AMENAZAS	VULNERABILIDAD	CONTRAMEDIDAS
VIRUS	NO TENER ANTIVIRUS	ANTIVIRUS
Encriptación de datos sensibles y secuestro de los datos (Ramsonware)	• Phising, ingeniería social, negligencia • acceso remoto no autorizado en sistemas no securizados	Firewalls, Gestión de acceso y credenciales, Educación en sguridad de los usuarios; Copias de seguridad
Acceso a sistemas o a información mediante Inyección de código: SQL Injection, Cross-Site Scripting - XSS...	Aplicaciones mal programadas o sistemas mal configurados	validación y saneamiento de entradas; pricipio de mínimos privilegios; monitorización y auditoria
Difusión de software dañino	Parada de sistema	Software de eliminación de virus y software maliciosos. Procedimientos de reinstalación y configuración del sistema. Copias de seguridad.
Escapes de información.	Pérdida de confidencialidad.	Uso de técnicas de encriptación.
Adware	Publicidad Maliciosa mediante POP UPS	Intalación de Antimalware
Ataque por canal lateral	Dispositivos que emiten señales y pueden ser analizados-hackeados	Blinding (encriptar temporalmente los datos y consumiendo tiempo de ejecución a las operaciones para dificultar al atacante)
Gusano	Sistemas operativos	Actualizaciones y parches de Seguridad
Spam	Publicidad no Deseada	informacion, filtros.
Spyware	Descarga de Sotware Malicioso detrás de publicidad	Evitar descagas de links desconocidos
Man in the middle	Robo de información o su modificacion.	Acceder solo a sitios web seguros con certificado, actualizar software, autenticación de dos pasos.
Esteganografía	Virus de malware a traves de ocultacion en imagenes	Herraminetas especificas o antivirus/anti malware
Secuestro de sesiones	Uso de conexiones inseguras (HTTP en vez de HTTPS)	Uso de HTTPS en las conexiones

Ataques SQL Injecction	Falta de validación de entradas de usuarios	Uso de consultas parametrizadas, validación y saneamiento de entradas y realizar revisiones de código. Control de acceso.
Troyanos	Acceso a Petición de Datos, Descarga Programas nuevos	Firewall configurado, Antivirus actualizado
Malware	Introducir Software Malicioso	No haga clic en enlaces sospechosos ni descargue archivos adjuntos de fuentes desconocidas
Clickjacking	Aplicaciones web fraudulentas para falsificar el producto	Verificar que la conexión de las páginas utilicen el protocolo de seguridad "HTTPS"
Ataques DDoS	Ausencia de firewall que controlen este tipo de ataques	Defensas contra DDoS basadas en CDN, Barrido de DDoS en la nube, firewall de aplicaciones web, Protección contra DDoS en las instalaciones, Protección contra DDoS híbrida y Señalización en la nube
Phising	Ataque de petición datos Confidenciales	No usar links desconocidos
Análisis de tráfico de la red	Conocimientos de las pautas de actividad de la empresa	Encapsulamiento de protocolos
Keyloggers	Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares	Vigilar la relentalización Equipos
Suplantación de la identidad del usuario	Pérdida completa de confidencialidad e integridad	Sistemas de autenticación fuertes
Robo de información por USB no autorizado	Puerto USB habilitados sin restricciones	Deshabilitar los puertos cuando no sean necesarios. Uso de software de control y cifrado de datos.
Acceso no autorizado	NO usar autenticación multifactor	Implementar autenticación multifactor
Ataques Man in de middle	Comunicaciones sin cifrar	Implemetar HTTPS y certificados de seguridad para las comunicaciones web
Ramsonware	Correos electrónicos fraudulentos, sitios web maliciosos y redes sociales	Mantener actualizados los programas, antivirus y procurar no entrar a enlaces sospechosos que comprometan la seguridad del equipo
Trashing	No eliminar los archivos de nuestra papelera de reciclaje	Eliminar los archivos de forma periodica o en el caso de que sea información comprometida usar algún tipo de programa que ayude a eliminarlos completamente para evitar su recuperación

Quishing	Escanear codigos QR sin verificar la fuente	URL oficial, siempre puedes ver si una web tiene Phishing
MANINTHEMIDDLE Manipulación de las comunicaciones entre cliente y servidor, pudiendo robar o modificar info	Comunicaciones no cifradas entre cliente y servidor	Utilizar protocolos seguros como https
Troyanos	Acceso a datos	Antivirus y firewall actualizado