GLOSARIO

ADMINITRACIÓN DE LA CONFIGURACIÓN: El control de cambios realizados a un conjunto de componentes de la configuración a lo largo del ciclo de vida del sistema.

ADMINISTRACIÓN DEL DESEMPEÑO: La capacidad de administrar cualquier tipo de medición incluyendo mediciones de empleados, equipo, proceso, operativas o financieras. El término denota un control de ciclo cerrado y la vigilancia periódica de la medición.

ANÁLISIS DE CAUSA RAÍZ: Proceso de aprendizaje a partir de las consecuencias, típicamente de los errores y problemas.

ARQUITECTURA DE LA INFORMACIÓN: estructura de los datos.

ARQUITECTURA DE LAS TI.: Estructura o marco integrado para evolucionar o dar mantenimiento a la TI existente y adquirir nuevas tecnologías para alcanzar las metas estratégicas y de negocio de la empresa.

ARQUITECTURA EMPRESARIAL: Mapa de rutas tecnológicas orientado al negocio para el logro de las metas y objetivos del mismo.

ARQUITECTURA EMPRESARIAL PARA TI: Respuesta en la entrega de TI, provista por procesos claramente definidos usando sus recursos (aplicaciones, información, infraestructura y personas).

ATENCIÓN AL USUARIO: El único punto de contacto dentro de la organización de TI para usuarios de los servicios prestados por TI.

AUTENTICACIÓN: El acto de verificar la identidad de un usuario y su elegibilidad para acceder a la informaiñon computarizada. La autenticación está diseñada para proteger contra conexiones de acceso fraudulentas.

CAPACIDAD: Contar con los atributos necesarios para realizar o lograr lo planificado.

CEO:Director-Ejecutivo.(Chief-Executive-Officer)

CFO: Director Financiero.(Chief-Financial-Officer).

CIO: Director de Información.(Chief-Information-Officer).
"La terminología de negocios en América Latina varia un poco con la terminología anglosajona y la europea.

En el caso del CEO su traducción directa sería Jefe Ejecutivo, aunque en la práctica comercial se le denomina Gerente General o Presidente Ejecutivo en muchos casos.

Igual sucede para el CFO, cuya traducción se asemeja a un Gerente Financiero, Gerente De Finanzas o Presidente de Finanzas.

CIO vendría a ser Gerente de Informática o Sistemas, o Presidente de Informática Sistemas."

Acción correctiva

(Inglés: Corrective action). Medida de tipo reactivo orientada a eliminar la causa de una no-conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

Acción preventiva

(Inglés: Preventive action). Medida de tipo pro-activo orientada a prevenir potenciales no-conformidades asociadas a la implementación y operación del SGSI.

Accreditation body

Véase: Entidad de acreditación.

Aceptación del Riesgo

(Inglés: Risk acceptance). Según [ISO/IEC Guía 73:2002]: Decisión de aceptar un riesgo.

Activo

(Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 133351:2004]: Cualquier cosa que tiene valor para la organización.

Alcance

(Inglés: Scope). Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Alerta

(Inglés: Alert). Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza

(Inglés: Threat). Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos

(Inglés: Risk analysis). Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Análisis de riesgos cualitativo

(Inglés: Qualitative risk analysis). Análisis de riesgos en el que se usa una escala de puntuaciones para situar la gravedad del impacto.

Análisis de riesgos cuantitativo

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

Asset

Véase: Activo.

Assets inventory

Véase: Inventario de activos.

Audit

Véase: Auditoría.

Auditor

(Inglés: Auditor). Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditor de primera parte

(Inglés: First party auditor). Auditor interno que audita la organización en nombre de ella misma. En general, se hace como mantenimiento del sistema de gestión y como preparación a la auditoría de certificación.

Auditor de segunda parte

(Inglés: Second party auditor). Auditor de cliente, es decir, que audita una organización en nombre de un cliente de la misma. Por ejemplo, una empresa que audita a su proveedor de outsourcing.

Auditor de tercera parte

(Inglés: Third party auditor). Auditor independiente, es decir, que audita una organización como tercera parte independiente. Normalmente, porque la organización tiene la intención de lograr la certificación.

Auditor jefe

(Inglés: Lead auditor). Auditor responsable de asegurar la conducción y realización eficiente y efectiva de la auditoría, dentro del alcance y del plan de auditoría aprobado por el cliente.

Auditoría

(Inglés: Audit). Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación

(Inglés: Authentication). Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Authentication

Véase: Autenticación.

Availability

Véase: Disponibilidad.

B

BS7799

Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera

es un conjunto de buenas prácticas para la gestión de la seguridad de la información -no es certificable- y la parte segunda especifica el sistema de gestión de seguridad de la información -es 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 estos últimos.

BSI

British Standards Institution. Comparable al AENOR español, es la Organización que ha publicado la serie de normas BS 7799, además de otros varios miles de normas de muy diferentes ámbitos.

Biometria

La biometría es una tecnología basada en el reconocimiento de una característica de seguridad y en una física e intransferible de las personas, como por ejemplo la huella digital. Los sistemas biométricos incluyen un dispositivo de captación y un software que interpreta la muestra física y la transforma en una secuencia numérica. En el caso de la huella digital, en ningún caso se extrae la imagen de la huella, sino una secuencia de números que la representan. Sus aplicaciones abarcan un gran número de sectores: desde el acceso seguro a computadores, redes, protección de carpetas electrónicas, marcacion de horario y control de acceso físico a un area determinada. El rendimiento de una medida biométrica se define generalmente en términos de tasa de falso positivo (False Acceptance Rate o FAR), la tasa de falso negativo (False NonMatch Rate o FNMR), y el fallo de tasa de alistamiento (Failure-to-enroll Rate, FTR o FER).

Blog

Versión reducida del término "web log". Es información que un usuario publica de forma fácil e instantánea en un sitio web. Generalmente un blog se lee en orden cronológico. Es muy habitual que dispongan de una lista de enlaces a

otros weblogs (denominada blogroll) y suelen disponer de un sistema de comentarios que permiten a los lectores establecer una conversación con el autor y entre ellos acerca de lo publicado..

Business Continuity Plan

Véase: Plan de continuidad del negocio.

C

Carriers

Operadores de telecomunicaciones propietarios de las redes troncales de Internet y responsables del transporte de los datos. Proporciona una conexión a Internet de alto nivel.

Certificado Digital

Acreditación emitida por una entidad o un particular debidamente autorizada garantizando que un determinado dato (una firma electrónica o una clave pública) pertenece realmente a quien se supone.

- Código Fuente

En ingles Source Code. Conjunto de instrucciones que componen un programa, escrito en cualquier lenguaje. Hay programas de código abierto que se pueden modificar si uno tiene el conocimiento (por lo general estos programas estan bajo licencia GPL), por ejemplo Linux, Openoffice, etc. Hay programas "de código cerrado" como por ejemplo Windows, Photoshop, y la mayoría de los programas comerciales, en donde el código es inaccesible y por lo tanto no se puede alterar la estructura del programa. En estos casos uno compra el programa, el programa es de uno, pero el código fuente o instrucciones del programa son del fabricante.

Comercio Electrónico

En inglés e-commerce. Es la compra y venta de bienes y servicios realizado a través del internet, habitualmente con el soporte de plataformas y protocolos de seguridad estandarizados. Existen varias formas de hacer negocios por internet:

- ***e-commerce de Empresa a Cliente (B2C- business to costumer) Modalidad de comercio electrónico en la cual las operaciones comerciales se realizan entre una empresa y sus usuarios finales.***
- ***e-commerce de Empresa a Empresa (B2B - business to business) Modalidad de comercio electrónico en la cual las operaciones comerciales se realizan entre empresas (una empresa y sus proveedores) y no con usuarios finales.***
- ***e-commerce de Cliente a Cliente (C2C - costumer to costumer) Modalidad de comercio electrónico en la cual las operaciones comerciales se realizan entre clientes como, por ejemplo, los sitios donde se realizan subastas.***
- ***e-business - Negocio Electrónico***
  Cualquier tipo de actividad empresarial realizada a través de las Tecnologías de la Información y las Comunicaciones.

Certification body

Véase: Entidad de certificación.

Criptografía

Se dice que cualquier procedimiento es criptográfico si permite a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo, luego de haberlo descifrado.

CRM

Customer Relationship Management. Manejo de la Relación con el Consumidor. Sistema automatizado de información sobre clientes cuyo objetivo es que estos puedan ser atendidos de la manera más personalizada posible.

Internet es uno de los soportes tecnológicos más importantes en CRM, a la vez que uno de sus principales canales de comunicación con los clientes.

Denegación de Servicio

Incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar. Habitualmente, la pérdida del servicio supone la indisponibilidad de un determinado servicio de red, como el correo electrónico, o la pérdida temporal de toda la conectividad y todos los servicios de red. En los peores casos, por ejemplo, un sitio web accedido por millones de personas puede verse forzado temporalmente a cesar de operar. Un ataque de denegación de servicio puede también destruir programas y archivos de un sistema informático. Aunque normalmente es realizado de forma intencionada y maliciosa, este tipo de ataques puede también ocurrir de forma accidental algunas veces. Si bien no suele producirse robo de información estos ataques pueden costar mucho tiempo y dinero a la persona u organización afectada.

CIA (confidential, integrity and availability or available).

Acrónimo inglés de confidencialidad, integridad y disponibilidad, los parámetros básicos de la seguridad de la información.

CID

Acrónimo español de confidencialidad, integridad y disponibilidad, los parámetros básicos de la seguridad de la información.

CISA

Certified Information Systems Auditor. Es una acreditación ofrecida por ISACA.

CISM

Certified Information Systems Manager. Es una acreditación ofrecida por ISACA.

CISSP

Certified Information Systems Security Professional. Es una acreditación ofrecida por ISC2.

Checklist

Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Clear desk policy

Véase: Política de escritorio despejado.

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 controles de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas, administradores, usuarios especializados, encargados, dueños de los datos y auditores.

Compromiso de la Dirección

(Inglés: Management commitment). Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Confidencialidad

(Inglés: Confidenciality). Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Confidenciality

Véase: Confidencialidad.

Contramedida

(Inglés: Countermeasure). Véase: Control.

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Control correctivo

(Inglés: Corrective control). Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. 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 disuasorio

(Inglés: Deterrent control). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.

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.

Control selection

Véase: Selección de controles.

Corrective action

Véase: Acción correctiva.

Corrective control

Véase: Control correctivo.

COSO

Committee of Sponsoring Organizations of the Treadway Commission. Comité de Organizaciones Patrocinadoras de la Comisión Treadway. Se centra en el control interno, especialmente el financiero.

D

Qué es un "DATA WAREHOUSE"...???

Un data warehousing es un almacenamiento simple, completo y consistente de datos obtenidos desde una variedad de fuentes, disponibles para el usuario final de forma tal que puedan entenderlos y utilizarlos en el contexto de los negocios.

Y UN "DATA MINING"...???

Data Mining no es mucho mas que la idea de pensar que existe conocimiento oculto en los datos. Desde este punto de vista caulquir tecnica que ayude a extraer mas de sus datos es util, es decir las tecnicas data mining forman un grupo heterogeneo. A través de varios diferentes tecnicas son usadas para diferentes propositos

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- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

Sistema de Gestión de la Seguridad de la Información

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

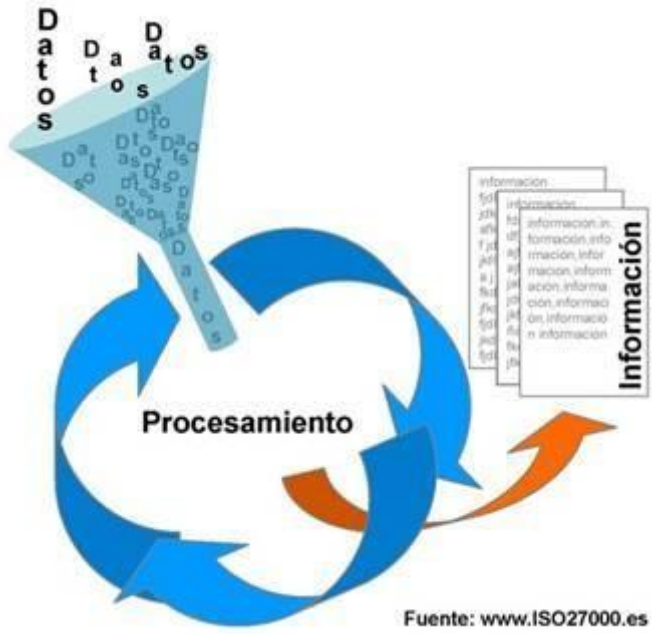
Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como la ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es imposible incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Qué es un SGSI?

SGSI es la abreviatura comúnmente utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS son las siglas equivalentes en el idioma inglés y en relación a *Information Security Management System*.

Por información se entiende toda aquella documentación en poder de una organización e independientemente de la forma en que se guarde o transmita (escrita, representada mediante diagramas o impresa en papel, almacenada electrónicamente, proyectada en imágenes, enviada por fax o correo, o, incluso, transmitida de forma oral en una conversación presencial o telefónica), de su origen (de la propia organización o de fuentes externas) y de la fecha de elaboración.



La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- *Confidencialidad: acceso a la información por parte únicamente de quienes estén autorizados.*
- *Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.*
- *Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.*

Datos Personales:

- Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

- Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

- Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

- Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

- Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

- Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

- Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

- Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

- Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

Delito Informático:

Según el ilustre penalista CUELLO CALON, los elementos integrantes del delito son:

El delito es un acto humano, es una acción (acción u omisión)

Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.

Debe corresponder a un tipo legal (figura de delito), definido por La Ley, ha de ser un acto típico.

El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.

La ejecución u omisión del acto debe estar sancionada por una pena.

Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que

cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por La Ley, que se realiza en el entorno informático y está sancionado con una pena.

Derecho:

" Para que exista el Derecho se necesita un mínimo de dos personas"

"El Derecho sólo ocurre en la vida social"

Los orígenes de la palabra Dº; en latín se decía IUS, en las lenguas romances se produjo la sustitución del término IUS por Dº, en latín vulgar se decía directum, que proviene de la palabra digiere, que significa gobernar, algunos sostienen que la influencia cristiana, que consideraba a la ley como el camino recto, esto explica la transformación en el idioma pero se conservaron las más intimas relacionadas con el IUS:

- *Iustittia: justicia; Iudex: Juez; Iudicare: juzgar; Iudicium: juicio, etc.*

En Roma imperial, el Dº es considerado como un conjunto de reglas o normas.

Acepciones de la palabra Dº.

- *Como ciencia o conocimiento: "el Dº es una ciencia cultural".*
- *Como ordenamiento o sistema normativo: "el Dº Chileno contempla fuertes sanciones para el aborto.*
- *Como facultad o poder: "el arrendador tiene el Dº a cobrar la renta".*
- *Como expresión de lo justo: "no hay Dº a que una persona sea tratada indignamente".*
- *Como sinónimo de deber jurídico: "cumple el Dº y paga la deuda".*

Hay quienes dicen que es un término equívoco estos se denominan analistas lógicos, dicen que la única manera de aclarar en que sentido se la usa es determinarlo según el contexto o circunstancia en que se emplea en concreto, otros dicen que es un

término análogo y son del movimiento el realismo Aristotélico-Tomista; Hay 2 tipos de Analogía:

1. *– Analogía de proporcionalidad: existen a lo menos 4 términos que se relacionan entre sí.*
2. *– Analogía de atribución: el vocablo se aplica a un objeto en particular que se llama analogado principal al cual le corresponde más propiamente la realidad significada, la que además se atribuye a otros objetos llamados analogados secundarios, por la relación que guardan con él, ya sea porque lo causan, manifiestan, expresan, o forman un efecto o consecuencia suya.*

La analogía propia del Dº es la de Atribución.

La pregunta ¿ Cuál es el analogado principal ? ha provocado los modelos de pensamientos:

- *Judicialista: El Dº stricto- sensu, es lo que aprueban o sería aprobable por los jueces.*

- *Subjetivista: Lo típico del Dº residiría en la facultad o potestad de actuar; o en el deber hacia otro.*

- *Realista: El Dº sería "la cosa misma debido a otro". No es el deber sino la cosa objeto del deber frente a un otro.*

Según este esquema, la norma, cualquiera sea su origen, es jurídica si crea, modifica, transmite o extingue un derecho, o sea, una cosa como "suya de alguien".

El aspecto más característico del Dº es el normativo, tanto el hombre común como al científico, lo jurídico se le aparece principalmente como un conjunto de normas, reglas de conducta.

NORMA JURÍDICA:

Es la ordenación justa de la conducta social, es pues una prescripción de la conducta humana determinada por una cierta norma, regla o medida y no de cualquier conducta sino de la Alteridad, esto es, referido a otro. El carácter de justo significa que tiene por objeto establecer "lo suyo de cada cual".

Si el analogado principal es la cosa misma que es debida a otro, la norma será jurídica porque dispone "lo que es debido". O sea por su contenido.

La cosa debida se colige que es susceptible de darse a otro efectivamente y este otro quedar satisfecho con tal acto y si así no fuere, poder exigir su cumplimiento incluso por la fuerza.

La norma jurídica tiene las características generales de toda norma (materia forma fines sanciones) pero adecuadas a ella, es también imperativa, bilateral, es coercible, atributiva, externa; tiene como 1er objetivo el pago o cumplimiento de la prestación y 2do el castigo del culpable.

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.

Detective control

Véase: Control detectivo.

Deterrent control

Véase: Control disuasorio.

Directiva

(Inglés: Guideline). Según [ISO/IEC 13335-1:2004]: una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disaster

Véase: Desastre.

Disponibilidad

(Inglés: Availability). Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de

permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

DRII

Instituto Internacional de Recuperación de Desastres.

DTI

Secretaría de Industria y Comercio del Reino Unido. Edita muchas guías prácticas en el ámbito de la seguridad de la información.

E

EDPAF

Fundación de Auditores del Procesamiento Electrónico de Datos(actualmente ISACF).

ENAC

Entidad Nacional de Acreditación. Es el organismo español de acreditación, auspiciado por la Administración, que acredita organismos que realizan actividades de evaluación de la conformidad, sea cual sea el sector en que desarrollen su actividad. Además de laboratorios, entidades de inspección, etc., también acredita a las entidades de certificación, que son las que a su vez certificarán a las empresas en las diversas normas.

Entidad de acreditación

(Inglés: Accreditation body). Un organismo oficial que acredita a las entidades certificadoras como aptas para certificar según diversas normas. Suele haber una por país. Son ejemplos de entidades de acreditación: ENAC (España), UKAS (Reino Unido), EMA (México), OAA (Argentina)...

Entidad de certificación

(Inglés: Certification body). Una empresa u organismo acreditado por una entidad de acreditación para auditar y certificar según diversas normas (ISO 27000, ISO 9000, ISO 14000, etc.) a empresas usuarias de sistemas de gestión.

ESF

Foro europeo de seguridad, en el que cooperan más de 70 multinacionales fundamentalmente europeas con el objeto de llevar a cabo investigaciones relativas a los problema comunes de seguridad y control en TI.

Evaluación de riesgos

(Inglés: Risk evaluation). Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento

(Inglés: information security event). Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva

(Inglés: Objective evidence). Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

F

Fase 1 de la auditoría

Fase en la que, fundamentalmente a través de la revisión de documentación, se analiza en SGSI en el contexto de la política de seguridad de la organización, sus objetivos, el alcance, la evaluación de riesgos, la declaración de aplicabilidad y los documentos principales, estableciendo un marco para planificar la fase 2.

Fase 2 de la auditoría

Fase en la que se comprueba que la organización se ajusta a sus propias políticas, objetivos y procedimientos, que el SGSI cumple con los requisitos de ISO 27001 y que está siendo efectivo.

First party auditor

Véase: Auditor de primera parte.

G

Gestión de claves

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

Gestión de riesgos

(Inglés: Risk management). Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Guideline

Véase: Directiva.

H

IEC

International Electrotechnical Commission. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.

IIA

Instituto de Auditores Internos.

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-.

Impact

Véase: Impacto.

Incidente

Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Information processing facilities

Véase: Servicios de tratamiento de información.

Information security

Véase: Seguridad de la información.

INFOSEC

Comité asesor en asuntos relativos a la seguridad de TI de la Comisión Europea.

Integridad

(Inglés: Integrity). Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Integrity

Véase: Integridad.

Inventario de activos

(Inglés: Assets inventory). Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, 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.

2021

ISACA

Information Systems Audit and Control Association. Publica CobiT y emite diversas acreditaciones en el ámbito de la seguridad de la información.

ISACF

Fundación de Auditoría y Control de Sistemas de Información.

ISC2

Information Systems Security Certification Consortium, Inc. Organización sin ánimo de lucro que emite diversas acreditaciones en el ámbito de la seguridad de la información.

ISO

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

ISO 17799

Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable.

ISO 19011

"Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

2021

ISO 27001

Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005

ISO 27002

Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio de oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007.

ISO 9000

Normas de gestión y garantía de calidad definidas por la ISO.

ISO 9000-3

Ingeniería del Software……???

ISO/IEC TR 13335-3

"Information technology . Guidelines for the management of IT Security .Techniques for the management of IT Security." Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.

ISO/IEC TR 18044

„Information technology . Security techniques . Information security incident management" Guía de utilidad para la gestión de incidentes de seguridad de la información.

ISSA

Information Systems Security Association.

NBS

Oficina Nacional de Normas de los EE.UU.

NIST

(ex NBS) Instituto Nacional de Normas y Tecnología, con sede en Washington, D.C.

No conformidad

(Inglés: Nonconformity). Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave

(Inglés: Major nonconformity). Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

Nonconformity

Véase: No conformidad.

O

Objective evidence

Véase: Evidencia objetiva.

Objetivo

(Inglés: Objetive). Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

OCDE

Organización de Cooperación y Desarrollo Económico. Tiene publicadas unas guías para la seguridad de la información.

P

PDCA

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).

Plan de continuidad del negocio

(Inglés: Bussines Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos

(Inglés: Risk treatment plan). Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad

(Inglés: Security policy). Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

Política de escritorio despejado

(Inglés: Clear desk policy). La política de la empresa que indica a los empleados que deben dejar su escritorio libre de cualquier tipo de informaciones susceptibles de mal uso al finalizar el día.

Preventive action

Véase: Acción preventiva.

Preventive control

Véase: Control preventivo.

Q

Qualitative risk analysis

Véase: Análisis de riesgos cualitativo.

Quantitative risk analysis

Véase: Análisis de riesgos cuantitativo.

R

Residual Risk

Véase: Riesgo Residual.

Riesgo

(Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual

(Inglés: Residual Risk). Según [ISO/IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

Risk

Véase: Riesgo.

Risk acceptance

Véase: Aceptación del riesgo.

Risk analysis

Véase: Análisis de riesgos.

Risk assessment

Véase: Valoración de riesgos.

Risk evaluation

Véase: Evaluación de riesgos.

Risk management

Véase: Gestión de riesgos.

Risk treatment

Véase: Tratamiento de riesgos.

Risk treatment plan

Véase: Plan de tratamiento de riesgos.

S

Sarbanes-Oxley

Ley de Reforma de la Contabilidad de Compañías Públicas y Protección de los Inversores aplicada en EEUU desde 2002. Crea un consejo de supervisión independiente para supervisar a los auditores de compañías públicas y le permite a este consejo establecer normas de contabilidad así como investigar y disciplinar a los contables. También obliga a los responsables de las empresas a garantizar la seguridad de la información financiera.

Scope

Véase: Alcance.

Security Policy

Véase: Política de seguridad.

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.

Segregation of duties

Véase: Segregación de tareas.

Seguridad de la información

Según [ISO/IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Selección de controles

Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SISTEMAS DE INFORMACIÓN!!!

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

El equipo computacional: el hardware necesario para que el sistema de información pueda operar.

El recurso humano que interactúa con el Sistema de Información, el cual está formado por las personas que utilizan el sistema.

Un sistema de información realiza cuatro actividades básicas: entrada, almacenamiento, procesamiento y salida de información.

SGSI

(Inglés: ISMS). Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Servicios de tratamiento de información

(Inglés: Information processing facilities). Según [ISO/IEC 27002:2005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

Sistema de Gestión de la Seguridad de la Información

(Inglés: Information Systems Management System). Ver SGSI.

SOA

Statement of Applicability. Véase: Declaración de aplicabilidad.

SSCP

Systems Security Certified Practitioner. Una acreditación de ISC2.

Statement of Applicability

Véase: Declaración de aplicabilidad.

T

TCSEC

Criterios de evaluación de la seguridad de los sistemas de computación, conocidos también con el nombre de Orange Book (Libro naranja), definidos originalmente por el Ministerio de Defensa de los EE.UU. Véase también ITSEC, el equivalente europeo.

Threat

Véase: Amenaza.

TickIT

Guía para la Construcción y Certificación del Sistema de Administración de Calidad del Software.

Tratamiento de riesgos

(Inglés: Risk treatment). Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

TECNOLOGÍAS DE LA INFORMACIÓN – TI

O.....La Tecnología Informática (IT), según lo definido por la asociación de la Tecnología Informática de América (ITAA) es "el estudio, diseño, desarrollo, puesta en práctica, ayuda o gerencia de los sistemas informáticos computarizados, particularmente usos del software y hardware." En fin, se ocupa del uso de computadoras y del software electrónico de convertir, de almacenar, de proteger, de procesar, de transmitir y de recuperar la información.

Y LAS TIC´S...???

Las tecnologías de la información y la comunicación (TIC) -la unión de los computadores y las comunicaciones- desataron una explosión sin precedentes de formas de comunicarse al comienzo de los años '90. A partir de ahí, la Internet pasó de ser un instrumento especializado de la

comunidad científica a ser una red de fácil uso que modificó las pautas de interacción social.

Por **Tecnologías de la información** o **Tecnologías de la información y de la comunicación** (TIC) se entiende un termino dilatado empleado para designar lo relativo a la informática conectada a Internet, y especialmente el aspecto social de éstos. Ya que Las nuevas tecnologías de la información y comunicación designan a la vez un conjunto de innovaciones tecnológicas pero también las herramientas que permiten una redefinición radical del funcionamiento de la sociedad; Un buen ejemplo de la influencia de los TIC sobre la sociedad es el gobierno electrónico.

En resumen las nuevas tecnologías de la Información y Comunicación son aquellas herramientas computacionales e informáticas que procesan, almacenan, sintetizan, recuperan y presentan información representada de la más variada forma. Es un conjunto de herramientas, soportes y canales para el tratamiento y acceso a la información. Constituyen nuevos soportes y canales para dar forma, registrar, almacenar y difundir contenidos informacionales. Algunos ejemplos de estas tecnologías son la pizarra digital (ordenador personal + proyector multimedia), los blogs, por supuesto, la web.

Para todo tipo de aplicaciones educativas, las TIC son medios y no fines. Es decir, son herramientas y materiales de construcción que facilitan el aprendizaje, el desarrollo de habilidades y distintas formas de aprender, estilos y ritmos de los aprendices.

U

UNE 71502

Norma española de ámbito local como versión adaptada de BS7799-2 (actual ISO 27001), que también guarda relación con UNEISO/IEC17799 mediante su Anexo A.

V

Valoración de riesgos

(Inglés: Risk assessment). Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidad

(Inglés: Vulnerability). Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

Vulnerability

Véase: Vulnerabilidad.

W

WG1, WG2, WG3, WG4, WG5

WorkGroup 1, 2, 3, 4, 5. Grupos de trabajo del subcomité SC27 de JTC1 (Joint Technical Committee) de ISO e IEC. Estos grupos de trabajo se encargan del desarrollo de los estándares relacionados con técnicas de seguridad de la información.