Unidad 1 / Escenario 2

Lectura fundamental

Los principios de la seguridad de la información: eje de estudio en el análisis de riesgos

Contenido

Palabras clave: disponibilidad, integridad, confidencialidad, riesgo, ataque informático.

1. Introducción

En el Escenario anterior, determinamos conceptos claves en torno a la seguridad de la información, desde el desglose del término y las diferencias con respecto a la seguridad informática hasta las referencias internacionales y herramientas que utilizan dichas referencias para la gestión de la seguridad de la información.

En este capítulo ampliaremos algunos conceptos fundamentales que son pilares para los diferentes roles que se pueden ejercer en el ambiente de la seguridad de la información y que son la base de toda la especialización.

2. Activos

Como hemos mencionado, la información es todo aquello que genera valor para una organización. Ese valor se ve representado en elementos tangibles o intangibles denominados activos. Decimos que son tangibles o intangibles porque contamos con evidencia real de su existencia. Por ejemplo, el conocimiento o *know how* tiene gran importancia para las organizaciones. Sin embargo, es un elemento intangible, que debe ser considerado dentro de la identificación de activos:

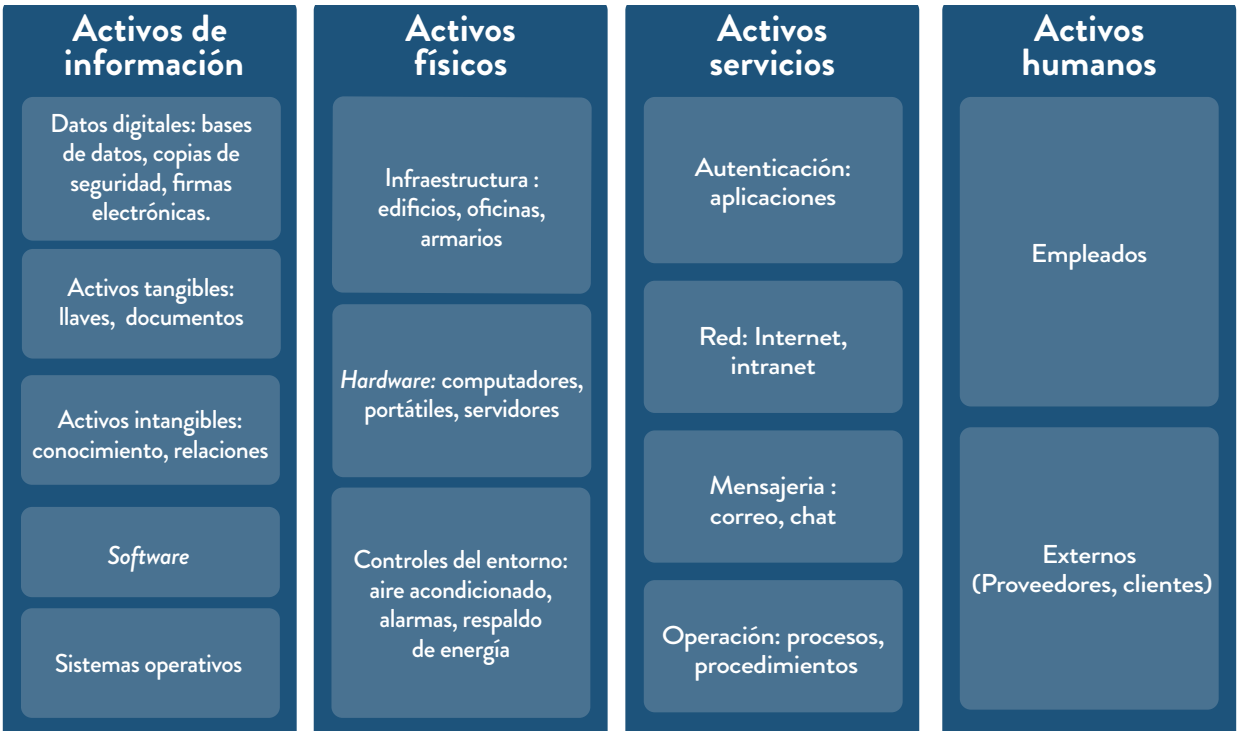

Figura 1. Ejemplo de clasificación de activos según su naturaleza

Fuente: elaboración propia

Los activos se clasifican de acuerdo con el tipo de almacenamiento, los componentes que utilizan, etc. La clasificación de estos dependerá de la organización y las referencias que utilice para su identificación. En la figura 1 se muestra un ejemplo de clasificación de activos.

Una vez identificados los activos, deben clasificarse utilizando el proceso elegido por la organización. Primero se define el tipo de activo: información, físico, servicios de TI, humanos. Esta no es la única clasificación, pero es la propuesta en el curso y la cual se tomará como referencia para la explicación.

Luego se realiza la ponderación (clasificación cualitativa y cuantitativa) para validar el grado de importancia del activo dentro de la organización. Pueden existir diferentes clasificaciones que expresan un nivel de importancia definido por la empresa: escalas del 1 al 5, como se muestra en la tabla 1, y del 1 al 3, como se muestra en la tabla 2, que se constituyen en las escalas de preferencia. Es importante que la descripción exprese realmente el valor del activo para la empresa con el fin de facilitar su identificación, puesto que dicho proceso lo realizará el encargado o dueño del activo.

Si en una misma tabla de identificación de activos incluimos una clasificación según su naturaleza y su valor, contamos con una descripción completa del activo, como se muestra en la tabla 3. Pueden existir más clasificaciones, como áreas de operación del activo, costo etc. y de acuerdo con dichas clasificaciones la definición del nivel varía. Para las tablas de los ejemplos, la consideración de valor se ha definido respecto a la operación de la empresa, es decir, qué tanto esta requiere dicho activo para operar.

Tabla 1. Clasificación de activos escala 1 a 5

Nivel	Descripción
5	Extremadamente importante: el activo es de suma importancia para la operación de toda la organización, la cual no puede operar si no está disponible.
4	Altamente importante: el activo es muy importante para áreas misionales en la organización. Estas áreas no pueden operar si no está disponible.
3	Importante: el activo es muy importante para áreas de apoyo dentro de la organización. Estas áreas no pueden operar si no está disponible.
2	Medianamente importante: el activo es importante para la organización; sin embargo, puede operar sin él durante un tiempo corto.
1	Mínimamente importante: el activo es importante para la organización; sin embargo, puede operar sin él durante un tiempo relativamente prolongado.

Fuente: elaboración propia

Tabla 2. Clasificación de activos escala 1 a 3

Nivel	Descripción
3	Altamente importante: el activo es de suma importancia para la operación de toda la organización. Esta no puede operar si no está disponible.
2	Medianamente importante: el activo es importante para la organización; sin embargo, puede operar sin él durante un tiempo corto.
1	Mínimamente importante: el activo es importante para la organización; sin embargo, puede operar sin él durante un tiempo relativamente prolongado.

Fuente: elaboración propia

Tabla 3. Clasificación completa del activo

Clase de activo	Entorno de TI global	Nombre del activo	Clasificación del activo	Ponderación
Tangible	Infraestructura física	Centro de datos	Extremadamente Importante	5
Tangible	Infraestructura física	Servidores	Extremadamente Importante	5
Tangible	Infraestructura física	Equipos de escritorio	Importante	3
Tangible	Infraestructura física	Equipos portátiles	Medianamente Importante	2
Tangible	Infraestructura física	Celulares	Medianamente Importante	2
Tangible	Infraestructura física	*Routers*	Extremadamente Importante	5
Tangible	Infraestructura física	*Switches*	Extremadamente Importante	5
Tangible	Infraestructura física	Medios extraíbles (por ejemplo, cintas, CD-ROM, DVD, discos duros, portátiles, dispositivos de almacenamiento PC Card, dispositivos de almacenamiento USB, etc.)	Altamente importante	4
Tangible	Reputación		Importante	3
Tangible	Buena voluntad		Importante	3
Tangible	Moral de empleados		Importante	3
Tangible	Productividad de empleados		Extremadamente Importante	5
Servicios de TI	Mensajería	Correo electrónico	Altamente Importante	4
Servicios de TI	Infraestructura básica	Protocolo de configuración dinámica de host (DHCP)	Extremadamente Importante	5
Servicios de TI	Infraestructura básica	Herramientas de configuración empresarial	Medianamente Importante	2

Clase de activo	Entorno de TI global	Nombre del activo	Clasificación del activo	Ponderación
Servicios de TI	Infraestructura básica	Uso compartido de archivos	Extremadamente Importante	5
Servicios de TI	Infraestructura básica	Almacenamiento de datos	Extremadamente Importante	5
Servicios de TI	Infraestructura básica	Acceso telefónico remoto	Poco Importante	1
Servicios de TI	Infraestructura básica	Telefonía	Poco Importante	1
Servicios de TI	Infraestructura básica	Acceso a red privada virtual (VPN)	Extremadamente Importante	5
Humanos	Personal de TI			2
Humanos	Proveedor			4
Humanos	Personal Operativo			5

Fuente: elaboración propia

Cada empresa decide, según la clasificación y ponderación de activos, sobre cuáles activos aplicará los controles. Para ello, se deben identificar vulnerabilidades, amenazas y riesgos de estos y entender a qué principio de seguridad afecta la posible materialización de un evento adverso, con el fin de mitigar efectivamente su impacto.

Como se recordará, los principios de la seguridad de la información son tres: disponibilidad, Integridad y Confidencialidad, los cuales se presentan en la figura 2. Proporcionar el cumplimiento a los activos garantiza el objetivo principal de la seguridad de la información. Veamos qué significa cada uno de estos principios.

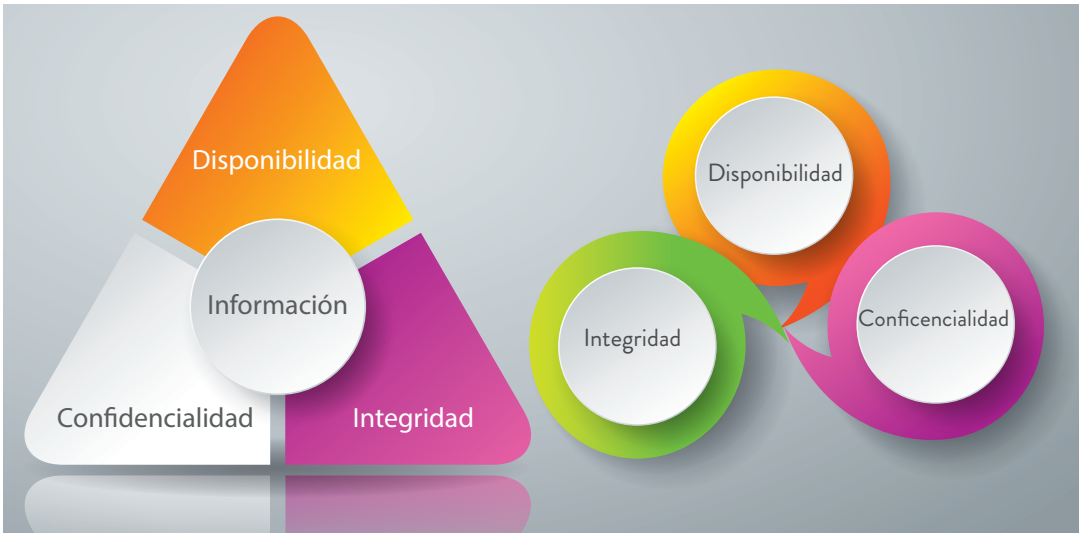

Figura 2. Principios de la seguridad de la información

Fuente: elaboración propia

3. Principios

3.1. Disponibilidad

La disponibilidad implica garantizar el acceso oportuno a la información que se requiera siempre y cuando cuente con autorización previa para acceder. Por dicha razón, las herramientas que se utilizan como medio de acceso (dispositivos de red, aplicaciones, computadores, personas, procesos etc.), deben contar con los recursos adecuados para funcionar de manera predecible y con un nivel de rendimiento aceptable, protegerse contra posibles interrupciones y, en caso de ser interrumpidos, estar en la capacidad de recuperarse de manera rápida y segura para que la operación de la empresa no se vea afectada de manera negativa (Harris, 2013).

Para alcanzar este objetivo es indispensable analizar la cantidad de elementos que intervienen en el proceso de acceso a un recurso. La red, por ejemplo, tiene muchas piezas que deben mantenerse en funcionamiento (*routers*, *switches*, servidores DNS, servidores DHCP, *proxies*, *firewalls*). De igual manera, el *software* cuenta con varios componentes que deben ejecutarse de manera saludable (sistema operativo, aplicaciones, *software antimalware*), las condiciones de entorno pueden afectar el acceso a dichos recursos (incendio, inundación, problemas eléctricos) y se pueden presentar posibles desastres naturales (terremoto, temblor) y robos o ataques físicos (Harris, 2013).

3.1.1. Ejemplos de controles

Toda empresa debe contar con un respaldo de sus archivos, puesto que el dispositivo de almacenamiento local en el cual se han creado puede fallar o ser atacado, sin permitir su acceso. Ataques como ransomware aprovechan esta debilidad de las empresas y, por tanto, al secuestrar la información, tienen la certeza de que los usuarios pagarán por ella, pues no poseen otra manera de recuperarla. Sin embargo, ¿qué significa el respaldo de datos?

El respaldo de datos es el proceso de copiar los elementos de información recibidos, transmitidos, almacenados, procesados y/o generados por un sistema en otros medios externos. Existen muchos mecanismos para tener respaldo, dependiendo de lo que se quiera asegurar; copias de la información en dispositivos de almacenamiento secundario y computadores paralelos ejecutando las mismas transacciones, son algunos ejemplos de este tipo de controles.

Aunque la organización cuente con un proceso automático para realizar dichas copias, es indispensable validar su funcionamiento con regularidad. Muchas empresas desconocen que su proceso presenta fallas hasta el momento que requieren hacer uso de alguna copia.

En la figura 3 se observan algunos dispositivos para guardar las copias. La recomendación general ha sido mantener respaldos locales y externos, de preferencia más de uno por cada tipo, determinando cuidadosamente el tiempo de permanencia de las copias y las transacciones simultáneas a realizar, de acuerdo con la operación de la empresa.

Figura 3. Medios de almacenamiento de información

Fuente: Freepik.com (2017)

Si el fallo se encuentra en algún elemento de operación, es decir, el incidente no se relaciona con el acceso a determinada información, sino con los medios que la almacenan o procesan (por ejemplo, falta de energía en el servidor de aplicaciones y, por tanto, falla en el acceso al sistema de información principal), es necesario contar con otra alternativa de acceso, o sea, tener definido un plan de contingencia para continuar la operación y recuperarse del incidente. Estos planes suelen ser una guía paso a paso, en la cual se definen cada uno de los procedimientos a seguir, sus responsables y las herramientas a considerar en caso de ser interrumpida parte o toda la operación de una empresa, con el objetivo de recuperarla. De acuerdo con las exigencias del plan, por el tipo de negocio, estos procedimientos pueden ser ejecutados por personas, sistemas informáticos o la combinación de estos elementos. En la figura 4 se presenta un esquema general con pasos sugeridos, puesto que un plan de recuperación de desastres está orientado al cumplimiento de continuidad del negocio, lo cual se constituye en toda una rama de estudio.

Figura 4. Ejemplo plan de contingencia y recuperación

Fuente: elaboración propia

3.2. Integridad

Este principio hace referencia a que la información debe ser fiable, certera y libre de manipulación por personal no autorizado. El *hardware*, el *software* y los elementos para la comunicación deben operar conjuntamente para preservar y procesar los datos correctamente o para transportar los mismos a los destinos, previamente indicados, sin ningún tipo de alteración. Los sistemas y la red deben estar protegidos contra intrusos o intervención externa. Los controles aplicables para cumplir con este principio garantizan que los atacantes o los errores de los usuarios no comprometan la integridad de los sistemas por acciones, tales como corrupción de archivos, modificación maliciosa, reemplazo de datos o falta de entrenamiento (Harris, 2013).

Los usuarios, muchas veces, afectan un sistema o la integridad de sus datos por error (aunque los usuarios internos también pueden cometer actos maliciosos). Por tal motivo, la seguridad no solo debe aplicar controles para el acceso, sino que también debe preocuparse por simplificar las acciones que los usuarios deben realizar en determinadas operaciones, de modo que los errores se vuelvan menos comunes (Harris, 2013).

3.2.1. Ejemplos de controles

En sistemas críticos, los archivos deben restringir la visualización y el acceso de los usuarios. Las aplicaciones deben proporcionar mecanismos que verifiquen valores de entrada válidos y razonables. Las bases de datos deben permitir que solo las personas autorizadas modifiquen los datos y los que están en tránsito deben estar protegidos por cifrado u otros mecanismos.

En general, la aplicación de controles para garantizar la integridad de los datos implica la ejecución de actividades preventivas, programación orientada al usuario y medidas de protección para el acceso a diferentes herramientas.

Figura 5. Protección de datos
Fuente: Makyzz (2017)

3.3. Confidencialidad

Este principio implica que la información mantiene un nivel de secreto y no todos los usuarios de la organización pueden acceder de manera indiscriminada a ella. Por el contrario, es necesario establecer niveles de privilegios para que solo las personas a cargo de la manipulación de información accedan a esta sin que un tercero no autorizado pueda intervenirla. Estos niveles de confidencialidad deben prevalecer mientras que los datos residen en sistemas y dispositivos dentro de la red a medida que se trasmiten y llegan a su destino.

Los atacantes pueden evitar los mecanismos de confidencialidad mediante el monitoreo de la red, robo de contraseñas, intervención de mecanismos de cifrado y la ingeniería social (lograr que un usuario final ejecute acciones que no realizaría si conociera sus consecuencias negativas y que pueden afectar la seguridad de la empresa, utilizando la manipulación y el engaño para tal fin) (Harris, 2013).

La confidencialidad se puede proporcionar mediante el cifrado de los datos tal como se almacenan y transmiten, aplicando un estricto control de acceso y clasificación de estos y capacitando al personal sobre los procedimientos adecuados de protección de datos.

3.3.1. Ejemplos de controles

La encriptación o cifrado de datos es el proceso que se sigue para enmascararlos con el objetivo de que sean incomprensibles para cualquier agente no autorizado. Esto se hace usando una clave especial y siguiendo una secuencia de pasos preestablecidos, conocida como "algoritmo de cifrado". El proceso inverso se conoce como descifrado y devuelve los datos a su estado original.

En resumen, como se muestra en la figura 6, para garantizar el cumplimiento del objetivo principal de la seguridad de la información es importante considerar controles suficientes, orientados al almacenamiento, protección y cifrado de datos.

Figura 6. Resumen protección de datos

Fuente: Freepik (2015)

¿Sabía que...?

Disponibilidad, integridad y confidencialidad son principios críticos de seguridad. Por lo anterior, hay que comprender su significado, entender cómo su ausencia puede afectar de manera negativa a la empresa y, de acuerdo con la identificación de activos realizada, seleccionar los mecanismos que garanticen su cumplimiento con el mayor grado de certeza posible.

3.4. Definiciones complementarias a los principios

Existen otros conceptos de interés que complementan el objetivo principal de seguridad de la información. Estos conceptos son autenticidad y no repudio.

3.4.1. La autenticidad

Tiene como objetivo asegurar la identidad de la información contenida en algún sistema, respecto a su origen y procedencia, con el fin de comprobar que dicha información proviene de la fuente que dice ser. Por ejemplo, cuando recibimos un mensaje de correo electrónico de un dominio conocido, el control para cumplir con el parámetro de autenticidad es validar que efectivamente la fuente de dicho mensaje es el dominio que dice ser y no ha habido una suplantación del mismo con fines maliciosos.

3.4.2. No repudio o irrenunciabilidad

Indica que ni el emisor ni el receptor, en un proceso de comunicación, pueden afirmar que la información trasmitida no proviene de sus fuentes.

Si la autenticidad prueba quién es el emisor y autor de un correo y cuál es su destinatario, el "no repudio" prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. Así, cuando se envía un mensaje, el receptor puede comprobar que, efectivamente, el supuesto emisor lo envió. De forma similar, cuando se recibe un mensaje, el emisor puede verificar que, de hecho, el supuesto receptor lo recibió.

En la figura 7 podemos identificar la relación que existe entre los conceptos vistos. En primera instancia, la información debe estar disponible. Luego, debe garantizarse el acceso solo a personal autorizado y establecer medidas para evitar alternaciones en la información. Quienes intervienen en las transacciones no pueden negar haberlas hecho, siempre y cuando se hayan realizado las acciones pertinentes para su protección.

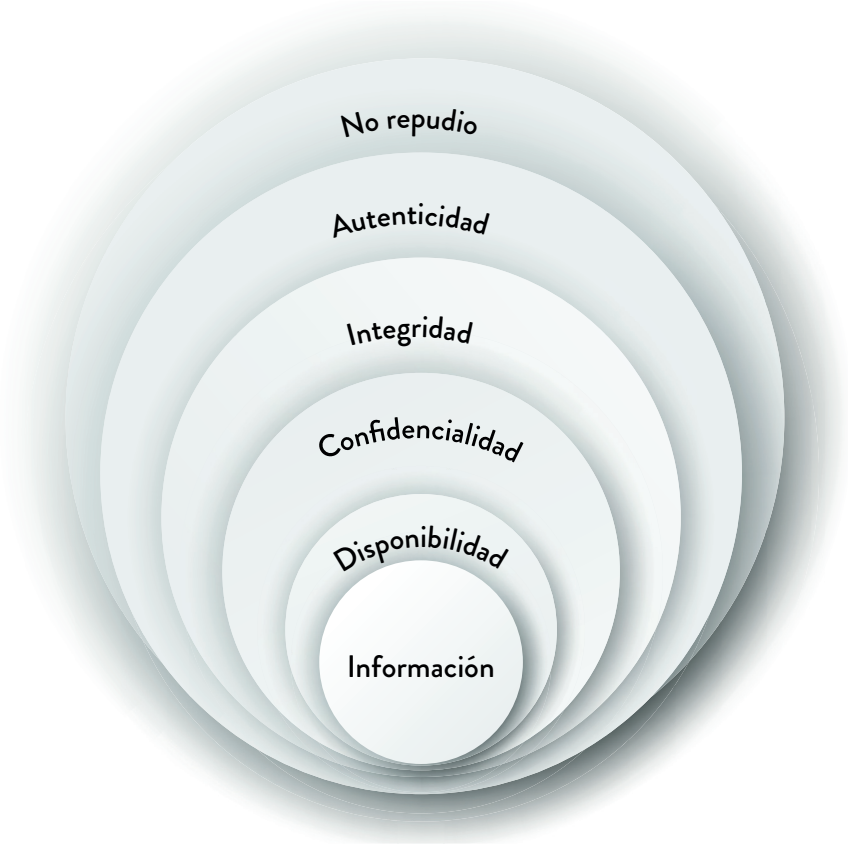

Figura 7. Relación de principios y conceptos complementarios en seguridad de la información

Fuente: elaboración propia

4. Vulnerabilidad, amenaza y riesgo

En el capítulo anterior se hizo la introducción a los conceptos de vulnerabilidad, amenaza y riesgo. Vamos a ampliar dicha información y brindaremos unos ejemplos para aclarar su alcance.

4.1. Vulnerabilidad

Hemos mencionado que la vulnerabilidad es intrínseca al activo u objeto de estudio, es decir, propio de su naturaleza. En términos empresariales podemos considerarla, además, como una falla de un equipo, persona o sistema que puede generar perjuicios en este o en los demás elementos que interactúen con él (ISO, 2009). Las principales causas de las vulnerabilidades en los sistemas de información se deben a:

- Debilidad en el diseño de los protocolos utilizados en las redes (FTP, SMTP, Telnet).
- Errores de programación, lo que justifica el uso continuo de parches.
- Configuración errónea de los sistemas de información o falla en la parametrización de estos.
- Políticas de seguridad deficientes o inexistentes.

En la tabla 4 se muestran ejemplos de vulnerabilidades comunes que se presentan en los diferentes tipos de activos de información de las empresas; son ejemplos generales para comprender los conceptos. En el ambiente empresarial este listado debe ser específico y según la clasificación de la información que se haya definido (Harris, 2013).

4.2. Amenaza

Una vez identificadas las vulnerabilidades, es importante definir qué factores externos pueden explotarlas, es decir, identificar la potencial ocurrencia de un evento adverso o no deseado debido a las vulnerabilidades del activo; o sea, lo que llamamos amenaza. Este evento puede producirse con diferentes grados de intensidad y duración, por lo cual el impacto varía (Harris, 2013).

4.3. Riesgo

Para las empresas lo primordial, en términos de seguridad, es estudiar los potenciales eventos adversos, con el fin de conocer la probabilidad de que ocurran. Esta probabilidad de ocurrencia es lo que se conoce como riesgo. En otras palabras, el riesgo es la posibilidad de que una amenaza explote una vulnerabilidad (Harris, 2013).

En la siguiente tabla se identifican las amenazas según las vulnerabilidades definidas según ISO 27005:

Tabla 4. Descripción de vulnerabilidades, amenazas y riesgos por tipo de activo

Tipo	Descripción Vulnerabilidad	Amenaza	Riesgo	Principio afectado
Hardware	Susceptibilidad a condiciones ambientales, tales como humedad, salinidad, polvo, etc.	Polvo, corrosión, congelamiento de los equipos o los medios	Destrucción parcial o total	Disponibilidad - Integridad
Hardware	Falta de trazabilidad de su ubicación	Manipulación no autorizada	Fuga de Información	Confidencialidad
Hardware	Mantenimiento insuficiente o con fallas	Incumplimiento en los procedimientos para el mantenimiento	Funcionamiento ineficiente	Disponibilidad - Integridad
Software	Falta de terminación de la sesión cuando se abandona la estación de trabajo	Abuso de los derechos	Fuga de Información	Confidencialidad
Software	Interface de usuario poco intuitiva o compleja	Error voluntario o involuntario en el uso	Indisponibilidad parcial o total del sistema	Disponibilidad - Integridad
Software	Fallas de programación	Corrupción de los datos	Indisponibilidad parcial o total del sistema	Disponibilidad - Integridad
RED	Tráfico sensible sin protección	Escucha subrepticia (escucha que se hace oculta con fines maliciosos)	Fuga de información	Confidencialidad
RED	Conexión deficiente de los cables	Falla del equipo de telecomunicaciones	Indisponibilidad parcial o total del sistema	Disponibilidad - Integridad
RED	Gestión inadecuada de la red	Saturación del sistema de información	Indisponibilidad parcial o total del sistema	Disponibilidad - Integridad
Personal	Ausencia del personal	Incumplimiento de l as obligaciones de la empresa	Indisponibilidad parcial o total del sistema	Disponibilidad - Integridad
Personal	Entrenamiento ineficiente en temas de seguridad	Error voluntario o involuntario en el uso	Fuga de Información	Confidencialidad Disponibilidad - Integridad
Personal	Trabajo no supervisado	Hurto de medios o documentos	Destrucción parcial o total	Confidencialidad
Espacio físico	Descuido en el control de acceso	Hurto de medios o documentos	Fuga de información	Disponibilidad - Integridad

Tipo	Descripción Vulnerabilidad	Amenaza	Riesgo	Principio afectado
Espacio físico	Ubicación en un lugar con inestabilidad energética	Pérdida del suministro de energía	Indisponibilidad parcial o total del sistema	Confidencialidad
Espacio físico	Fallas estructurales	Daño a las personas y equipos	Destrucción parcial o total	Disponibilidad - Integridad
Empresa	Falta o insuficiencia en los contratos con clientes, proveedores y personal interno referente a seguridad	Abuso de los derechos	Fuga de información	Confidencialidad
Empresa	Falta de procedimientos para control de cambios	Incumplimiento en la entrega de servicios]o productos	Indisponibilidad parcial o total del sistema	Disponibilidad - Integridad
Empresa	Falta de procedimientos del cumplimiento de derechos intelectuales	Uso de *software* ilegal	Destrucción parcial o total	Disponibilidad - Integridad

Fuente: **elaboración propia**

5. Ataques informáticos

Comprendidos los conceptos principales sobre seguridad de la información, es necesario aclarar un último término que es bastante utilizado en el medio de la seguridad y cuyo efecto se espera evitar: ataque informático.

Un ataque informático hace referencia a todo intento que se realiza para eludir los controles de seguridad en un sistema, cuyo propósito de evasión es comprometer el sistema con algún fin malicioso, es decir, afectar la disponibilidad, confidencialidad o integridad de la información (interrumpir la operación de un sistema, manipularlo para obtener algún tipo de ventaja que afecte a la organización, robar información etc.). Estos ataques son ideados por personas que utilizan sus conocimientos en informática para aprovechar las vulnerabilidades de un sistema.

La motivación de un atacante puede ser variada: reconocimiento dentro de una comunidad por pertenecer a determinada ideología, venganza (empleado insatisfecho), simple curiosidad o interés en la materia, dinero, y hasta espionaje y terrorismo.

Un ataque activo se caracteriza porque su objetivo es alterar la integridad y disponibilidad de la información.

Un ataque pasivo se caracteriza porque su objetivo es interceptar la información, sin modificarla, afectando principalmente el principio de confidencialidad.

Un ataque interno es iniciado por un agente interno dentro del perímetro de seguridad definido, es decir, personal autorizado para acceder a los recursos del sistema, pero los utiliza de una manera no aprobada por quienes le otorgaron la autorización.

Un ataque externo es un ataque iniciado desde fuera del perímetro por un usuario no autorizado o ilegítimo del sistema (un "extraño"). Este usuario puede acceder y lanzar el ataque con recursos internos, con el fin de evitar que se descubra el origen del ataque.

Tabla 5. Resumen ataques informáticos más comunes

Ataque	Tipo	Descripción	Ejemplos
Scan	Pasivo	Su objetivo es escuchar y revisar algún punto (regularmente un puerto) de la víctima, con el fin de identificar datos relevantes que faciliten un posterior ataque. En este tipo de arremetida no hay intervención de los sistemas.	Port Scan, Idle Scan
Denial-of-service attack	Activo	Su objetivo es que el sistema de la víctima no se encuentre disponible o afectar su conectividad. Esto se logra gracias a la sobrecarga de solicitudes que debe atender el sistema durante el ataque, la afectación de los recursos computacionales y el gran consumo de ancho de banda que puede producir el ataque.	SYN Flood: intenta abrir conexiones TCP con direcciones falsas ICMP Flood: envía innumerables solicitudes de Ping UDP Flood: genera grandes cantidades de paquetes UDP hacia la víctima Smurt Attack
Spoofing	Activo	Su objetivo es engañar a la víctima, por lo cual se utilizan técnicas para falsificar la procedencia de los datos, es decir, hacerse pasar por una entidad válida para la víctima, por lo cual el atacante accede a un sistema e información confidencial, entre otros.	P, ARP, DNS, WEB, Email Spoofing, suplantación de cualquier protocolo

Ataque	Tipo	Descripción	Ejemplos
Man in the middle	Activo	Su objetivo es intervenir una comunicación en secreto para manipularla y enviar información diferente a dos entidades, engañándolas, de tal manera que no saben que la comunicación ha sido afectada.	ARP Poisoning
Brute Force	Activo	Su objetivo es descubrir la contraseña de un sistema o aplicación, probando todas las posibles combinaciones hasta lograr el acceso.	Ataque puro o de diccionario
Social Engineering	Activo	Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizarían y que revelan todo lo necesario para superar las barreras de seguridad.	*Phising*

Fuente: elaboración propia

Referencias

Enter.co. (2016). La ingeniería social: el ataque informático más peligroso. Recuperado de http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/

Harris, S. (2013). All in One CISSP Exam Guide. New York: McGraw Hill.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). (2009). Information Technology. SecurityTechniques. Information Security Management Systems. Overview and vocabulary. Geneva: ISO.

Referencias de imágenes

Freepik. (2015). *Resumen protección de datos* [Vectores]. Recuperado de https://www.freepik.es/vector-gratis/banderas-de-cifrado-de-datos_768935.htm#term=encrypted data&page=1&position=6

Macrovector - Freepik.com. (2017). *Medios de almacenamiento de información* [Vectores]. Recuperado de https://www.freepik.es/vector-gratis/iconos-sobre-almacenamiento-de-datos_1008315.htm#term=data storage&page=1&position=18

Makyzz - Freepik.com. (2017). *Protección de datos* [Vectores]. Recuperado de https://www.freepik.es/vector-gratis/concepto-de-seguridad-de-datos_1063670.htm#term=encrypted data&page=1&position=1

pss.mex.net. (s.f.). *Ejemplo plan de contingencia y recuperación* [Infografía]. Recuperado de https://blogrecursosytecnologia.com/category/plan-de-recuperacion-ante-desastres/

INFORMACIÓN TÉCNICA

FACULTAD DE
INGENIERÍA, DISEÑO
E INNOVACIÓN

Módulo 1: Teoría de la Seguridad

Unidad 1: Principios de la seguridad de la información

Escenario 2: Principios e introducción al análisis de resgos

Autor: Alexandra Peña Daza

Asesor Pedagógico: Angie Viviana Laitón Fandiño
Diseñador Gráfico: Henderson Jhoan Colmenares
Asistente: Alejandra Morales