Seguridad en redes, protección de datos y políticas en ciberseguridad.

Breve descripción:

En un entorno digital en constante evolución, garantizar la seguridad de la información es esencial. Este componente formativo aborda los fundamentos de la ciberseguridad, la protección de redes, la gestión de datos personales y las políticas organizacionales, incorporando estándares como ISO 27001 y herramientas prácticas para mitigar riesgos y enfrentar amenazas cibernéticas.

Mayo 2025

Tabla de contenido

Introducción 4

1. Seguridad en redes 7

1.1. Conceptos asociados a la seguridad en redes 8

1.2. Modelo OSI y su relación con la ciberseguridad 9

1.3. Topologías de red 10

1.4. Controles típicos de seguridad en una red 11

1.5. Casos reales de seguridad en redes 13

1.6. Seguridad en redes inalámbricas 15

2. Protección de datos personales y privacidad 16

2.1. Habeas Data y normatividad relacionada 19

2.2. Herramientas de ciberseguridad 20

2.3. Buenas prácticas para la ciberseguridad y el ciberespacio 22

3. Las políticas y documentación en ciberseguridad 26

3.1. Administración de la Política de Seguridad de la Información 28

3.2. Documentación derivada de la política 30

3.3. Norma ISO 27001 y otros estándares 31

Síntesis 34

Material Complementario 35

Glosario 36

Referencias bibliográficas 38

Créditos 41

Introducción

Este componente formativo aborda la seguridad en redes, la protección de datos personales y la gestión de políticas en ciberseguridad. En un entorno digital cada vez más interconectado, es fundamental garantizar la integridad, confidencialidad y disponibilidad de la información mediante estrategias como el uso del modelo OSI, controles de red y buenas prácticas de protección.

La privacidad y el derecho al Habeas Data adquieren relevancia ante la creciente circulación de datos sensibles, lo que exige el uso de herramientas y acciones concretas para minimizar riesgos. A su vez, la implementación de políticas de seguridad y la adopción de estándares como la norma ISO 27001 permiten establecer lineamientos eficaces para proteger los activos de información.

Comprender estos elementos fortalece la capacidad de respuesta ante amenazas cibernéticas y promueve una cultura organizacional orientada a la prevención y al cumplimiento normativo. Para comprender la importancia del contenido y los temas abordados, se recomienda acceder al siguiente video.

Video 1. Seguridad en redes, protección de datos y políticas en ciberseguridad

Enlace de reproducción del video

Síntesis del video: Seguridad en redes, protección de datos y políticas en ciberseguridad
En el mundo digital actual, garantizar la seguridad en redes y la protección de datos personales es más importante que nunca. La interconexión de dispositivos y la constante circulación de información sensible requieren mecanismos efectivos para proteger la integridad, confidencialidad y disponibilidad de los datos. Para ello, es esencial comprender el modelo OSI (Open Systems Interconnection), las diferentes topologías de red y los controles de seguridad, los cuales permiten prevenir accesos no autorizados y mitigar riesgos como los ataques

informáticos. Estos conceptos son fundamentales para establecer una infraestructura tecnológica segura.

La protección de datos personales, respaldada por el derecho de Habeas Data, juega un papel crucial en la preservación de la privacidad. El uso adecuado de herramientas y buenas prácticas en ciberseguridad es necesario para minimizar vulnerabilidades y garantizar la privacidad de los usuarios en un entorno digital expuesto a amenazas.

Además, la implementación de políticas de seguridad de la información, junto con normativas internacionales como la ISO 27001, proporciona un marco sólido para gestionar la seguridad de los datos y establecer directrices claras dentro de las organizaciones.

Comprender estos elementos fortalece la capacidad de respuesta ante amenazas cibernéticas y promueve una cultura organizacional orientada a la prevención y el cumplimiento normativo.

1. Seguridad en redes

La seguridad en redes constituye un pilar esencial en el entorno digital actual, donde la constante digitalización de la información y la interconexión de dispositivos han incrementado los riesgos para la integridad, confidencialidad y disponibilidad de los datos. Este ámbito va mucho más allá de la instalación de firewalls o antivirus; se trata de un enfoque integral que abarca el diseño arquitectónico de las redes, el control de accesos y la formación de los usuarios.

El modelo OSI (Open Systems Interconnection), por ejemplo, ofrece una estructura lógica que permite analizar las vulnerabilidades presentes en cada capa de comunicación. Mientras la capa física requiere mecanismos de control de acceso físico, la capa de aplicación demanda estrategias específicas contra amenazas como malware o ataques de ingeniería social. A su vez, técnicas como la segmentación de redes, el uso de redes privadas virtuales (VPN) y el cifrado de extremo a extremo fortalecen la protección frente a accesos no autorizados e intercepciones.

Uno de los mayores desafíos continúa siendo el factor humano. La mayoría de incidentes de ciberseguridad se originan en errores o descuidos por parte de los usuarios, lo que hace indispensable implementar políticas claras, programas de formación continua y protocolos de respuesta ante incidentes.

Normas internacionales como la ISO 27001 orientan la adopción de buenas prácticas y controles efectivos, siempre que sean aplicadas de forma consciente y adaptativa. La seguridad en redes debe asumirse como un proceso constante que evoluciona con las amenazas, y representa una inversión estratégica para proteger los activos digitales y garantizar la confianza en el entorno organizacional.

1.1. Conceptos asociados a la seguridad en redes

En el panorama digital actual, la seguridad en redes representa un pilar esencial para salvaguardar la integridad, confidencialidad y disponibilidad de la información. Las redes actúan como el sistema circulatorio de las organizaciones contemporáneas, facilitando el flujo continuo de datos entre dispositivos, usuarios y sistemas. No obstante, esta conectividad permanente también incrementa la exposición a amenazas cibernéticas, que van desde ataques de ransomware altamente sofisticados hasta intrusiones silenciosas orientadas al robo de información crítica.

La seguridad en redes trasciende el uso de herramientas tecnológicas; se configura como una disciplina estratégica que integra hardware, software, normativas y la formación del recurso humano. Su propósito es establecer un entorno digital resiliente, en el que los datos puedan circular y almacenarse con un nivel mínimo de riesgo, garantizando la protección de las organizaciones y los usuarios.

Entre los principios fundamentales que rigen esta área se encuentran:

- ✓ **Confidencialidad**: restringe el acceso a la información únicamente a usuario autorizados.
- ✓ **Integridad**: asegura que los datos no sean modificados sin autorización.
- ✓ **Disponibilidad**: garantiza el acceso oportuno a los sistemas y datos.
- ✓ **Autenticación**: verifica la identidad de quienes acceden a los recursos digitales.

Estos conceptos constituyen la base de múltiples estrategias de ciberseguridad aplicadas en sectores empresariales y gubernamentales, con el fin de proteger la infraestructura de red frente a un entorno de amenazas en constante evolución.

1.2. Modelo OSI y su relación con la ciberseguridad

El modelo OSI (Open Systems Interconnection) es una referencia teórica que describe cómo interactúan los sistemas de comunicación a través de una red. Se organiza en siete capas, cada una con funciones específicas:

1) **Capa física**: maneja la transmisión de datos en forma de señales eléctricas, ópticas o de radio.
2) **Capa de enlace de datos**: asegura la transferencia libre de errores entre dispositivos directamente conectados.
3) **Capa de red**: encargada del direccionamiento y encaminamiento de los paquetes a través de distintas redes.
4) **Capa de transporte**: garantiza la entrega confiable y en orden de los datos entre sistemas extremos.
5) **Capa de sesión**: establece, mantiene y finaliza sesiones de comunicación entre aplicaciones.
6) **Capa de presentación**: gestiona el formato de los datos, su compresión y el cifrado.
7) **Capa de aplicación**: proporciona servicios directamente al usuario final, como correo electrónico o navegación web.

Para presentar cómo funciona el modelo OSI en un proceso cotidiano, se puede considerar el caso de una comunicación por correo electrónico. Emma desea enviar un mensaje a su colega Javier. Ella redacta el mensaje en su aplicación de correo, lo que

involucra la capa de aplicación. Luego, el texto se convierte a un formato estándar en la capa de presentación, y se inicia una conexión mediante la capa de sesión.

La capa de transporte fragmenta el mensaje en paquetes, mientras la capa de red determina la ruta más eficiente. La capa de enlace de datos garantiza que cada paquete llegue sin errores, y en la capa física, los datos se transmiten como señales a través del medio físico.

Este recorrido evidencia que la seguridad es esencial en cada capa, desde el cifrado en la capa de presentación, hasta la protección contra accesos no autorizados en las capas de red y enlace. Comprender el modelo OSI permite identificar en qué puntos se deben aplicar controles para proteger la información de forma integral.

1.3. Topologías de red

La forma en que se estructuran las redes influye directamente en su rendimiento, escalabilidad y nivel de seguridad. Estas estructuras, conocidas como topologías de red, determinan cómo se conectan los dispositivos entre sí y cómo fluye la información a través de ellos.

Algunas de las topologías más comunes incluyen:

a) Topología en estrella

Todos los dispositivos están conectados a un nodo central, generalmente un `switch` o `router`. Su principal ventaja es la facilidad de configuración y gestión, ya que cualquier cambio o fallo en un nodo periférico no afecta al resto de la red. Sin embargo, si el nodo central presenta una falla, toda la red se ve comprometida, lo que lo convierte en un punto crítico de seguridad.

b) Topología en bus

Utiliza un único canal de comunicación compartido por todos los dispositivos. Es económica y fácil de instalar, pero sufre problemas de colisión de datos y sufre una alta vulnerabilidad: un daño en el cable principal puede interrumpir toda la red.

c) Topología en anillo

Cada dispositivo está conectado con el siguiente formando un círculo cerrado. Los datos circulan en una sola dirección o en ambas, según el diseño. Aunque es eficiente en el uso de recursos, un fallo en un solo nodo puede afectar la transmisión, a menos que se implementen mecanismos de autorrecuperación.

d) Topología en malla

Cada nodo está interconectado con múltiples dispositivos. Esta topología ofrece alta redundancia y confiabilidad, ideal para entornos que requieren máxima disponibilidad y tolerancia a fallos, aunque implica un mayor costo y complejidad en la implementación.

Comprender estas estructuras permite seleccionar la más adecuada según los requerimientos de seguridad, rendimiento y disponibilidad de cada organización.

1.4. Controles típicos de seguridad en una red

La protección de una red requiere una combinación de herramientas, políticas y buenas prácticas diseñadas para prevenir, detectar y responder a amenazas. Entre los controles más comunes y efectivos se encuentran:

1) **Firewalls**: actúan como barreras entre redes internas y externas, filtrando el tráfico según reglas establecidas para bloquear accesos no autorizados.

2) **Sistemas de Detección y Prevención de Intrusos (IDS/IPS)**: analizan el tráfico de red en tiempo real para identificar comportamientos anómalos y, en el caso de los IPS, detener amenazas activamente.
3) **Cifrado de datos**: garantiza la confidencialidad de la información durante la transmisión mediante protocolos como TLS o mediante el uso de redes privadas virtuales (VPN).
4) **Autenticación multifactor (MFA)**: añade capas adicionales de verificación, como códigos temporales o biometría, para reforzar el acceso seguro a sistemas sensibles.
5) **Segmentación de redes**: divide la red en zonas o subredes independientes para limitar el movimiento lateral de amenazas en caso de una brecha.
6) **Listas de control de acceso (ACL)**: permiten definir reglas precisas sobre qué usuarios o dispositivos pueden acceder a determinados recursos o servicios.
7) **Control de acceso basado en roles (RBAC)**: asigna permisos de acuerdo con las funciones laborales, reduciendo la exposición innecesaria a información sensible.
8) **Sistemas SIEM (Security Information and Event Management)**: recopilan, correlacionan y analizan eventos de seguridad para detectar ataques complejos y generar alertas en tiempo real.
9) **Control de acceso a la red (NAC)**: evalúa el cumplimiento de políticas de seguridad en los dispositivos antes de permitir su conexión a la red.
10) **Prevención de pérdida de datos (DLP)**: monitoriza y restringe el envío no autorizado de información confidencial fuera de la organización.

11) **Copias de seguridad y recuperación ante desastres**: aseguran la disponibilidad de la información en caso de fallos, ataques o eventos inesperados.

Estos controles deben implementarse de manera coordinada, adaptándose al contexto de cada organización y actualizándose constantemente para enfrentar nuevas amenazas.

1.5. Casos reales de seguridad en redes

La seguridad en redes es esencial para proteger la información y las infraestructuras tecnológicas de las organizaciones frente a una amplia variedad de amenazas cibernéticas. A lo largo de los años, diversas empresas y entidades gubernamentales han sido víctimas de ataques que han comprometido no solo la confidencialidad de los datos, sino también la confianza de los usuarios. Estos incidentes evidencian la necesidad de contar con medidas de seguridad efectivas y un enfoque estratégico que abarque desde la protección física de los sistemas hasta la educación continua de los usuarios. A continuación, se presentan dos casos reales que muestran cómo la falta de controles adecuados puede resultar en consecuencias devastadoras para las organizaciones y sus clientes.

Caso 1: el ataque a Yahoo

En 2013 y 2014, Yahoo sufrió una de las mayores brechas de seguridad de la historia, comprometiendo más de 3.000 millones de cuentas de usuario. Los atacantes explotaron una vulnerabilidad en el sistema de seguridad de Yahoo, logrando acceder a información personal sensible como correos electrónicos, contraseñas y datos de seguridad. Lo más alarmante de este caso fue la falta de cifrado en ciertas bases de

datos, lo que permitió que los datos fueran accesibles incluso cuando se empleaban contraseñas cifradas.

La brecha de seguridad pasó desapercibida durante varios años, lo que evidenció la importancia de contar con monitoreo constante, cifrado robusto y autenticación multifactor como medidas preventivas. Este incidente subraya la necesidad de aplicar buenas prácticas de seguridad desde el diseño de los sistemas hasta su implementación.

Caso 2: el ciberataque a una empresa de energía

En 2015, un sofisticado ataque cibernético dirigido a la red eléctrica de Ucrania dejó a cientos de miles de personas sin electricidad durante varias horas. Los atacantes, presuntamente respaldados por un grupo de hackers rusos, utilizaron técnicas de phishing para obtener credenciales de acceso de los empleados y, finalmente, comprometieron los sistemas de control industrial. Este ataque demostró la vulnerabilidad de las infraestructuras críticas y la importancia de implementar segmentación de redes, monitoreo constante y políticas de control de acceso más estrictas.

Además, la rapidez con la que los atacantes se infiltraron destacó la necesidad de mejorar la capacitación en seguridad cibernética y la conciencia de los empleados sobre los riesgos asociados con el phishing y otros vectores de ataque.

Estos casos enseñan cómo las brechas de seguridad no solo afectan a las organizaciones, sino también a sus usuarios y a la infraestructura crítica. Desde la implementación de conceptos fundamentales como la confidencialidad e integridad de los datos, hasta la adopción de medidas de seguridad avanzadas como firewalls,

segmentación de redes y cifrado, cada aspecto de la seguridad en redes es vital para fortalecer las defensas. El modelo OSI proporciona una base teórica para entender en qué capas de comunicación deben aplicarse las medidas de seguridad, mientras que las topologías de red y los controles de seguridad juegan un papel crucial en la prevención de ataques cibernéticos. A medida que las amenazas evolucionan, mantenerse actualizado con las mejores prácticas y estándares de seguridad es esencial para proteger los datos y la privacidad en un mundo cada vez más digitalizado.

1.6. Seguridad en redes inalámbricas

Las conexiones inalámbricas son una parte integral de la vida digital moderna, ya que permiten que dispositivos como laptops, smartphones y tablets se conecten a la red sin necesidad de cables físicos. Estas redes funcionan a través de un identificador llamado SSID (Service Set Identifier), el cual es visible para los dispositivos cercanos. Aunque es posible configurar un router inalámbrico para que no difunda su SSID, este método no debe considerarse una solución definitiva para proteger la red, ya que los ciberdelincuentes aún pueden detectar la red mediante técnicas de análisis.

Una de las primeras medidas para mejorar la seguridad de una red inalámbrica es cambiar el SSID predeterminado y la clave inicial de acceso del router. Además, es crucial activar las opciones de seguridad inalámbrica, como el cifrado WPA2 o WPA3, para proteger la transmisión de datos. Estas tecnologías de cifrado son esenciales para evitar que los datos sean interceptados por personas no autorizadas.

Sin embargo, es importante tener en cuenta que incluso con WPA2 o WPA3 activado, las redes inalámbricas pueden seguir siendo vulnerables a ciertos ataques, como el ataque de diccionario o el ataque de fuerza bruta. Por ello, es recomendable implementar otras medidas complementarias, como el uso de redes privadas virtuales

(VPN) para proteger la privacidad de las comunicaciones y asegurarse de que los dispositivos conectados a la red estén adecuadamente protegidos con software antivirus y firewalls.

La seguridad en redes inalámbricas es un aspecto crítico en el contexto de la ciberseguridad, ya que la facilidad de acceso a estas redes también aumenta el riesgo de intrusiones. Implementar las mejores prácticas y mantener una vigilancia constante es fundamental para proteger la red contra posibles amenazas.

2. Protección de datos personales y privacidad

En la era digital, la protección de los datos personales y la privacidad se ha convertido en un aspecto fundamental. Millones de personas comparten diariamente información en línea sin ser plenamente conscientes de los riesgos asociados. Desde interacciones en redes sociales hasta transacciones bancarias, nuestros datos circulan constantemente por la red, lo que los convierte en un blanco atractivo para los ciberdelincuentes.

El derecho a la privacidad y a la protección de los datos ha motivado la creación de leyes y regulaciones que buscan salvaguardar la información de los ciudadanos. A continuación, se presentan algunos conceptos clave relacionados:

- ✓ **Datos personales**: cualquier información que permita identificar a una persona, como el nombre, dirección, número de teléfono, correo electrónico, información financiera o datos biométricos.
- ✓ **Privacidad**: es el derecho de cada individuo a controlar su información personal, así como a decidir cómo, cuándo y con quién compartirla.

- ✓ **Ciberseguridad**: conjunto de medidas y prácticas orientadas a proteger los sistemas informáticos y los datos digitales frente a accesos no autorizados, ataques y otros riesgos.
- ✓ **Habeas Data**: es un derecho fundamental que permite a cualquier persona conocer, actualizar y rectificar la información personal almacenada en bases de datos públicas o privadas. Está reconocido en legislaciones como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Protección de Datos Personales en varios países de América Latina. Este derecho otorga a los ciudadanos la posibilidad de:
    - Solicitar información sobre los datos que una organización almacena sobre ellos.
    - Rectificar datos incorrectos o desactualizados.
    - Eliminar información que ya no sea necesaria o que se haya recolectado de manera indebida.

Como un caso real se encuentra el escándalo de Facebook y Cambridge Analytica, considerado una de las mayores crisis de privacidad de datos en la historia reciente. Este hecho se dio a conocer en 2018, cuando se reveló que la consultora británica Cambridge Analytica accedió de manera indebida a los datos personales de aproximadamente 87 millones de usuarios de Facebook sin su consentimiento.

¿Cómo ocurrió la filtración?

a) En 2014, Aleksandr Kogan, investigador de la Universidad de Cambridge, desarrolló una aplicación llamada This Is Your Digital Life, que ofrecía un test de personalidad.

b) Al instalarla, los usuarios otorgaban acceso a su información y también a la de sus contactos, debido a las políticas permisivas de Facebook en ese momento.
c) Aunque solo 270.000 personas utilizaron la app, se extrajeron datos de millones de perfiles adicionales sin autorización.
d) La información recolectada fue vendida a Cambridge Analytica, que la utilizó para crear perfiles psicológicos y diseñar campañas políticas altamente segmentadas, influyendo en procesos como la elección de Donald Trump (EE.UU., 2016) y el referéndum del Brexit (Reino Unido).

A continuación, se presentan los impacto y consecuencias de esta filtración:

- ✓ Facebook fue duramente criticado por su falta de control sobre los datos de los usuarios.
- ✓ La empresa fue sancionada con multas millonarias, incluyendo 5.000 millones de dólares por parte de la Comisión Federal de Comercio (FTC) de EE.UU.
- ✓ Este escándalo impulsó reformas legales y una mayor conciencia sobre la necesidad de regular el uso de datos personales.
- ✓ Cambridge Analytica se disolvió en mayo de 2018, tras la presión internacional y la pérdida de credibilidad.

Este caso evidenció la urgente necesidad de que las plataformas digitales adopten políticas más transparentes y responsables frente al tratamiento de los datos personales, así como de fortalecer la legislación en torno a la privacidad y la protección de la información.

2.1. Habeas Data y normatividad relacionada

El Habeas Data es un derecho fundamental que garantiza a las personas el control sobre su información personal contenida en bases de datos públicas o privadas. Este derecho protege la privacidad y permite a los ciudadanos conocer, actualizar, rectificar y, en ciertos casos, eliminar sus datos personales cuando hayan sido recolectados o tratados de forma indebida.

La finalidad del Habeas Data es garantizar que los datos personales sean tratados conforme a los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y seguridad. Su ejercicio fortalece la autonomía del individuo en la era digital y promueve la responsabilidad en el tratamiento de la información.

Es importante relacionar las principales facultades del Habeas Data:

- ✓ Consultar los datos personales almacenados por cualquier entidad pública o privada.
- ✓ Actualizar y corregir la información que resulte incompleta, inexacta o desactualizada.
- ✓ Solicitar la supresión de datos cuyo tratamiento no respete los principios legales o ya no sea necesario.
- ✓ Revocar la autorización otorgada para el tratamiento de los datos, cuando no exista una obligación legal o contractual que lo impida.

Diversos países han establecido normativas que garantizan el derecho al Habeas Data y regulan el tratamiento de los datos personales, buscando proteger la privacidad de los ciudadanos y establecer responsabilidades claras para quienes gestionan dicha información:

A. **Colombia**: la Ley 1266 de 2008 y la Ley 1581 de 2012 son los principales marcos legales sobre protección de datos personales en Colombia. Estas normas establecen los deberes de los responsables del tratamiento de datos y los derechos de los titulares. Además, la Sentencia C-748 de 2011 de la Corte Constitucional reafirma el Habeas Data como un derecho autónomo e independiente, complementario al derecho a la intimidad.
B. **Unión Europea**: el Reglamento General de Protección de Datos (GDPR), en vigor desde 2018, es una de las normativas más estrictas a nivel global. Otorga a los ciudadanos europeos amplios derechos sobre sus datos personales, incluyendo el derecho al olvido y a la portabilidad de datos.
C. **Latinoamérica**: países como México, Argentina, Brasil, Chile y Perú han adoptado leyes específicas que reconocen el Habeas Data y regulan el tratamiento de datos personales. La Ley General de Protección de Datos Personales (LGPD) en Brasil es un ejemplo reciente que establece obligaciones similares al GDPR europeo.

En resumen, el Habeas Data no solo protege la privacidad de los ciudadanos, sino que también impone a las organizaciones la responsabilidad de tratar los datos de manera ética, segura y transparente.

2.2. Herramientas de ciberseguridad

La ciberseguridad se apoya en diversas herramientas diseñadas para prevenir, detectar y responder a amenazas digitales que pueden comprometer la privacidad, la integridad y la disponibilidad de los datos. Estas herramientas son fundamentales tanto en entornos personales como corporativos, y su uso adecuado fortalece las defensas frente a ciberataques.

a) **Antivirus y antimalware**: son programas que detectan, bloquean y eliminan software malicioso, como virus, troyanos, spyware o ransomware. Algunas soluciones modernas, como Bitdefender o Kaspersky, integran motores de análisis en tiempo real y escaneo basado en inteligencia artificial para prevenir amenazas emergentes.

b) **Gestores de contraseñas**: permiten crear, almacenar y recuperar contraseñas complejas sin necesidad de memorizarlas. Aplicaciones como LastPass, Bitwarden o 1Password aseguran las credenciales mediante cifrado, ayudando a evitar prácticas inseguras como usar la misma contraseña en múltiples servicios.

c) **Autenticación Multifactor (MFA):** añade una capa extra de seguridad al requerir más de una forma de autenticación para acceder a una cuenta o sistema. Por ejemplo, además de la contraseña, se puede requerir un código enviado al celular o una huella digital. Esto dificulta que un atacante acceda, aunque tenga la clave principal.

d) **Redes Privadas Virtuales (VPN)**: cifran el tráfico de internet del usuario y ocultan su dirección IP, proporcionando anonimato y seguridad en redes públicas. Son útiles para proteger la navegación cuando se usa Wi-Fi en lugares como cafeterías o aeropuertos, y para acceder a contenido restringido geográficamente.

e) **Firewalls**: actúan como una barrera entre una red segura y otra no confiable, filtrando el tráfico entrante y saliente. Pueden ser de hardware o software, y son esenciales para bloquear accesos no autorizados.

f) **Sistemas de detección y prevención de intrusos (IDS/IPS)**: estas herramientas monitorean el tráfico de red en busca de patrones

sospechosos. Si se detecta una amenaza, pueden generar alertas (IDS) o actuar directamente para bloquear el ataque (IPS).

El uso combinado de estas herramientas, junto con prácticas seguras como la actualización constante del software y la formación en ciberseguridad, permite mitigar de manera efectiva los riesgos asociados a las amenazas digitales actuales.

2.3. Buenas prácticas para la ciberseguridad y el ciberespacio

La protección de los datos personales y la seguridad en el entorno digital requieren una participación activa tanto del usuario como de las organizaciones. A continuación, se presentan buenas prácticas divididas en dos niveles: el del usuario final y el de la infraestructura tecnológica.

Desde el rol del usuario final:

- ✓ **Usar contraseñas seguras y diferentes para cada cuenta**: emplear contraseñas robustas es esencial para evitar accesos no autorizados. El uso de gestores de contraseñas como Bitwarden, LastPass o 1Password facilita la creación, almacenamiento y actualización de contraseñas complejas.
- ✓ **Evitar compartir información sensible en redes sociales**: publicar ubicaciones en tiempo real, rutinas o datos familiares puede facilitar ataques dirigidos como el robo de identidad, acoso o fraudes. Los ciberdelincuentes suelen analizar redes sociales para responder preguntas de seguridad o suplantar identidades.
- ✓ **Revisar los permisos de las aplicaciones antes de instalarlas**: muchas aplicaciones solicitan acceso a funciones innecesarias como micrófono,

cámara o geolocalización. Es importante revisar estos permisos para evitar que se recopile o venda información sin consentimiento.

- ✓ **Actualizar frecuentemente el software y los sistemas operativos**: las actualizaciones corrigen vulnerabilidades críticas. Ignorarlas deja los dispositivos expuestos a ataques como ransomware, spyware o brechas de seguridad.
- ✓ **Evitar redes Wi-Fi públicas sin protección**: estas redes pueden ser interceptadas por atacantes. El uso de VPN (Red Privada Virtual) es recomendable para cifrar la conexión y proteger la privacidad.

Desde la gestión de la Infraestructura Tecnológica (TI):

a) **Evaluar los riesgos**: conocer qué activos deben protegerse ayuda a asignar recursos y justificar las inversiones en ciberseguridad.
b) **Establecer políticas de seguridad**: incluir roles claros, normas sobre contraseñas, uso de dispositivos, acceso a la información y acciones frente a incidentes.
c) **Implementar medidas de seguridad físicas**: controlar el acceso a servidores, redes y espacios críticos, así como contar con sistemas de extinción de incendios adecuados.
d) **Controlar los recursos humanos**: verificar antecedentes y establecer protocolos de acceso según el perfil de cada trabajador.
e) **Realizar copias de seguridad periódicas**: es fundamental automatizar respaldos y probar su restauración con regularidad para evitar la pérdida de datos.

f) **Mantener los sistemas actualizados**: instalar parches de seguridad para prevenir ataques por vulnerabilidades conocidas.

g) **Aplicar controles de acceso**: definir niveles de privilegio y permisos diferenciados por funciones y áreas.

h) **Monitorear la red**: usar herramientas de análisis de tráfico, detección de intrusiones y alertas para reaccionar en tiempo real ante amenazas.

i) **Capacitar a los usuarios**: sensibilizar sobre fraudes comunes como phishing, ransomware o ingeniería social. La educación continua es clave.

j) **Cifrar la información**: todo dato confidencial (archivos, correos, bases de datos) debe estar cifrado para evitar accesos indebidos incluso si se pierde el dispositivo.

A continuación, se presentan algunos casos representativos que permiten analizar vulnerabilidades comunes en el ámbito digital, así como identificar buenas y malas prácticas en la protección de la información.

A. Caso 1. Uso inadecuado de contraseñas

Una persona adquiere un nuevo portátil y se le solicita actualizar la contraseña de la red. Al tener dificultades para recordar sus contraseñas personales, consulta a un amigo, quien le sugiere reutilizar una contraseña ya existente. Además, le confiesa que suele anotarlas en la última página de su agenda.

Análisis: esta actitud revela una baja cultura de ciberseguridad. Reutilizar contraseñas incrementa el riesgo de accesos no autorizados si alguna de ellas se ve comprometida. Además, almacenarlas en papel sin protección es un riesgo físico

evidente. Es recomendable el uso de gestores de contraseñas y autenticación multifactor.

B. Caso 2. Accesos innecesarios a plataformas sensibles

Una analista de soporte técnico recibe privilegios de administrador en la plataforma de gestión de clientes debido a un error en la configuración de permisos. Sin ser consciente de ello, accede a información sensible como datos bancarios y contratos.

Análisis: este incidente resalta la importancia de implementar controles de acceso adecuados. La falta de segmentación de permisos puede derivar en filtración de información, incluso si el acceso es involuntario. El principio de menor privilegio debe ser una norma básica en la infraestructura TI.

C. Caso 3. Phishing y robo de credenciales

Laura, una emprendedora, recibe un correo que simula provenir de su proveedor de pagos. Ingresa sus datos en un enlace falso, lo que resulta en el robo de sus credenciales y movimientos no autorizados en su cuenta bancaria.

Análisis: este caso presenta una técnica común de ciberataque, el phishing. Resalta la necesidad de verificar los remitentes, evitar ingresar datos en enlaces no verificados, y contar con protección adicional como la autenticación multifactor. La educación en ciberseguridad es clave para prevenir estos incidentes.

D. Caso 4. Ransomware en el sector salud

Una enfermera en un hospital en Bogotá accede a un enlace malicioso desde su correo. Horas después, los sistemas hospitalarios se bloquean con un mensaje de

ransomware solicitando un rescate en criptomonedas. Las operaciones son suspendidas y se impone una multa por violación de la normativa de protección de datos.

Análisis: el caso evidencia la vulnerabilidad de infraestructuras críticas como la salud. La capacitación del personal, los filtros de seguridad en correos y las copias de respaldo son esenciales. Además, demuestra cómo una acción individual puede comprometer todo un sistema institucional.

Caso 5. Software sin actualizar en entidades públicas

Un funcionario en Cali conecta su portátil sin actualizar a la red interna municipal. Hackers aprovechan una vulnerabilidad conocida para acceder a bases de datos con información de dos millones de ciudadanos, que luego es vendida en la dark web.

Análisis: este incidente subraya la importancia de mantener actualizados los sistemas. Las actualizaciones y parches de seguridad corrigen errores críticos. El descuido en este aspecto puede generar consecuencias graves como robo de identidad, fraudes y pérdida de credibilidad institucional.

3. Las políticas y documentación en ciberseguridad

En la era digital, la información se ha convertido en uno de los activos más valiosos para organizaciones e individuos. La creciente cantidad de amenazas cibernéticas y el aumento en la sofisticación de los ataques han hecho necesario establecer políticas de seguridad de la información. Estas políticas permiten proteger los datos, minimizar los riesgos y garantizar los principios fundamentales de la ciberseguridad: la confidencialidad, la integridad y la disponibilidad.

La Política de Seguridad de la Información es un conjunto de normas y directrices que establece cómo se protege la información dentro de una organización. Su objetivo

principal es prevenir accesos no autorizados, asegurar el correcto funcionamiento de los sistemas y responder de manera efectiva ante posibles incidentes.

A partir de esta política, se generan documentos clave que definen la estructura operativa de la seguridad informática en las organizaciones. Entre ellos se destacan:

a) **Normas de seguridad**: son especificaciones técnicas y organizativas diseñadas para aplicar la política de seguridad.

- ✓ **Ejemplo 1**: una empresa tecnológica implementa una norma que obliga a usar autenticación multifactor (MFA) para acceder a sistemas internos.
- ✓ **Ejemplo 2**: un banco exige el cifrado completo de disco en todos sus dispositivos corporativos, para evitar accesos indebidos en caso de extravío.

b) **Procedimientos de seguridad**: son descripciones detalladas sobre cómo aplicar las normas establecidas.

- ✓ **Ejemplo 1**: una empresa define un procedimiento de gestión de contraseñas en el que los empleados deben cambiarlas cada 90 días y utilizar combinaciones alfanuméricas seguras.
- ✓ **Ejemplo 2**: un hospital establece un procedimiento que restringe el acceso a las historias clínicas, permitiendo el ingreso únicamente al personal autorizado mediante permisos diferenciados.

c) **Plan de Continuidad del Negocio (BCP)**: son estrategias para garantizar la operación de la organización frente a interrupciones o incidentes de seguridad.

- ✓ **Ejemplo 1**: una tienda virtual implementa servidores de respaldo en la nube, lo que le permite mantener su plataforma activa durante una caída del centro de datos principal.
- ✓ **Ejemplo 2**: un banco diseña un plan para que sus cajeros automáticos sigan operando, aunque ocurra una falla en su infraestructura de TI.

d) **Plan de respuesta a incidentes**: establece las acciones que se deben tomar ante vulneraciones o ciberataques.

- ✓ **Ejemplo 1**: una empresa de software define un protocolo que, ante un ataque de ransomware, requiere desconectar los sistemas afectados, alertar al equipo de seguridad y restaurar desde copias de seguridad.
- ✓ **Ejemplo 2**: un hospital activa un protocolo específico ante accesos no autorizados a registros médicos, que incluye la revocación de credenciales comprometidas y una auditoría para evaluar el alcance del incidente.

3.1. Administración de la Política de Seguridad de la Información

La administración de la Política de Seguridad de la Información es un proceso estratégico orientado a proteger los datos críticos de una organización. Su objetivo principal es establecer directrices claras para preservar la confidencialidad, integridad y disponibilidad de la información, en alineación con los objetivos institucionales y los requisitos legales y normativos.

Un paso fundamental en esta administración es la evaluación de riesgos, que permite identificar los activos valiosos, las amenazas potenciales y las vulnerabilidades existentes. Este análisis facilita la priorización de controles y la asignación eficiente de recursos. Con base en ello, se definen normas y procedimientos específicos para la

implementación de controles técnicos (como cifrado, cortafuegos o firewalls) y controles organizacionales (roles, funciones y responsabilidades).

La alta dirección cumple un papel clave al aprobar y respaldar la Política de Seguridad de la Información, lo cual demuestra compromiso con la cultura de seguridad y garantiza los recursos necesarios para su aplicación. En paralelo, es esencial establecer programas de capacitación y concienciación para que todo el personal comprenda sus responsabilidades, desde el uso adecuado de contraseñas hasta la notificación de incidentes.

La política debe integrar un Plan de Continuidad del Negocio, que defina cómo mantener las operaciones ante eventos críticos, y un Plan de Respuesta a Incidentes, que establezca las acciones necesarias frente a brechas de seguridad. Ambos planes deben ser probados de forma periódica mediante simulacros y ejercicios controlados.

La monitorización y auditoría son componentes clave para evaluar el cumplimiento de la política. Herramientas como los sistemas SIEM (Security Information and Event Management) permiten el análisis en tiempo real de los registros de actividad, mientras que las auditorías internas y externas verifican la eficacia de los controles establecidos.

El marco normativo ISO/IEC 27001 brinda una estructura estandarizada para la implementación y gestión de la Política de Seguridad de la Información. Este modelo incorpora el ciclo de mejora continua PDCA (Planificar, Hacer, Verificar, Actuar), y su certificación constituye un respaldo frente a clientes, socios y entes reguladores.

Entre los desafíos más comunes se encuentran la resistencia al cambio por parte de los colaboradores y la evolución constante de las amenazas cibernéticas, lo que

requiere actualizaciones frecuentes de la política. Por ello, esta no debe entenderse como un documento estático, sino como un instrumento dinámico que debe revisarse de forma anual o ante cambios significativos en la tecnología, el entorno normativo o la infraestructura.

Una política de seguridad efectiva debe lograr un equilibrio entre protección y productividad, evitando controles excesivos que interfieran con la operatividad. Su éxito depende del compromiso colectivo, donde cada miembro de la organización asuma la protección de la información como una responsabilidad compartida.

3.2. Documentación derivada de la política

La documentación derivada de la Política de Seguridad de la Información incluye varios documentos clave que permiten implementar, gestionar y auditar las directrices establecidas. Cada uno de estos documentos desempeña un papel crucial en la ejecución de políticas de seguridad de manera eficiente y en el cumplimiento de los requisitos organizacionales y legales. Los principales documentos derivados son:

- ✓ **Normas de seguridad**

Especifican los requisitos técnicos y organizacionales para aplicar las políticas de seguridad de la información, como las normativas sobre la autenticación multifactor o el cifrado de dispositivos corporativos.

- ✓ **Procedimientos de seguridad**

Detallan las acciones a seguir para implementar las normas de seguridad, tales como las pautas para la creación y gestión de contraseñas o los procedimientos de acceso a sistemas críticos.

- ✓ **Planes de continuidad del negocio**

Establecen las estrategias para mantener las operaciones esenciales ante incidentes de seguridad, asegurando que la empresa pueda seguir funcionando en caso de una crisis.

- ✓ **Planes de respuesta a incidentes**

Definen las acciones específicas que deben tomarse ante la detección de un incidente de seguridad, como el protocolo de restauración tras un ataque de ransomware o el procedimiento de respuesta ante un acceso no autorizado.

3.3. Norma ISO 27001 y otros estándares

La ISO 27001 es un estándar internacional clave para la gestión de seguridad de la información. Establece los requisitos para crear, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Su principal objetivo es proteger la confidencialidad, integridad y disponibilidad de la información mediante un enfoque sistemático, minimizando riesgos y asegurando el cumplimiento con normativas legales.

Beneficios clave de la implementación de la ISO 27001:

- ✓ **Protección de datos**: reduce vulnerabilidades ante ciberataques y fugas de datos.
- ✓ **Cumplimiento normativo**: ayuda a la organización a alinearse con leyes y regulaciones.
- ✓ **Confianza de clientes**: la certificación ISO 27001 es reconocida globalmente y mejora la reputación corporativa.

- ✓ **Mejora continua**: enfoque basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) que fomenta la mejora constante del SGSI.

La ISO 27001 se estructura en 10 cláusulas principales que abarcan aspectos como la planificación, evaluación de riesgos, y mejora continua, y está estrechamente relacionada con otros estándares de la serie ISO 27000 que cubren diferentes aspectos de la seguridad de la información y la privacidad.

Algunos estándares complementarios de la familia ISO 27000 incluyen:

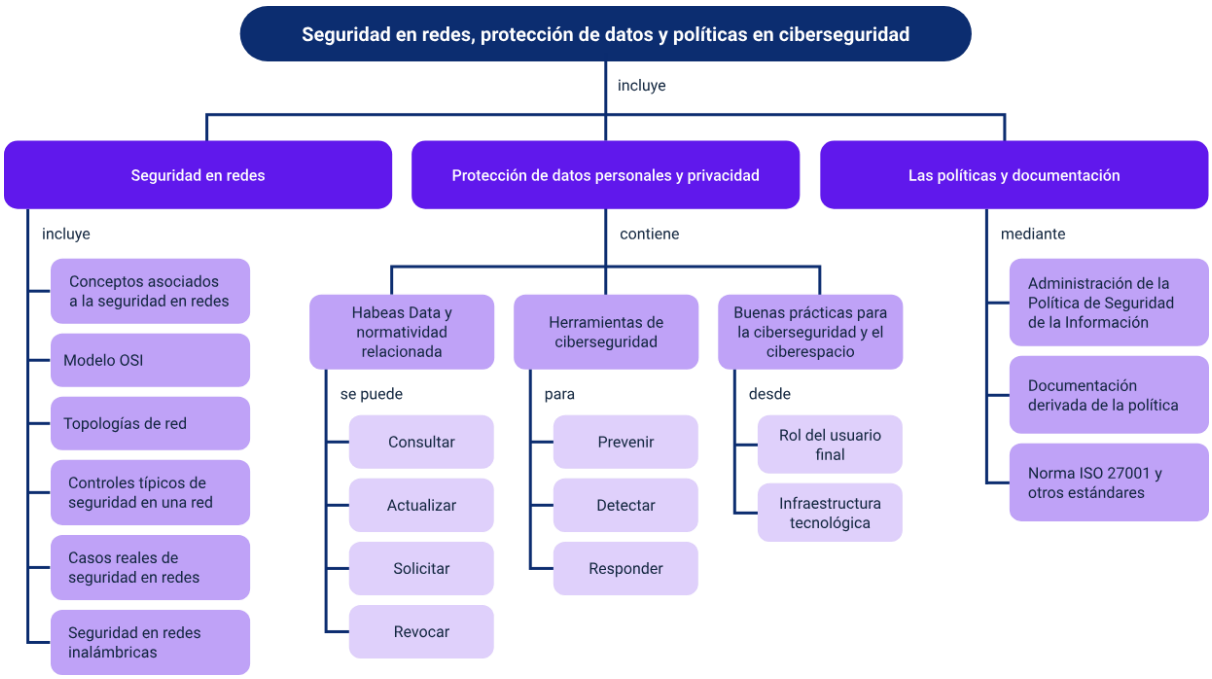
- ✓ ISO/IEC 27000 – Vocabulario y principios básicos.
- ✓ ISO/IEC 27002 – Código de prácticas para controles de seguridad.
- ✓ ISO/IEC 27005 – Gestión de riesgos.
- ✓ ISO/IEC 27017 – Seguridad en la nube.
- ✓ ISO/IEC 27018 – Protección de datos personales en la nube.
- ✓ ISO/IEC 27701 – Extensión para privacidad (PIMS).
- ✓ ISO/IEC 27031 – Resiliencia TI para continuidad del negocio.
- ✓ ISO/IEC 27034 – Seguridad en aplicaciones.
- ✓ ISO/IEC 27040 – Almacenamiento seguro.
- ✓ ISO/IEC 27035 – Gestión de incidentes.

En conclusión, la Norma ISO 27001 no actúa de forma aislada, sino que forma parte de una familia de estándares que permiten construir un sistema de gestión integral y robusto en materia de seguridad de la información. Estos estándares complementarios proporcionan lineamientos específicos sobre control, gestión de riesgos, privacidad, continuidad del negocio, seguridad en la nube, entre otros aspectos críticos. Su implementación coordinada fortalece la capacidad de una organización para

proteger sus activos de información, garantizar el cumplimiento normativo y responder eficazmente ante incidentes, consolidando así una cultura organizacional orientada a la seguridad y mejora continua.

Síntesis

Este componente formativo aborda los principios fundamentales de la seguridad en redes, incluyendo conceptos clave, el modelo OSI, las topologías de red y los controles de seguridad, así como casos reales y particularidades de redes inalámbricas. También se enfoca en la protección de datos personales y la privacidad, integrando el análisis del Habeas Data, las herramientas de ciberseguridad y las buenas prácticas en el ciberespacio. Finalmente, se profundiza en la administración de la Política de Seguridad de la Información, la documentación derivada de dicha política y el marco normativo representado por la norma ISO 27001 y los estándares complementarios, esenciales para una gestión integral de la ciberseguridad.



Material Complementario

Tema	Referencia	Tipo de material	Enlace del recurso
Seguridad en redes	Ecosistema de Recursos Educativos Digitales SENA. (2023). Seguridad en la red [Video]. YouTube.	Video	https://www.youtube.com/watch?v=TwacC-0rwFs
Protección de datos personales y privacidad	Ecosistema de Recursos Educativos Digitales SENA. (2023). Buenas prácticas y criterios de seguridad en la red [Video]. YouTube.	Video	https://www.youtube.com/watch?v=ODHXTKN4-Ok
Las políticas y documentación en ciberseguridad	Ecosistema de Recursos Educativos Digitales SENA. (2021). Ataques a la seguridad de la red [Video]. YouTube.	Video	https://www.youtube.com/watch?v=x56FT_OVARQ

Glosario

Autenticación Multifactor (MFA): método de seguridad que requiere múltiples formas de verificación para acceder a un sistema.

Cifrado: proceso de codificar datos para proteger su confidencialidad durante la transmisión o almacenamiento.

Confidencialidad: principio que garantiza que la información solo sea accesible para usuarios autorizados.

Firewall: sistema que filtra el tráfico de red para bloquear accesos no autorizados.

GDPR (Reglamento General de Protección de Datos): normativa europea que regula el tratamiento de datos personales.

Habeas Data: derecho que permite a las personas controlar su información personal en bases de datos.

IDS/IPS (Sistemas de Detección y Prevención de Intrusiones): herramientas que monitorean y bloquean actividades maliciosas en redes.

Integridad: principio que asegura que los datos no sean alterados de manera no autorizada.

ISO 27001: estándar internacional para implementar Sistemas de Gestión de Seguridad de la Información (SGSI).

Modelo OSI (Open Systems Interconnection): marco teórico de siete capas que describe cómo se comunican los sistemas en una red.

Privacidad: derecho a controlar cómo se recopila, usa y comparte la información personal.

Riesgo: posibilidad de que una amenaza explote una vulnerabilidad, causando daños.

Segmentación de red: división de una red en partes para limitar el acceso y contener brechas.

VPN (Red Privada Virtual): tecnología que cifra la conexión a Internet para proteger la privacidad.

WPA2/WPA3: protocolos de cifrado para redes inalámbricas que evitan accesos no autorizados.

Referencias bibliográficas

Asociación Española de Normalización (UNE). (2021). Publicada la Norma UNE-EN ISO/IEC 27701 para la Gestión de la Privacidad de la Información. https://www.une.org/la-asociacion/sala-de-informacion-une/notas-de-prensa/publicada-la-norma-une-en-isoiec-27701-para-la-gestion-de-la-privacidad-de-la-informacion/

Caballero Velasco, M. Á. (2015). El libro del hacker. Anaya Multimedia.

Cano, J. E. (2018). Ciberseguridad y protección de datos personales en Colombia. Ediciones Jurídicas Gustavo Ibáñez.

Congreso de Colombia. (2012). Ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de Colombia. (2013). Decreto 1377 de 2013 reglamentario de la Ley 1581 de 2012.

Ferrer, E. A. (2023). Estudios de cibercrimen. Ediciones Olejnik.

Gómez, L. A., & Rodríguez, M. P. (2020). Gestión de riesgos en seguridad informática: Enfoque práctico para organizaciones colombianas. Editorial Universidad del Rosario.

Instituto Nacional de Ciberseguridad de España (INCIBE). (2022). Guía de introducción a la ciberseguridad.

Instituto Nacional de Tecnologías de la Comunicación (INTECO). (2017). Guía para la implementación de ISO 27001 en pymes.

ISACA. (2013). COBIT 5: A business framework for the governance and management of enterprise IT. ISACA.

Joyanes Aguilar, L. (2018). Industria 4.0: La cuarta revolución industrial. Alfaomega.

Martínez, R. H. (2019). Protección de datos y habeas data en Latinoamérica. Editorial Legis.

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity – Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Organización Internacional de Normalización (ISO). (2015). ISO/IEC 27032:2012 Guidelines for cybersecurity.

Organización Internacional de Normalización (ISO). (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. https://www.iso.org/standard/54534.html

Paredes, A. R. Z., Quevedo, I. M. S., & Chalacán, L. J. M. (2020). Seguridad informática en las PyMES de la ciudad de Quevedo. Journal of Business and Entrepreneurial Studies: JBES, 4(2), 232–241.

Pérez, C. A., & González, F. J. (2021). Seguridad en redes y criptografía aplicada. Ediciones de la U.

Perlroth, N. (2017). All 3 Billion Yahoo Accounts Were Affected by 2013 Attack. The New York Times. https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Ramírez, E. M. (2017). Manual de cumplimiento GDPR para empresas colombianas. Editorial Temis.

Rincón, O. L. (2022). Ciberseguridad estratégica: Enfoque desde la normativa colombiana. Universidad Externado de Colombia.

Stallings, W. (2019). Cryptography and network security: Principles and practice (7th ed.). Pearson.

Superintendencia de Industria y Comercio (SIC). (2020). Guía para la implementación del Principio de Responsabilidad Demostrada.

Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer networks (5th ed.). Pearson Education.

Wikipedia. (2025, abril 21). Escándalo de datos de Facebook-Cambridge Analytica. Wikipedia. https://es.wikipedia.org/wiki/Esc%C3%A1ndalo_de_datos_de_Facebook-Cambridge_Analytica

Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Créditos

Nombre	Cargo	Centro de Formación y Regional
Milady Tatiana Villamil Castellanos	Responsable Ecosistema de Recursos Educativos Digitales (RED)	Dirección General
Diana Rocío Possos Beltrán	Responsable de línea de producción	Centro de Comercio y Servicios - Regional Tolima
Javier Eduardo Díaz Machuca	Experto temático	Centro de Comercio y Servicios - Regional Tolima
Viviana Esperanza Herrera Quiñonez	Evaluadora instruccional	Centro de Comercio y Servicios - Regional Tolima
Oscar Ivan Uribe Ortiz	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
Juan Daniel Polanco Muñoz	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
Sebastian Trujillo Afanador	Desarrollador Fullstack	Centro de Comercio y Servicios - Regional Tolima
Ernesto Navarro Jaimes	Animador y productor audiovisual	Centro de Comercio y Servicios - Regional Tolima
Jorge Eduardo Rueda Peña	Evaluador de contenidos inclusivos y accesibles	Centro de Comercio y Servicios - Regional Tolima

Nombre	Cargo	Centro de Formación y Regional
Jorge Bustos Gómez	Validador y vinculador de recursos educativos digitales	Centro de Comercio y Servicios - Regional Tolima