



PANORAMA DE AMENAZAS ENISA 2023

Extracto de las principales amenazas y recomendaciones

*Grupo de Trabajo sobre Ciberseguridad
Comisión de Sociedad Digital*

RANSOMWARE

El **ransomware** es un tipo de malware que toma por completo el control del equipo bloqueando o cifrando la información del usuario para, a continuación, pedir dinero a cambio de liberar o descifrar los ficheros del dispositivo.



Suponen el **31,3% de los incidentes registrados** en el periodo julio 2022 – julio 2023

Recomendaciones

- Implementar una **estrategia de copias de seguridad segura y redundante**. Mantener copias de seguridad de los datos sin conexión y cifradas que se comprueben periódicamente, siguiendo tus procedimientos de copia de seguridad.
- Crear, mantener y poner en práctica un **plan de respuesta a incidentes que se ponga a prueba periódicamente**.
- **Documentar** los flujos de comunicación, incluidos los procedimientos de respuesta y notificación durante un incidente. La **ransomware Response Checklist de CISA^(*)** puede ayudar a preparación.
- Asegurar que se dispone una **infraestructura de Internet segura**. Realizar **análisis periódicos de vulnerabilidades** para identificarlas y solucionarlas. Instalar **actualizaciones** (de seguridad) y **parches** con regularidad.
- Garantizar que la tecnología de **acceso remoto** u otros servicios expuestos estén **configurados de forma segura**, y que las políticas de **autenticación multifactor** y **contraseñas seguras** se gestionen, auditen y apliquen de forma activa en las cuentas de usuario.
- Aplicar los principios de **mínimo privilegio y separación de funciones**.
- **Concienciación y formación periódicas** en materia de seguridad son fundamentales, ya que el ransomware suele basarse en la ingeniería social **para inducir a los usuarios** a hacer clic en un enlace.
- **Colaborar** con homólogos y con los CERT nacionales.
- **Supervisar** la ejecución de procesos para **detectar anomalías**.
- Utilice el **filtrado de correo electrónico** para detectar mensajes maliciosos y eliminar archivos adjuntos ejecutables.
- Asegurar que sus **activos** están **inventariados, gestionados y bajo control**.
- Desplegar EDR/XDR^(*) y asegurar que las firmas están actualizadas.
- Utilizar **listas de aplicaciones permitidas, bloqueando** la ejecución de **software no autorizado**.

(*) Ver en Glosario

MALWARE

El **malware** es un programa informático (software, en inglés) cuya principal característica es que se ejecuta sin el conocimiento ni autorización del propietario o usuario del equipo infectado y realiza funciones en el sistema que son perjudiciales para el usuario y/o para el sistema.



Suponen el **8,24% de los incidentes registrados** en el periodo julio 2022 – julio 2023

Recomendaciones

- Todas las incluidas en caso del **ransomware** (ver anterior). A modo de resumen:

- **Estrategia de copias de seguridad segura y redundante**
- **Plan de respuesta a incidentes que se ponga a prueba periódicamente.**
- **ransomware Response Checklist de CISA**
- **infraestructura de Internet segura**
- **análisis periódicos de vulnerabilidades**
- Instalar **actualizaciones** (de seguridad) y **parches** con regularidad.
- **acceso remoto** u otros servicios expuestos estén **configurados de forma segura**, y que las políticas de **autenticación multifactor** y **contraseñas seguras**.
- **mínimo privilegio y separación de funciones.**
- **Concienciación y formación periódicas**
- **Colaborar** con homólogos y con los CERT
- **Supervisar** la ejecución de procesos para **detectar anomalías**
- **Filtrado de correo electrónico**
- **Activos** están **inventariados, gestionados y bajo control.**
- Desplegar EDR/XDR
- **listas de aplicaciones permitidas**



- Implementar la **detección de malware** para todos los **canales de entrada/salida**, incluidos los sistemas de correo electrónico, red, web y aplicaciones en todas las plataformas aplicables (es decir, servidores, infraestructura de red, ordenadores personales y dispositivos móviles).
- **Inspeccionar el tráfico SSL/TLS^(*)** permitiendo al **cortafuegos descifrar** lo que se **transmite hacia y desde** sitios web, comunicaciones por correo electrónico y aplicaciones móviles.

(*) Ver en Glosario

INGENIERÍA SOCIAL

La **Ingeniería social** es una técnica que emplean los ciberdelincuentes para ganarse la confianza del usuario y conseguir así que haga algo bajo su manipulación y engaño, como puede ser ejecutar un programa malicioso, facilitar sus claves privadas o comprar en sitios web fraudulentos.



*Suponen el **7,88%** de los incidentes registrados en el periodo julio 2022 – julio 2023*

Recomendaciones

- **Revisar y actualizar los planes de respuesta** a incidentes para adaptarlos a las **últimas tendencias identificadas** en materia de ataques de ingeniería social.
- Mantener una **visión general de la huella digital** de su organización y actualice esta información con frecuencia. Lo ideal es que esta actualización se realice automáticamente y que los cambios en la huella digital activen una alerta para investigaciones de seguimiento.
- **Designar a una persona** dentro de la organización para que realice investigaciones OSINT^(*) periódicas sobre su organización (asumiendo el papel de “outsider”).
- **Registrar de forma preventiva dominios** que se parezcan al nombre de la organización, incluidos TLD alternativos.
- **Revisar periódicamente la configuración del dominio** de la organización para que admita **mecanismos antifalsificación y de autenticación para filtrar el correo electrónico**.
- Adaptar las **formaciones de sensibilización** para tener en cuenta las nuevas **tendencias de la ingeniería social**. Considerar la posibilidad de impartir **formación a medida** centrada en los **departamentos** (RRHH, ventas, finanzas, personal informático y de seguridad, etc.)
- Asegurar que la infraestructura de la organización en la que pueden detectarse ataques de ingeniería social está **“preparada para la investigación forense”**, lo que significa que los registros pertinentes se recopilan con detalles suficientes para respaldar las investigaciones de respuesta a incidentes. Los registros deben ser completos, fiables, precisos y coherentes.
- Utilizar **funciones de seguridad del correo electrónico** que notifiquen al usuario el **envío de un mensaje** de un usuario con el que no haya interactuado antes.
- **Suscribirse fuente de transparencia de certificados**. Supervisar los nuevos dominios emitidos en busca de nombres que se parezcan al nombre o a los activos de su organización. **Suscribirse** a las alertas de los sitios de supervisión de violación de datos.
- Desplegar **reglas de detección que alerten de la presencia (o apertura) de archivos de imagen de disco** en sistemas en los que estos tipos de archivos no suelen estar presentes.
- **Bloquear el uso de imágenes de disco intercambiadas por correo electrónico**.
- Permitir sólo **aplicaciones de editores verificados** o para permisos específicos de bajo riesgo.

(*) Ver en Glosario

AMENAZAS CONTRA LOS DATOS

Las **amenazas contra los datos** tienen como objetivo bloquear el acceso a los datos, así como manipularlos (por ejemplo, envenenarlos) para interferir en el comportamiento del sistema.



Suponen el **20,1% de los incidentes registrados** en el periodo julio 2022 – julio 2023

Recomendaciones

- Contar con un equipo de especialistas con la habilidad y los conocimientos necesarios para responder a las violaciones de datos y mantener la **disponibilidad, confidencialidad e integridad de los datos**.
- Contar con una **estrategia de mitigación** adecuada: **conocimiento** de los **activos** que pueden ser **objeto de un ataque**, así como una evaluación de riesgos adecuad.
- Planificación y presupuestación adecuadas de los riesgos de la gestión de datos (violaciones y filtraciones de datos).
- Conformidad y la certificación.
- **Gestión de autorizaciones:** Los errores humanos y las malas configuraciones están en la base de muchas violaciones de datos. Una gestión adecuada de las autorizaciones que revise los privilegios de acceso en función de los cambios en los derechos de los usuarios y de los usuarios que abandonan una organización es clave para reducir los posibles ataques de amenazas internas.
- **Arquitecturas de confianza cero:** Las arquitecturas de confianza cero pueden aumentar la postura de seguridad de un sistema mediante la aplicación del paradigma "**nunca confíes, siempre verifica**".
- **Contraseñas únicas y seguras:** Las contraseñas únicas evitan el **compromiso de múltiples sistemas** con la violación de una sola contraseña. Las contraseñas seguras pueden aumentar la solidez del sistema frente a los ataques. Un gestor de contraseñas puede simplificar las actividades de los usuarios. La **autenticación multifactor** puede utilizarse para reforzar el proceso de autenticación mediante token o huellas dactilares.
- **Formación y educación de los usuarios:** Tanto el personal de seguridad informática como los usuarios finales deben recibir formación profesional y conocer las tendencias más recientes en ciberseguridad.
- **Auditoría de la seguridad de los datos:** identificar las lagunas y vulnerabilidades organizativas, así como el uso indebido de los datos. Las auditorías de seguridad pueden ser realizadas por expertos en seguridad o por terceros (por ejemplo, un modelo de pruebas de penetración), evaluando el riesgo de violación de datos.
- **Data sanitation:** protección de los datos a través de distintas técnicas, como la anonimización, la generalización, el cifrado, el enmascaramiento o el filtrado.
- Las contramedidas contra la manipulación (Data Poisonig^(*)) de datos.

(*) Ver en Glosario



AMENAZAS CONTRA LOS DATOS

- Soluciones de **prevención de pérdida de datos**: Inspeccionar y controlar la gestión y transferencia de archivos es clave para evitar que datos sensibles y personales o propiedad intelectual no salgan de la red corporativa o lleguen a un usuario sin acceso.
- **Copias de seguridad de los datos**: Las copias de seguridad de los datos son fundamentales para poder recuperarse rápidamente de los ataques. Las ubicaciones de las copias de seguridad deben estar distribuidas geográficamente y separadas para evitar que sean manipuladas por el mismo ataque. La redundancia geográfica también puede ayudar a prevenir daños originados por catástrofes naturales y apagones repentinos.
- **Crear un equipo de especialistas**: contar con un equipo de especialistas con las habilidades y conocimientos necesarios para **responder a ataques DDoS** para mantener la disponibilidad y el funcionamiento del sistema; conocimiento de los activos que pueden ser objeto de un ataque
- **Restauración del servicio**: debería existir un plan B para restaurar rápidamente los servicios críticos para el negocio y reducir el tiempo medio de recuperación.
- **Actualizar y parchear sistemas**: las reglas básicas de actualizar y parchear todos los sistemas deberían convertirse en un mantra, especialmente en escenarios que involucren Internet de las cosas (IoT) y dispositivos inteligentes.
- **Desplegar recursos suficientes para aumentar el costo de un ataque**: los ataques de denegación de servicio distribuido (DDoS) pueden contrarrestarse desplegando la mayor cantidad de recursos posible o trasladando el sistema objetivo a una infraestructura potente (por ejemplo, infraestructura en la nube). Por ejemplo, cuanto mayor sea el ancho de banda de un sistema o servicio, más difícil o costoso será un ataque exitoso para un ciberdelincuente.
- **Detección de anomalías** en las actividades de la red que pueden ser un **indicador** de un ataque de denegación de servicio distribuido (**DDoS**).
- Formación y educación en ciberseguridad: los ataques de denegación de servicio distribuido (DDoS) a menudo se basan en un conjunto sólido de actividades en la preparación que van desde la construcción de botnets hasta la coordinación y orquestación del ataque. Las medidas correctivas para estas amenazas dependen de una formación y educación correctas y completas en ciberseguridad.



ATAQUES A LA CADENA DE SUMINISTRO

Suponen menos del 1% de los incidentes registrados en el periodo julio 2022 – julio 2023

*El ataque a la cadena de suministro se dirige a la relación entre las organizaciones y sus proveedores. Para que un ataque se clasifique como ataque a la cadena de suministro, **tanto el proveedor como el cliente deben ser objetivos**. Esta definición excluye aquellos incidentes en los que, por ejemplo, las Librerías de los desarrolladores se vieron comprometidas pero sin el objetivo de atacar a una víctima específica.*

Recomendaciones

- Establecer un programa de **Gestión de Riesgos de Ciberseguridad en la Cadena de Suministro**(C-SCRM)
- Incluir a los **proveedores** clave en los **planes y ejercicios de continuidad del negocio y respuesta** a incidentes.
- En las campañas de concientización, incluir una advertencia de que los usuarios **no deben reutilizar contraseñas en diferentes proveedores**.
- **Eliminar brechas entre la seguridad física y la ciberseguridad**. Asegurar que el acceso físico a los dispositivos esté restringido y autenticado.
- Establecer protocolos para la **divulgación de vulnerabilidades y la notificación de incidentes**, así como protocolos para la **comunicación con terceras** partes durante los incidentes.
- Llevar a cabo **evaluaciones** por cuenta de terceros de los **proveedores críticos** (incluir en la evaluación tanto el software (o hardware) como el enfoque de un proveedor hacia la ciberseguridad). Confiar en la documentación aportada por el proveedor, pero verificar.
 - **Mantener** (y verificar automáticamente) un **inventario de proveedores** de hardware, software y servicios **de confianza**. Las conexiones desde dispositivos o software desconocidos o patrones de tráfico anormales de proveedores de servicios deben activar una alerta para inspecciones adicionales.
 - Implementar **procesos de gestión de parches** para verificar dependencias no utilizadas, dependencias no mantenidas o previamente vulnerables, características, componentes, archivos y documentación innecesarios. Asegurar que todo el software esté actualizado.
 - **Documentar y alinear responsabilidades** en servicios en la nube gestionados como SaaS o PaaS. Establecer una **política de gestión de vulnerabilidades** (identificación y rastreo).
 - Aplicar **políticas de 'una vez y estás fuera'** con respecto a productos de proveedores que sean falsificados o no coincidan con las especificaciones acordadas contractualmente y/o documentadas.
 - Incluya **requisitos de seguridad** en todas las solicitudes de **propuestas y contratos**. Asegúrese de la integridad del arranque y exija seguridad en firmware y controladores.

Glosario

- **EDR:** Endpoint detection and response (EDR) es una solución de seguridad integrada que proporciona supervisión en tiempo real de los dispositivos endpoint. Recopila continuamente datos de los endpoints y permite un análisis rápido por parte de los equipos de seguridad y una respuesta automatizada basada en reglas.
- **XDR:** Las plataformas de detección y respuesta ampliadas (XDR) ofrecen detección y respuesta multicapa. Estas herramientas recopilan y correlacionan datos de varias capas de seguridad, incluidos correos electrónicos, puntos finales, servidores, nubes, redes y aplicaciones.
- **Ransomware Response Checklist:** Lista de comprobación recomendada por la Agencia estadounidense de ciberdefensa (CISA), en caso de sufrir un ataque de ransomware, a modo de guía a través del proceso de respuesta, desde la detección hasta la contención y erradicación:
 - **Determinar** qué sistemas se han visto afectados y aislarlos inmediatamente.
 - Sólo en el caso de que no pueda desconectar los dispositivos de la red, apagar para evitar una mayor propagación de la infección por ransomware.
 - **Clasificar** los sistemas afectados para su restauración y recuperación.
 - **Consultar** con su equipo de respuesta a incidentes para desarrollar y documentar una comprensión inicial de lo que ha ocurrido basándose en el análisis inicial.
 - **Involucrar** a los equipos internos y externos y a las partes interesadas para que sepan qué pueden aportar para ayudarle a mitigar, responder y recuperarse del incidente.
 - **Tomar** una imagen del sistema y una captura de memoria de una muestra de los dispositivos afectados (por ejemplo, estaciones de trabajo y servidores).
 - **Consultar** a las fuerzas de seguridad federales sobre los posibles descifradores disponibles, ya que los investigadores de seguridad ya han descifrado los algoritmos de cifrado de algunas variantes de ransomware.
- **TLS (Transport Layer Security):** protocolo utilizado para ofrecer seguridad y privacidad en las comunicaciones. Su utilización más conocida es en las páginas web por medio del conocido HTTPS (Hypertext Transfer Protocol Secure).
- **SSL (Secure Sockets Layer):** antecesor de TLS. Se trata de un protocolo cuya primera versión publicada fue la 2.0 en febrero del año 1995 (la primera no llegó a publicarse). Debido a los errores con los que contaba su diseño, en 1996 se liberó la versión 3.0. De esta última versión de SSL nace la primera versión de TLS en el año 1999, que es el actual protocolo utilizado en las páginas web HTTPS.

Glosario

- **OSINT ([Open Source Intelligence](#))**: técnica que se centra en la recopilación, evaluación y análisis de información pública a través de distintos métodos y técnicas, con el objetivo de descubrir vulnerabilidades o recolectar información sensible que puedan llegar a ser amenazas.
- **TLD ([Top Level Domain](#))**: Dominio de primer o más alto nivel en la jerarquía de DNS, genérico (gTLD) o por país (ccTLD), como por ejemplo ".com" o ".es"
- **DNS ([Domain Name Service](#))**: se refiere tanto al servicio de Nombres de Dominio, como al servidor que ofrece dicho servicio. El servicio DNS asocia un nombre de dominio con información variada relacionada con ese dominio. Su función más importante es traducir nombres inteligibles para las personas en direcciones IP asociados con los sistemas conectados a la red con el propósito de poder localizar y direccionar estos sistemas de una forma mucho más simple.
- **Data poisoning**: implica la alteración deliberada y maliciosa de datos para comprometer el rendimiento de un sistema (generalmente asociado a los ámbitos de la Inteligencia Artificial y el Aprendizaje Automático).

Otros recursos INCIBE

RANSOMWARE MALWARE

Infografías y videos:

- [Qué no te secuestren el ordenador!: medidas para evitarlo \(infografía\)](#)
- [Evita los engaños en la red. Utiliza soluciones antifraude](#)
- [Aprende Ciberseguridad: ransomware](#)

Guía:

- [Ransomware: una guía de aproximación para el empresario](#)

INCIBE:

- [Ayuda ransomware](#)
- [Temáticas Malware](#)
- [Aprende ciberseguridad: Malware](#)

AMENAZAS CONTRA LOS DATOS

INCIBE:

- [PROTECCIÓN DE LA INFORMACIÓN](#)
- [Cómo gestionar una fuga de información . Una guía de aproximación para el empresario](#)

INGENIERÍA SOCIAL

INCIBE: [Temáticas Ingeniería social](#)

[Aprende ciberseguridad: Ingeniería Social](#)

- ❖ [¿Qué es la ingeniería social?](#) (vídeo OSI)
- ❖ [Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse](#) (blog Protege Tu Empresa)
- ❖ [Técnicas de ingeniería social: ¿Cómo consiguen engañarnos?](#) (infografía OSI)
- ❖ [¿Sabes cómo funciona un ciberataque que utiliza ingeniería social?](#) (blog Protege Tu Empresa)
- ❖ [Detecta el fraude](#) (juego de mesa OSI)
- ❖ [Evita los engaños en la red: utiliza soluciones antifraude](#) (infografía Protege Tu Empresa)

ATAQUES A LA CADENA DE SUMINISTRO

INCIBE:

- [Sectores Estratégicos](#)
- [Cadena de suministros](#)