ESTÁNDAR DE SEGURIDAD

"GLOSARIO TÉRMINOS DE SSI-MTT"

Est-SSI-05 v1.0

Subsecretaría de Transportes

Gobierno de Chile

SUBSECRETARÍA DE TRANSPORTES

Noviembre 2017

	Nombre	Cargo	Firma	Fecha
Aprobado por	Matías Schöll	Presidente Comité Seguridad de la Información		27 - 11 - 2017
Elaborado por	Roy Mac Kenney	Encargado de Seguridad de la Información		23/11/2017

Nota de equidad de género:

El uso de un lenguaje que no discrimine ni marque diferencias entre hombres y mujeres ha sido una preocupación en la elaboración de este documento. Sin embargo, y con el fin de evitar la sobrecarga gráfica que supondría utilizar en español o/a para marcar la existencia de ambos sexos, se ha optado por utilizar el masculino genérico, en el entendido de que todas las menciones en tal género representan siempre a todos/as, hombre y mujeres, abarcando claramente ambos sexos.

GLOSARIO DE TÉRMINOS, SIGLAS Y DEFINICIONES

Todas las definiciones generales y glosario de términos utilizados en los documentos del Sistema de Gestión de Seguridad de la Información se encuentran integrados en este Estándar de Seguridad "Glosario de Términos de SSI-MTT", el que se mantendrá publicado en la sección "Seguridad de la Información" de la Intranet institucional.

Acción correctiva: (inglés: Corrective action). Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Acción preventiva: (inglés: Preventive action). Medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.

Aceptación del riesgo: (inglés: Risk acceptance). Decisión informada de asumir un riesgo concreto.

Activo: (inglés: Asset). 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. Véase además Activo de Información.

Activos de Información: Todos aquellos personas y elementos que contienen o manipulan información de valor para la institución. También son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la SISS. Los niveles de los activos de información consideran:

- La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.).
- Los Equipos / Sistemas / Infraestructura que soportan esta información.
- Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

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

Administración de Riesgos: Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los activos información.

Amenaza: (inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. 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).

Análisis de riesgos: (inglés: Risk analysis). Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo: (inglés: Qualitative risk analysis). Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la

probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: (inglés: Quantitative risk analysis). Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

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.

Área segura: Áreas que han sido designada de acceso restringido. Puede ser una oficina cerrada con llave, o varias salas en el interior del perímetro de seguridad física, que pueden ser cerradas con llaves.

Asset: Véase: Activo.

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.

Auditor: (inglés: Auditor). Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.

Auditoría: (inglés: Audit). Proceso sistemático, independiente y documentado para obtener evidencias de auditoriía y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autenticación: (inglés: Authentication). Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad: (inglés: Authenticity). Propiedad de que una entidad es lo que afirma ser.

Availability: Véase: Disponibilidad.

BIA: Elemento utilizado para estimar la afectación que podría padecer una organización como resultado de la ocurrencia de algún incidente o un desastre. Un primer objetivo consiste en proveer una base para identificar los procesos críticos para la operación de la institución, el segundo se refiere a la priorización de ese conjunto de procesos, siguiendo criterios de impacto al "negocio". Luego debe entregar los requerimientos de RTO y RPO para el tiempo de recuperación y potencial pérdida de datos no respaldados.

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 (bot net).

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.

BS 7799: Norma británica de seguridad de la información, publicada por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera era un conjunto de buenas prácticas para la gestión de la seguridad de la información -no certificable- y la parte segunda especificaba el sistema de gestión de seguridad de la información -certificable-. La parte primera es el origen de ISO 17799 e ISO 27002 y la parte segunda de ISO 27001. Como tal estándar, ha sido derogado ya, por la aparición de éstos últimos.

BSI: British Standards Institution, la entidad de normalización del Reino Unido, responsable en su día de la publicación de la norma BS 7799, origen de ISO 27001. Su función como entidad de normalización es comparable a la de INN en Chile.

Business Continuity Plan: Véase: Plan de Continuidad del Negocio.

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.

CIA: Acrónimo inglés de Confidentiality, Integrity y Availability, las dimensiones o principios básicos de seguridad de la información.

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.

CID: Confiabilidad, Integridad y Disponibilidad. Ver CIA

Clúster: Corresponde a un conjunto de computadores que están unidos entre ellos comportándose como si fuesen un solo equipo.

CobiT: Control Objectives for Information and related Technology. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacional y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Confidencialidad: (inglés: Confidentiality). Es la necesidad de que la información esté en poder de quien corresponda para el desarrollo de las funciones respectivas, con la oportunidad e integridad requerida. Es una propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Contramedida: (inglés: Countermeasure). Véase: Controles.

Controles: Medidas para mitigar el riesgo, incluyendo políticas, procedimientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. Son concebidos para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Control correctivo: (inglés: Corrective control). Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo: (inglés: Detective control). Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasivo: (inglés: Deterrent control). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

Control preventivo: (inglés: Preventive control). Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Corrección: (inglés: Correction). Acción para eliminar una no conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.

Data Center: Es una instalación empleada para albergar los sistemas de información y sus componentes asociados, como las telecomunicaciones y los sistemas de almacenamiento.

Declaración de aplicabilidad: (inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

DEMING: Ciclo DMING: PDCA; Ver Gestión de Mejora Continua.

Desastre: (inglés: Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva o directriz: (inglés: Guideline). Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: (inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. Es asegurar que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Dueño o responsable de la Información: Es la persona que ha sido asignada como responsable de la integridad, confidencialidad y disponibilidad del activo de información.

Elemento Tecnológico: Cualquier dispositivo de hardware / software.

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.

Escenarios de Continuidad: Asociado a los escenarios base de continuidad de negocios, respecto a la indisponibilidad de recursos críticos, como personal, instalaciones, tecnología o proveedores. Se les llama comúnmente los 4 escenarios "Sin": Sin Personal Crítico, Sin Instalaciones, Sin Tecnología, Sin Proveedores; más un quinto para cualquier otro escenario que genere crisis en la institución, no necesariamente producto de los cuatro anteriores.

Estimación de riesgos: (inglés: Risk evaluation). Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

Estrategias de Recuperación y Restauración: Corresponde a la o las estrategias de recuperación y restauración que la institución haya establecido para enfrentar cada uno de los escenarios planteados y que satisfacen los requerimientos de RTO, RPO y priorización señalado por el BIA.

Evaluación de Riesgos: (inglés: Risk assessment). Proceso global de identificación, análisis y estimación de riesgos. Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, con análisis de probabilidad de que ocurran y su potencial impacto en la operatoria de la SISS.

Evento de Seguridad de la Información: Ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las medidas de protección, o una situación previamente desconocida que puede ser relevante para la seguridad.

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.

Gestión de claves: (inglés: Key management). Controles referidos a la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información: (inglés: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de Mejora Continua: Modelo que permite acercarse a la optimización y resiliencia de un proceso dado. Uno de los más utilizados es Deming, o PDCA (Plan; Do; Check; Act).

Gestión de riesgos: (inglés: Risk management). Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos. Es un conjunto de actividades coordinadas para mitigar amenazas utilizando recursos y estrategias.

Gusanos: Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, lo que contrasta con los virus, puesto que requieren la propagación de un archivo anfitrión infectado.

Hardware: Son los computadores personales, Servidores, equipos de comunicaciones, incluyendo pantalla, teclado, mouse, unidad central (cpu), Teléfono Celular, unidad de CD/DVD (externa o interna), PDA, Routers, switches, lector de banda, impresoras, scanners, teléfonos, fax y cables.

ID de usuario: Se refiere al identificador único de un usuario.

Identificación de riesgos: (inglés: Risk identification). Proceso de encontrar, reconocer y describir riesgos.

IDS: Sistema de Detección de Intrusos (en inglés - Intrusion Detection System).

Impacto: (inglés: Impact). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.-.

Incidente de Seguridad de la Información: (inglés: Information security incident). Un incidente de seguridad es uno o varios eventos de seguridad de la información, no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de afectar la disponibilidad, integridad o confidencialidad de los activos de información y que por tanto su existencia ha sido declarada como Incidente de Seguridad de la Información.

Información: Es un activo que, como otros activos importantes del negocio, es esencial para una organización y requiere en consecuencia una protección adecuada.

Information Security Management System (ISMS): Véase: Sistema de Gestión de Seguridad de la Información (SGSI).

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.

Integridad: (inglés: Integrity). Uno de las propiedades de la Información, parte de la Triada CIA. Asegurar que la información y sus métodos de procesos son exactos y completos.

Inventario de activos: (inglés: Assets inventory). Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IRCA: International Register of Certified Auditors. Acredita a los auditores de diversas normas, entre ellas ISO 27001.

ISACA: Information Systems Audit and Control Association. Publica CobiT y gestiona diversas acreditaciones personales en el ámbito de la auditoría de sistemas y la seguridad de la información.

ISC2: Information Systems Security Certification Consortium, Inc. Organización sin ánimo de lucro que gestiona diversas acreditaciones personales en el ámbito de la seguridad de la información, como CISSP.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

ISO/IEC 27001: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial. Su homologación chilena por INN, es Nch-ISO 27001:2013.

ISO/IEC 27002: Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable. Su homologación chilena por INN, es Nch-ISO 27002:2013.

ITIL: IT Infrastructure Library. Un marco de gestión de los servicios de tecnologías de la información.

ITSEC: Criterios de evaluación de la seguridad de la tecnología de información. Se trata de criterios unificados adoptados por Francia, Alemania, Holanda y el Reino Unido. También cuentan con el respaldo de la Comisión Europea (véase también TCSEC, el equivalente de EEUU).

Malware: Es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. 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 fechorías.

Medios de procesamiento de la información: Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

Negación de servicio (DoS): La negación de servicio es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o lugar en una 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.

Networking: Concepto utilizado para referirse a actividades de configuración y administración redes informáticas, switch, routers y relacionados.

No conformidad: (inglés: Nonconformity). Incumplimiento de un requisito.

No repudio: Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

PDCA: Ciclo Deming. Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.

Perímetro de Seguridad Física: Se logra estableciendo barreras alrededor de las instalaciones del negocio, por ejemplo, una pared o una puerta de entrada controlada o una recepción atendida.

Personal Clave: Además del el coordinador de emergencias y los equipos directivo y operativo, se debe contemplar a los funcionarios que el equipo directivo defina como "clave" para el restablecimiento de las áreas críticas de la institución, lo que dependerá del nivel de contingencia.

Phishing: A diferencia de la heurística o los exploradores de huella digital, el software de seguridad de bloqueo de comportamiento se integra al sistema operativo de un equipo anfitrión y supervisa el comportamiento de los programas en tiempo real en busca de acciones maliciosas. El software de bloqueo de comportamiento bloquea acciones potencialmente dañinas, antes de que tengan oportunidad de afectar el sistema. La protección contra el comportamiento peligroso debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Plan de Continuidad del Negocio (PCN): (inglés: Bussines Continuity Plan o BCP). Plan orientado a permitir la continuación de las principales funciones del negocio o procesos críticos en el caso de un evento imprevisto que los ponga en peligro.

Plan de tratamiento de riesgos: (inglés: Risk treatment plan). Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política: Intención y directriz general expresada formalmente por la autoridad máxima en la institución.

Procesos Relevantes: Los procesos claves son aquellos que se deben priorizar para el restablecimiento del funcionamiento de las áreas definidas como críticas y que son el corazón de La Institución y que componen la cadena del valor de la organización.

Propietario del riesgo: (inglés: Risk owner). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

RA: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

RA/BIA: Nemotécnico de Risk Assessment y Business Impact Analysis.

Registro (Log): Cada elemento de un sistema de información genera una serie de registros de eventos del tipo "Error", "Advertencia" e "Información".

Reglamento Interno: Procedimiento cuyo objetivo fundamental es preservar la salud e integridad física y mental del personal, así como los bienes de cada dependencia u oficina.

Riesgo: (inglés: Risk).

- Es la probabilidad de un evento con potencial perjuicio o daño.
- Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual: (inglés: Residual risk). El riesgo que permanece tras el tratamiento del riesgo.

RPO: Recovery Point Objective (RPO). Objetivo de punto de recuperación, define la pérdida de datos máxima tolerable que se acepta ante una situación de desastre, por no estar considerada en los mecanismos de respaldo convencionales.

RTO: Recovery Time Objective. El tiempo u objetivo de recuperación o RTO por sus siglas en inglés es el tiempo definido dentro del nivel de servicio en el que un proceso de negocio debe ser recuperado después de un desastre o pérdida para así evitar consecuencias debido a la ruptura de continuidad servicios críticos.

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. Una vez instalados, el atacante puede realizar prácticamente cualquier función en el sistema, incluyendo acceso remoto, intercepción de comunicaciones, así como procesos de ocultamiento, archivos, claves de registro y canales de comunicación.

Salvaguarda: (inglés: Safeguard). Véase: Control.

Segregación de tareas: (inglés: Segregation of duties). Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la Información: (inglés: Information security). Preservación de la confidencialidad, integridad y disponibilidad de la información. La seguridad de la información es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio y minimizar los daños, procurando la preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguridad de los Activos de Información: Es proteger, resguardar y asegurar la disponibilidad, privacidad, confidencialidad e integridad de los activos de información y tecnologías para su procesamiento a efecto de garantizar la continuidad operacional de la institución. Ver "Seguridad de la Información".

Selección de controles: (inglés: Control selection). Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: (inglés: ISMS). Véase: Sistema de Gestión de la Seguridad de la Información.

Sistema de Gestión de Seguridad de la Información (SGSI): (inglés: Information Security Management System). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua. Parte del sistema de gestión global, basada en un enfoque de riesgo de negocio; cuyo fin es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Sistema de Información: Un sistema de información (SI) es un conjunto de elementos de Hardware y Software orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior. Todos estos elementos interactúan para procesar los datos (incluidos los procesos manuales y automáticos) y dan lugar a información más elaborada.

SoA: Acrónimo inglés de Statement of Applicability. Véase: Declaración de aplicabilidad.

Software: Son los programas de aplicación, sistemas de información, Paginas o portales web, o aplicaciones, sistemas operativos y rutinas de comunicación o de uso general.

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: Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas. La información de identificación personal es la información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de personas no estaría dispuesta a compartir con nadie e incluye datos bancarios, números de cuentas de tarjeta de crédito y contraseñas. Los receptores de esta información pueden ser sistemas o partes remotas con acceso local.

SSI: Sistema de Seguridad de la Información. Véase Sistema de Gestión de Seguridad de la Información

Storage: Corresponde al lugar físico donde se almacena la información.

Tratamiento de riesgos: (inglés: Risk treatment). Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad: (inglés: Accountability). Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Triada CIA: Ver CIA

UPS: Corresponde a una fuente de suministro eléctrico que posee una batería con el fin de seguir entregando energía a un dispositivo.

Vector de ataque: Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

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 (inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.