Seguridad informática

La seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras.[1] Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

La definición de seguridad de la información no debe ser confundida con la de «seguridad informática», ya que esta última solo 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 informática es la disciplina que se encarga de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Puesto simple, la seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como los mismos computadores. Nadie a cargo de seguridad debe determinar quién y cuándo puede tomar acciones apropiadas sobre un ítem en específico. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización en organización. Independientemente, cualquier compañía con una red debe tener una política de seguridad que se dirija a la conveniencia y la coordinación.

Objetivos

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

La infraestructura computacional: es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar por que los equipos funcionen adecuadamente y anticiparse en caso de fallos, robos, incendios, sabotajes, desastres

naturales, fallos en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

Los usuarios: son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.

La información: esta es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA

Para lograr sus objetivos, la seguridad informática se fundamenta en tres principios:

- Confidencialidad
- Integridad
- Disponibilidad

PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA

Confidencialidad

Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático.

Basándose en este principio, las herramientas de seguridad informática deben proteger al sistema de invasiones, intrusiones y accesos, por parte de personas o programas no autorizados.

Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que usuarios, ordenadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.

Integridad

Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático.

Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.

Este principio es particularmente importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, ordenadores y procesos comparten la misma información.

Disponibilidad

Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático.

Basándose en este principio, las herramientas de Seguridad Informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran.

Este principio es particularmente importante en sistemas informáticos cuyo compromiso con el usuario, es prestar servicio permanente.

Factores de riesgo

Tecnológicos: fallas de hardware y/o software, fallas en el aire acondicionado, falla en el servicio eléctrico, ataque por virus informáticos, etc.

Ambientales: factores externos, lluvias, inundaciones, terremotos, tormentas, rayos, suciedad, humedad, calor, entre otros.

Humanos: hurto, adulteración, fraude, modificación, revelación, pérdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, intrusión, alteración, etc.

Factores tecnológicos de riesgo

Virus informáticos: Definición

Un virus informático es un programa (código) que se replica, añadiendo una copia de sí mismo a otro(s) programa(s).

Los virus informáticos son particularmente dañinos porque pasan desapercibidos hasta que los usuarios sufren las consecuencias, que pueden ir desde anuncios inocuos hasta la pérdida total del sistema.

Sus principales características son:

Auto-reproducción: Es la capacidad que tiene el programa de replicarse (hacer copias de sí mismo), sin intervención o consentimiento del usuario.

Infección: Es la capacidad que tiene el código de alojarse en otros programas, diferentes al portador original.

Virus informáticos: Propósitos

Afectar el software: Sus instrucciones agregan nuevos archivos al sistema o manipulan el contenido de los archivos existentes, eliminándolo parcial o totalmente. Afectar el hardware: Sus instrucciones manipulan los componentes físicos. Su principal objetivo son los dispositivos de almacenamiento secundario y pueden sobrecalentar las unidades, disminuir la vida útil del medio, destruir la estructura lógica para recuperación de archivos (FAT) y otras consecuencias.

Virus informáticos: Clasificación

La inmensa cantidad de virus existentes, sus diferentes propósitos, sus variados comportamientos y sus diversas consecuencias, convierten su clasificación en un proceso complejo y polémico.

A continuación se presentan las categorías que agrupan a la mayoría de los virus conocidos. Sin embargo, es importante considerar que la aparición diaria de virus cada vez más sofisticados, puede llevar al surgimiento de nuevas categorías en cualquier momento.

Virus informáticos: Clasificación

Virus genérico o de archivo: Se aloja como un parásito dentro de un archivo ejecutable y se replica en otros programas durante la ejecución.

Los genéricos acechan al sistema esperando que se satisfaga alguna condición (fecha del sistema o número de archivos en un disco). Cuando esta condición "catalizadora" se presenta, el virus inicia su rutina de destrucción.

Virus mutante: En general se comporta igual que el virus genérico, pero en lugar de replicarse exactamente, genera copias modificadas de sí mismo.

Virus recombinables: Se unen, intercambian sus códigos y crean nuevos virus.

Virus "Bounty Hunter" (caza-recompensas): Están diseñados para atacar un producto antivirus particular.

Virus específicos para redes: Coleccionan contraseñas de acceso a la red, para luego reproducirse y dispersar sus rutinas destructivas en todos los ordenadores conectados.

Virus de sector de arranque: Se alojan en la sección del disco cuyas instrucciones se cargan en memoria al inicializar el sistema. El virus alcanza la memoria antes que otros programas sean cargados e infecta cada nuevo disquete que se coloque en la unidad.

Virus de macro: Se diseñan para infectar las macros que acompañan a una aplicación específica.

Una macro es un conjunto de instrucciones que ejecutan una tarea particular, activada por alguna aplicación específica como MS –Word o MS –Excel.

Son virus muy fáciles de programar y se dispersan rápidamente a través de anexos a e-mail, copia de archivos usando disquetes, etc.

Virus de Internet: Se alojan en el código subyacente de las páginas web. Cuando el usuario accede a esos sitios en Internet, el virus se descarga y ejecuta en su sistema, pudiendo modificar o destruir la información almacenada.

Son de rápida y fácil dispersión, puesto que se alojan y viajan en un medio de acceso multitudinario: Internet.

Factores humanos de riesgo

Hackers

Los hackers son personas con avanzados conocimientos técnicos en el área informática y que enfocan sus habilidades hacia la invasión de sistemas a los que no tienen acceso autorizado.

En general, los hackers persiguen dos objetivos: Probar que tienen las competencias para invadir un sistema protegido. Probar que la seguridad de un sistema tiene fallas.

Crackers

Los crackers son personas con avanzados conocimientos técnicos en el área informática y que enfocan sus habilidades hacia la invasión de sistemas a los que no tienen acceso autorizado.

En general, los crackers persiguen dos objetivos: Destruir parcial o totalmente el sistema. Obtener un beneficio personal (tangible o intangible) como consecuencia de sus actividades.

Mecanismos de Seguridad Informática

Conceptos

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático.

Existen muchos y variados mecanismos de seguridad informática. Su selección depende del tipo de sistema, de su función y de los factores de riesgo que lo amenazan.

Clasificación según su función

Preventivos: Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.

Detectivos: Actúan antes de que un hecho ocurra y su función es revelarla presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.

Correctivos: Actúan luego de ocurrido el hecho y su función es corregirlas consecuencias.

En conclusión

La seguridad de la informática es un tema de muy alto impacto en la realidad virtual y tecnológica del mundo, ya que, así como se desarrollan software para el beneficio y facilidad de algunas actividades, también se crean software que su fin es robar información de manera desautorizada a diferentes entidades, empresas hasta usuarios individuales.

Links:

https://grupo4herramientasinformatica.blogspot.com/2016/03/la-seguridad-informatica.html

https://rentadvisor.com.co/seguridad-informatica-caracteristicas/

https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

https://es.slideshare.net/yamyortiz17/seguridad-informatica-7915096

tecnología de la información código de buenas practicas para la gestión de la seguridad de la información

objeto y campo de aplicación

esta norma ofrece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener y mejorar la seguridad en una organización . persigue proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una practica eficaz de la gestión de la seguridad.

La norma puede servir como una guía practica para desarrollar estándares organizacionales de seguridad y practicas efectivas de la gestión de la seguridad . igualmente, permite proporcionar confianza en las relaciones entre organizaciones. Las recomendaciones que se establecen esta norma deberían elegirse y utilizarse de acuerdo con la lesgilacion aplicable en la materia.

Términos y definiciones

Para los fines de esta norma son de aplicación las definiciones siguientes:

Activo: algo que tenga valor para la organización.

Control: herramienta de la gestión, incluido políticas, pautas, estructuras organizacionales, que pueden ser de manera administrativa, técnica, gerencial o legal.

Pauta: descripción que aclara que es lo que se debe hacer y como se hace, con el fin de alcanzar los objetivos planteados en las políticas.

Instalaciones de proceso de información: sistemas de información, servicio o infraestructura, o locaciones físicas que los almacena.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas.

Evento de seguridad de información: es una ocurrencia identificada de un sistema, servicio, o red, el cual indica una posible brecha de la política de seguridad de información o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad.

Incidente de seguridad de información: es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de la información.

Política: dirección general y formal expresada por la gerencia.

Riesgo: combinación de la probabilidad de un evento y sus consecuencias.

Análisis del riesgo: uso sistematico de la información para identificar fuentes y estimar el riesgo.

Evaluación del riesgo: proceso general de análisis y evaluación del riesgo.

Valoración del riesgo: proceso de comparación del riesgo estimado contra el criterio del riesgo dado para determinar el significado de este.

Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización considerando el riesgo.

Tratamiento del riesgo: proceso de selección e implementación de medidas para modificar el riesgo.

Terceros: persona que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión.

Amenaza: causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.

Vulnerabilidad: debilidad de un activo o grupo de activos que pueden ser explotados por una o mas amenazas.

Estructura de este estándar

Clausulas

Cada clausula contiene un numero de categorías de seguridad. Las 11 clausulas (acompañadas por el numero de categorías principales de seguridad incluidas en cada clausula) son:

A) Política de seguridad(1);
B) Organizando la seguridad de información(2);
C) Gestión de activos(2);
D) Seguridad en recursos humanos(3);
E) Seguridad física y ambiental(2);
F) Gestión de comunicaciones y operaciones(10);
G) Control de acceso(7);
H) Adquisición, desarrollo y mantenimiento de sistemas de información(6);
I) Gestión de incidentes de los sistemas de información(2);
J) Gestión de continuidad del negocio(1);
K) Cumplimiento(3);

Categorías principales de seguridad

Cada categoría principal de seguridad contiene:

a) Un objeto de control declarando lo que se debe alcanzar.
b) Uno o mas controles que pueden ser aplicados para alcanzar el objetivo de control.

Las descripciones del control son estructuradas de la siguiente manera:

Control

Define específicamente la declaración de control para satisfacer el objetivo de control.

Guía de implementación

Provee información mas detallada para apoyar la implementación del control y conocer el objetivo de control. Algunas guias pueden ser no convenientes para todos los casos, por lo tanto algunas otras formas de implementar el control pueden ser mas apropiadas.

Evaluación y tratamiento del riesgo

Evaluando los riesgos de seguridad

La evaluación de riesgos debe identificar, cuantificar y priorizar riesgos contra el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados deben guiar y determinar la apropiada acción de gestión y las prioridades para manejar la información de los riesgos de seguridad y para implementar controles seleccionados para proteger estos riesgos. El proceso de evaluación de riesgos y de seleccionar controles puede requerir que sea realizado un numero de veces con el fin de cubrir diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debe incluir un alcance sistematico sobre la estimación de la magnitud del riesgo (análisis del riesgo) y sobre el proceso de comparar el riesgo estimado con el criterio para determinar el significado de los riesgos (valoración del riesgo).

Las evaluaciones del riesgo deben ser analizadas periódicamente para incluir los cambios en los requerimientos del sistema y en la situación del riesgo, por ejemplo en los activos, amenazas, vulnerabilidades, impactos, valoración del riesgo y cuando los cambios significativos ocurran. Estas evaluaciones del riesgo deben ser emprendidas de una forma metódica, capaz de producir resultados comparables y reproducirlos.

Tratando riesgos de seguridad

Tratamiento de riesgo de la organización debe decidir el criterio para determinar si es que los riesgos son aceptados o no. Los riesgos pueden ser aceptados si, por ejemplo se evalúa que el riesgo es menor o que el costo de tratarlo no es rentable para la organización. Estas decisiones deben ser grabadas.

Para cada uno de los riesgos identificados, siguiendo la evaluación del riesgo, se necesita realizar una decisión del tratamiento del riesgo. Posibles opciones para el tratamiento del riesgo incluye:

a) Aplicar controles apropiados para reducir riesgos.
b) Riesgos aceptados objetivamente y con conocimiento satisfaciendo claramente el criterio para la aceptación del riesgo y la política de la organización.
c) Evitar riesgos no permitiendo realizar acciones que puedan causar que estos riesgos ocurran.
d) Transferir los riesgos asociados a terceros como son los proveedores y asegurados.

Política de seguridad

Objetivo: dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones.

Documento de política de seguridad de la información

Control: la gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.

Guía de implentacion

Debería establecer el compromiso de la gerencia y el enfoque de la organización para gestionar la seguridad de la información. El documento debería contener como minimo la siguiente informacion:

a) Una definición de seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permite compartir la información.
b) El establecimiento del objetivo de la gerencia como soporte de los objetivos y principios de la seguridad de la información.
c) Un marco para poder colocar los objetivos de control y mandos, incluyendo la estructura de evaluación de riesgo y gestión del riesgo.
d) Una breve explicación de las políticas, principios, normas y requisitos de conformidad mas importantes para la organización, por ejemplo:

    1. Conformidad con los requisitos legislativos y contractuales.
    2. Requisitos de formación en seguridad.
    3. Gestión de la continuidad del negocio.
    4. Consecuencias de las violaciones de la política de seguridad.

Revisión y evaluación

Control:

Política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo y efectividad.

Guía de implementación:

La política debería tener un propietario que sea del desarrollo, revisión y evaluación de la política de seguridad. La revisión debe incluir oportunidades de evaluación para mejorar la política de seguridad de información de la organización y un acercamiento a la gestión de seguridad de información de información en respuesta a los cambios en el ambiente técnico.

La revisión de la política de seguridad de información debe tener en cuenta los resultados de las revisiones de la gestión. Deben existir procedimientos definidos de la gestión de la revisión.

Aspectos organizativos para la seguridad

Organización interna

Objetivo: gestionar la seguridad de la información dentro de la organización.

Debe establecer una estructura de gestión para iniciar y controlar la implantación de la seguridad de la información dentro de la organización.

Es conveniente organizar foros de gestión adecuados con las gerencias para aprobar la política de seguridad de la información, asignar roles de seguridad y coordinar la implantación de la seguridad en toda la organización.