LISTA DE COTEJO

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA	NOMBRE DEL CURSO: SEGURIDAD INFORMÁTICA UNIDAD: I
NOMBRE DEL DOCENTE: ROSARIO CARVAJAL HERNÁNDEZ	FIRMA DEL DOCENTE

DATOS GENERALES DEL PROCESO DE EVALUACION

NOMBRE DEL ALUMNO: GOMEZ ALEMAN MIGUEL ABDEL	No. DE CONTROL: 21140374	FIRMA DEL ALUMNO:
PRODUCTO: REPORTE DE INVESTIGACIÓN	FECHA: 28/FEB/2025	PERIODO ESCOLAR: FEB - JUN 2025

INSTRUCCIONES DE APLICACIÓN

Revisar las actividades que se solicitan y marque con una X en los apartados "SI" cuando la evidencia se cumple; en caso contrario marque "NO". En la columna "OBSERVACIONES" escriba indicaciones que puedan ayudar al alumno a saber cuáles son las condiciones no cumplidas, si fuese necesario.

VALOR DEL REACTIVO	CARACTERÍSTICA A CUMPLIR (REACTIVO)	CUMPLE		OBSERVACIONES
		SI	NO	
5	Material a utilizar: Se apegó a los criterios previamente establecidos.	X		
5	Creatividad: Plasmó los temas con ingenio.	X		
0	Originalidad: El producto es único.	X		
5	Contiene todos los temas relacionados a la unidad.	X		
5	Claridad y Estructura: Se da a entender el tema que se está tratando.	X		
0	Responsabilidad: Entregó el producto en la fecha y hora señalada.	X		
20%	**CALIFICACIÓN**	20%		

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA

INGENIERÍA INFORMÁTICA

MATERIA:

SEGURIDAD INFORMÁTICA

TEMA:

“REPORTE DE INVESTIGACIÓN DE SEGURIDAD INFORMÁTICA”

ALUMNO:

ABDIEL MIGUEL GOMEZ ALEMAN

OCTAVO SEMESTRE

GRUPO 810-B

DOCENTE:

M.T.I. ROSARIO CARVAJAL HERNÁNDEZ

15 DE FEBRERO DE 2025

INTRODUCCIÓN

La seguridad informática es un tema de creciente relevancia debido al crecimiento y expansión de las tecnologías de la información y las comunicaciones. Los sistemas informáticos son vulnerables a diversas amenazas que pueden comprometer la confidencialidad, la integridad y la disponibilidad de los datos, lo que puede afectar tanto a usuarios individuales como a organizaciones de cualquier tamaño. La protección de la información se ha convertido en una prioridad para gobiernos, empresas y personas, ya que los ataques cibernéticos no solo tienen repercusiones económicas, sino también sociales y políticas.

El presente trabajo de investigación aborda las definiciones de seguridad informática, las principales amenazas a las que estamos expuestos en internet y las técnicas y prácticas de aseguramiento de sistemas que se utilizan para mitigar estos riesgos. A través de una revisión de conceptos y de amenazas emergentes, se busca ofrecer una comprensión integral sobre cómo protegerse en un mundo digital cada vez más complejo.

DEFINICIONES DE SEGURIDAD INFORMÁTICA

Según Voutssas [1], la seguridad informática es “el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización”

Del mismo modo, Gómez [2] define la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o software.

Por su parte, Kissel [3] la define como la protección de información y sistemas de información de acceso no autorizado. En efecto, con base en estas definiciones, la seguridad informática se vincula con tres elementos básicos: la información que, como activo intangible, representa quizá el elemento más sensible y vulnerable; el software, cuya pérdida o modificación mal intencionada puede representar severos quebrantos económicos u operativos no solo hacia el usuario sino a toda una institución; y el hardware, que al fallar provoca retrasos en la operación diaria y la consecuente pérdida de tiempo y costos elevados.

PRINCIPALES AMENAZAS POR INTERNET

La seguridad informática enfrenta una variedad de amenazas en el entorno digital, y estas amenazas son cada vez más sofisticadas. Estas amenazas afectan tanto a individuos como a organizaciones y pueden tener consecuencias devastadoras, desde la pérdida de datos hasta el robo de identidad, pasando por daños a la infraestructura crítica.

1. Malware (software malicioso)

El malware es uno de los principales riesgos en la seguridad informática. Incluye cualquier tipo de software diseñado para dañar, interrumpir u obtener acceso no autorizado a sistemas informáticos. Existen diferentes tipos de malware, cada uno con un objetivo y funcionamiento específico:

- **Virus**: Se propaga a través de archivos y programas, y puede replicarse en otros sistemas, alterando o destruyendo archivos.
- **Troyanos**: Se presentan como software legítimo, pero en realidad están diseñados para permitir acceso remoto a los atacantes.
- **Ransomware**: Secuestra los datos de una víctima y exige un rescate para liberarlos. Este tipo de malware ha experimentado un aumento significativo en los últimos años.
- **Spyware**: Monitorea las actividades de un usuario sin su consentimiento, generalmente con el fin de robar información personal.
- **Adware**: Muestra anuncios no deseados, generalmente con fines comerciales, y puede ralentizar los sistemas.

Los ataques de malware pueden generar pérdida de datos, robo de información personal, corrupción de archivos, interrupciones en el servicio y grandes costos económicos para la recuperación de los sistemas.

2. Phishing y ataques de ingeniería social

El phishing es una de las técnicas más utilizadas por los ciberdelincuentes para robar credenciales de acceso o información confidencial. Consiste en engañar a las víctimas para que proporcionen datos personales mediante la falsificación de comunicaciones oficiales, como correos electrónicos, sitios web o mensajes de texto.

- **Spear phishing**: Es una versión más dirigida del phishing, donde los atacantes se centran en una persona o grupo específico, personalizando los mensajes para aumentar la probabilidad de éxito.
- **Vishing**: Phishing realizado por teléfono, en el cual los atacantes se hacen pasar por representantes de una empresa para obtener datos sensibles.
- **Smishing**: Phishing a través de mensajes SMS, que inducen a la víctima a hacer clic en enlaces maliciosos o descargar archivos adjuntos.

El phishing puede llevar al robo de identidades, fraudes financieros, acceso no autorizado a sistemas internos y exposición de información personal o corporativa.

3. Ataques de denegación de servicio (DoS) y denegación de servicio distribuida (DDoS)

Los ataques de DoS y DDoS están diseñados para saturar un servidor, red o sistema de forma que se vuelva inaccesible para los usuarios legítimos. En un ataque de DoS, un único atacante envía grandes cantidades de tráfico a un sistema objetivo para sobrecargarlo. En un DDoS, varios sistemas distribuidos (a menudo bots o dispositivos comprometidos) participan en el ataque, lo que hace que sea más difícil detenerlo. Estos ataques pueden interrumpir operaciones comerciales, causar pérdidas financieras y afectar la reputación de las empresas.

4. Exploits de vulnerabilidades

Los exploits son programas o técnicas utilizadas para aprovechar fallas de seguridad en software o hardware. Los atacantes pueden utilizar vulnerabilidades no parcheadas en sistemas operativos, aplicaciones web, servicios de red y otros programas para obtener acceso no autorizado o realizar otras acciones maliciosas.

- **Zero-day**: Se refiere a una vulnerabilidad que es explotada antes de que se haya lanzado un parche de seguridad. Los atacantes pueden aprovechar este tipo de vulnerabilidades sin que las víctimas tengan conocimiento de ellas.
- **Exploits en aplicaciones web**: Estos incluyen ataques como la inyección SQL, el cross-site scripting (XSS) y el cross-site request forgery (CSRF).

El uso de exploits puede comprometer gravemente la seguridad de los sistemas, permitiendo a los atacantes robar información, acceder a redes internas, o causar la interrupción de servicios críticos.

5. Robo de identidad y fraude en línea

El robo de identidad es uno de los crímenes cibernéticos más dañinos. Los atacantes obtienen información personal sensible (como números de tarjeta de crédito, contraseñas, o datos bancarios) a través de diversas técnicas como phishing, malware o incluso la filtración de datos en violaciones de seguridad.

- **Fraude de tarjetas de crédito**: Los ciberdelincuentes pueden robar los datos de las tarjetas de crédito y realizar compras no autorizadas.
- **Suplantación de identidad**: Los atacantes pueden hacerse pasar por otras personas para obtener acceso a cuentas bancarias, servicios financieros o realizar compras fraudulentas.

El robo de identidad puede resultar en pérdidas financieras significativas para las víctimas y daños irreparables a la reputación de una persona o empresa.

6. Ataques de Man-in-the-Middle (MitM)

En los ataques Man-in-the-Middle, los atacantes interceptan la comunicación entre dos partes para robar o manipular los datos que se transmiten. Esto puede ocurrir en redes Wi-Fi no seguras, donde los atacantes interceptan el tráfico de datos, o cuando las conexiones no están cifradas adecuadamente. Los atacantes pueden robar información sensible, como credenciales de acceso o datos bancarios, sin que las víctimas se den cuenta.

7. Ataques a la infraestructura crítica

Las infraestructuras críticas, como las redes de energía, agua, telecomunicaciones y sistemas de transporte están cada vez más conectadas a internet y son vulnerables a ataques cibernéticos. Un ataque exitoso a estas infraestructuras podría tener consecuencias graves para la seguridad nacional, la economía o la salud pública.

- **Stuxnet**: Este es uno de los casos más conocidos de un ataque dirigido a una infraestructura crítica, específicamente a las instalaciones nucleares de Irán. Utilizó malware altamente sofisticado para sabotear las centrifugadoras nucleares.

Los ataques a infraestructuras críticas pueden paralizar sectores completos de la economía, causar daños a gran escala y poner en riesgo la vida humana.

8. IoT (Internet de las Cosas) y dispositivos conectados

Con la creciente adopción de dispositivos conectados a Internet (IoT), como cámaras de seguridad, termostatos, vehículos, y dispositivos médicos, surgen nuevas vulnerabilidades. Muchos de estos dispositivos tienen medidas de seguridad insuficientes y pueden ser fácilmente comprometidos. Los dispositivos IoT comprometidos pueden ser utilizados en ataques DDoS, espiar a las víctimas o incluso ser controlados de forma remota para realizar acciones maliciosas.

9. Ataques a la cadena de suministro

Los atacantes también pueden apuntar a las empresas a través de sus proveedores o socios. Esto se conoce como un ataque a la cadena de suministro, en el que los ciberdelincuentes comprometen una empresa o software que una organización utiliza, con el fin de infiltrarse en sus sistemas.

- **Ataques a través de actualizaciones de software**: Un ejemplo famoso de esto fue el ataque SolarWinds, donde los atacantes insertaron código malicioso en una actualización de software legítima.

Estos ataques pueden tener consecuencias devastadoras, afectando a varias organizaciones simultáneamente e incluso comprometiendo sistemas gubernamentales.

10. Vulnerabilidades en la nube

A medida que más empresas y personas migran a servicios basados en la nube, se amplían las posibilidades de amenazas a la seguridad. Las amenazas incluyen la exposición de datos, malas configuraciones de seguridad y la falta de control sobre los servicios gestionados en la nube. Las brechas en la seguridad de la nube pueden resultar en la filtración de información confidencial o en la interrupción de servicios empresariales clave.

11. Cryptojacking

El cryptojacking es el uso no autorizado de un dispositivo para minar criptomonedas. Los atacantes infectan computadoras o servidores con malware que utiliza los recursos del sistema para extraer monedas sin que la víctima lo sepa.

12. Ataques a redes sociales

Los ataques a redes sociales incluyen el robo de cuentas, suplantación de identidad y la difusión de desinformación. Estos ataques pueden afectar la reputación personal o empresarial, además de ser utilizados para propagar engaños o realizar estafas.

13. Ataques de Cross-Site Scripting (XSS)

En los ataques de XSS, los atacantes inyectan scripts maliciosos en sitios web legítimos. Estos scripts pueden robar cookies de sesión, redirigir a usuarios a sitios falsificados o ejecutar acciones maliciosas en nombre del usuario.

14. Botnets

Una botnet es una red de dispositivos comprometidos (bots) que pueden ser controlados remotamente por los atacantes para ejecutar diversas actividades maliciosas, como enviar spam, realizar ataques DDoS o propagar malware.

15. Ataques de DNS Spoofing (envenenamiento de caché DNS)

El DNS spoofing o envenenamiento de caché DNS es una técnica en la que los atacantes engañan a los servidores DNS para redirigir a los usuarios a sitios web falsificados. Al hacerlo, pueden robar información personal, instalar malware o propagar contenido malicioso. Este ataque pone en riesgo tanto a individuos como a empresas que dependen de los sistemas de nombres de dominio (DNS) para acceder a servicios en línea.

16. Exploits en dispositivos de red (routers, firewalls, etc.)

Los dispositivos de red como routers y firewalls pueden ser vulnerables a ataques si no están debidamente configurados o si se utilizan contraseñas débiles. Los atacantes pueden aprovechar estas fallas para obtener acceso a redes privadas, interceptar comunicaciones o incluso tomar el control de dispositivos en una red, comprometiendo así toda la infraestructura.

TÉCNICAS DE ASEGURAMIENTO DEL SISTEMA

Las técnicas de aseguramiento de sistemas en seguridad informática son esenciales para proteger los sistemas y redes frente a amenazas y vulnerabilidades. Estas técnicas buscan garantizar la confidencialidad, integridad y disponibilidad de la información.

1. Control de acceso

El control de acceso es uno de los pilares fundamentales en la seguridad informática. Se encarga de restringir el acceso a recursos del sistema según los derechos asignados a los usuarios.

- **Autenticación**: Asegura que el usuario que accede al sistema sea quien dice ser. Las técnicas más comunes son:
  - **Contraseñas**: Métodos tradicionales, aunque son vulnerables si no se gestionan adecuadamente.
  - **Autenticación multifactor (MFA)**: Requiere varios factores de autenticación, como algo que el usuario sabe (contraseña), algo que el usuario tiene (token, teléfono móvil) y algo que el usuario es (biometría).
  - **Biometría**: Uso de características físicas (huellas dactilares, reconocimiento facial, etc.) para autenticar al usuario.
- **Autorización**: Se refiere a qué puede hacer un usuario después de autenticarse. Los modelos más comunes son:
  - **Discrecional (DAC)**: El propietario del recurso decide quién tiene acceso.
  - **Basado en roles (RBAC)**: Los permisos se asignan según el rol que desempeña el usuario en la organización.
  - **Basado en atributos (ABAC)**: El acceso depende de políticas basadas en atributos como el cargo del usuario o el contexto de la solicitud.

- **Auditoría y monitoreo**: La auditoría es crucial para asegurar que los usuarios sólo realicen las actividades para las que tienen permiso. Esto implica registrar todas las acciones que los usuarios realizan en el sistema.

2. Criptografía

La criptografía es fundamental para proteger la confidencialidad y la integridad de los datos. Existen varias técnicas y algoritmos criptográficos utilizados para asegurar las comunicaciones y la información almacenada:

- **Criptografía simétrica**: Usa una única clave tanto para cifrar como para descifrar los datos. Un ejemplo popular es el AES (Advanced Encryption Standard).
- **Criptografía asimétrica**: Utiliza un par de claves (una pública y una privada). Ejemplos comunes son el RSA y el ECC (Elliptic Curve Cryptography).
- **Funciones hash**: Son algoritmos unidireccionales que generan un valor fijo (el "hash") para cualquier entrada de longitud variable. Se utilizan para verificar la integridad de los datos, como en el caso de los checksums o la firma digital.
- **Protocolos criptográficos**: Tecnologías como SSL/TLS aseguran la transmisión de datos entre los usuarios y servidores, protegiendo la información en tránsito.

3. Seguridad en redes

El aseguramiento de redes es fundamental para proteger los datos que viajan a través de redes locales o internet. Existen diversas técnicas y dispositivos para prevenir y mitigar ataques en redes:

- **Cortafuegos (Firewalls)**: Controlan el tráfico de red entre diferentes redes y se utilizan para bloquear o permitir la entrada o salida de datos según reglas predefinidas.
- **Sistemas de detección y prevención de intrusos (IDS/IPS)**: Detectan patrones de tráfico inusuales que podrían indicar un ataque y, en algunos casos, pueden prevenir estos ataques de manera activa.

- **Red privada virtual (VPN)**: Encripta el tráfico de red y permite una conexión segura a través de redes públicas, lo que garantiza la confidencialidad de los datos.
- **Segmentación de redes**: Consiste en dividir la red en subredes más pequeñas para reducir el impacto de un posible ataque. Esto facilita también el monitoreo y la administración de la seguridad.

4. Protección contra malware

El malware incluye virus, troyanos, ransomware, spyware y otras formas de software malicioso que pueden comprometer la seguridad de los sistemas. Las técnicas de protección incluyen:

- **Antivirus y antimalware**: Son herramientas de software diseñadas para detectar, bloquear y eliminar el malware.
- **Análisis de comportamiento**: En lugar de detectar malware mediante firmas conocidas, esta técnica observa el comportamiento del sistema y de los programas para identificar actividades sospechosas.
- **Sandboxes**: Aísla y ejecuta el código sospechoso en un entorno controlado para estudiar su comportamiento sin comprometer el sistema real.

5. Protección de endpoints

Los endpoints (dispositivos finales como computadoras, teléfonos móviles y servidores) son puntos clave de entrada para los ataques. Las técnicas de protección incluyen:

- **Antivirus en endpoints**: Instalación de software de seguridad directamente en los dispositivos para detectar y neutralizar amenazas.
- **Control de dispositivos**: Limitar qué dispositivos se pueden conectar a los endpoints (por ejemplo, puertos USB, redes Wi-Fi, etc.).
- **Actualización y parches**: Mantener el sistema operativo y el software de los endpoints actualizados es esencial para protegerse contra vulnerabilidades conocidas.

6. Pruebas de penetración y auditoría de seguridad

Las pruebas de penetración (pentesting) y auditorías de seguridad son técnicas proactivas utilizadas para identificar vulnerabilidades en los sistemas antes de que los atacantes las exploten:

- **Pruebas de penetración**: Consisten en simular ataques reales para evaluar las debilidades del sistema y su resistencia a diversos tipos de amenazas.
- **Auditorías de seguridad**: Implican la revisión y el análisis de la infraestructura, el código, las políticas y los procedimientos de seguridad de la organización.

7. Resiliencia y recuperación ante desastres

La resiliencia se refiere a la capacidad de un sistema para recuperarse de un ataque o incidente de seguridad. La recuperación ante desastres es una parte clave de esto:

- **Copia de seguridad (backups)**: La realización de copias de seguridad periódicas de datos y sistemas críticos es crucial para la recuperación de información en caso de ataque.
- **Planes de respuesta a incidentes**: Desarrollar y ensayar procedimientos específicos para hacer frente a diferentes tipos de incidentes de seguridad.
- **Continuidad del negocio**: Establecer estrategias para mantener las operaciones críticas durante o después de un ataque o desastre.

8. Seguridad en la nube

El uso de servicios en la nube ha incrementado enormemente, lo que ha creado nuevos retos en términos de seguridad. Algunas prácticas para asegurar la nube incluyen:

- **Cifrado de datos**: Asegurar que los datos almacenados y transmitidos en la nube estén cifrados para protegerlos contra accesos no autorizados.
- **Seguridad en el proveedor de la nube**: Evaluar la seguridad proporcionada por el proveedor de servicios en la nube y garantizar que se cumplan las normativas y políticas de privacidad.

- **Control de acceso basado en la nube**: Implementar controles de acceso estrictos y autenticación multifactor en los servicios en la nube.

9. Gestión de vulnerabilidades

Las vulnerabilidades son puntos débiles en los sistemas que pueden ser explotados por atacantes. La gestión de vulnerabilidades incluye:

- **Evaluación de vulnerabilidades**: Herramientas de escaneo que identifican debilidades en los sistemas, aplicaciones y redes.
- **Parches y actualizaciones**: Asegurar que se apliquen los parches de seguridad de manera oportuna para mitigar las vulnerabilidades conocidas.
- **Monitoreo de amenazas**: Detectar nuevas vulnerabilidades y amenazas emergentes a través del monitoreo constante y análisis de seguridad.

CONCLUSIÓN

El aseguramiento de los sistemas informáticos es una tarea compleja que requiere la implementación de técnicas y herramientas en múltiples capas, tanto en el software, hardware y red. Las técnicas de aseguramiento deben ser integradas en todos los aspectos del ciclo de vida de un sistema para proporcionar una defensa eficaz contra las amenazas cibernéticas. La evolución constante de las amenazas exige que las organizaciones adopten enfoques dinámicos y adaptativos, combinando políticas de prevención, detección y respuesta ante incidentes.

REFERENCIAS:

[1] J. Voutssas M., “Preservación documental digital y seguridad informática”, *Investigación bibliotecológica*, vol. 24, no. 50, p. 131, 2010 [En línea]. Disponible en: https://ibit.ly/lBtnl [Accedido: 15-feb-2025]

[2] A. Gómez, *Enciclopedia de la seguridad informática*. España: RA-MA, 2006.

[3] R. Kissel, *Glossary of Key Information Security Terms*, National Institute of Standards and Technology, 2012.

[4] A. Gómez Vieites, *Enciclopedia de la Seguridad Informática*, 2ª ed. Grupo Editorial RA-MA, 2011 [En línea]. Disponible en: https://t.ly/DECFQ [Accedido: 15-feb-2025]

[5] M. A. Caballero Velasco, L. Baus Lerma y D. Cilleros Serrano, *Ciberseguridad paso a paso Diseña tu estrategia*. ANAYA MULTIMEDIA, 2023 [En línea]. Disponible en: https://t.ly/qKNZ8 [Accedido: 15-feb-2025]

[6] J. M. Ortega Candel, *Ciberseguridad Manual práctico*. Ecoe Ediciones, 2024 [En línea]. Disponible en: https://t.ly/vAmjX [Accedido: 15-feb-2025]

[7] A. Arreola García, *Ciberseguridad ¿Por qué es importante para todos?* Siglo XXI Editores México, 2019 [En línea]. Disponible en: https://t.ly/qJ_UZ [Accedido: 15-feb-2025]

[8] A. E. Mata García, *Ciberseguridad. Curso Práctico*. RA-MA S.A., 2024 [En línea]. Disponible en: https://t.ly/i-mdI [Accedido: 15-feb-2025]

[9] W. M. Abad Parrales *et al.*, *La ciberseguridad práctica aplicada a las redes, servidores y navegadores web*. 3Ciencias, 2019 [En línea]. Disponible en: https://t.ly/45vS0 [Accedido: 15-feb-2025]

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA

INGENIERÍA INFORMÁTICA

MATERIA:

SEGURIDAD INFORMÁTICA

TEMA:

“9 MEDIDAS DE SEGURIDAD INFORMÁTICA”

ALUMNO:

ABDIEL MIGUEL GOMEZ ALEMAN

OCTAVO SEMESTRE

GRUPO 810-B

DOCENTE:

M.T.I. ROSARIO CARVAJAL HERNÁNDEZ

20 DE MARZO DE 2025

ÍNDICE

LAS 9 MEDIDAS QUE ASEGURAN LA INFORMACIÓN DE TU EMPRESA

1. Controles de acceso a los datos más estrictos.
2. Realizar copias de seguridad.
3. Utilizar contraseñas seguras.
4. Proteger el correo electrónico.
5. Contratar un software integral de seguridad.
6. Utilizar software DLP (prevención de pérdidas de datos.
7. Trabajar en la nube.
8. Involucrar a toda la empresa en la seguridad.
9. Monitorización continua y respuesta inmediata.

9 HERRAMIENTAS DE SEGURIDAD

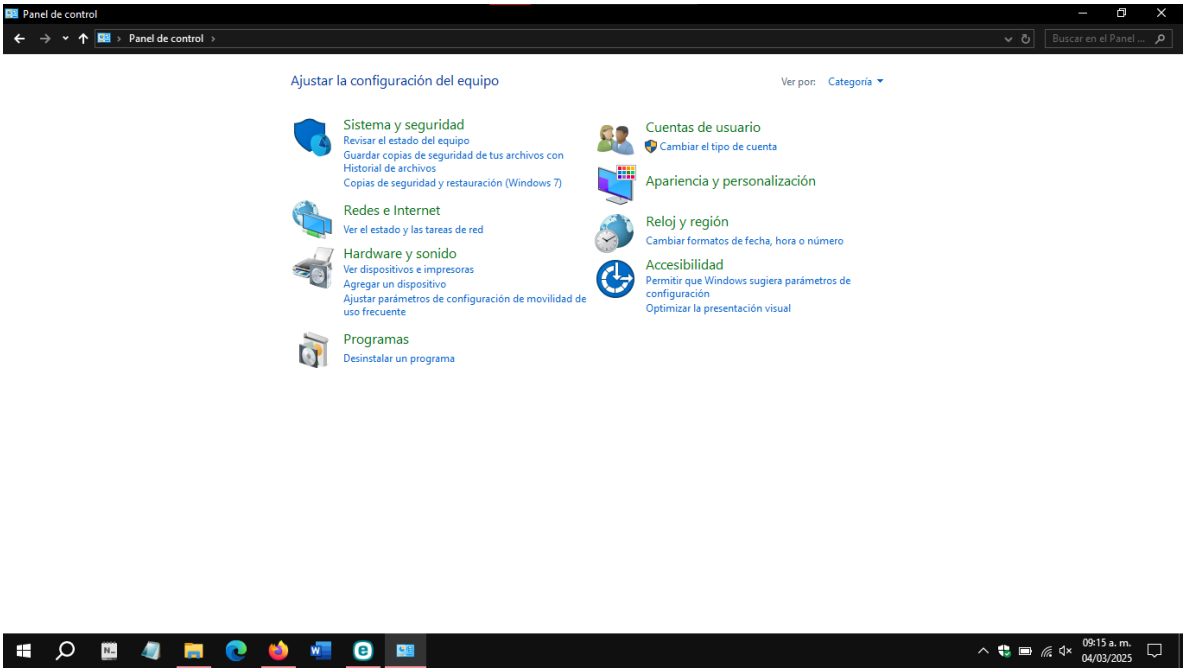
1. ANTIVIRUS

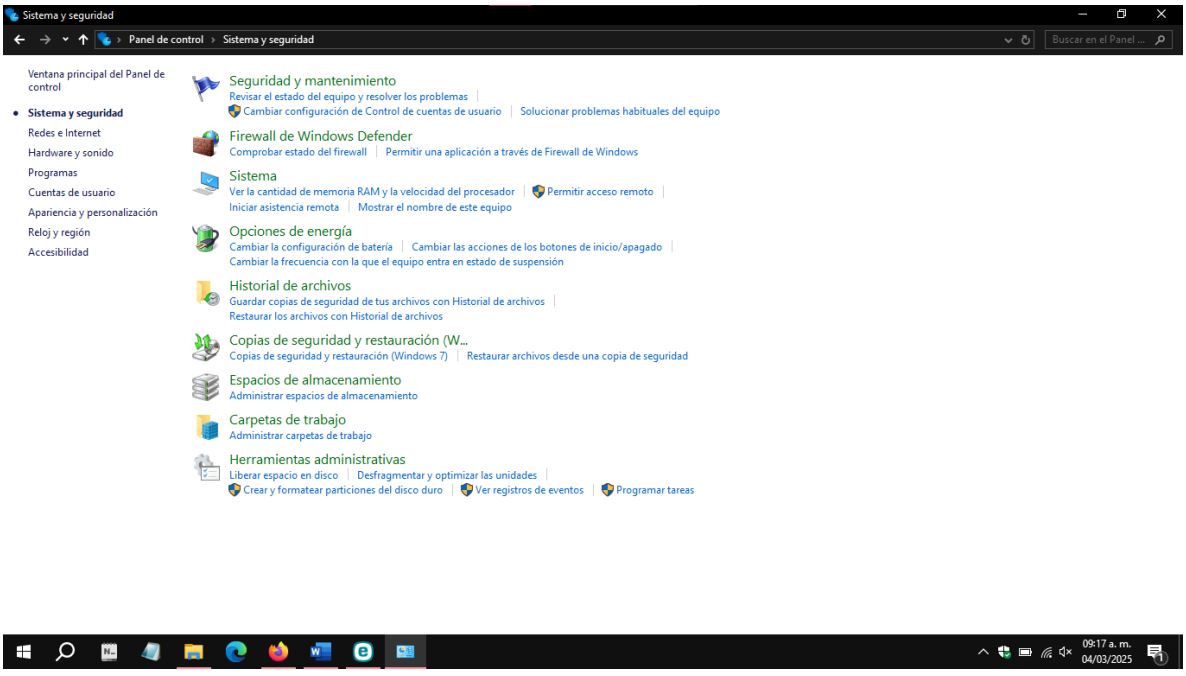
AVAST FREE	ESET SMART SECURITY	NORTON	AVIRA	MCAFFE	BITDEFENDER	KASPERSKY
Cortafuegos	Motor de detección	Proteccion contra Malware y Amenazas en tiempo real	Analisis de virus	Firewall	Análisis rapido	Protección antivirus en tiempo real
Escudos de archivo	Aprendizaje automático avanzado	Firewall Inteligente	Escáner antivirus basado en la nube.	Administrador de contraseñas	Análisis del sistema	Escaneo de archivos y aplicaciones
Escudo de ransomware	Bloqueador de exploits	Seguridad para Navegación Web	Optimización del dispositivo.	Destructor de archivos	Análisis de vulnerabilidades	Protección web y antiphishing
Escudo web	Protección contra ataques basados en scripts	Protección contra Ransomware	Gestor de contraseñas.	Protección web	VPN	Actualizaciones automáticas
Analisis de virus	Anti-Phishing	VPN Segura	Gerente de Tráfico de la Red.	Supervision de identidad	SAFEPAY	Modo Juego
Inspector de red	Protección del acceso a la Web	Adminstrador de contraseñas	Recupera los archivos.	VPN segura	Cryptomining pro	$449.00 --> 1 Device (Kaspersky Standard) --> 1 año
Cuarentena	HIPS (incluida la Protección contra ransomware)	Control Parental	Protección web.	Costo $599 al año un dispositivo	Protección de amenzas online	$719.00 --> 1 Device (Kaspersky Plus) --> 1 año
Alertas de hackeo	Antispam	Protección de Identidad	Phantom VPN.		Anti-Tracker	$839 --> 1 Device (Kaspersky Premium) --
Modo no molestar	Cortafuegos	Optimización de Dispositivos	Cuarentena		Antirobo	
Alerta de Hackeo	Inspector de red	Compatibilidad y Planes	Opciones de protección		herramientas decifrado	Kaspersky gana el premio al "Producto del año"
Disco de Rescate	Protección de cámara web	Norton plus: $500.00 el primer año	Cortafuegos		Antispam	
$24.00 POR MES	Protección contra los ataques de red		Seguridad del navegador		$850 MXN	
	Protección contra botnets		Gestor de Contraseñas			
	Banca y navegación seguras		Avira Internet Security: 723.46 pesos (solo el primer año)			
	Privacidad y seguridad del navegador		Avira Prime: 1,240.37 pesos (solo el primer año)			
	Control parental					
	Antirrobo					
	Password Manager					
	ESET Secure Data					
	ESET LiveGuard					
	Antispyware					
	Protocolo SSL/TLS					
	Precio: $1,260 anual 1 equipo					

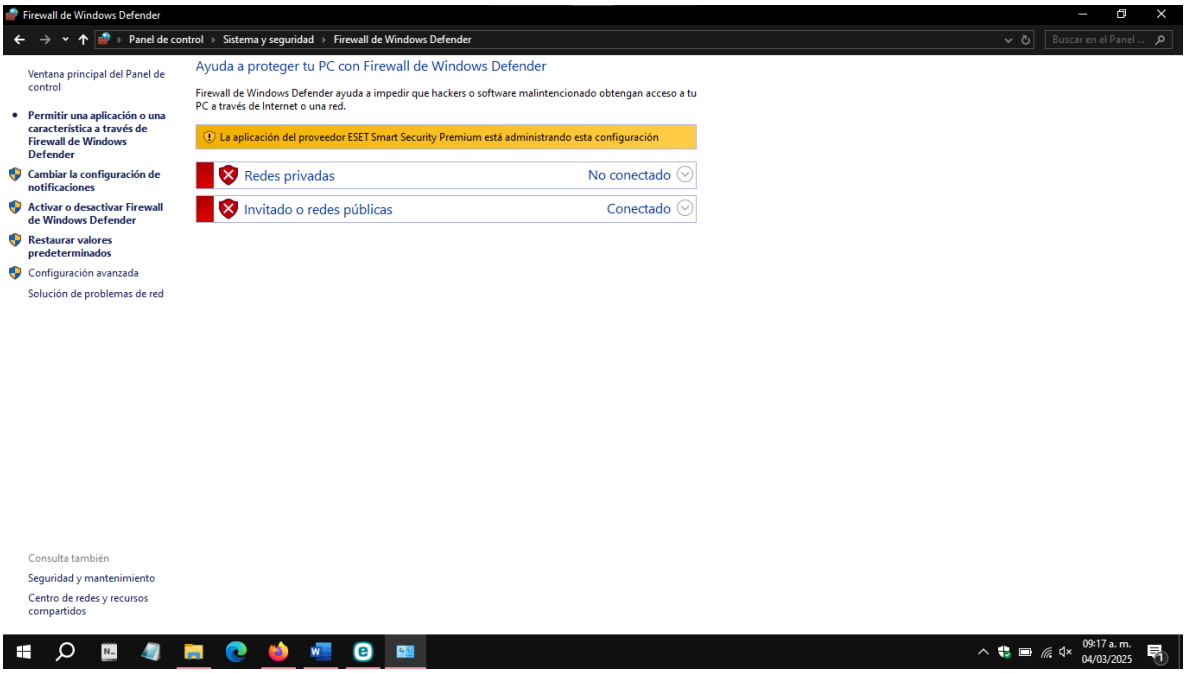
2. FIREWALL DE SOFTWARE

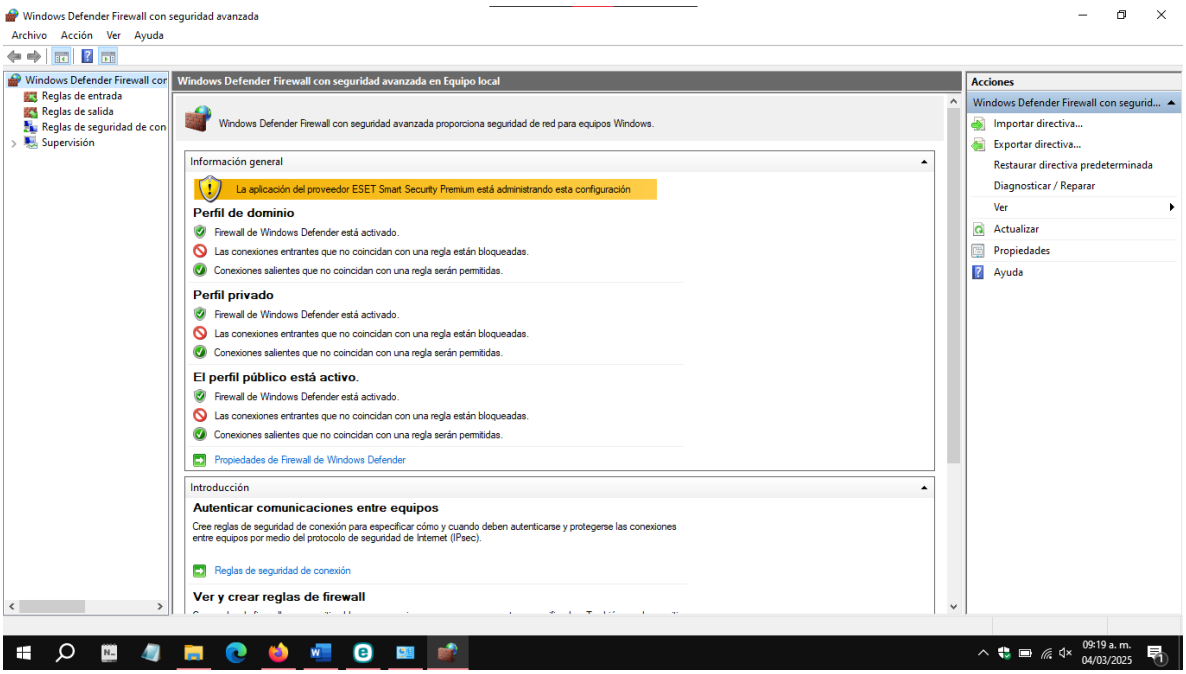
Definición: “bloquean el acceso y salida de información para ser evaluada por medio de su código”.

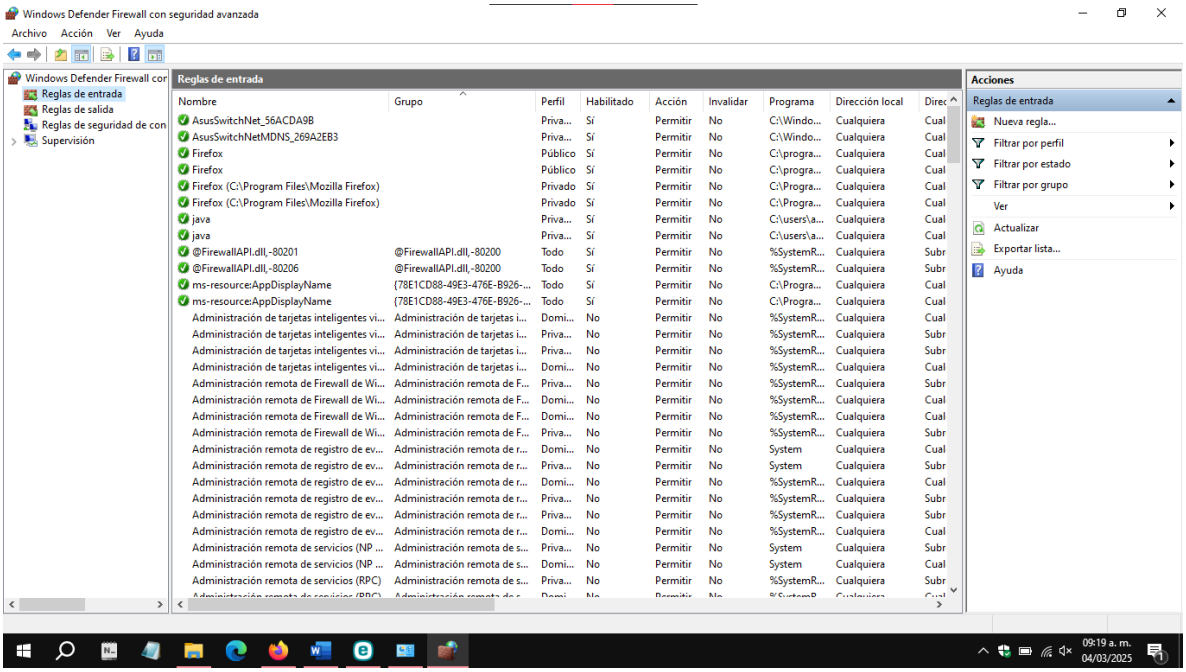
Activar firewall en Windows 10:

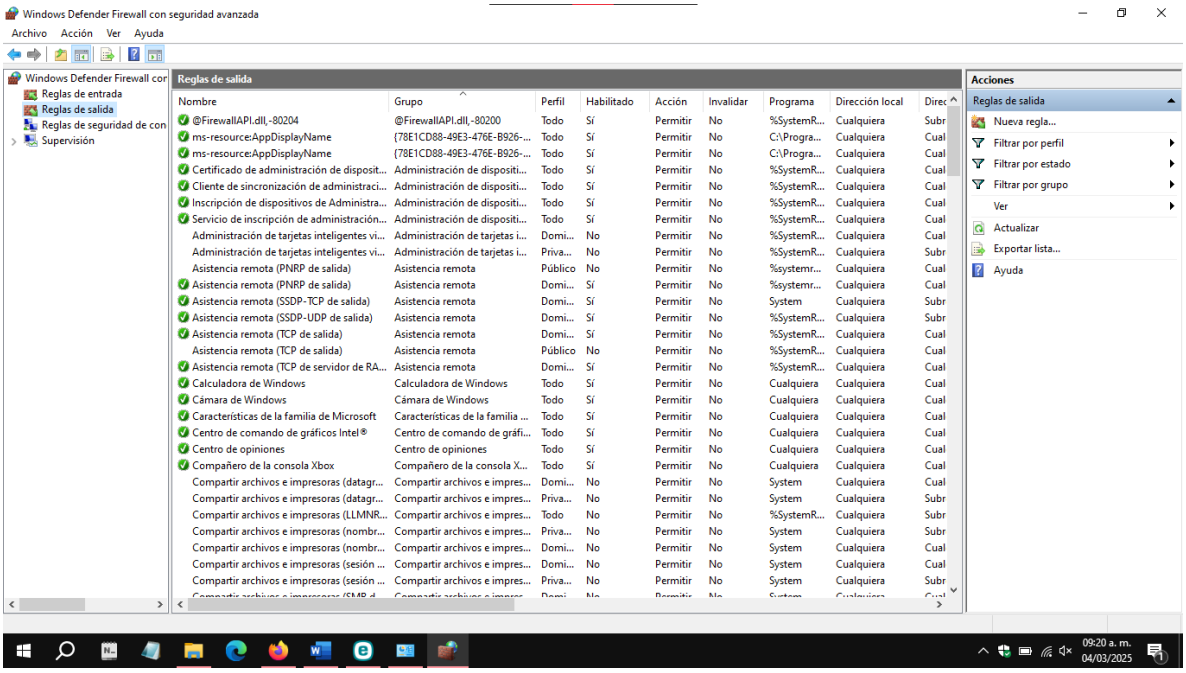





Firewall de Windows Defender
Panel de control › Sistema y seguridad › Firewall de Windows Defender
Buscar en el Panel ...
Ventana principal del Panel de control
Permitir una aplicación o una característica a través de Firewall de Windows Defender
Cambiar la configuración de notificaciones
Activar o desactivar Firewall de Windows Defender
Restaurar valores predeterminados
Configuración avanzada
Solución de problemas de red
Ayuda a proteger tu PC con Firewall de Windows Defender
Firewall de Windows Defender ayuda a impedir que hackers o software malintencionado obtengan acceso a tu PC a través de Internet o una red.
La aplicación del proveedor ESET Smart Security Premium está administrando esta configuración
Redes privadas
No conectado
Invitado o redes públicas
Conectado
Consulta también
Seguridad y mantenimiento
Centro de redes y recursos compartidos
09:17 a. m.
04/03/2025

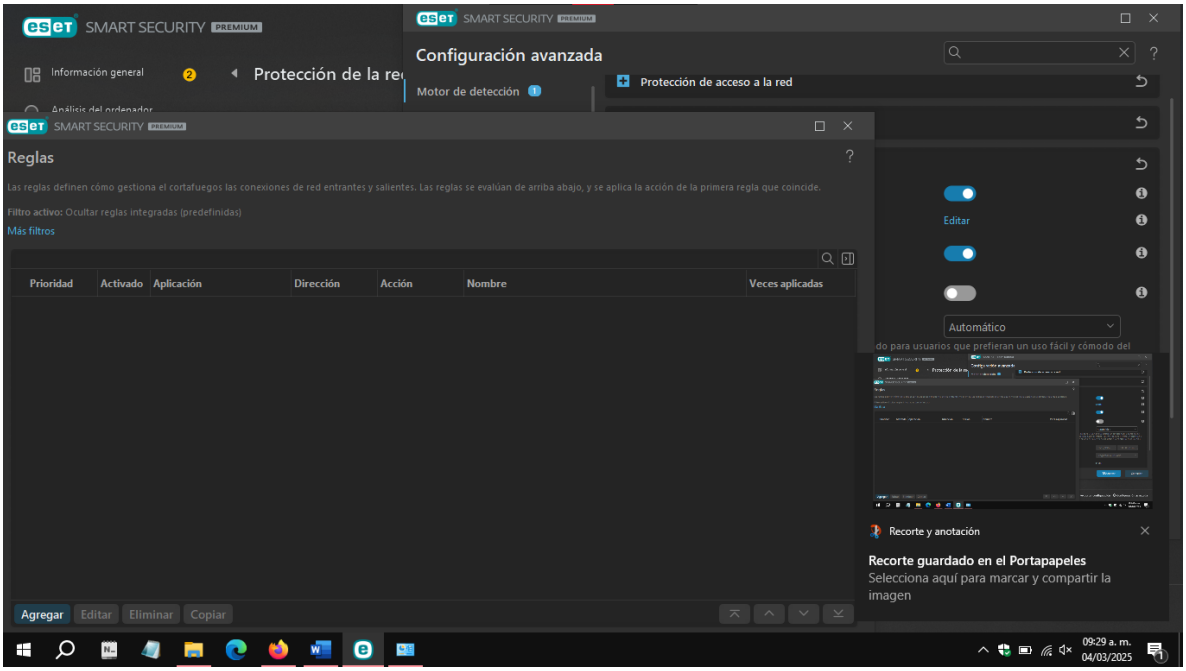

Windows Defender Firewall con seguridad avanzada
Archivo Acción Ver Ayuda
Windows Defender Firewall cor
Reglas de entrada
Reglas de salida
Reglas de seguridad de con
Supervisión
Windows Defender Firewall con seguridad avanzada en Equipo local
Windows Defender Firewall con seguridad avanzada proporciona seguridad de red para equipos Windows.
Información general
La aplicación del proveedor ESET Smart Security Premium está administrando esta configuración
Perfil de dominio
Firewall de Windows Defender está activado.
Las conexiones entrantes que no coincidan con una regla están bloqueadas.
Conexiones salientes que no coincidan con una regla serán permitidas.
Perfil privado
Firewall de Windows Defender está activado.
Las conexiones entrantes que no coincidan con una regla están bloqueadas.
Conexiones salientes que no coincidan con una regla serán permitidas.
El perfil público está activo.
Firewall de Windows Defender está activado.
Las conexiones entrantes que no coincidan con una regla están bloqueadas.
Conexiones salientes que no coincidan con una regla serán permitidas.
Propiedades de Firewall de Windows Defender
Introducción
Autenticar comunicaciones entre equipos
Cree reglas de seguridad de conexión para especificar cómo y cuando deben autenticarse y protegerse las conexiones entre equipos por medio del protocolo de seguridad de Internet (IPsec).
Reglas de seguridad de conexión
Ver y crear reglas de firewall
Acciones
Windows Defender Firewall con segurid...
Importar directiva...
Exportar directiva...
Restaurar directiva predeterminada
Diagnosticar / Reparar
Ver
Actualizar
Propiedades
Ayuda
09:19 a. m.
04/03/2025





Nota: ESET Internet Security toma el control de Firewall por estar instalado en el Sistema Operativo.

Firewall de ESET SMART SECURITY:



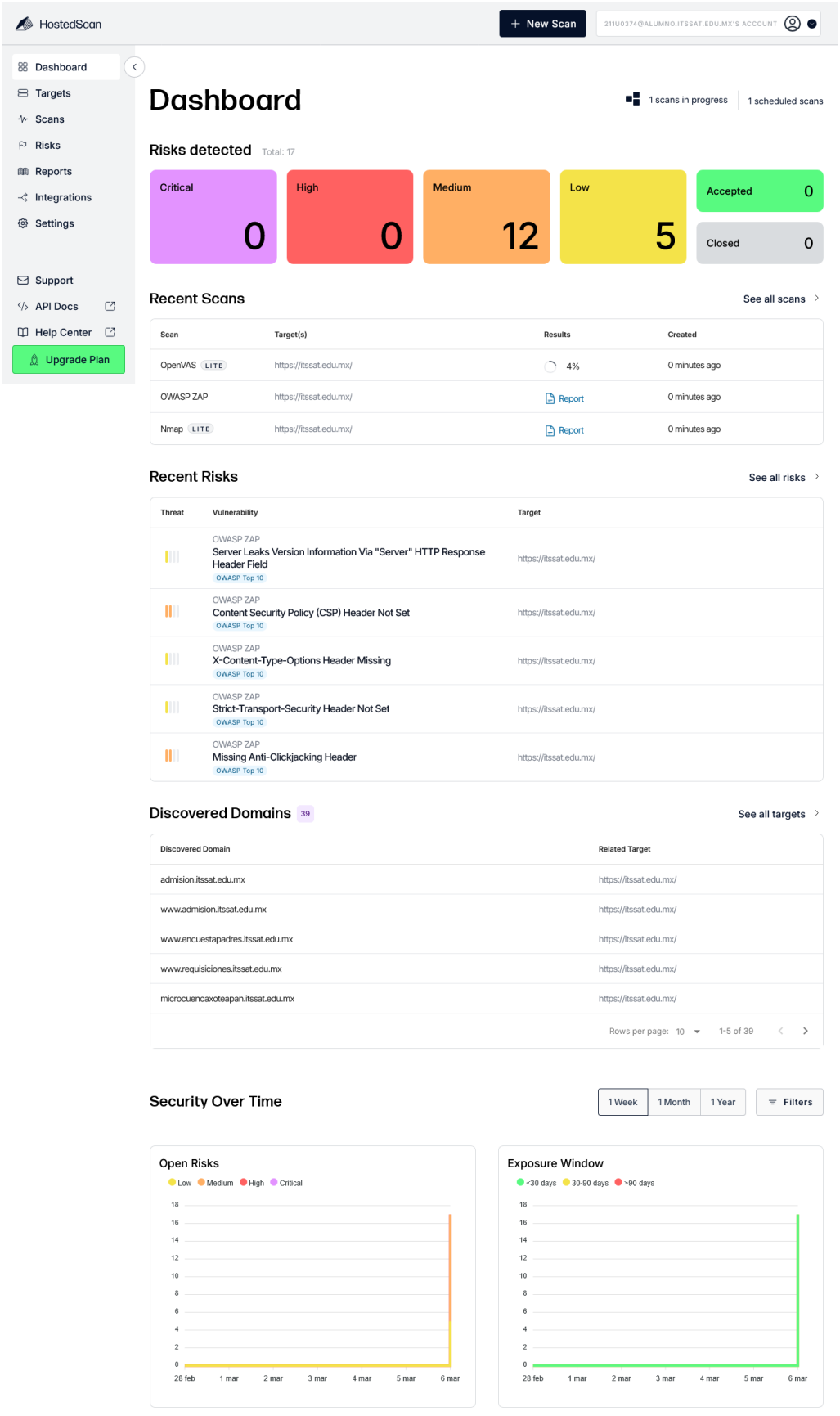
3. CERTIFICADOS SSL

DEFINICIÓN: “Estos recursos dotan de mayor seguridad a los sitios web mediante capas de sockets seguros. Esto significa, solo cuando se activa un certificado de este tipo, se permite el acceso a un servidor web.”

4. ESCÁNER DE VULNERABILIDADES

“Los escáneres de vulnerabilidades evalúan el estado de un sistema, red o plataformas para detectar aquellas zonas, más vulnerables, y alertar sobre posibles brechas de seguridad.”

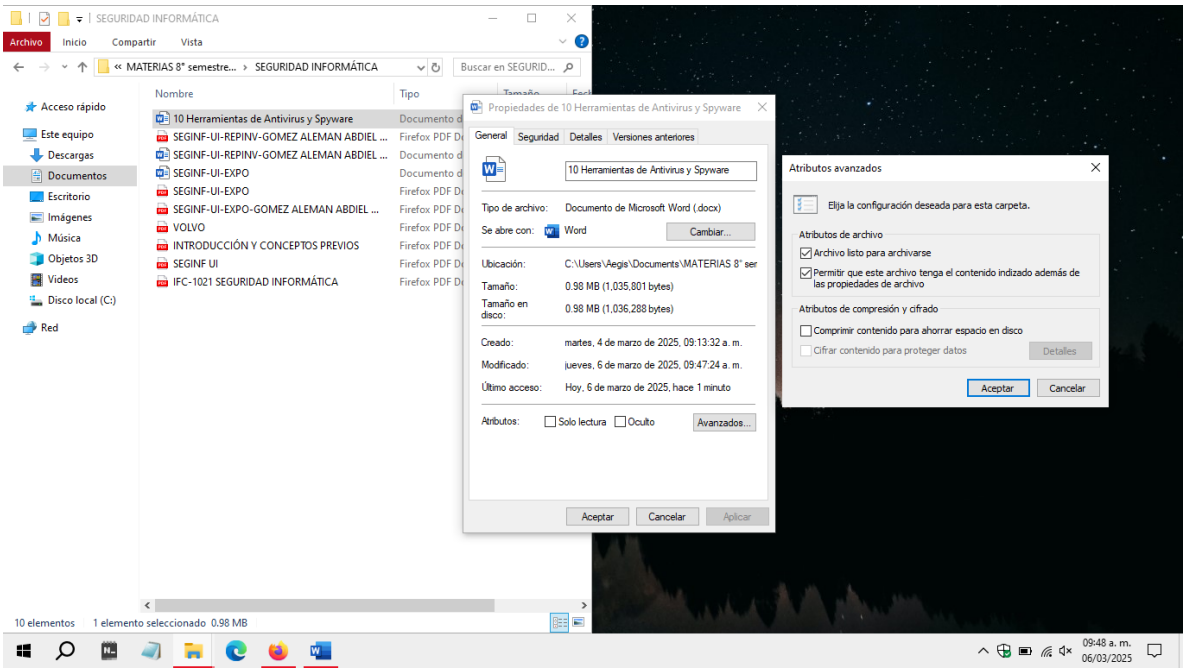
Escaneo de vulnerabilidades del sitio web: https://itssat.edu.mx/ con la herramienta https://hostedscan.com/


HostedScan
+ New Scan
211U0374@ALUMNO.ITSSAT.EDU.MX'S ACCOUNT
Dashboard
Targets
Scans
Risks
Reports
Integrations
Settings
Support
API Docs
Help Center
Upgrade Plan
Dashboard
1 scans in progress
1 scheduled scans
Risks detected
Total: 17
Critical 0
High 0
Medium 12
Low 5
Accepted 0
Closed 0
Recent Scans
See all scans
Scan
Target(s)
Results
Created
OpenVAS LITE
https://itssat.edu.mx/
4%
0 minutes ago
OWASP ZAP
https://itssat.edu.mx/
Report
0 minutes ago
Nmap LITE
https://itssat.edu.mx/
Report
0 minutes ago
Recent Risks
See all risks
Threat
Vulnerability
Target
OWASP ZAP
Server Leaks Version Information Via "Server" HTTP Response Header Field
OWASP Top 10
https://itssat.edu.mx/
OWASP ZAP
Content Security Policy (CSP) Header Not Set
OWASP Top 10
https://itssat.edu.mx/
OWASP ZAP
X-Content-Type-Options Header Missing
OWASP Top 10
https://itssat.edu.mx/
OWASP ZAP
Strict-Transport-Security Header Not Set
OWASP Top 10
https://itssat.edu.mx/
OWASP ZAP
Missing Anti-Clickjacking Header
OWASP Top 10
https://itssat.edu.mx/
Discovered Domains 39
See all targets
Discovered Domain
Related Target
admision.itssat.edu.mx
https://itssat.edu.mx/
www.admision.itssat.edu.mx
https://itssat.edu.mx/
www.encuestapadres.itssat.edu.mx
https://itssat.edu.mx/
www.requisiciones.itssat.edu.mx
https://itssat.edu.mx/
microcuencaxoteapan.itssat.edu.mx
https://itssat.edu.mx/
Rows per page: 10
1-5 of 39
Security Over Time
1 Week
1 Month
1 Year
Filters
Open Risks
Low
Medium
High
Critical
18
16
14
12
10
8
6
4
2
0
28 feb
1 mar
2 mar
3 mar
4 mar
5 mar
6 mar
Exposure Window
<30 days
30-90 days
>90 days
18
16
14
12
10
8
6
4
2
0
28 feb
1 mar
2 mar
3 mar
4 mar
5 mar
6 mar

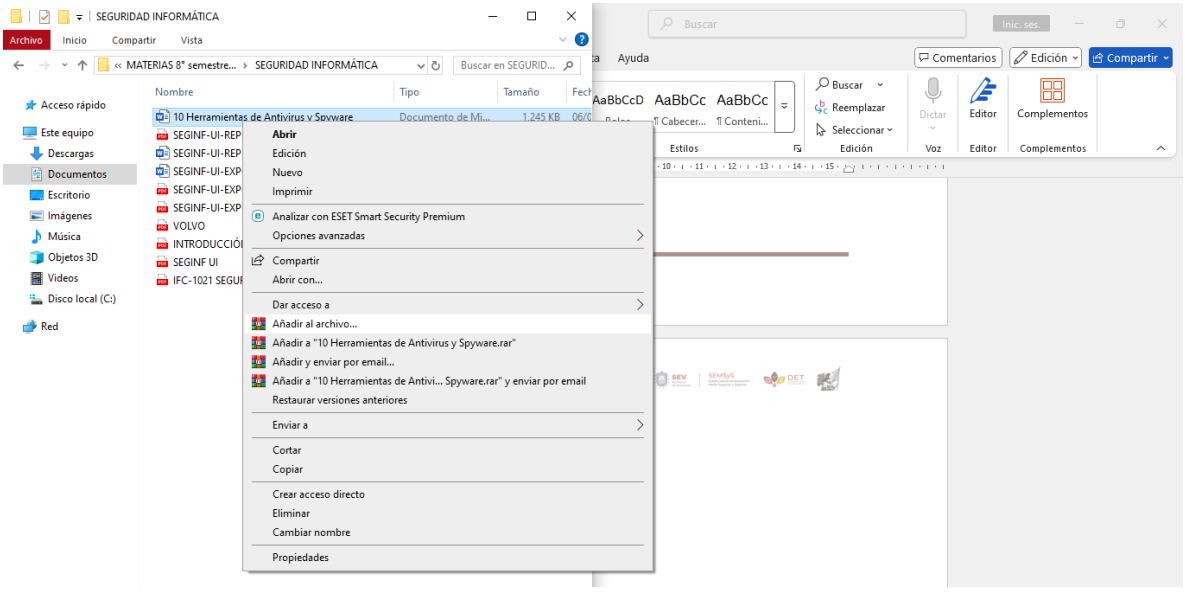
5. ENCRIPTADORES

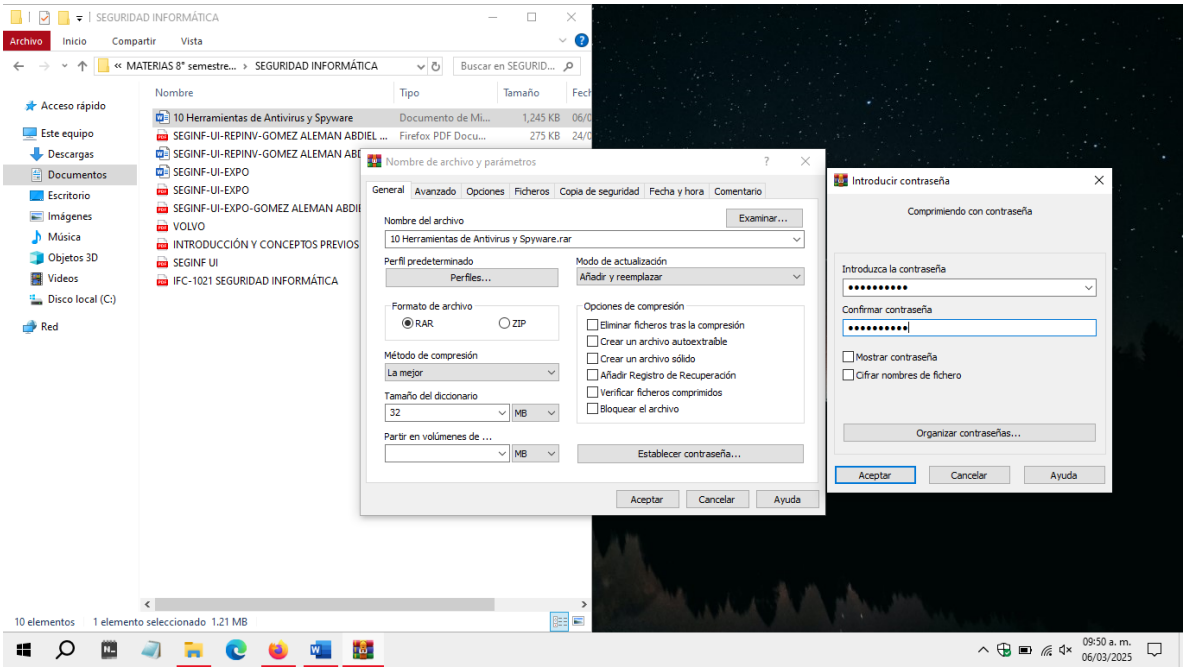
DEFINICIÓN: “Un encriptador está optimizado para codificar archivos, documentos o datos y transmisiones con la certeza de que no serán legibles en caso de que se extravíen o sean objeto de un robo de información.”

Cifrado de archivo en Windows 10:



Añadir contraseña a un archivo/carpeta comprimida con Winrar en Windows 10:





6. SERVIDORES PROXY

"La función de los proxy es mantener la privacidad de un sistema y el anonimato de los usuarios de una red, al momento de solicitar y enviar información. Estos actúan como intermediarios entre un repositorio de datos y un solicitante para tercerizar las solicitudes y filtrar interacciones sin poner en riesgo tu integridad."

Los diferentes tipos de servidores proxy

Existen diversos tipos de servidores proxy disponibles, cada uno diseñado para un uso específico.

- **Proxy HTTP**: Empleados en entornos corporativos y educativos, estos proxys limitan el acceso a ciertos sitios o contenidos basándose en políticas de seguridad o reglamentos preestablecidos.
- **Proxy transparente**: Pasan las solicitudes y respuestas sin alteraciones, mientras ocultan la dirección IP real del usuario. Son comúnmente usados para el registro de datos o control parental.

- **Proxy anónimo**: Esconden la dirección IP del usuario, permitiendo navegar de forma anónima por la red. A diferencia de los proxys transparentes, no incluyen la dirección IP real en los encabezados HTTP.
- **Reverse proxy**: Ubicados en el lado del servidor web, un reverse proxy sirve como punto de acceso desde Internet hacia uno o varios servidores internos. A menudo se utilizan para balanceo de carga, SSL offloading y seguridad de servidores internos.
- **Elite proxy**: Proporcionan el máximo nivel de privacidad y seguridad al ocultar la dirección IP del usuario y no revelar la presencia de un proxy.
- **Proxy distorting**: Este tipo de proxy esconde la dirección IP real del usuario pero entrega una dirección IP falsa en los encabezados HTTP, generando un engaño sobre el origen de la solicitud.
- **Proxy SOCKS**: Se usan para el enrutamiento de paquetes entre un cliente y un servidor a través de un servidor proxy usando el protocolo SOCKS. Normalmente se emplean en aplicaciones P2P o juegos en línea.

7. ALMACENAMIENTO DE RESPALDO

"Algunas formas de hacerlo es mediante: Memorias extraíbles para archivos pequeños o documentos específicos. Discos duros externos para respaldar volúmenes más grandes de información o bases de datos completas. Espacios de almacenamiento en espejo que resguardan copias de tu información en dos o más lugares para evitar pérdidas."

Software de prevención de pérdida de datos: Kickidler

Características útiles

- Interceptar: archivos, comunicaciones de texto y voz en chats de mensajería, correos electrónicos o redes sociales.
- Evitar las capturas de pantalla de datos importantes.
- Identificar a los empleados que están estresados, borrachos o bajo los efectos de las drogas con la opción de tomar huellas digitales.

- La habilidad de consultar archivos bloqueados para determinar qué información está almacenada en las computadoras de los empleados.
- Notificaciones sobre incidentes y actividad sospechosa de los empleados.
- Prohibiendo el uso de todos los dispositivos USB para evitar copiar datos corporativos.
- Localizar empleados incluso si tienen una VPN habilitada.
- Detección facial para identificar el acceso no autorizado a una computadora.
- Monitoreo de la actividad de los empleados y análisis del comportamiento de los empleados.
- Corre en Windows, Linux, macOS, admite múltiples servidores y tiene requisitos del sistema mínimos.

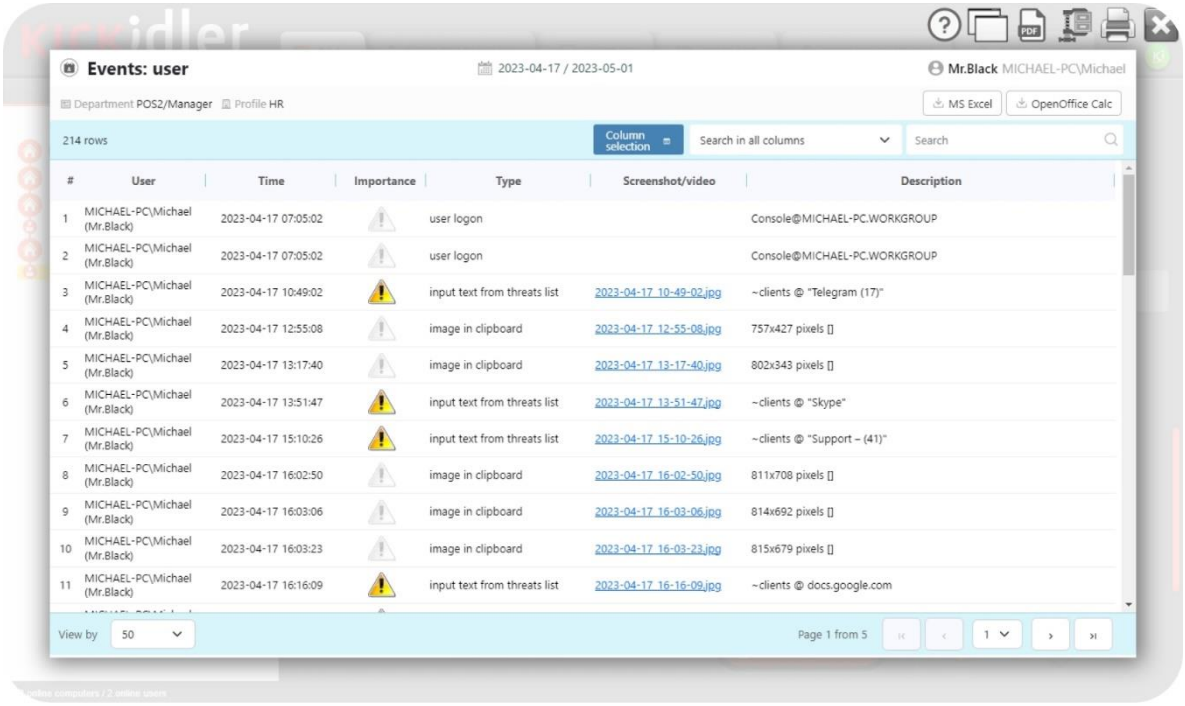
Ventajas y desventajas

- Ventajas: El software tiene requisitos del sistema mínimos: requiere un servidor básico y es adecuado para PC de gama baja.
- Desventajas: Cuando el software se instala manualmente en modo público, se notificará a los empleados la implementación de la solución de monitoreo.

Nombre /sitio web	Idiomas admitidos	Opciones de implementación	Requisitos del sistema	Razones para comprar	Razones para evitar	Precio (costo por una PC por mes)	Periodo de prueba
Kickidler	Armenio, Brasileño, Búlgaro, Chino, Inglés, Portugués, Ruso, Español	Solución local	Windows Mac iOS Android	+ Solución integral y rentable con una variedad de informes de rendimiento + Seguimiento en tiempo real de cualquier infracción + Políticas de precios claras y sistema de descuentos + Equipo de asistencia	- Sin servicio en la nube por el momento (en desarrollo)	1 mes – $9.99 3 meses – $8.33 ($25) 6 meses – $6.67 ($40) 1 año – $5.5 ($66) 3 años – $3.67 ($132) ** Descuento de hasta el 30% disponible dependiendo de la cantidad*	+ Opción de prueba gratuita de 14 días

				técnica con capacidad de respuesta		*de computadoras a monitorear*	

Prevención de amenazas internas



8. GENERADORES DE CONTRASEÑA

"crean y resguardan códigos de seguridad para ser utilizados solo desde ciertos equipos y para cuentas específicas. Estas contraseñas suelen ser complejas y se componen por números, letras y símbolos que dificultan su replicación."

ESET Password Generator:

El generador de contraseña es online se accede mediante la dirección: https://www.eset.com/mx/password-generator/. Su característica es que se puede ajustar el número total de caracteres de 4 a 64, además permite usar mayúsculas, minúsculas, números y símbolos.

9. VPN

DEFINICIÓN: "funciona como una red privada virtual que solo conecta equipos o usuarios específicos e impide que alguien más pueda entrar de manera online a ellas."

Proxy vs VPN: ¿cuáles son las diferencias?

En cuestiones de seguridad y privacidad en línea, a menudo se comparan servidores proxy y redes privadas virtuales (VPN). A pesar de que ambos ofrecen beneficios para mejorar el anonimato y el acceso seguro a Internet, operan de manera muy distinta y cumplen con propósitos diferentes.

Funcionamiento	
Proxy	Funciona como intermediario para tu tráfico de internet, disimulando tu dirección IP real de los sitios web que visitas. Puede proporcionar una caché de datos, pero no cifra tus datos.
VPN	Crea un túnel seguro entre tu dispositivo e Internet. Todos los datos transmitidos están cifrados, brindando una protección completa contra interceptaciones e intrusiones.
Seguridad	
Proxy	Principalmente usado para evitar restricciones geográficas o para un anonimato limited. Ofrece menos protección contra interceptaciones de tráfico.
VPN	Perfecta para una seguridad total en redes no seguras como el Wi-Fi público. Cifra todo el tráfico, protegiendo así de manera efectiva los datos sensibles.
Compatibilidad	
Proxy	Fáciles de configurar para aplicaciones específicas como navegadores web. Podrían no ser compatibles con todas las aplicaciones que utilizan Internet.
VPN	Opera a nivel de sistema, abarcando todas las conexiones a Internet del dispositivo, haciéndola compatible con casi todas las aplicaciones de web e Internet.

REFERENCIAS:

[1] Material de clase, *googledrive*, 2025 [En línea] Disponible en: https://ibit.ly/w-jrl [Accedido: 24-mar-2025]

GUIA DE OBSERVACIÓN PARA EXPOSICIÓN

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA	NOMBRE DEL CURSO: SEG. INF.
NOMBRE DEL DOCENTE: MTI. ROSARIO CARVAJAL HERNÁNDEZ	TEMA: 1.4 OBJETIVOS DE LA SEG. INFORMATICA UNIDAD: I
OBJETIVO DE LA EXPOSICIÓN:	

DATOS GENERALES DEL PROCESO DE EVALUACIÓN		
NOMBRE DE LOS ALUMNOS:	NO. DE CONTROL:	FIRMA DEL ALUMNO:
1.- GOMEZ ALEMAN M.A.	1.- 21140374	1.-
2.-	2.-	2.-
3.-	3.-	3.-
4.-	4.-	4.-
5.-	5.-	5.-

INSTRUCCIONES DE APLICACIÓN

Revisar los documentos o actividades que se solicitan y marque con una X en los apartados "SI" cuando la evidencia a evaluar se cumple; en caso contrario marque "NO". En la columna "OBSERVACIONES" ocúpela cuando tenga que hacer comentarios referentes a lo observado.

VALOR DEL REACTIVO	CARACTERÍSTICA A CUMPLIR (REACTIVO)	CUMPLE		OBSERVACIONES
		SI	NO	
	Aspectos Individuales (18 %)			
3	Dominio del Tema (divagaciones, claridad, uso de ejemplos)	X		
3	Orden y Claridad en la Exposición	X		
3	Dominio del Auditorio	X		
3	Dicción	X		
3	Manejo del Tiempo	X		
3	Presentación (limpieza y formalidad)	X		
	Material (15 %)			
3	Esquema de Diapositiva	X		
3	Portada	X		
3	Ortografía	X		
3	Originalidad	X		
3	Secuencia estructurada	X		
	Grupal (7 %)			
3	Puntualidad	X		
4	Organización	X		
—	Integración	—		
—	Colaboración	—		
40 %	CALIFICACIÓN:	1.- 40.-		
		2.-		
		3.-		
		4.-		
		5.-		

RIESGOS INFORMÁTICOS DE VOLVO CARS

Materia: Seguridad Informática

Alumno: Abdiel Miguel Gomez Aleman

PRINCIPALES RIESGOS INFORMÁTICOS

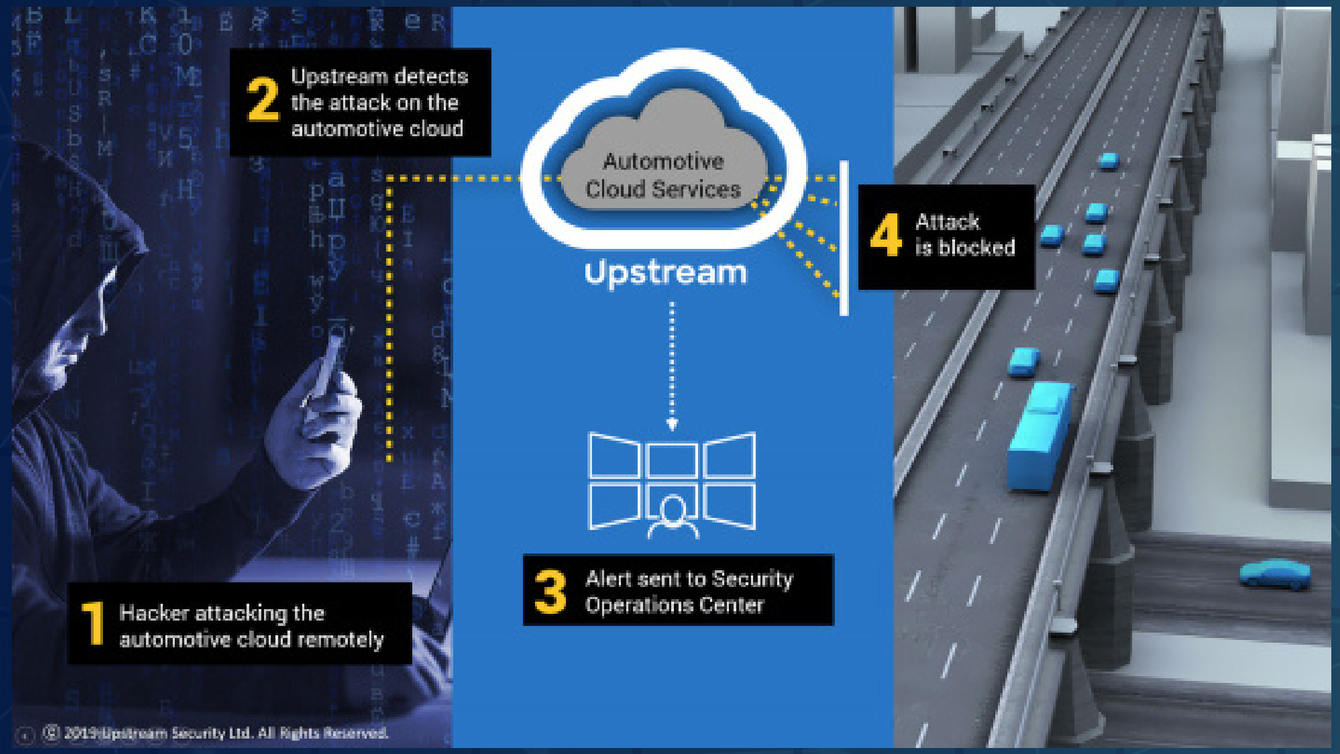
1. Ataques Remotos a la Conectividad del Vehículo

Volvo utiliza protocolos de seguridad como SSL y sistemas de gestión de certificados, pero cualquier vulnerabilidad en estos sistemas podría permitir ataques de interceptación de datos y manipulación remota.

2. Riesgos en la Aplicación Móvil Volvo On Call

- La aplicación Volvo On Call permite a los usuarios desbloquear, arrancar y controlar ciertas funciones de su vehículo de manera remota.
- Un atacante podría aprovechar credenciales débiles o dispositivos móviles comprometidos para tomar el control del vehículo.

PRINCIPALES RIESGOS INFORMÁTICOS



3. Seguridad del Módem del Vehículo y Actualizaciones de Software

El módem del vehículo representa la puerta de entrada a la conectividad con Internet. Si no está bien asegurado, podría ser utilizado por atacantes para interceptar o manipular datos.

4. Riesgos en el Desarrollo de Vehículos Autónomos

- Un atacante podría manipular sensores o sistemas de IA para desorientar al vehículo o generar accidentes.
- Un fallo en la ciberseguridad de los algoritmos de conducción podría ser catastrófico

OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

1. Confidencialidad

2. Integridad

3. Disponibilidad

4. Autenticación

COSTOS ASOCIADOS

- **Inversión en infraestructura de seguridad**: *$106,587,250.00*
- **Capacitación y concientización**: *$1,065,872.50*
- **Mantenimiento y actualizaciones**: *$42,634,900.00*
- **Gestión de incidentes**: *$106,587,250.00*

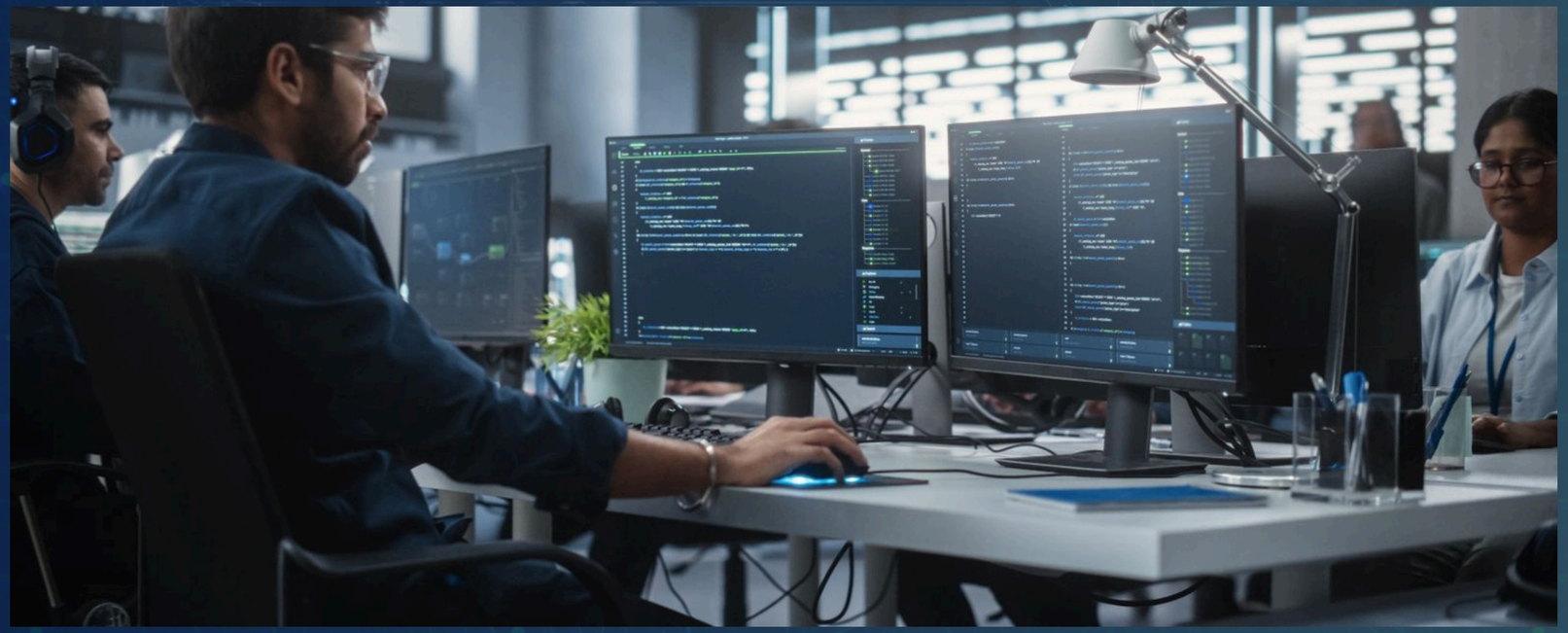


TABLA DE VULNERABILIDADES Y AMENAZAS

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad
R-1	Datos	Robo y Alteración de Datos	Datos visibles, falta de políticas de acceso y encriptación, ransomware	Medio
R-2	Datos	Ransomware	Datos mal respaldados, falta de copias de seguridad	Alta
R-3	Sistemas	Malware	Uso de software no actualizado, falta de protección antivirus	Alta
R-4	Sistemas	Ataques de Denegación de Servicio (DDoS)	Recursos limitados, no protección ante tráfico malicioso	Alta
R-5	Sistemas	Exploits de Vulnerabilidades	Software desactualizado, sin parches de seguridad críticos	Alta
R-6	Infraestructura de Red	Ataques de Man-in-the-Middle (MitM)	Conexiones no cifradas o configuraciones inseguras	Alta
R-7	Infraestructura de Red	Acceso no autorizado	Intrusos que vulneran la red para obtener acceso a información confidencial	Alta
R-8	Aplicaciones	Inyección SQL	Falta de validación de entradas, código vulnerable	Medio
R-9	Aplicaciones	Cross-Site Scripting (XSS)	Falta de validación de entradas en aplicaciones web	Medio
R-10	Personal	Phishing y Extorsiones	Empleados sin capacitación en ciberseguridad, contraseñas débiles, falta de autenticación multifactor	Alta

CONCLUSIÓN

Volvo Cars enfrenta una serie de riesgos informáticos importantes, incluidos ciberataques, vulnerabilidades en los vehículos conectados, filtraciones de datos y riesgos relacionados con la cadena de suministro digital. Para mitigar estos riesgos, la empresa debe centrarse en mantener altos estándares de seguridad en torno a los objetivos clave de la seguridad informática: confidencialidad, integridad, disponibilidad y autenticación.

BIBLIOGRAFÍA:

[1] “Cybersecurity in Volvos”, volvo.custhelp.com, 2023 [En línea]. Disponible en: https://ibit.ly/2fypc [Accedido: 16-feb-2025]

[2] A. Bokesand y C. Sandberg, “Connected Vehicle Cybersecurity Volvo Group Trucks Technology”, 2019 [En línea]. Disponible en: https://ibit.ly/DS1gY [Accedido: 16-feb-2025]

[3] “Volvo Trucks Driver Guide”, Volvo Trucks Driver Guide, 2024. [En línea]. Disponible en: https://ibit.ly/YawFQ [Accedido: 16-feb-2025]

¡GRACIAS!

SEGURIDAD INFORMÁTICA - UNIDAD I

Puntos totales 11/12

INTRODUCCIÓN A LAS REDES DE DATOS

Se ha registrado el correo del encuestado (**211u0374@alumno.itssat.edu.mx**) al enviar este formulario.

✓ Proteger el uso, fiabilidad, integridad y seguridad de la red para evitar que la información sea modificada o robada. *1/1

- ○ Seguridad de Hw
- ◉ Seguridad en la red ✓
- ○ Seguridad de Sw

✓ Conjunto de procedimientos y herramientas que se implementan para proteger la información. *1/1

- ○ Cibernetica
- ◉ Ciberseguridad ✓
- ○ Ciberdelincuencia

✓ De dónde provienen las amenazas de la seguridad informática * 1/1

- ○ Personas empleadas y desempleadas
- ◉ Personas, amenazas lógicas y catástrofes ✓
- ○ Bombas y guerras

✓ Los elementos que protege la seguridad informática son: * 1/1

- ◉ Hw, Sw y datos ✓
- ○ Hw, Sw y el internet
- ○ Hw y Sw

✓ Uno de los objetivos de la ciberseguridad es ... * 1/1

- ◉ Generar confianza entre los clientes, proveedores y el mercado ✓
- ○ Garantizar los ingresos
- ○ Las dos anteriores

✓ Año en que se formó en Europa el comité de expertos en delitos informáticos *1/1

- ○ 2005
- ○ 1985
- ◉ 1995 ✓

✓ Los aspectos que considera la seguridad informática son: * 1/1

- ○ Confidencialidad, totalidad y disponibilidad
- ○ Confidencialidad, integridad y persistencia
- ◉ Confidencialidad, integridad y disponibilidad ✓

✗ Los tipos de amenazas son: * 0/1

- ◉ Robo, suplantación, modificación ✗
- ○ Interrupcion, interceptación, modificación y fabricación
- ○ Las dos anteriores

Respuesta correcta

- ◉ Interrupcion, interceptación, modificación y fabricación

NOMBRE DEL ALUMNO *

ABDIEL MIGUEL GOMEZ ALEMAN

✓ Encuentran las vulnerabilidades existentes en los equipos desde su fabricación, hasta los dispositivos de entrada y salida que están conectados. *1/1

- ○ Seguridad de Sw
- ◉ Seguridad de Hw ✓
- ○ Seguridad en la red

✓ Son los mecanismos que emplea la seguridad informática * 1/1

- ◉ Prevención, Detección y Recuperación ✓
- ○ Análisis, Búsqueda y Encuentro
- ○ Hallazgos y Recuperación

✓ Los errores en el software generan vulnerabilidades y es uno de los mayores riesgos de seguridad. *1/1

- ○ Seguridad de red
- ○ Seguridad de Hw
- ◉ Seguridad en la Sw ✓

✓ Se consideran el primer virus y antivirus del mundo. * 1/1

- (●) Creeper y Reaper ✓
- ( ) Reaper y Creeper
- ( ) Freaper y Breaper
- ( ) Otro: _____