**Universidad Nacional Autónoma de México**

**Facultad de Ingeniería** portada

División de Ciencias de la Ingeniería

Semestre 2025 – 2

**Sistemas Operativos**

*Tarea 8: Herramientas de trabajo*

Profesor: Cruz Sergio Aguilar Diaz

Grupo 02

Muñoz San Agustin Victoria Monserrat

Fecha de entrega: 19 de mayo de 2024

Contenido

[**Investigar los siguientes conceptos de Seguridad** 2](#_Toc195186458)

[ *Conceptos de seguridad informática* 2](#_Toc195186459)

[ *¿Qué es Ciberseguridad y sus conceptos básicos?* 3](#_Toc195186460)

[ *Define los siguientes conceptos:* 5](#_Toc195186461)

[o Amenaza 5](#_Toc195186462)

[o Vulnerabilidad 6](#_Toc195186463)

[o Ataque 7](#_Toc195186464)

[o Intruso 8](#_Toc195186465)

[ *¿Qué es malware y sus diferentes variedades?* 9](#_Toc195186466)

[ *¿Qué herramientas existen para proteger los sistemas?* 14](#_Toc195186467)

[ *¿Cuáles son algunas recomendaciones para protección de la información?* 16](#_Toc195186468)

[**Conclusiones** 18](#_Toc195186469)

[**Bibliografía** 19](#_Toc195186470)

# **Investigar los siguientes conceptos de Seguridad**

## *Conceptos de seguridad informática*

La seguridad informática, que es la abreviatura de seguridad de la Tecnología de la Información, es la práctica de proteger el activo informático de una organización sistemas informáticos, redes, dispositivos digitales, datos (de accesos no autorizados, filtración de datos, ciberataques y otras actividades maliciosas).

El ámbito de la seguridad informática es amplio y a menudo implica una mezcla de tecnologías y soluciones de seguridad. Trabajan conjuntamente para hacer frente a las vulnerabilidades de los dispositivos digitales, las redes informáticas, los servidores, las bases de datos y las aplicaciones informáticas.

Los ejemplos más citados de seguridad informática incluyen disciplinas de seguridad digital, como seguridad endpoint, seguridad en la nube, seguridad de red y seguridad de aplicaciones. Pero la seguridad de TI también incluye medidas de seguridad física (por ejemplo, cerraduras, tarjetas de identificación, cámaras de vigilancia) necesarias para proteger edificios y dispositivos que albergan datos y activos de TI.

La seguridad informática a menudo se confunde con la seguridad cibernética, una disciplina más estrecha que es técnicamente un subconjunto de seguridad informática. La ciberseguridad se centra principalmente en proteger a las organizaciones de ataques digitales, como ransomware, malware y estafas de phishing. Mientras que la seguridad de TI brinda servicios a toda la infraestructura técnica de una organización, incluidos sistemas de hardware, aplicaciones de software y endpoints, como computadoras portátiles y dispositivos móviles. La seguridad de TI también protege la red de la empresa y sus diversos componentes, como data centers físicos y basados en la nube.

## *¿Qué es Ciberseguridad y sus conceptos básicos?*

La ciberseguridad se refiere a cualquier tecnología, práctica y política para prevenir los ataques cibernéticos o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el ransomware y otros programas maliciosos, las estafas de phishing, el robo de datos y otras amenazas cibernéticas.

* **Contraseñas:** Claves que utilizamos para iniciar sesión o registrarnos en alguna aplicación o página web. Están formadas por una serie de caracteres (letras, números y caracteres especiales), que, en función de su complejidad, pueden hacerlas más seguras.
* **Copia de seguridad:** Copia de nuestros archivos y programas que puede almacenarse en otros dispositivos o soportes para evitar perder nuestra información en caso de fallo, pérdida o robo.
* **Spam:** Correo de tipo publicitario o malicioso no deseado que llega a nuestra bandeja de entrada con el único propósito de vendernos un producto, hacernos caer en algún fraude o infectar nuestros dispositivos.
* **Cifrado:** Proceso que sirve para convertir un documento o un archivo en una versión ilegible para todas aquellas personas que no posean la clave para descifrarlo. Sirve para proteger la información de todas aquellas personas que no deberían acceder a ella bajo ningún concepto.
* **Certificado digital:** Icono en forma de candado que suele aparecer a la izquierda de algunas URL de páginas web. Este icono significa que es una web que ha sido certificada por una entidad certificadora que acredita que se trata de una web segura. Lamentablemente, por sí mismo no implica que la web sea segura, ya que los ciberdelincuentes son capaces de engañar a estas entidades para utilizar sus certificados en sitios web fraudulentos y dotarlos de mayor credibilidad.
* **Cookies:** Pequeños archivos que contienen información que ha recopilado una determinada página web que hemos visitado y que se almacenan en nuestros dispositivos. Sirven principalmente para recabar información sobre nuestros hábitos de navegación y mostrarnos publicidad dirigida con información que pueda ser de nuestro interés.
* **Bulos:** Cadenas de mensajes con noticias o eventos alarmantes que no provienen de ninguna fuente fiable y solo buscan desinformar y crear confusión entre los usuarios que los reciben, principalmente a través de redes sociales y chats.

## *Define los siguientes conceptos:*

### Amenaza

Una amenaza de ciberseguridad se refiere a cualquier situación o caso que pueda tener consecuencias negativas para las operaciones, funciones, marca, reputación o imagen percibida de una empresa. Una amenaza de este tipo también puede afectar al acceso a los datos, su integridad y su valor, así como a las personas, los procesos y las tecnologías que participan en la gestión de dichos datos. Las amenazas cibernéticas suelen surgir cuando un ciberataque establece como objetivo los datos, sistemas informáticos, redes o dispositivos de una organización para obtener un acceso no autorizado o explotar cualquier vulnerabilidad del sistema de información, y comprometer así su confidencialidad, integridad o disponibilidad.

¿Por qué es importante la ciberseguridad?

Las amenazas de ciberseguridad pueden manifestarse de diversas formas, que incluyen virus, malware, ransomware, estafas de phishing y ataques de denegación de servicio (DoS). Las amenazas a la ciberseguridad plantean un riesgo especial para las organizaciones, al tener el potencial de provocar grandes pérdidas financieras, dañar la marca de una empresa e interrumpir sus operaciones. Las amenazas de ciberseguridad más habituales que pueden encontrarse las empresas incluyen las siguientes:

* **Brechas de datos:** Una brecha de datos se produce cuando un individuo no autorizado consigue acceder a datos confidenciales que pertenecen a una organización, y que pueden incluir información de clientes o empleados. Las consecuencias de las brechas de datos pueden abarcar desde las pérdidas financieras y de datos privados hasta daños a la reputación de la organización.
* **Ataques DoS y DDoS:** Un ataque DoS (denegación de servicio) consiste en sobrecargar un sistema con tráfico o solicitudes excesivas para bloquearlo o lograr que deje de estar disponible. Estos ataques pueden disrumpir gravemente las operaciones empresariales. Un ataque de denegación de servicio distribuido (DDoS) lleva lo anterior un paso más allá, al implicar a varios sistemas para sobrecargar simultáneamente al atacado, de modo que resulta todavía más efectivo para dejar sin conexión a un sitio web o sistema informático.

### Vulnerabilidad

En informática, una vulnerabilidad es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad. Las vulnerabilidades pueden ser de varios tipos, pueden ser de tipo hardware, software, procedimentales o humanas y pueden ser explotadas o utilizadas por intrusos o atacantes.

Para entenderlo mejor, una vulnerabilidad puede ser, por ejemplo:

* Un servicio de un sistema de computación corriendo en un determinado puerto lógico.
* Sistemas y aplicaciones no actualizados o parcheados que presentan múltiples vulnerabilidades.
* Una red Wifi abierta.
* Un puerto abierto en un firewall.
* Un insuficiente o inexistente control de acceso físico a las instalaciones.
* La no aplicación de una política de gestión de contraseñas.

Tipos de vulnerabilidad informática

* **Buffer overflow o desbordamiento de buffer:** se da cuando las aplicaciones no controlan la cantidad de datos que copian en el buffer y que al sobrepasar el tamaño de este pueden modificar zonas de memoria contiguas afectando a los datos que albergan.
* **Cross Site Scripting:** se basa en que los atacantes incrustan scripts en páginas web legítimas afectadas por esta vulnerabilidad y por las que navega el usuario. Este introduce datos como por ejemplo, su usuario y su contraseña, pero no en la web legítima si no en la del atacante, que roba así sus datos.
* **Inyección de SQL:** cuando no se validan los datos de entrada a formularios que se comunican con bases de datos se podría ejecutar código SQL malicioso que por ejemplo permitiera obtener datos confidenciales o corromper los datos de las tablas.



### Ataque

Un ciberataque es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital. Los actores de amenazas lanzan ciberataques por todo tipo de motivos, desde pequeños robos hasta actos de guerra. Utilizan varias tácticas, como ataques de malware, estafas de ingeniería social y robos de contraseñas, para obtener acceso no autorizado a sus sistemas objetivo.

¿Cuál es el objetivo de los ataques cibernéticos?

Los actores de amenazas suelen irrumpir en las redes informáticas porque buscan algo específico. Los objetivos comunes incluyen:

* Dinero
* Datos financieros de empresas
* Listas de clientes
* Datos de clientes, entre ellos información de identificación personal (PII) u otros datos personales confidenciales
* Direcciones de correo electrónico y credenciales de inicio de sesión
* Propiedad intelectual, como secretos comerciales o diseños de productos

En algunos casos, los atacantes cibernéticos no tienen intención de robar nada. Más bien, simplemente desean alterar los sistemas de información o la infraestructura de TI para perjudicar a una empresa, una agencia gubernamental u otro objetivo.

### Intruso

Un intruso es cualquier entidad (persona, software o incluso sistema automatizado) que accede o intenta acceder a un sistema informático o red sin autorización. Su objetivo puede ser espiar, robar datos, sabotear sistemas, causar interrupciones o simplemente explorar debilidades del sistema.

Tipos de Intrusos

* **Intruso externo:** Es alguien que no tiene ningún permiso legítimo para acceder al sistema.
  + Ejemplos: hackers, cibercriminales, scripts automatizados que buscan vulnerabilidades en internet.
* **Intruso interno:** Es un usuario que tiene algún nivel de acceso legítimo pero abusa de ese acceso.
  + Ejemplos: empleados descontentos, administradores que acceden a datos sin autorización específica.
* **Intrusos pasivos:** Observan o recolectan información sin modificarla.
  + Ejemplo: un espía que intercepta comunicaciones sin ser detectado.
* **Intrusos activos:** Realizan acciones que alteran o dañan el sistema.
  + Ejemplo: un atacante que borra archivos, instala malware o modifica configuraciones.

Métodos que usan los intrusos para acceder

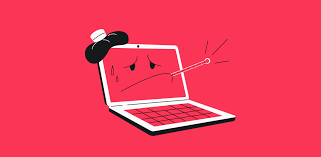
* **Explotación de vulnerabilidades:** Usan errores del software o configuraciones incorrectas.
* **Ingeniería social:** Manipulan a las personas para obtener acceso.
* **Fuerza bruta:** Prueban muchas combinaciones de contraseñas hasta encontrar la correcta.
* **Puertas traseras (backdoors):** Usan accesos ocultos creados maliciosamente.



## *¿Qué es malware y sus diferentes variedades?*

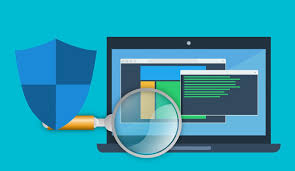
El malware hace referencia a aplicaciones o código malintencionados que dañan o alteran el uso habitual de los dispositivos de punto de conexión. Cuando un dispositivo se infecta con malware, puede que se acceda a él sin autorización, que los datos se pongan en peligro o que se te impida el acceso al dispositivo salvo que pagues un rescate.

Tipos de malware

* **Phishing:** El atacante se hace pasar por una fuente creíble para robar información confidencial a través de correos electrónicos, sitios web, mensajes de texto u otras formas de comunicación electrónica. Estos ataques proporcionan un mecanismo de distribución de malware. En los ataques habituales, se roban nombres de usuario, contraseñas, datos de la tarjeta de crédito e información bancaria.
* **Spyware:** El spyware se instala en un dispositivo sin el consentimiento del usuario o sin informar convenientemente. Cuando se instala, puede supervisar el comportamiento online, recopilar información confidencial, cambiar la configuración del dispositivo y disminuir su rendimiento.
* **Adware:** Se instala en un dispositivo sin el consentimiento del usuario. Pero, se centra en mostrar publicidad agresiva, normalmente en forma de elementos emergentes, para obtener dinero a través de los clics. Esta publicidad con frecuencia ralentiza el rendimiento del dispositivo. Los tipos de adware más peligrosos también pueden instalar software adicional, cambiar la configuración del explorador y hacer que un dispositivo sea vulnerable a otros ataques de malware.
* **Vulnerabilidades de seguridad y kits de vulnerabilidades de seguridad:** Las vulnerabilidades de seguridad utilizan las vulnerabilidades del software para sortear las protecciones de seguridad de un equipo e infectarlo. Los hackers malintencionados realizan análisis en busca de sistemas obsoletos con vulnerabilidades críticas y, después, se aprovechan de dichas vulnerabilidades implementando software malintencionado. Mediante la inclusión de shellcode en una vulnerabilidad de seguridad, los ciberdelincuentes pueden descargar más malware que infecta dispositivos y se infiltra en organizaciones.
* **Malware sin archivos:** Este tipo de ciberataque pueden llegar a través de paquetes de red malintencionados que se aprovechan de una vulnerabilidad y, después, instalan software malintencionado que reside únicamente en la memoria del kernel. Las amenazas sin archivos son especialmente difíciles de descubrir y quitar porque la mayoría de los programas antivirus no están diseñados para analizar el firmware.
* **Malware de macros:** Formas de automatizar tareas habituales con rapidez. El software malintencionado de las macros se aprovecha de esta funcionalidad e infecta archivos adjuntos del correo electrónico y archivos ZIP. Para engañar a los usuarios y hacer que abran los archivos, los ciberdelincuentes suelen ocultar el malware en archivos camuflados como facturas, recibos y documentos legales.
* **Ransomware:** Amenaza a una víctima con destruir o bloquear el acceso a datos críticos hasta que se pague un rescate. Los ataques son controlados por humanos, que tienen como objetivo una organización, usan configuraciones erróneas de seguridad y del sistema habituales para infiltrarse en la organización, recorrer su red empresarial y adaptarse al entorno y a cualquier debilidad. Un método habitual es el robo de credenciales, a través del cual un ciberdelincuente puede robar las credenciales de un empleado real para hacerse pasar por esa persona y acceder a sus cuentas.
* **Rootkits:** Oculta el malware en un dispositivo durante el máximo tiempo posible, a veces incluso años, para que robe información y recursos de manera continuada. Mediante la interceptación y modificación de los procesos estándar del sistema operativo, un rootkit puede alterar la información que el dispositivo presenta sobre sí mismo. Los rootkits también pueden conceder privilegios administrativos o elevados del dispositivo a los ciberdelincuentes, para que puedan controlar un dispositivo por completo y realizar acciones potencialmente malintencionadas, como robar datos, espiar a la víctima e instalar malware adicional.
* **Ataques a la cadena de suministro:** Este tipo de malware, que tiene como objetivo proveedores y desarrolladores de software, accede a códigos fuente, procesos de compilación o mecanismos de actualización en aplicaciones legítimas. Cuando un ciberdelincuente encuentra un protocolo de red no seguro, una infraestructura de servidor sin protección o prácticas de codificación no seguras, se infiltra, cambia los códigos fuente y oculta el malware en los procesos de compilación y actualización.
* **Estafas de soporte técnico:** Las estafas de soporte técnico, un problema que afecta a todo el sector, utilizan tácticas de intimidación para engañar a los usuarios y hacer que paguen por servicios de soporte técnico innecesarios que se pueden anunciar para resolver problemas falsos relacionados con un dispositivo, una plataforma o software. Con este tipo de software malintencionado, un ciberdelincuente puede llamar a un usuario directamente y fingir que es un empleado de una empresa de software. Cuando se han ganado la confianza del usuario, los atacantes suelen instar a las posibles víctimas a instalar aplicaciones o a proporcionar acceso remoto a sus dispositivos.
* **Troyanos:** Los troyanos aparentan ser aplicaciones o archivos legítimos para que el usuario se los descargue sin saberlo. Una vez descargados, pueden hacer lo siguiente:
  + Descargar e instalar malware adicional, como virus o gusanos.
  + Usar el dispositivo infectado para el fraude por clic.
  + Registrar las pulsaciones de teclas y los sitios web que visitas.
  + Enviar información (por ejemplo, contraseñas, detalles de inicio de sesión y el historial de exploración) sobre el dispositivo infectado a un hacker malintencionado.
  + Conceder al ciberdelincuente el control del dispositivo infectado.
* **Software no deseado:** Cuando un dispositivo tiene software no deseado, el usuario puede experimentar modificaciones en la experiencia de exploración web, falta de control sobre las descargas y las instalaciones, mensajes engañosos y cambios no autorizados en la configuración del dispositivo. Algunos tipos de software no deseado se instalan junto con software que los usuarios pretenden descargar.
* **Gusanos:** Suelen encontrarse en archivos adjuntos del correo electrónico, mensajes de texto, programas de uso compartido de archivos, sitios web de redes sociales, recursos compartidos de red y unidades extraíbles, y se distribuyen a través de una red aprovechando las vulnerabilidades de seguridad y copiándose a sí mismos. En función del tipo de gusano, puede robar información confidencial, cambiar tu configuración de seguridad o impedir que accedas a los archivos.
* **Mineros de monedas:** Los mineros de monedas utilizan los recursos informáticos de un dispositivo para la minería de criptomonedas. Las infecciones de este tipo de malware suelen empezar con un archivo adjunto del correo electrónico que intenta instalar malware o un sitio web que utiliza las vulnerabilidades de los exploradores web o se aprovecha de la potencia de procesamiento del equipo para agregar malware a los dispositivos.

## *¿Qué herramientas existen para proteger los sistemas?*

La selección adecuada y la implementación efectiva de estas herramientas son fundamentales para establecer una defensa robusta contra una amplia gama de amenazas cibernéticas, incluidos el malware, el phishing, el ransomware y los ataques de denegación de servicio (DDoS), entre otros.

* **Firewalls:** Actúan como una barrera entre redes internas seguras y redes externas no confiables, como Internet. Filtran el tráfico entrante y saliente basado en reglas de seguridad predeterminadas, lo que ayuda a prevenir accesos no autorizados y ataques cibernéticos.
* **Antivirus:** Los programas antivirus son esenciales para detectar y eliminar malware, como virus, troyanos y spyware. Utilizan firmas y algoritmos de detección de comportamiento para identificar amenazas y eliminarlas antes de que causen daño. Además, algunos antivirus modernos ofrecen protección en tiempo real y análisis heurístico avanzado.
* **Sistemas de Detección y Prevención de Intrusiones (IDS/IPS):** Los IDS monitorean continuamente una red en busca de actividades sospechosas o anómalas y generan alertas cuando detectan una posible intrusión. Los IPS, por otro lado, no solo detectan, sino que también previenen activamente los ataques al bloquear el tráfico malicioso.
* **Escáneres de Vulnerabilidades:** Estas herramientas identifican debilidades y agujeros de seguridad en sistemas y aplicaciones. Al realizar análisis regulares, los escáneres de vulnerabilidades permiten a las organizaciones fortalecer sus sistemas y reducir la superficie de ataque.
* **Herramientas de Gestión de Identidad y Acceso (IAM):** Las IAM ayudan a garantizar que solo los usuarios autorizados puedan acceder a los sistemas y datos. Utilizan métodos de autenticación como contraseñas, autenticación de dos factores y biometría para proteger el acceso.
* **Sistemas de Gestión de Eventos e Información de Seguridad (SIEM):** Los SIEM recopilan y analizan datos de seguridad de diversas fuentes para proporcionar una visión integral de la seguridad de la organización. Ayudan a detectar, responder y gestionar incidentes de seguridad de manera eficiente
* **Herramientas de Autenticación Multifactor (MFA):** Añade una capa adicional de seguridad al requerir múltiples formas de verificación antes de conceder acceso a un sistema. Esto puede incluir una combinación de contraseñas, códigos enviados a dispositivos móviles y datos biométricos.
* **Análisis de Tráfico de Red:** Estas herramientas monitorizan el tráfico de red en tiempo real para detectar comportamientos anómalos que puedan indicar un ataque cibernético. Al analizar patrones de tráfico, las organizaciones pueden identificar y mitigar amenazas potenciales.
* **Herramientas de Análisis de Malware:** Estas herramientas se centran en el análisis profundo de archivos y software en busca de malware utilizando técnicas como la emulación y el análisis de comportamiento para identificar amenazas que podrían pasar desapercibidas para los antivirus tradicionales.

Soluciones Tecnológicas Avanzadas

Para resolver problemas complejos y optimizar procesos en diversos sectores, presentamos tecnologías de vanguardia que permiten a las empresas innovar, mejorar la eficiencia operativa y ofrecer mejores servicios a sus clientes. Al adoptar tecnologías avanzadas, las organizaciones pueden mantenerse competitivas en un mercado en constante evolución, adaptarse rápidamente a los cambios y aprovechar nuevas oportunidades de negocio. Estas soluciones son:

* **Data Security Plus:** Data Security Plus de ManageEngine ofrece visibilidad en tiempo real sobre el acceso a los datos y herramientas para prevenir la pérdida de datos (DLP) y el acceso no autorizado. Sus características incluyen auditoría de archivos, análisis de archivos, prevención de fugas de datos y valoración de riesgos de datos.
* **ServiceDesk Plus:** Esta solución facilita la gestión de incidentes de seguridad y el cumplimiento normativo. Permite registrar, rastrear y resolver eficientemente incidentes de seguridad de datos personales, desde su detección hasta su resolución final.

## *¿Cuáles son algunas recomendaciones para protección de la información?*

* **Procura crear contraseñas seguras:** Utilizar la misma contraseña en todas las cuentas y que incluya fechas de nacimiento, aniversarios o números de teléfono te deja vulnerable ante los ciberataques. Por lo que una contraseña más elaborada será más difícil de adivinar por otros. Usa al menos 12 caracteres, entre ellos mayúsculas, minúsculas, símbolos y números. Además, para mayor seguridad te sugerimos crear contraseñas a partir de parafrases y cambiarlas cada 6 meses.
* **Usa la autenticación multifactor:** Esta función consiste en añadir dos o más factores para que un usuario tenga acceso a una aplicación o página web. Es como un muro extra de seguridad contra diferentes tipos de ciberataques, por lo que hace más complicado que hagan uso de tus datos personales.
* **Evita conectarte frecuentemente a redes públicas de Wi-Fi:** Existen muchos establecimientos que ofrecen Wi-Fi gratuito, lo cual es muy útil cuando estamos fuera de casa o de viaje. Sin embargo, te recomendamos utilizar tus datos o esperar a que llegues a casa, ya que no conocemos las medidas de seguridad de estos lugares públicos y los ciberatacantes podrían estar accediendo a todos los dispositivos que se conectan a ella.
* **Asegúrate de navegar en sitios web verificados:** Ingresa información o descarga archivos únicamente en sitios seguros. Para comprobar si es uno, apóyate en esta página o fíjate si la URL comienza con 'https' o ayuda; esto significa que cumple con el protocolo SSL (Secure Sockets Layer) y que los datos que compartas viajan por un canal cifrado.
* **Actualiza tus equipos periódicamente:** Las actualizaciones, además de añadir funcionalidades nuevas a tus dispositivos o cambios de diseños, también resuelven fallas de ciberseguridad de las versiones anteriores. Así que es fundamental que mantengas los programas y los sistemas de todos tus dispositivos actualizados.
* **Evita instalar aplicaciones de dudosa procedencia:** Instala aplicaciones que solo provengan de páginas o tiendas oficiales. Existen programas maliciosos que engañan a los usuarios para ser descargados y luego se ejecutan de forma oculta para tener acceso total a tu dispositivo y obtener tus datos personales.
* **Aprende a utilizar VPN para navegar en Internet:** Puedes mejorar tus medidas de seguridad al conectarte a Internet a través de una Red Privada Virtual (VPN), en vez de hacerlo directamente con el módem o router. Existe una gran variedad de VPN, entre ellos están: HMA, Private Internet Access, ExpressVPN y ‍CyberGhost VPN.
* **Utiliza un gestor de contraseñas:** Puede ser difícil recordar tus nombres de usuario y contraseñas de cada plataforma que utilizas, por lo que un gestor de contraseñas es la mejor solución, ya que genera por ti contraseñas seguras y las llena en el momento.
* **Instala antimalwares:** Los antivirus ya no son tan eficientes como los antimalwares, así que instalar uno de estos aumentará significativamente la protección de tu información ante las vulnerabilidades. Algunos pueden ser SentinelOne y Malware Bytes.
* **No compartas información personal en las redes sociales:** Todas las redes sociales tienen la opción de configurar la privacidad como necesites; tú eres el que define si tendrás un perfil público, privado o con restricciones de quién puede ver lo que publicas.

# **Conclusiones**

Después de estudiar los temas relacionados con la seguridad informática, me doy cuenta de lo esencial que es estar preparado frente a los riesgos digitales. Vivimos en una era donde casi toda nuestra información personal, académica o laboral depende de dispositivos y redes conectadas. Por eso, entender cómo proteger esa información se ha vuelto una necesidad, no una opción. Aprendí que una amenaza puede venir de muchos lugares, ya sea por un atacante externo o incluso desde dentro de una organización. También comprendí que una vulnerabilidad, por pequeña que parezca, puede abrir la puerta a un ataque que comprometa nuestros datos. El concepto de intruso me ayudó a entender que no siempre se trata de alguien con malas intenciones desde fuera, sino que puede ser un usuario legítimo que abusa de sus permisos.

Me quedó claro qué es el malware, cómo actúa y las muchas formas que puede tomar, desde virus hasta ransomware. Además, descubrí un conjunto amplio de herramientas de protección, como antivirus, firewalls, sistemas de detección de intrusos, cifrado y backups, que son fundamentales para mantener la seguridad. También tomé conciencia de que la mejor defensa comienza con uno mismo: usar contraseñas seguras, no confiar en mensajes sospechosos, tener buenos hábitos de navegación, y capacitarme continuamente. Proteger la información no es algo que se haga una sola vez, sino un compromiso constante. En definitiva, este tema me ayudó a ver que todos tenemos un rol activo en la protección digital, y que la prevención, el conocimiento y la responsabilidad son las claves para mantener nuestros sistemas y datos a salvo.

# **Bibliografía**

Anónimo (s.f). Amenaza de ciberseguridad. Hewlett Packard. Recuperado el 16 de abril de 2025 de https://www.hpe.com/mx/es/what-is/cybersecurity-threats.html

Anónimo (s.f). ¿Qué es una vulnerabilidad informática? Banco Santander. Recuperado el 16 de abril de 2025 de https://www.bancosantander.es/glosario/vulnerabilidad-informatica

Anónimo (2021). Conceptos básicos de ciberseguridad que debes conocer. INCIBE. Recuperado el 16 de abril de 2025 de https://www.incibe.es/ciudadania/blog/conceptos-basicos-de-ciberseguridad-que-debes-conocer

Anónimo. (s.f.) ¿Qué es el malware? Microsoft. Recuperado el 16 de abril de 2025 de https://www.microsoft.com/es-mx/security/business/security-101/what-is-malware

IBM. (s.f.). ¿Qué es la seguridad de TI? IBM. Recuperado el 16 de abril de 2025 de https://www.ibm.com/mx-es/topics/it-security

IBM. (s.f.). ¿Qué es un ciberataque? IBM. Recuperado el 16 de abril de 2025 de https://www.ibm.com/mx-es/topics/cyber-attack

Ambit Iberia Team. (2024). Herramientas y Tecnologías para Mejorar la Seguridad Informática. AMBIT IBERIARecuperado el 16 de abril de 2025 de https://www.ambit-iberia.com/blog/herramientas-y-tecnologias-seguridad-it

García, J. (2024). 12 consejos para proteger tus datos personales. Delta Protect. Recuperado el 16 de abril de 2025 de https://www.deltaprotect.com/blog/como-proteger-tus-datos-personales