Unidad 1 / Escenario 1

Lectura fundamental

Definiciones de la seguridad de la información

Contenido

Palabras clave: Seguridad, información, línea base, políticas de seguridad de la información, marcos de referencia seguridad de la información.

1. Introducción a la seguridad de la información

En nuestros días, hablar de información no es ajeno a nuestra cotidianidad debido a que constantemente la estamos enviando o recibiendo desde diferentes fuentes: la casa, la radio, la televisión, redes sociales y los diferentes medios de comunicación.

No obstante, el concepto de información ha adquirido una singular importancia tanto en el entorno empresarial como en el entorno personal, de manera que se nos hace necesaria protegerla para concebir un ambiente de tranquilidad en las transacciones que realizamos.

¿A qué se debe esta situación? ¿Por qué escuchamos y hablamos de temas como protección de datos personales, hackers, entre otros conceptos relacionados, independientemente del rol que ejercemos en nuestra empresa?

Para responder a estos cuestionamientos se hace necesario aclarar dos conceptos fundamentales: información y seguridad.

Información, cuyo equivalente latín es indicium, para la Real Academia Española significa: "Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada" (RAE, 2017). Es decir, desde el punto de vista semántico podemos afirmar que la información brinda conocimiento y, por tanto, nos permite ampliar el juicio que tenemos sobre un tópico determinado, permitiendo que lo comprendamos a un nivel superior.

Sin embargo, no todo lo que recibimos como información cumple cabalmente esta definición, gracias al volumen que se maneja en los diferentes medios, la diversidad de opiniones válidas que pueden existir entre un individuo y otro, su origen y tiempo de producción. En otras palabras, el concepto de información se ve afectado por los actores mismos de la comunicación (emisor, receptor, mensaje, canal).

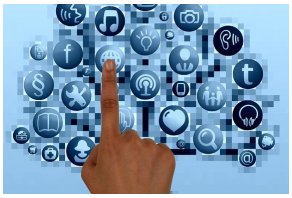
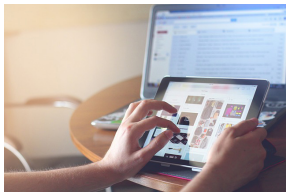
Es por esto que referentes de clase mundial, como lo son las normas internacionales, han estado de acuerdo en que la información debe evaluarse como aquello que genera o posee valor para el destinatario, sin desconocer la naturaleza misma del conocimiento que brinda (ISO, 2009).

Veamos la definición propuesta por la norma ISO 27001:2013 con respecto al concepto de información:

Todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración (ISO, 2013).

En este sentido, podemos identificar que la información tiene 4 elementos fundamentales, que se presentan en la siguiente tabla:

Tabla 1. Elementos de la información

DATOS:	ORDEN:	VERACIDAD:	VALOR:
Emitidos o recibidos. Eje fundamental de la información	Es la lógica; lo que le da sentido	La fuente es confiable	Utilidad, el fin con el que se usa
			
Figura 1. Datos *Fuente:* Geralt (s.f.)	**Figura 2. Orden** *Fuente:* Geralt (s.f.)	**Figura 3. Veracidad** *Fuente:* Geralt (s.f.)	**Figura 4. Valor** *Fuente:* fancycrave1 (s.f.)

Fuente: elaboración propia

El objetivo de esta tabla es presentar los elementos fundamentales que debe cumplir la información y establecer algún tipo de secuencia, es decir primero están los datos, estos se ordenan para que tengan sentido, se valida su procedencia (que sea confiable) y por último adquieren valor para una empresa por el modo como se usan, no encontré un grupo de imágenes que expresara esto.

1.1. Clasificación de la información

Las organizaciones se han preocupado por todo lo referente a la información que producen y reciben; por tal motivo, se ha clasificado de acuerdo con su valor, los requisitos legales que deba cumplir, la sensibilidad y el nivel de criticidad que tiene para una empresa. Es decir, no basta con identificar la información, sino que es necesario cuantificar el valor que tiene para la organización con el fin de distinguir qué tan sensible es dicha información a la pérdida, la divulgación o falta de disponibilidad.

Sin embargo, estos no son los únicos criterios existentes para clasificar la información, puesto que el desarrollo de políticas estatales, tales como protección de datos personales, ha permitido que se amplíen los niveles de clasificación.

No existen reglas estrictas sobre los niveles de clasificación que una organización debería utilizar, lo cual depende más de sus necesidades; no obstante, en la siguiente tabla se sugiere una clasificación general, la cual suele utilizarse en la industria (Harris, 2013).

Tabla 2. Clasificación de la información

Clasificación	Definición	Ejemplo
Pública	Información que puede ser divulgada sin que ocasione perjuicios a la organización o una persona. Preferiblemente no se divulga.	Cantidad de personal trabajando en un proyecto.
Privada	Información personal que no debe ser divulgada. Su difusión puede afectar negativamente a la empresa o persona.	Información médica.
Confidencial	Información que solo debe conocer la compañía. Esta información se encuentra exenta de transmisión de acuerdo con las leyes y regulaciones donde se utilice. Su divulgación puede afectar negativamente a la empresa.	Códigos de programación.
Sensible	Información que requiere un cuidado especial para garantizar la integridad y confidencialidad, protegiéndola de modificación o eliminación no autorizada.	Información financiera.
No clasificada	La información no es sensible ni se encuentra clasificada.	Manuales de dispositivos, como computadores.
Sensible pero no clasificada	La información tiene un nivel de secreto menor que la información sensible, puesto que si se revela podría no ocasionar daños.	Respuesta de los puntajes de algún *test*.
Secreta	Información que no debe ser revelada, pues podría generar daños a nivel nacional. Esta clasificación suele utilizarse en ambientes militares.	Planes de despliegue de tropas.
Ultra secreta	Información que no debe ser revelada, pues tiene implicaciones perjudiciales a nivel nacional. Esta clasificación suele utilizarse en ambientes militares.	Información de satélites espía.

Fuente: Harris (2013)

1.2. Procedimientos de clasificación de datos

La clasificación de la información es el primer paso para iniciar una gestión eficiente de esta y, de esta forma, requiere la definición de actividades que sigan una secuencia lógica.

A continuación, acorde con Harris (2013), se propone un paso a paso de las actividades a seguir para alcanzar el objetivo de organizar y clasificar correctamente la información:

1. Definir los niveles de clasificación: puede utilizarse alguna norma o buena práctica ya establecida o la empresa los puede definir, según lo considere necesario.
2. Especificar los criterios que determinan cómo se clasifican los datos: esto varía de una organización a otra, por lo cual se deben unificar los criterios para su definición.

3. Identificar los dueños de la información dentro de la empresa: estas personas serán las encargadas de clasificar la información de acuerdo con los niveles y criterios establecidos.
4. Identificar quien actuará como custodio de los datos: quién será el responsable de preservar los datos y los niveles de seguridad que se han establecido.
5. Identificar los mecanismos de protección: aquí se pueden utilizar herramientas, como el análisis de riesgos, para cumplir con dicho objetivo.
6. Documentar cualquier excepción que aplique a lo anteriormente establecido: en caso de que conciernan dichas excepciones.
7. Indicar los métodos que pueden utilizarse para transferir la custodia de la información: solo en caso de requerirse.
8. Crear un procedimiento para revisar periódicamente la clasificación y propiedad: esto implica comunicar los cambios a los afectados (dueños y custodios).
9. Difundir los procedimientos para desclasificar los datos.
10. Sensibilizar al personal sobre el uso de la información para que este entienda cómo manejar la información en los diferentes niveles de clasificación definidos.

1.2. Definición de informática

Según la Real Academia de la Lengua Española, informática se define como el "conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras" (RAE, 2017).

Por tratamiento de la información podemos considerar su almacenamiento, procesamiento y transmisión.

1.3. Definición de información

Teniendo claro el concepto de información, es fundamental comprender y asimilar el concepto de seguridad.

Seguridad, viene del latín securitas, que significa "certeza, sin temor a preocuparse". Desde este origen etimológico latino, podemos establecer que se encuentra conformado por el vocablo securus (cuya definición acabamos de mencionar) y el sufijo dad, significa "cualidad".

La Real Academia Española lo define como "cualidad de seguro" (RAE, 2017), siendo la definición de seguro: "Libre y exento de riesgo, cierto, indubitable, firme o bien sujeto, que no falla o que ofrece confianza" (RAE, 2017). El riesgo, en términos generales, puede entenderse como la proximidad de un daño, afectación por una situación, persona o elemento.

De acuerdo con lo anterior, se puede afirmar que seguridad es la cualidad de un objeto de estar libre de riesgo, ser confiable y certero.

Al igual que el término de información, la seguridad presenta diferentes clasificaciones con relación a los aspectos de la vida cotidiana que involucra, como puede ser la seguridad de las personas en el entorno laboral, de los alimentos, de los productos, del negocio, de la información, entre otros.

1.4. Seguridad de la información y seguridad informática: ¿Conceptos iguales o diferentes?

Hemos realizado un recorrido por los conceptos de información, informática y seguridad. Ahora bien, es importante asociarlos para establecer la diferencia entre los conceptos de seguridad informática y seguridad de la información.

Es claro que seguridad implica una cualidad, que la información hace referencia a la generación de valor y que la informática es una ciencia que permite el tratamiento automático de información (datos) por medio de sistemas computacionales.

Por lo tanto, la seguridad informática implica garantizar que los sistemas computacionales que se utilizan para el procesamiento de datos se encuentren libre de riesgos, que sean confiables y ciertos. La seguridad de la información hace referencia al conjunto de medidas que se deben aplicar para garantizar que, independientemente del medio de trasmisión, tipo de información, nivel de criticidad y valor que tenga para una organización, la información esté exenta de riegos para que sea certera y confiable.

La seguridad de la información tiene un sentido más amplio que el término de seguridad informática y está orientada a gestionar eficientemente los recursos tecnológicos, físicos, humanos y procedimentales que aportan utilidad a la empresa para su operación, con el fin de que la afectación de esta sea mínima por daños ocasionados, consciente o inconscientemente, por terceros, fuera o dentro de la organización.

Partiendo de dicho concepto, se han desarrollado buenas prácticas, recomendaciones y estándares internacionales que brindan un marco conceptual en el tema de seguridad de la información y que facilitan su gestión.

Uno de ellos es la norma ISO 27001: 2013 (versión más reciente), la cual expresa el término de seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas implicados en su tratamiento dentro de una organización.

Para comprender a profundidad la definición anterior, es importante conocer los términos descritos, que en el mundo de la seguridad de la información se conocen como los principios de seguridad de la información. Estos principios parten de la definición establecida por la Real Academia de la Lengua Española, tanto para seguridad como para información. Por ahora, vamos a plantear una definición sencilla de ciertas palabras, la cual será ampliada en el escenario 2 de la presente unidad.

Disponibilidad: la información debe ser utilizable por quien la necesita en todo momento.

Confidencialidad: la información debe ser transferible solo entre los entes autorizados.

Integridad: la información debe ser confiable y certera, sin alteraciones de ningún tipo.

Así pues, podemos concluir que la seguridad de la información es el conjunto de medidas tanto preventivas como correctivas que ayudan a las organizaciones a garantizar la disponibilidad, integridad y confidencialidad de la información, con el fin de minimizar el impacto que cualquier riesgo pueda generar sobre esta. La seguridad de la información incluye a la seguridad informática, por lo cual es más apropiado utilizar el término seguridad de la información para referirse a la protección de activos de información cuya esencia no sea exclusivamente tecnología. Sin embargo, frente a esta discusión hay múltiples opiniones y todo deriva de la traducción desde el idioma inglés al castellano.

1.5. Otras definiciones de interés en seguridad de la información

Existen varios términos alrededor de la seguridad de la información que se utilizan indistintamente y los cuales es importante aclarar, principalmente para una buena gestión de la seguridad dentro de las organizaciones, la cual se logra evitando cualquier elemento que afecte a un activo de información, como se muestra en la figura 5. En esta imagen se evidencia la relación entre los conceptos vulnerabilidad, amenaza, riesgo y control, puesto que un virus (amenaza) ha sido detectado por el antivirus (control), evitando daño en el funcionamiento (riesgo) del computador (activo). Estos términos se amplían a continuación.

Figura 5. Control de virus

Fuente: Kalhh (s.f.)

En esta imagen se evidencia la relación entre los conceptos vulnerabilidad, amenaza, riesgo y control, puesto que un virus (amenaza) ha sido detectado por el antivirus (control), evitando daño en el funcionamiento (riesgo) del computador (activo). Estos términos se amplían a continuación:

- **Activo de información:** todo aquello que tiene un valor para la empresa (ISO, 2009), especialmente monetario, como las personas, su conocimiento, sistemas, etc.

Figura 6. Activos de información

Fuente: Bloomua (s.f.)

- **Vulnerabilidad:** falla propia o intrínseca del activo por su naturaleza o por la ausencia de controles y que se considera una debilidad del activo. Esta falla puede ser explotada por una amenaza y convertirse en un riesgo. Las vulnerabilidades se consideran sobre el *software*, el *hardware*, los procedimientos o los mismos recursos humanos.
- **Exposición:** consecuencia peligrosa que genera una vulnerabilidad y por la cual esta puede ser explotada.
- **Amenaza:** peligro potencial externo al activo. A diferencia de la vulnerabilidad, que es propia de la naturaleza del activo, las amenazas dependen de la exposición que pueda tener el activo.
- **Riesgo:** probabilidad de que una amenaza explote una vulnerabilidad y el impacto que esta situación genera a nivel legal, comercial, de imagen, etc.

En la siguiente figura se puede observar que el computador era vulnerable por el control de acceso que tenía, razón por la que quedó expuesto y la amenaza aprovechó la vulnerabilidad, materializándose el riesgo, cuyo impacto fue económico (robo de dinero).

Figura 7. Riesgo materializado

Fuente: Jemastock (s.f.)

- **Control:** elemento que se utiliza para mitigar un riesgo. Dependiendo del activo, su clasificación y nivel de riesgo, el control puede ser administrativo, técnico o físico y se utiliza para disuadir a un posible atacante, prevenir la ocurrencia de un incidente, o identificar, corregir y restaurar si el incidente ya ha ocurrido.

En síntesis...

La definición de seguridad de la información se encuentra influenciada por diferentes entidades mundialmente reconocidas, las cuales concuerdan en que el término implica mantener libre de riesgo aquello que tiene valor para una empresa, sin importar el medio por el cual se transmite, origina o recibe. En otras palabras, la seguridad de la información hace referencia a garantizar la disponibilidad, integridad y confidencialidad de la información. Para lograrlo es fundamental definir el proceso de clasificación de la información, incluyendo la manera en que dicho proceso se mantendrá actualizado y la identificación de vulnerabilidades, amenazas y riesgos asociados a la información, para aplicar controles suficientes que eviten daños en las empresas.

2. Objetivos de la seguridad de la información

Hasta aquí, hemos avanzado en la definición de conceptos claves que se utilizan en seguridad de la información. Conociendo estas definiciones, podemos entender la importancia de la seguridad de la información en las organizaciones, desde el punto de vista de los objetivos que debe cumplir; garantizarla en un entorno corporativo no solo implica definir controles que se aplican una única vez, sino que es un proceso reiterativo y dinámico, que requiere actualización constante por parte de quienes intervienen en el proceso, teniendo como base los objetivos que se esperan alcanzar. Dichos objetivos se pueden resumir en:

- Asegurar el adecuado uso de los recursos (de cualquier tipo), las aplicaciones, y los sistemas, clasificándolos en activos de información con el nivel de criticidad que corresponda según la organización.
- Analizar las vulnerabilidades y amenazas a las cuales está expuesto un activo, para la correcta identificación de riesgos y sus respectivos controles que minimicen el impacto si un riesgo llega a materializarse.

- Gestionar correctamente los incidentes de seguridad que puedan presentarse, de tal manera que se realicen las respectivas correcciones, una vez ocurra el incidente, y lograr la correcta recuperación de la operación.
- Cumplir el marco legal, con los requisitos establecidos a nivel de empresa, en lo referente a seguridad de la información y de acuerdo con el país o el sector en el que se desempeña la operación de la empresa.

2.1. Buenas prácticas, modelos y marcos para el cumplimiento de los objetivos de la seguridad de la información

Diferentes organizaciones alrededor del mundo han desarrollado sus propias prácticas para la gestión de la seguridad de la información, cuyo propósito es cumplir los objetivos identificados anteriormente, los cuales permiten controlar los riesgos, gestionar eficientemente los procesos y alcanzar un desarrollo empresarial sostenible.

A continuación, se hace un desglose sencillo de buenas prácticas, estándares y marcos de referencia en seguridad de la información, clasificados de acuerdo con el enfoque que le han brindado sus creadores (Harris, 2013).

2.1.1. Desarrollo del programa de seguridad

- Normas internacionales de la serie ISO / IEC 27000 sobre cómo desarrollar y mantener un SGSI desarrollado por ISO e IEC. Han sido reconocidas por la industria la gestión de seguridad.

2.1.2. Desarrollo de arquitectura empresarial

- Marco de arquitectura empresarial Zachman Framework: utilizado para definir y comprender un entorno empresarial; desarrollado por John Zachman.
- Marco de arquitectura TOGAF Enterprise: utilizado para definir y comprender un entorno empresarial; desarrollado por The Open Group.
- Marco de arquitectura del Departamento de Defensa de DoDAF EE. UU.: asegura la interoperabilidad de los sistemas para cumplir los objetivos de la misión militar.

- Marco de arquitectura MODAF: utilizado principalmente en el apoyo militar a misiones realizadas por el Ministerio de Defensa británico.

2.1.3. Desarrollo de la arquitectura empresarial de seguridad

- Marco SABSA: arquitectura de seguridad empresarial basado en el riesgo de mapas de iniciativas comerciales, similares al marco Zachman.

2.1.4. Desarrollo de controles de seguridad

- CobiT: conjunto de objetivos de control para la gestión de TI desarrollado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) y el IT Governance Institute (ITGI).
- SP 800-53: conjunto de controles para proteger los sistemas federales de EE. UU., elaborados por el Instituto Nacional de Estándares y Tecnología (NIST).

2.1.5. Gobierno corporativo

- COSO: conjunto de controles corporativos internos para ayudar a reducir el riesgo de fraude financiero, desarrollado por el Comité de Patrocinio Organizaciones (COSO) de la Comisión Treadway.

2.1.6. Gestión de proceso

- Procesos ITIL: para permitir la gestión de servicios de TI; desarrollados por el Oficina de Comercio Gubernamental del Reino Unido.
- Estrategia de gestión Six Sigma Business: desarrollada por Motorola con el objetivo de mejorar los procesos comerciales.
- Proceso de Integración del Modelo de Madurez de Capacidades (CMMI): modelo de mejora desarrollado por Carnegie Mellon.

2.2. Si ya se ha seleccionado un referente, ¿cómo implementarlo?

Existen una serie de herramientas utilizadas en las diferentes normas, modelos, buenas prácticas y marcos de seguridad de la información, que facilitan el cumplimiento de los objetivos de esta y, por tanto, contribuyen en la adopción de cualquier referente.

Estas herramientas suelen distinguirse por estar orientadas al cumplimiento estratégico o táctico de los objetivos. A continuación, se presentan sus definiciones, alcances y nivel de importancia en seguridad de la información.

2.2.1. Políticas

Es una declaración de obligatorio cumplimiento, aprobada por la alta gerencia, que define el papel de la seguridad de la información dentro de la organización. La aprobación de la alta gerencia incluye la definición del proceso a seguir para establecer el programa de seguridad y todo lo que este debe contener, como los objetivos, responsabilidades y el valor estratégico y táctico de la seguridad. Esta política debe abordar leyes aplicables, regulaciones, necesidades, problemas y/u oportunidades a nivel de seguridad de la organización y del nivel de riesgo que se espera aceptar, y debe indicar las actividades futuras que se deben ejecutar, en términos de seguridad, en toda la organización (Harris, 2013).

¿Sabía que…?

Los referentes indicados anteriormente se mencionan por ser los de mayor aceptación en las empresas. Varios de estos pueden implementarse en una misma empresa, sin que uno sea mejor que otro. Esto dependerá del tipo de negocio, política de seguridad establecida y objetivos a lograr a nivel empresarial.

2.2.2. Estándares

Se refieren a actividades, acciones o reglas obligatorias. Los estándares pueden apoyar y reforzar la dirección a una política. Los estándares de seguridad pueden especificar cómo se usarán los productos de hardware y software; también se pueden usar para indicar el comportamiento esperado del usuario.

Proporcionan un medio para garantizar que las tecnologías específicas, las aplicaciones, los parámetros y los procedimientos se implementen de manera uniforme (estandarizada) en toda la organización (Harris, 2013).

Figura 8. Relación de herramientas de acuerdo con el cumplimiento de objetivos

Fuente: elaboración propia

La idea es representar que las herramientas hacen parte de la cadena de documentación, siendo el nivel más bajo los procedimientos, pero indicado que tanto estándares, recomendaciones y procedimientos son de orden táctico.

2.2.3. Línea base

El término línea base se refiere a un punto en el tiempo que actúa como referencia para cambios futuros y también se utiliza para establecer el nivel mínimo de protección requerido. En seguridad, se pueden definir líneas bases por grupo de activos identificados, por sistemas etc., lo que indica la necesidad de configuración y el nivel de protección que se le brindará según su criticidad. Las mediciones futuras que se realicen para determinar el cumplimiento de controles tendrán como punto de referencia la línea base (Harris, 2013).

2.2.4. Las recomendaciones

Son acciones sugeridas y guías operativas para usuarios, personal de TI, personal de operaciones y otros, cuando no se aplica una norma específica. Mientras que los estándares son normas de obligatorio cumplimiento, las recomendaciones son sugerencias con enfoques generales que brindan la flexibilidad necesaria para circunstancias imprevistas (Harris, 2013).

2.2.5. Los procedimientos

Son actividades completamente detalladas y definidas paso a paso que indican lo que se debe realizar para lograr un objetivo determinado. Las actividades establecidas en los procedimientos pueden ser desarrolladas por usuarios finales, personal de TI, directivos, personal de operaciones, proveedores y clientes, entre otros, cuya intervención sea indispensable para alcanzar el objetivo. Los procedimientos detallan cómo la política, los estándares y las directrices se implementarán realmente en un entorno operativo. Deben ser lo suficientemente detallados para ser comprensibles y útiles para un grupo diverso de personas. Se consideran el nivel más bajo en la cadena de documentación porque están más cerca de los activos de información (en comparación con las políticas) (Harris, 2013).

En síntesis...

El objetivo de la seguridad de la información es garantizar la disponibilidad, integridad y confidencialidad de esta. Para lograrlo, las organizaciones cuentan con diferentes referentes aceptados a nivel mundial y que hacen uso de herramientas, tales como procedimientos, recomendaciones, definición de líneas base, estándares y políticas, que facilitan su adopción.

Referencias

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.

Real Academia Española (RAE) (2017). *Diccionario de la lengua española.* Recuperado de http://dle.rae.es/?id=LXrOqrN

Referencias de imágenes

Bloomua. (s.f.). *Activos de información* [Vectores]. Recuperado de https://es.123rf.com/search.php?word=activo+de+informacion&srch_lang=es&imgtype=&Submit=+&t_word=&t_lang=es&orderby=0&sti=msyslo637vyd4rvp98|&mediapopup=31672130

Fancycravel. (s.f.). *Valor* [Fotografía]. Recuperado de https://pixabay.com/es/ipad-comprimido-tecnolog%C3%ADa-contacto-820272/

Geralt. (s.f.). *Datos* [Fotografía]. Recuperado de https://pixabay.com/es/social-medios-de-comunicaci%C3%B3n-1989152/

Geralt. (s.f.). *Orden* [Fotografía]. Recuperado de https://pixabay.com/es/social-medios-de-comunicaci%C3%B3n-1989152/

Geralt. (s.f.). *Veracidad* [Fotografía]. Recuperado de https://pixabay.com/es/cadena-articulada-personales-2850276/

Jemastock. (s.f.). *Riesgo materializado* [Vectores]. Recuperado de https://www.freepik.es/vector-premium/pirata-informatico-robando-cuentas-hackeo-dinero_2451045.htm

kalhh. (s.f.). *Control de virus* [Fotografía]. Recuperado de https://pixabay.com/es/equipo-virus-troyano-programa-1446108/

INFORMACIÓN TÉCNICA

FACULTAD DE
INGENIERÍA, DISEÑO
E INNOVACIÓN

Módulo 1: Teoría de la Seguridad

Unidad 1: Principios de la seguridad de la información

Escenario 1: Definiciones de la seguridad de la información

Autor: Alexandra Peña Daza

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