- **Adware**: Código malicioso que despliega anuncios no deseados, frecuentemente en forma de pop-ups, y puede recopilar información sobre los hábitos de navegación del usuario.
- **Antivirus**: Programa diseñado para detectar y eliminar virus informáticos. Identifican y eliminan software malicioso, como virus y malware, que pueda comprometer la integridad de sistemas y datos.
- **Auditoría informática**: Examen y evaluación formal de los sistemas informáticos, infraestructura, políticas y operaciones de una organización. Inspección minuciosa para garantizar que la tecnología funcione de manera segura y eficiente, respaldando los objetivos generales del negocio.
- **Autenticación multifactor** *(MFA)*: Refuerza la seguridad del acceso al requerir múltiples formas de verificación antes de permitir la entrada, como contraseñas y códigos generados. La autenticación multifactor *(MFA)* añade capas de seguridad a los procesos de inicio de sesión tradicionales.
- **Botnets**: Conjuntos de dispositivos infectados controlados remotamente por un atacante para realizar acciones coordinadas, como ataques DDoS.
- **Ciberseguridad**: Área de la informática que se enfoca específicamente en la protección de sistemas, redes y programas informáticos contra amenazas digitales. Su alcance abarca la prevención, detección y respuesta a ataques cibernéticos. Esto incluye la protección contra malware, phishing, ataques de denegación de servicio (DDoS), y otras tácticas empleadas por actores malintencionados.
- **Ciclo de vida del desarrollo de software** *(SDLC, por sus siglas en inglés)*: Metodología estandarizada utilizada para la creación de aplicaciones informáticas. Proceso integral que abarca todas las etapas del desarrollo, desde la concepción inicial hasta el mantenimiento continuo. Además de definir las fases de desarrollo, el SDLC también funciona como una metodología de gestión de proyectos, permitiendo una organización y control eficientes.
- **DDoS** *(Distributed Denial of Service):* Ataque que intenta hacer que un servicio online no esté disponible mediante el uso masivo de tráfico falso.
- **Blue Team**: Grupo especializado en defender los sistemas y redes de ciberamenazas y ataques. Utilizan herramientas y estrategias, como identificar fallas de seguridad y verificar la efectividad de cada medida de seguridad implementada, para prevenir infracciones y mantener los datos seguros.
- **Red Team**: Grupo especializado en simular ataques informáticos reales dentro de una organización. El objetivo de estos equipos es identificar y corregir debilidades de seguridad, antes de que las aprovechen los ciberdelincuentes reales.

- **Purple Team**: Es un enfoque colaborativo, en el que los miembros tanto del lado defensivo (Equipo azul) como del ofensivo (Equipo rojo) trabajan juntos para mejorar la seguridad general, mediante la simulación de ataques, la identificación de debilidades y la mejora de las defensas.
- **Evaluación de vulnerabilidades** *(VA)*: Proceso fundamental para la seguridad informática. Sirve para identificar las debilidades en los sistemas informáticos y de red que los atacantes podrían aprovechar.
- **Firewall**: Sistema de seguridad de red que monitorea y controla el tráfico de entrada y salida. Actúa como una barrera protectora entre una red privada y el tráfico no autorizado de Internet. Los firewalls monitorean y controlan el tráfico basándose en un conjunto de reglas predefinidas.
- **Gestión de contraseñas**: Prácticas y herramientas para crear, almacenar y proteger contraseñas.
- **Gestión de Vulnerabilidades**: Identifica, evalúa y mitiga vulnerabilidades en sistemas y aplicaciones para prevenir posibles explotaciones por parte de atacantes.
- **Gobernanza de la seguridad de la información**: Proceso mediante el cual una organización gestiona su programa de seguridad informática. Funciona como el timón que dirige las actividades de seguridad y garantiza que se logren los objetivos de ciberseguridad.
- **Gusanos** *(Worms)*: Tipo de software malicioso que se propaga automáticamente a través de redes y sistemas. Aprovecha vulnerabilidades para infectar dispositivos conectados.
- **IDS** *(Intrusion Detection System)*: Sistema que monitorea redes o sistemas en busca de actividades maliciosas.
- **Ingeniería social**: Táctica astuta que utilizan los ciberdelincuentes para engañar a las personas y vulnerar las protecciones tecnológicas. En lugar de atacar directamente los sistemas informáticos, la ingeniería social se enfoca en las personas que los utilizan.
- **Malware**: Software diseñado con intenciones maliciosas con el objetivo de dañar o infiltrar en sistemas y dispositivos.
- **Pentesting** *(Pruebas de penetración)*: Evaluación de seguridad mediante simulación de ataques para identificar y corregir vulnerabilidades.
- **Phishing** *(suplantación de identidad)*: Conjunto de técnicas que persiguen un engaño. Los atacantes envían correos electrónicos o mensajes de texto falsos, que parecen provenir de una fuente legítima, como un banco o una empresa de tecnología. Estos mensajes intentan ganarse la confianza de la víctima y engañarla para que revele información confidencial, o haga clic en enlaces maliciosos que descargan malware
- **Ransomware**: Tipo de malware o código malicioso que encripta archivos en el sistema de la víctima y exige un rescate para restaurar el acceso. Puede causar daños significativos al bloquear el acceso a archivos críticos.

- **Riesgo**: Probabilidad de que una amenaza explote una vulnerabilidad y cause un impacto adverso en los activos de información de una organización. En términos simples, el riesgo surge de la combinación de la amenaza que busca explotar una vulnerabilidad específica.
- **Sistemas de detección de amenazas** *(TDS)*: Monitorean continuamente la red en busca de patrones anómalos que puedan indicar actividad maliciosa. Ayudan a identificar amenazas antes de que causen daño significativo.
- **Sistemas de prevención de intrusiones** *(IPS):* Detectan y previenen intrusiones en tiempo real, analizan patrones de tráfico y bloquean actividades maliciosas.
- **Spam** *(Correos basura)*: Consiste en correos electrónicos no solicitados que inundan la bandeja de entrada y obstaculizan la llegada de mensajes importantes.
- **Spoofed Emails**: Técnica usada para falsificar el encabezado de un correo electrónico, haciendo creer que el mensaje proviene de un remitente legítimo pero, en realidad, es falso.
- **Spyware**: Código que recopila información del usuario sin su conocimiento, como hábitos de navegación, contraseñas o datos personales, y los envía a terceros.
- **Tríada CIA**: Modelo fundamental en la seguridad de la información que se basa en tres pilares: confidencialidad, integridad, disponibilidad. Estos principios son esenciales para proteger la información y garantizar su correcto funcionamiento. La Tríada CIA ayuda a las organizaciones a proteger sus activos de información, mantener la confianza de los usuarios y cumplir con las regulaciones.
- **Troyanos** *(Trojans)*: Programas que aparentan ser legítimos pero ocultan intenciones maliciosas. Pueden permitir el acceso no autorizado o descargar malware adicional.
- **Virus**: Código malicioso que se adjunta a archivos legítimos y se propaga cuando estos archivos son ejecutados. Pueden infectar programas y replicarse a sí mismos en otros archivos