerlos operativos e incluso poder recuperarse ante un desastre.

La información que describe a un activo debe contener como mínimo:

- Identificación del activo: Un código para ordenar y localizar los activos.
- Tipo de activo: A qué categoría de las anteriormente mencionadas pertenece el activo.
- Descripción: Una breve descripción del activo para identificarlo sin ambigüedades.
- Propietario: Quien es la persona a responsable del activo.
- Usuario: Quien es la persona que lo usa
- Custodio: Quien resguarda el activo
- Ubicación: Dónde está físicamente el activo. En el caso de información en formato electrónico, en qué equipo se encuentra.

(*Si desea conocer más en detalle consulte la guía de gestión de activos del modelo de seguridad y privacidad de la información*).

7. DETERMINAR LAS POSIBLES VULNERABILIDADES Y AMENAZAS DE LA ARQUITECTURA TECNOLOGICA QUE PROCESA LA INFORMACION.

7.1. VULNERAVILIDADES

A continuación se describen algunas vulnerabilidades dependiendo de su origen de generación; esto no quiere decir que sean las únicas.

Físicas

Posibilidad de que el sistema tiene de ser atacado físicamente, por alteración, robo o destrozo del sistema informático.

Contramedidas

Cámaras de vigilancia

Natural

Grado en el que el sistema puede verse alterado por sucesos naturales, como un incendio, una inundación, terremotos…

Contramedidas

Por ejemplo, para los incendios, medidas anti incendio, como extintores, detectores de humo.

Hardware y Software

Fallos y debilidades de los aparatos informáticos, como un fallo en el disco duro (el cabezal del dispositivo, a los tres meses, se estropea, por un defecto de fabricación). También son vulnerabilidades de este nivel el software que da errores, “bugs”, pudiendo afectar al acceso a los datos o a la integridad de las aplicaciones.

Contramedidas

Servicio técnico de la empresa que proporciona el software, a nuestra disposición para detectar esos fallos y subsanarlos.

El clustering, que consiste en una colección de discos interconectados que se comportan como un único disco virtual, con la diferencia del aumento de prestaciones y de las características de redundancia. La implementación más

sencilla de un cluster es con dos servidores y el único propósito es garantizar la funcionalidad del conjunto; es decir, que si uno se cae el otro tome la responsabilidad, justo en el punto del proceso donde se produjo el fallo. Los clientes sólo notaran una demora de unos segundos mientras se regeneran los datos y, superado ese momento, el funcionamiento será el normal. El objetivo del clustering es minimizar las consecuencias de las caídas de los servidores por medio de una arquitectura que, al menos mantendrá un servidor activo ante cualquier fallo del resto de los componentes del sistema.

Comunicaciones

Ahora, debido a la proliferación de redes locales, intranets, la Internet, etc., existe la posibilidad de que se vean vulneradas, por ejemplo, por culpa de un hacker que entra en nuestra base de datos a través de Internet.

Contramedidas

Firewalls, administradores que supervisan las comunicaciones, IDS, IPS entre otras.

Humana:

Es la más sutil de todas. Los usuarios pueden alterar la seguridad de nuestro sistema informático, las personas que están en contacto directo con nuestros sistemas informáticos, como los administradores, personas autorizadas, empleados… Teóricamente son las más controlables.

Contramedidas

Por ejemplo, que dos personas a la vez tengan que introducir una clave cada uno (utilizado en entornos militares).

Otra posibilidad es que un usuario que disponga de una cuenta en nuestra base de datos provoque una vulnerabilidad. Una solución ante esto podría ser separar cada servicio en una máquina distinta, como tener el servidor de correo electrónico en una máquina y el servidor de cuentas en otra, no todo en una sola máquina (como es el caso de anubis.uji.es). Es importante para evitar estas vulnerabilidades no tener usuarios directos.

7.2. AMENAZAS:

Clasificadas desde el punto de vista del efecto que causan al aprovechar una vulnerabilidad.

Intercepción:

Cuando se consigue acceso a una parte del sistema sin autorización. Son difíciles de detectar porque se accede sin modificar los datos.

Modificación:

Cuando alguien accede de manera no autorizada a una parte del sistema y además se modifican datos.

Interrupción:

Puede ser indefinida o momentánea. Una interrupción del funcionamiento del sistema puede ser accidental, y entonces es difícilmente controlable. Este tipo de amenazas son las más frecuentes y las menos dañinas.

Generación:

Cuando existe la posibilidad de añadir programas no autorizados. Es el caso, por ejemplo, de los virus.

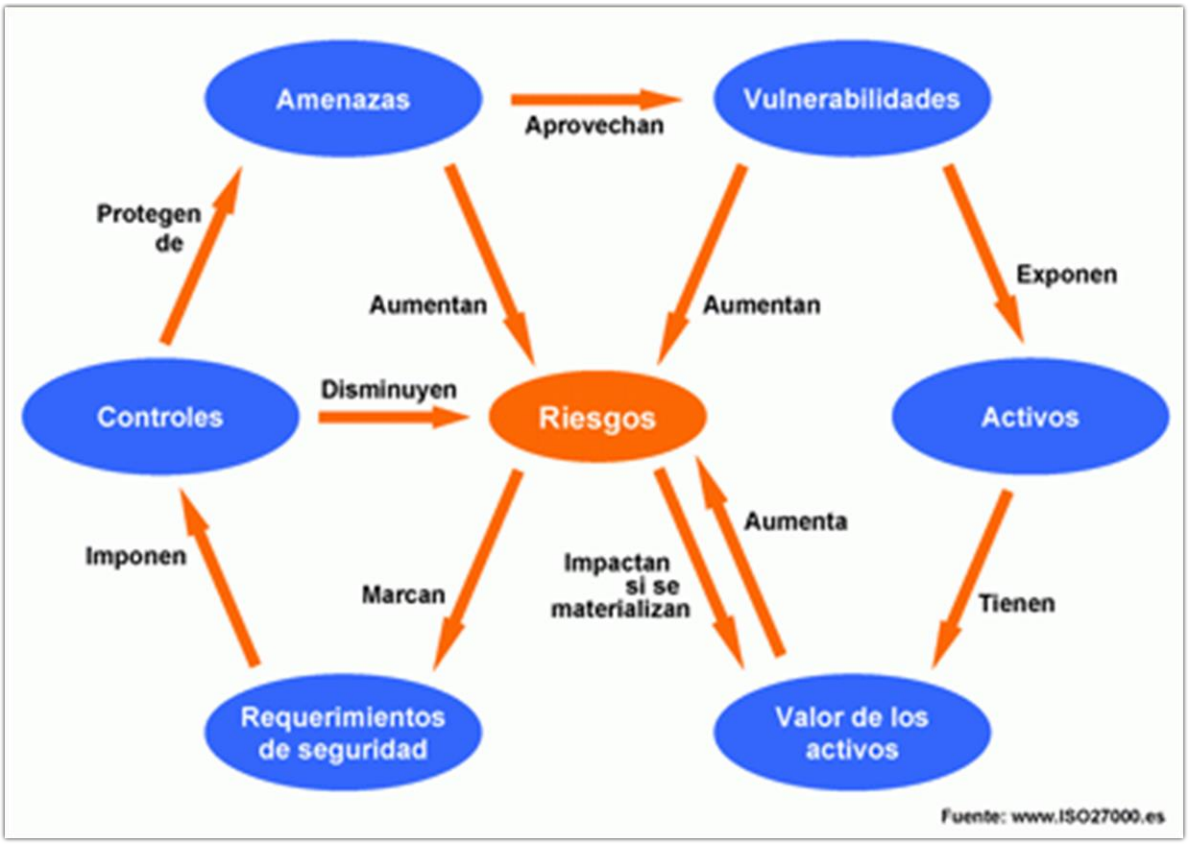
8. EVALUE LOS RIESGOS A LOS QUE ESTAN EXPUESTOS SUS ACTIVOS

El enfoque de riesgos se basa en la identificación de las amenazas y vulnerabilidades presentes en los activos de información de los procesos de una organización, y cómo pueden afectar las actividades impidiendo lograr sus objetivos.

Una buena práctica seria tener en cuenta los siguientes puntos a la hora de analizar riesgos de seguridad de la información

- Definir el enfoque organizacional para la valoración del riesgo
- Identificar una metodología de valoración del riesgo que sea adecuada a un SGSI y que se adapte a la metodología de análisis de riesgo desarrollada una empresa. Ejemplo de metodologías(una buena combinación es ISO 31000 + ISO 27005)
- Desarrollar criterios para la aceptación de riesgos, e identificar los niveles de riesgo aceptables teniendo en cuenta la metodología aplicada en en la empresa o la seleccionada.
- Identificar los Riesgos
- Identificar las amenazas a los activos relacionados previamente.
- Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.
- Identificar los riesgos teniendo en cuenta la Confidencialidad, Disponibilidad y la Integridad de los activos.
- Analizar y evaluar los riesgos:
- Estimar los niveles de los riesgos.
- Determinar la aceptación del riesgo o la necesidad de su tratamiento.
- Identificar y evaluar las opciones para el tratamiento de los riesgos.
- Seleccionar los controles para el tratamiento de los riesgos. (ISO 27002; COBIT; ITIL…)

Así, el objetivo de esta actividad es generar los procedimientos adecuados para la administración de riesgos; y a su vez generar un plan de tratamiento de riesgos que deberá ser ejecutado por la empresa



Fuente: www.ISO27000.es

(***Si desea conocer más en detalle consulte la guía de gestión de riesgos del modelo de seguridad y privacidad de la información***).

9. RECOMENDACIONES

- Actualice y licencie su cortafuegos y antivirus.
- Realice revisión periódica de su listado de contactos y practique la utilización de firma digital o autenticación del mensaje a través de hash.
- No realice transacciones desde páginas web no confiables
- No instale herramientas de escritorio remoto, siempre y cuando no se almacene un llavero de claves seguro y confiable.
- Evite conectarse desde redes inalámbricas abiertas que no tienen ninguna seguridad.
- Cerciórese de la información de contacto con el fin de verificar el auténtico originador del mensaje.
- No descomprima archivos de extensión desconocida sin antes verificar el “vista previa” el contenido del mismo.
- Elimine correos electrónicos “Spam”, de esta forma evitará ir a sitios web no seguros.
- Actualice los parches de seguridad del navegador web.
- Gestión adecuada de información confidencial y de terceros (títulos financieros, chequeras, tarjetas, productos crediticios, etc.)
- Implemente servidor de correos electrónicos SPF (Sender Polcy Framework).

Casos como el llamado VIRUS de la DIAN, fue alertado por primera vez por el CAIVIRTUAL, como lo consignaron medios de comunicación nacionales y sitios Web especializados, donde la institución policial es referente de consulta por parte de expertos y ciberusuarios.

El Centro Cibernético Policial alertó sobre la presencia de ‘malware’ en correos electrónicos relacionados con supuestas cuentas de cobro de la Dirección de Impuestos y Aduanas Nacionales (Dian).

Tomado de: ElTiempo.com

Recomendaciones PYMES:http://www.ccp.gov.co/ciberseguridad/recomendaciones/pymes

10. SUGERENCIAS:

En caso de ser víctima no olvide que:

- Debe preservar la página, sitio web, correo electrónico, objeto del ataque, apóyese del área de sistemas para tomar esta evidencia que será útil dentro de la investigación formal.
- Documente la evidencia recolectada y haga uso de los protocolos de cadena de custodia.
- Aislé los navegadores no configurados o sin actualizar
- Active la configuración del cortafuegos/filtrado de spam
- No Instale herramientas de acceso remoto o desactive las mismas al momento de dejar en desuso el equipo de cómputo.
- Revise la configuración del cliente de correo de correo de su empresa de manera confiable
- Clasifique la Información de su empresa de manera que los ciberdelincuentes no tengan acceso a información financiera.
- Realice respaldos o Backups de su información
- Haga una lista de chequeo de los sitios web visitados o consultados para que sean validados como fuentes originales de sitios transaccionales.
- Ajuste me manera periódica las políticas de uso de antivirus
- Revise constantemente la prestación de servicios ante terceros y servicios de soporte