JAYMON SECURITY
Cyberintelligence & Solutions

INFOSEC

y

CIBERSEGURIDAD

JAYMON SECURITY S.L.

JAYMON SECURITY
Cyberintelligence & Solutions

SEGURIDAD DE LA INFORMACIÓN

I. Seguridad de la información

“ Conjunto de medidas preventivas empleadas para controlar y proteger los datos en cualquier ámbito, tanto en nuestra vida cotidiana como en la laboral “

Ejemplos:

✓ Creación de copias de seguridad.

✗ No actualizar el sistema operativo de los dispositivos.

Fuente:Delegado de protección de datos

II. Seguridad de la información

JAYMON SECURITY
Cyberintelligence & Solutions

La seguridad de la información garantiza 3 pilares fundamentales:

DISPONIBILIDAD

Que la información necesaria esté disponible en todo momento.

Poder escuchar un audio de WhatsApp sin ningún impedimento.

INTEGRIDAD

Que la información no haya sufrido modificaciones.

Tener la misma imagen en Google Fotos y en el álbum de casa.

CONFIDENCIALIDAD

Que la información sea únicamente accesible para personal autorizado.

Documentos o información de un grupo de WhatsApp.

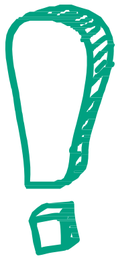
Las normas ISO 27001 afirman que una buena seguridad de la información debe asegurar estos 3 pilares

III. Seguridad de la información

JAYMON SECURITY
Cyberintelligence & Solutions

NORMAS ISO

"Son normas de seguridad establecidas por la Organización Internacional para la Estandarización con el objetivo de orientar, coordinar, simplificar y unificar los usos para conseguir menos coste y mayor efectividad."



IMPORTANTE : No confundir este concepto con seguridad informática, la cual se centra en la protección de instalaciones informáticas.

International Organization for Standardization
ISO
27001

Fuente: Teorema

IV. Seguridad de la información

La seguridad de la información también identifica y protege cualquier tipo de dato, garantizando su seguridad durante todo el ciclo de su vida.

Las soluciones de seguridad de la información facilitan el tratamiento adecuado de estos datos. Ayudan a sujetos y organizaciones a cumplir con las normativas vigentes mediante la gestión y control de la información en uso, reposo y tránsito.

La información que requiere de esa protección varía dependiendo de la normativa de cumplimiento.

Industria
Tipo de datos

V. Seguridad de la información

JAYMON SECURITY
Cyberintelligence & Solutions

Sistemas de Gestión de la Seguridad de la Información (SGSI)

"Colección de medidas y procedimientos que se crean en una organización o sujeto para gestionar y controlar la seguridad de la información. Estos sistemas permiten asegurarse de que los datos estén a salvo por si ocurre cualquier problema impredecible".

SGSI

Esquema Nacional de Seguridad en España

Es una norma legal española que establece el marco de referencia para que los sistemas de información digital de las Administraciones Públicas, y de las empresas y profesionales que les prestan servicios, alcancen y mantengan la seguridad necesaria.

ens
Esquema Nacional de Seguridad

JAYMON SECURITY
Cyberintelligence & Solutions

CIBERSEGURIDAD

I. CIBERSEGURIDAD

"Práctica de proteger su información digital, dispositivos y activos. Esto incluye información personal, cuentas, archivos, fotos e incluso el dinero."

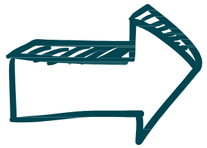
(Microsoft, 2022)

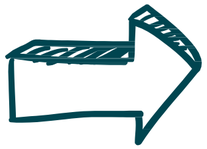
La ciberseguridad puede actuar en todas las áreas cotidianas en las que se usen dispositivos electrónicos.

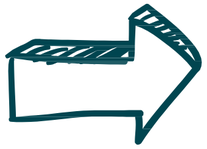
II. CIBERSEGURIDAD

JAYMON SECURITY
Cyberintelligence & Solutions

La ciberseguridad también se rige bajo unos principios fundamentales:

1. CONFIDENCIALIDAD  Asegurarse de que la información llegue única y exclusivamente a la persona que debe llegar.

2. INTEGRIDAD  Asegurarse de que la información no ha sido modificada y tampoco se modifique por nadie que no deba hacerlo.

3. DISPONIBILIDAD  Capacidad de tener acceso a la información y servicios en todo momento y situación por quien tenga autorización para hacerlo.

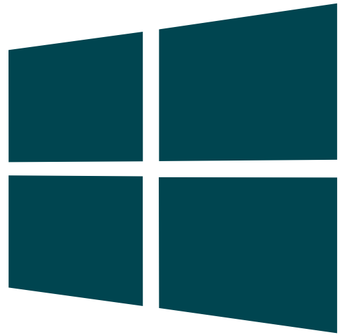
III. CIBERSEGURIDAD

JAYMON SECURITY
Cyberintelligence & Solutions

Dentro de la ciberseguridad podemos diferenciar:

Seguridad física — HARDWARE

Seguridad lógica — SOFTWARE



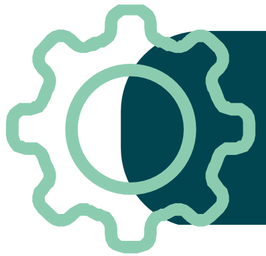
III. CIBERSEGURIDAD

JAYMON SECURITY
Cyberintelligence & Solutions

Seguridad física

Se refiere a las medidas y prácticas adoptadas para proteger los dispositivos físicos de amenazas externas, daños y accesos no autorizados.

EJEMPLO ⇨ Poner control de acceso físico para los dispositivos con la finalidad de mantenerlos protegidos.



Planes de contingencia

Políticas de copias de seguridad

III. CIBERSEGURIDAD

JAYMON SECURITY
Cyberintelligence & Solutions

Seguridad lógica

Se enfoca en proteger el software y la información de amenazas digitales a través de protocolos de autenticación, cifrado y control de acceso.

FINALIDAD : reducir las amenazas y riesgos al máximo, respetando los principios fundamentales de la ciberseguridad.

OBJETIVOS

Garantizar que los procedimientos son correctos y seguros.

Restringir el acceso a archivos y programas a los que no se deba acceder.

III. CIBERSEGURIDAD

JAYMON SECURITY
Cyberintelligence & Solutions

ELEMENTOS

Seguridad lógica

CONTROLES DE ACCESO

Asegurando la confidencialidad para que sólo tengan acceso aquellas personas autorizadas.

PROTECCIÓN ANTI MALWARE

A través de programas informáticos que detectan ataques maliciosos a los dispositivos.

FACTOR HUMANO

Normalmente es el mayor riesgo a nivel de seguridad. Hay que formar a los trabajadores para favorecer la prevención.

JAYMON SECURITY
Cyberintelligence & Solutions

DIFERENCIAS ENTRE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

JAYMON SECURITY
Cyberintelligence & Solutions

	SEGURIDAD DE LA INFORMACIÓN	CIBERSEGURIDAD
ALCANCE	Requiere proteger la información en todas sus formas.	Se centra únicamente en datos digitales.
PARÁMETROS DE PROTECCIÓN	Proteger la información de posibles riesgos y los sistemas informáticos que lo almacenan.	Protección en redes, dispositivos y sistemas contra ciberataques.
ENFOQUE	Técnicas que las empresas utilizan para proteger sus datos y sistemas.	Tecnología que protege los sistemas de información.

JAYMON SECURITY
Cyberintelligence & Solutions

DEFINICIÓN DE VULNERABILIDAD

JAYMON SECURITY
Cyberintelligence & Solutions

I. DEFINICIONES

VULNERABILIDAD

INSTITUTO NACIONAL DE CIBERSEGURIDAD

"Fallo técnico o deficiencia de un programa que puede permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota."

(INCIBE, 2022)

Fuente:muyseguridad.net

"Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible"

(INCIBE, 2022)

JAYMON SECURITY
Cyberintelligence & Solutions

II. TIPOS GENERALES

Las vulnerabilidades pueden estar causadas por diferentes aspectos:

- Dispositivo → Hardware
- Sistema → Software
- Fallo en los procedimientos
- Error humano

EJEMPLO

Una red Wifi pública abierta a la que nos conectamos. Estas redes públicas pueden ser utilizadas por delincuentes para capturar información de nuestros dispositivos o incluso tomar el control total de ellos.

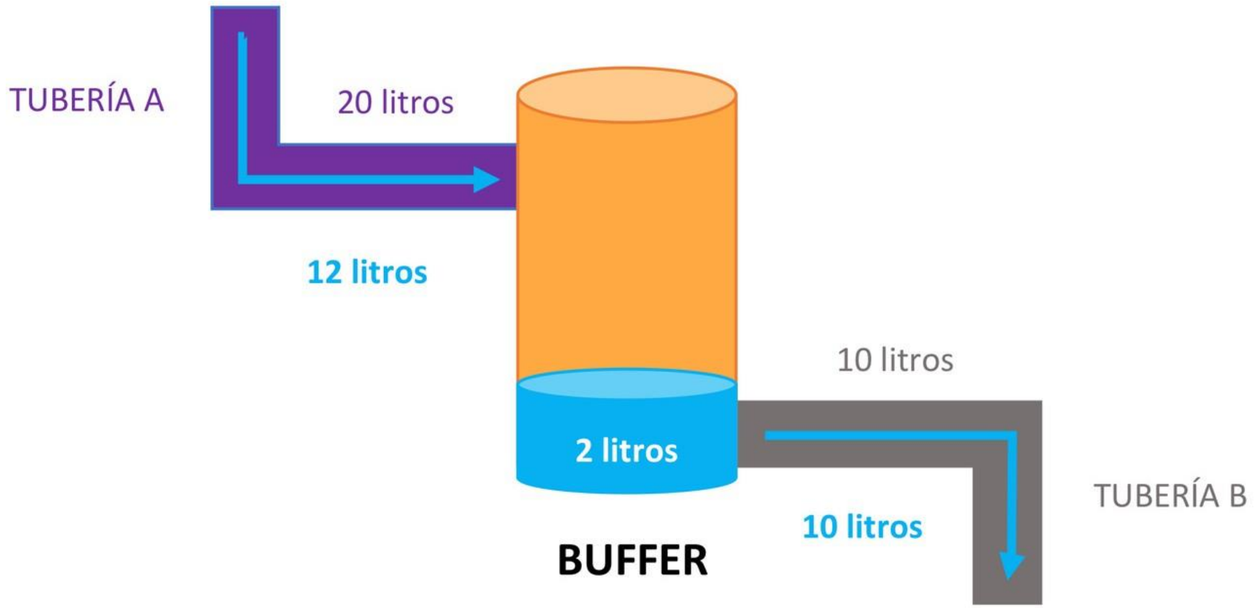
En este ejemplo, la vulnerabilidad sería a través de un error humano.

III. TIPOS ESPECÍFICOS

1 Desbordamiento del Buffer

Ocurre cuando las aplicaciones no controlan la cantidad de datos que copian en el buffer, y al sobrepasar esta cantidad de datos se pueden modificar ciertas zonas que afectan directamente a los datos guardados.

* **Buffer** → espacio temporal en el que se almacenan los datos de la memoria de nuestros dispositivos mientras la información se envía de un sitio a otro.



JAYMON SECURITY
Cyberintelligence & Solutions

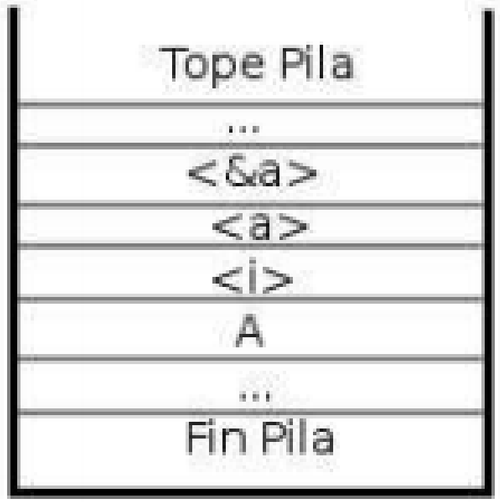
III. TIPOS ESPECÍFICOS

2 Error de formato en cadenas

Ocurre cuando las aplicaciones no validan datos del usuario. De esta manera un atacante pueda tener acceso a datos confidenciales o dañar el sistema.

Ejemplo

Una aplicación web que solicita al usuario ingresar su año de nacimiento, pero no valida bien esta entrada. Un atacante podría introducir una cadena maliciosa, como "1990; DROP TABLE users;", que podría resultar en la eliminación de la tabla "users" de la base de datos.

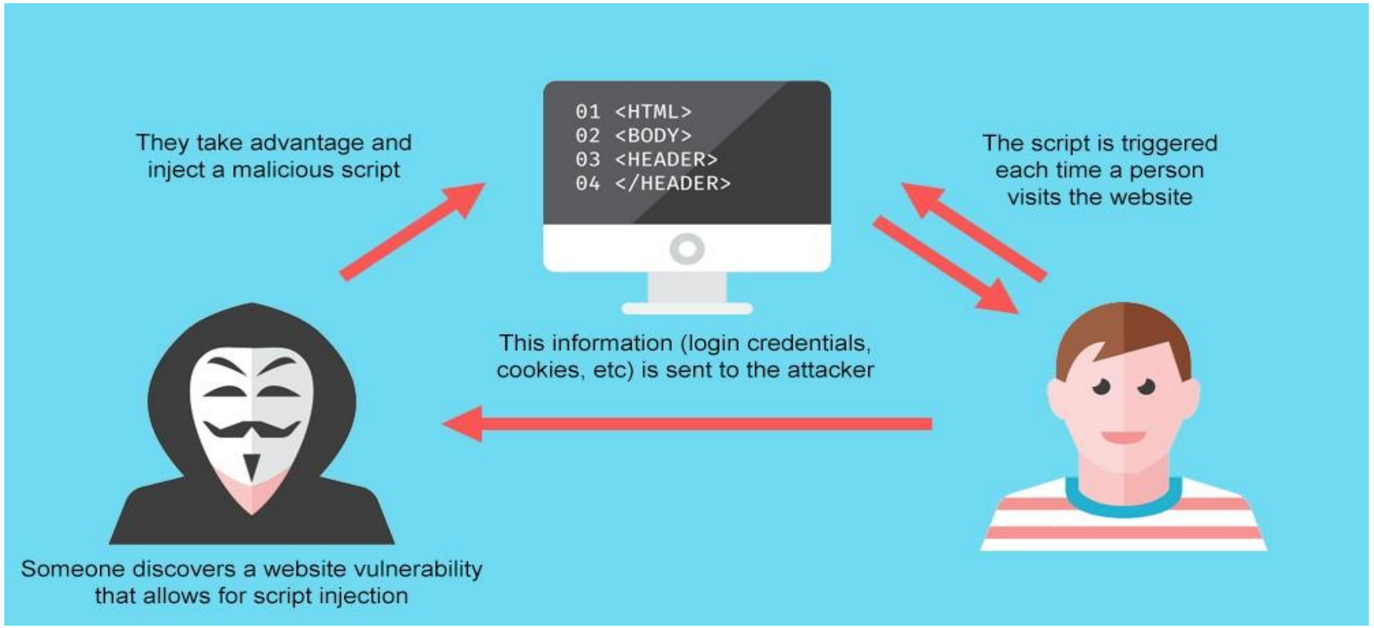


III. TIPOS ESPECÍFICOS

3 Inyección de código entre sitios

Se basa en que los atacantes pueden inyectar código malicioso en páginas web legítimas afectadas por esta vulnerabilidad y por las que navegan los usuarios. Estos introducen datos en los formularios web infectados (como por ejemplo sus credenciales de acceso), y son enviados al atacante.

<Cross site scripting>
(XSS)



Fuente: blogging

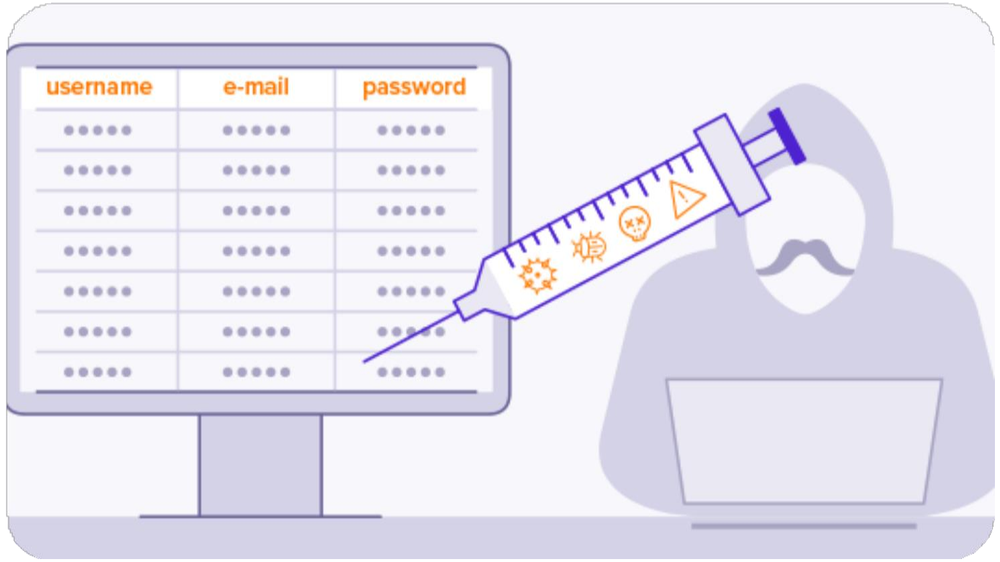
JAYMON SECURITY
Cyberintelligence & Solutions

III. TIPOS ESPECÍFICOS

3 Inyección de SQL

Es un tipo de ciberataque en el cual un atacante inyecta código propio en un sitio web con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos. Una vez dentro, puede controlar la base de datos del sitio web y secuestrar la información de los usuarios.

La inyección de SQL no es una amenaza enfocada en el usuario. Es responsabilidad de las personas que gestionan los sitios web el prevenir estos ataques.



Fuente:Avast

JAYMON SECURITY
Cyberintelligence & Solutions

ORIGENES DE VULNERABILIDADES

JAYMON SECURITY
Cyberintelligence & Solutions

I. ORÍGENES

Existen diferentes niveles de vulnerabilidades dependiendo de la gravedad y el tipo de amenaza que generen.

Todas las que sean públicas tienen un número CVE (Common Vulnerabilities and Exposures).

Estas vulnerabilidades están recogidas en una base de datos (CVE Details). Cada una de ellas presenta una descripción y forma de mitigación.

Fuente: eAprende.com

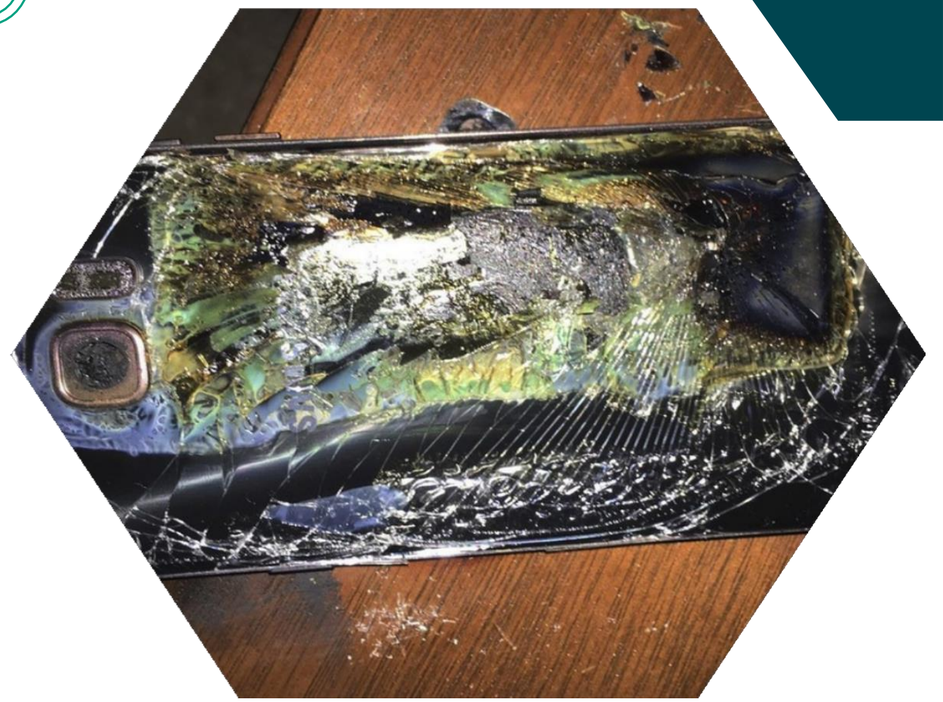
II. ORÍGENES

Dentro de las vulnerabilidades informáticas destacan:

1 Fallos en el diseño

Normalmente se asocian a errores o fallos de diseño del sistema. Son fallas en los programas del dispositivo.

También puede deberse al propio proceso de fabricación del dispositivo físico.



Fuente: The Wall Street Journal

III. ORÍGENES

2 Errores de configuración

Surgen por una configuración incorrecta, lo cual deja a los dispositivos inseguros poniendo en riesgo sus datos.

Una configuración incorrecta o una mala actualización de nuestro dispositivo móvil puede dejar la puerta abierta a los ciberdelincuentes.

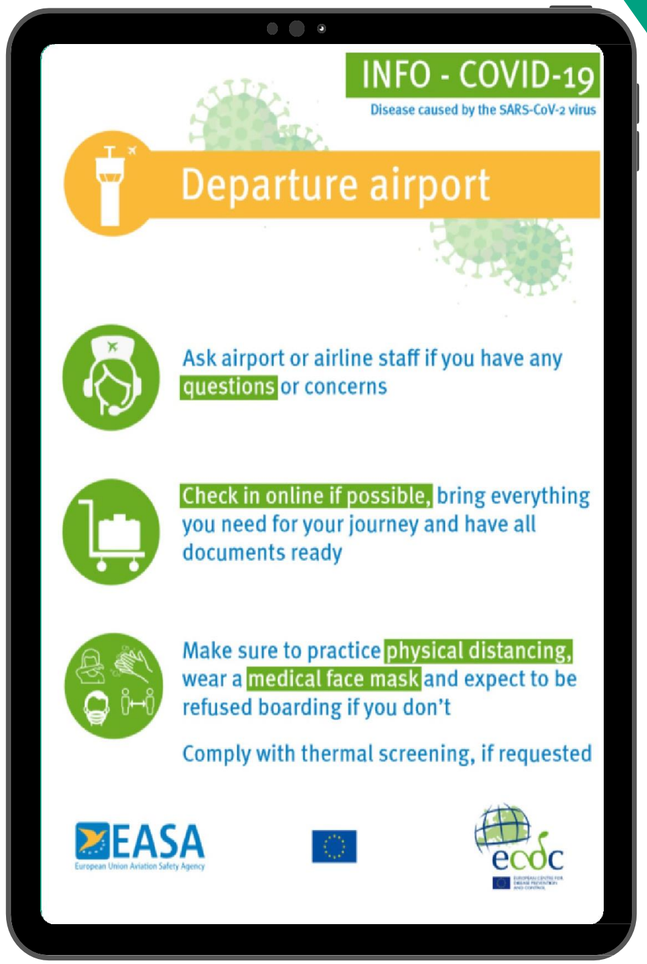
Fuente: BigBang News

IV. ORÍGENES

3 Carencias en procedimientos

Procedimientos que no contemplan adecuadamente todas las posibilidades de ejecución y que, por lo tanto, pueden contener vulnerabilidades.

Los procedimientos deben estar muy bien detallados y explicados para que no haya duda alguna, y que no haya ningún error durante la ejecución del proceso.



Fuente: Seguridadaerea.gob.es

V. ORÍGENES

4 Vulnerabilidades inducidas por empleados

Tras la pandemia del COVID -19, muchas empresas se han adaptado al teletrabajo.

Para muchas personas es un ámbito completamente novedoso y por tanto son los más vulnerables a sufrir ciberataques o amenazas.

Por ello se requiere concienciación y formación en ciberseguridad.

VI. ORÍGENES

4 Vulnerabilidades inducidas por empleados

Aquí podemos encontrar dos tipos de empleados:

INSIDERS VOLUNTARIOS

Aquellos que generan esa vulnerabilidad intencionadamente con el objetivo de dañar la empresa.

INSIDERS INVOLUNTARIOS

Son aquellos que por errores suyos no intencionados se genera una vulnerabilidad en la empresa.

JAYMON SECURITY
Cyberintelligence & Solutions

IMPACTOS ORGANIZACIONALES

I. IMPACTOS ORGANIZACIONALES

"La evaluación o medición del cambio generado en la organización por implantar una innovación" (Álvarez, 1996)

Añadir que este impacto puede ser tanto positivo como negativo, tanto para la sociedad, la propia empresa u otras áreas.

Podemos detectar diferentes tipos de impactos tanto para la empresa cómo para otras áreas de influencia. Estos impactos serán mencionados en las siguientes diapositivas.

JAYMON SECURITY
Cyberintelligence & Solutions

II. IMPACTOS ORGANIZACIONALES

IMPACTO REPUTACIONAL

Un impacto negativo de este tipo puede provocar pérdidas potenciales del capital financiero, social o participaciones en el mercado debido a los daños con los que se ha relacionado la propia empresa.

EJEMPLO

Una empresa está financiando terrorismo.

II. IMPACTOS ORGANIZACIONALES

IMPACTO ECONÓMICO

Un impacto negativo de este tipo puede ser debido a un error o descuido. Este impacto puede generar grandes pérdidas económicas que pueden llevar a la empresa a su disolución.

EJEMPLO

Se detecta que la empresa está cometiendo blanqueo de capitales. El impacto económico sería la multa correspondiente al delito.

II. IMPACTOS ORGANIZACIONALES

IMPACTO SOCIAL

El impacto social puede definirse como el grado de afectación o de incidencia que tiene un proyecto, evento u organización en la sociedad (Concepto, 2022).

- Impacto social positivo: aquel que la sociedad percibe cómo beneficioso, ya sea por creación de nuevas oportunidades, atención de necesidades, etc.

- Impacto social negativo: aquel que la sociedad percibe cómo una amenaza contra su actividad de negocio.

JAYMON SECURITY
Cyberintelligence & Solutions

II. IMPACTOS ORGANIZACIONALES

IMPACTO AMBIENTAL

Es la alteración del medio ambiente, provocada directa o indirectamente por un proyecto o actividad en un área determinada. Es decir, es la modificación del ambiente ocasionada por al acción del hombre o la naturaleza. (Responsabilidad Social Empresarial y Sustentabilidad, 2022).

EJEMPLO

El incremento de vuelos comerciales conlleva el aumento de quema de combustible. Los gases provocan el efecto invernadero a través del CO_2 y contribuye al calentamiento global.

JAYMON SECURITY
Cyberintelligence & Solutions

DEFINICIÓN DE AMENAZAS

I. DEFINICIONES

JAYMON SECURITY
Cyberintelligence & Solutions

AMENAZA

"Existencia de un posible peligro que surge de un hecho o acción, de cuya circunstancia o hecho se produciría un daño."

Las ciberamenazas se desarrollan en el ciberespacio, las cuales son cada vez más sofisticadas.

OBJETIVO PRINCIPAL

Comprometer la seguridad de un sistema y con ello, el acceso, disponibilidad, integridad y/o confidencialidad.

JAYMON SECURITY
Cyberintelligence & Solutions

SIN LIMITES

No existen fronteras en el ciberespacio.

Pueden alcanzar cualquier parte del mundo.

GRAN MAGNITUD

Los daños derivados pueden causar impacto a nivel mundial.

ECONÓMICO

Escasos recursos.

Son accesibles a cualquier persona.

ANONIMATO

Operaciones remotas controladas desde cualquier lugar.

Difícil identificar a los autores intelectuales

JAYMON SECURITY
Cyberintelligence & Solutions

II. AMENAZA vs VULNERABILIDAD

VULNERABILIDAD

La vulnerabilidad se puede definir como una debilidad que tiene un sistema, por lo que la información y los datos se pueden encontrar comprometidos.

Ej.- La página web del banco X no está actualizada ni tiene las medidas de protección adecuadas, por lo que ese sitio es vulnerable para determinadas amenazas.

AMENAZA

La amenaza se entiende como la posibilidad de que ocurra una situación que pueda provocar un daño sobre un sistema.

Ej.- Si la página web del banco X está actualizada y tiene las medidas de protección adecuadas, la página web no será vulnerable, pero no estarían exentos de sufrir otro tipo de amenaza o ataque.

JAYMON SECURITY
Cyberintelligence & Solutions

II. AMENAZA vs VULNERABILIDAD

Una amenaza puede surgir tras el aprovechamiento de una vulnerabilidad, que puede aparecer aunque un dispositivo esté bien protegido.

Las medidas básicas de protección son actualizaciones de software o antivirus.

Por lo tanto, la vulnerabilidad aparece cuando los sistemas o equipos no disponen de la protección adecuada que provoca la posibilidad de un ataque, mientras que, la amenaza es un peligro existente, el cual no depende directamente de si un equipo es vulnerable o no, sino que entran en juego otros factores (factor humano, etc.).

JAYMON SECURITY
Cyberintelligence & Solutions

POSIBLES FUENTES DE AMENAZA

JAYMON SECURITY
Cyberintelligence & Solutions

I. POSIBLES FUENTES DE AMENAZA

1

Malware

Programa informático malicioso, cuyo objetivo radica en introducirse en otros dispositivos y comprometer su seguridad. Se ejecuta sin el conocimiento ni la autorización del usuario del equipo "infectado", y realiza funciones perjudiciales: robar información, eliminar datos, bloquear o modificar información del usuario o de los sistemas.

Ejemplo

"Wannacry": Malware tipo Ransomware cuyo objetivo es encriptar todos los datos del equipo infectado de forma que el usuario no pueda acceder a ellos, salvo con una clave que solo podrían obtener previo pago de un rescate en criptodivisas.

JAYMON SECURITY
Cyberintelligence & Solutions

II. POSIBLES FUENTES DE AMENAZA

2 Ingeniería Social

Técnicas de manipulación psicológica con el objetivo de que los usuarios revelen información confidencial. Los ataques de ingeniería social usan como canales: el correo electrónico, llamadas telefónicas, aplicaciones de mensajería, redes sociales, etc.

La ingeniería social basa su comportamiento en una premisa básica: es más fácil manejar a las personas que a las máquinas.

Ejemplo.

Estafa del CEO: El atacante suplanta la identidad del CEO de una empresa para conseguir que sus empleados realicen transferencias bancarias.

JAYMON SECURITY
Cyberintelligence & Solutions

III. POSIBLES FUENTES DE AMENAZA

3

Amenazas Persistentes Avanzadas (APTs)

Ataques incesantes dirigidos a empresas para robar datos e información confidencial.

Lo que diferencia a esta amenaza de las otras, es que los delincuentes dejan "puertas traseras" en los sistemas vulnerados para poder acceder a ellos cuando lo deseen y seguir escalando el nivel del ataque.

Ejemplo.

RSA (compañía inglesa). El ataque se debió a una campaña de phishing que explotó una vulnerabilidad de Abobe Flash de una hoja de Excel. Los atacantes robaron información confidencial.

JAYMON SECURITY
Cyberintelligence & Solutions

IV. POSIBLES FUENTES DE AMENAZA

4

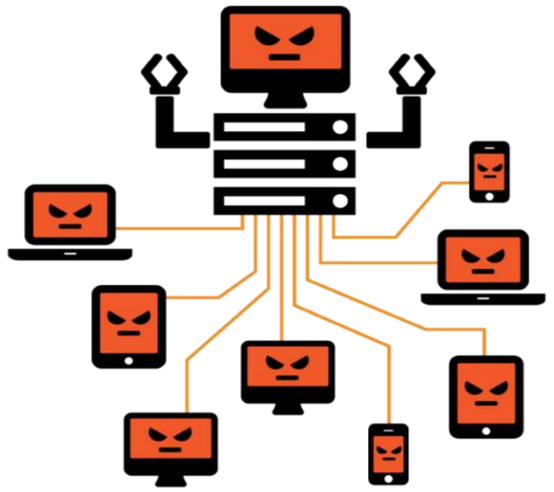
Redes de robots "Botnets"

Conjunto de equipos infectados que se encuentran controlados por un malware de manera remota.

Ataques de Denegación de Servicio (DDoS): El ciberdelincuente que tenga el control de la botnet, indicará a todos sus zombis que accedan a la vez a una determinada página web para saturarla y provocar que deje de funcionar con el objetivo de chantajear.

Ejemplo.

Cloudflare en 2022 sufrió un DDoS con más de 26 millones de solicitudes por segundo realizadas por dispositivos infectados de una misma Botnet.



JAYMON SECURITY
Cyberintelligence & Solutions

V. POSIBLES FUENTES DE AMENAZA

5

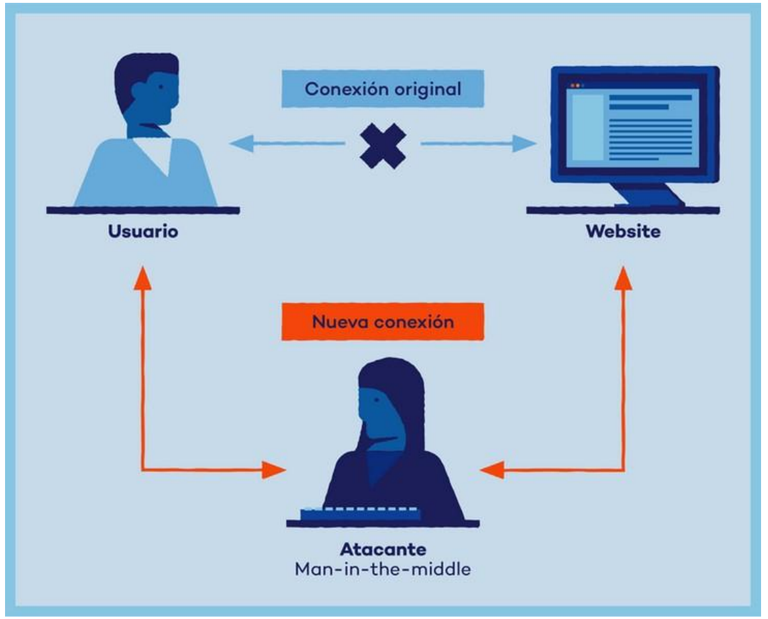
Ataque Man In The Middle (MITM)

Permite a un atacante manipular el tráfico de información entre dos o más dispositivos.

El objetivo puede ser escuchar la comunicación, obtener información sensible, o suplantar la identidad de alguna de las partes.

Ejemplo.

Caso de un empresario en Navarra: Tras haber reclamado el pago de una factura por un importe de 44.000€ a su cliente, éste le informó que ya se había abonado. La factura enviada por correo fue interceptada antes de llegar al destinatario y modificaron la cuenta bancaria para el pago. Tipo de MITM: Business Email Compromise (BEC).



JAYMON SECURITY
Cyberintelligence & Solutions

PROCEDENCIA DE LAS AMENAZA

JAYMON SECURITY
Cyberintelligence & Solutions

	ATAQUES	SUCESOS FÍSICOS
CONCEPTO	Aquellos causados por la intervención humana, se clasifican en ataques internos o externos.	Se producen cuando ha habido algún fallo imprevisto en los sistemas, que hace que sean más vulnerables.
EJEMPLO	Los internos se llevan a cabo dentro de la propia empresa, causados por usuarios con acceso legítimo. Los externos se originan fuera de la empresa y son causados por terceros sin autorización.	Fallo en la configuración o ejecución del sistema o equipo (técnicos). Incendio o inundaciones (naturales).

JAYMON SECURITY
Cyberintelligence & Solutions

	NEGLIGENCIA	DECISIONES INSTITUCIONALES
CONCEPTO	Descuido u omisión en el cumplimiento de una obligación que comprende un riesgo para la empresa. Tener agujeros de seguridad da paso a importantes vulnerabilidades del sistema.	Son aquellas decisiones de las personas con cierto poder e influencia sobre el sistema.
EJEMPLO	No tener los dispositivos y el software actualizados, no poseer antivirus o no realizar controles de vulnerabilidades y seguridad.	Mal manejo de contraseñas u optar por no usar cifrado.

JAYMON SECURITY
Cyberintelligence & Solutions

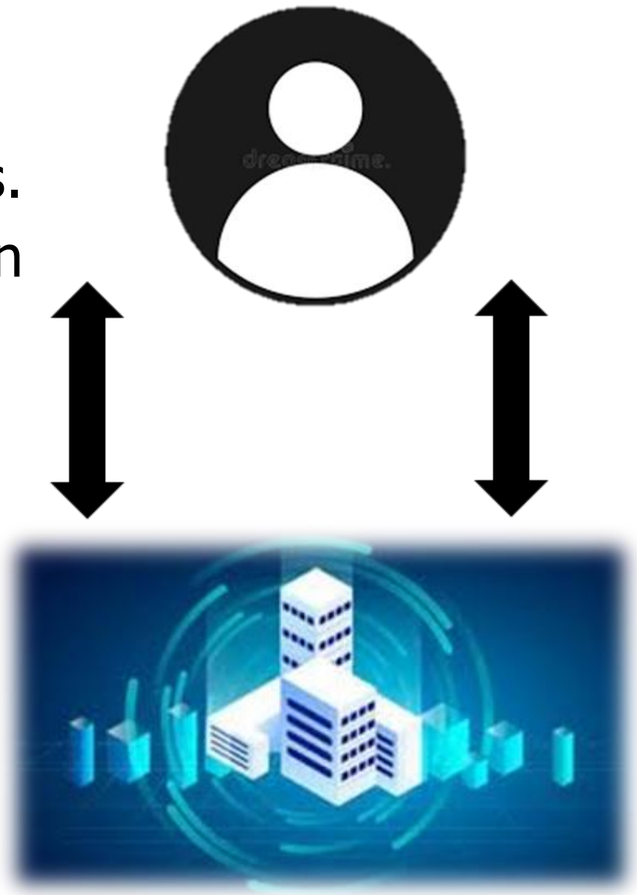
MÉTODOS DE DEFENSA

JAYMON SECURITY
Cyberintelligence & Solutions

V. MÉTODOS DE DEFENSA

EMPRESAS

- Tener los dispositivos de la empresa actualizados y con antivirus.
- Formar a los empleados.
- Realizar copias de seguridad con regularidad.
- Reforzar y cambiar con frecuencias las contraseñas.
- Tener políticas de seguridad actualizadas y completas.
- Contratar una empresa de ciberseguridad – Hacking Ético.



PARTICULARES

- Concienciación personal.
- Tener los sistemas actualizados.
- Tener contraseñas largas y seguras.
- Utilizar sistemas de seguridad o antivirus.
- Evitar conexiones WiFi públicas.
- No descargar archivos o abrir enlaces dudosos.

JAYMON SECURITY
Cyberintelligence & Solutions

VECTORES DE ATAQUE

JAYMON SECURITY
Cyberintelligence & Solutions

I. DEFINICIONES

VECTORES DE ATAQUE

Medio de ataque que emplean los ciberdelincuentes para entrar en una red o sistema.

El objetivo es transmitir a un equipo un código malicioso, el cual les permitirá a los atacantes tomar el control total o parcial del equipo.

Normalmente, los vectores de ataque utilizan fallos o agujeros de seguridad, los cuales pueden ser explotados para llevar a cabo un ataque determinado.

II. DEFINICIONES

VECTORES DE ATAQUE

"Medio por el cual un pirata informático puede hacer llegar un programa malicioso (malware) a un ordenador o cualquier otro dispositivo conectado a la red. Este malware, les permitirá controlar total o parcialmente el equipo objetivo. Las finalidades son diversas aunque la más común es la económica"

¿Sabías qué…?

Si existen vulnerabilidades hay vectores de ataque que puede que tengan éxito.

Estos están presentes en ordenadores, aplicaciones, servidores de correo electrónico, software, páginas web, navegadores, redes…

JAYMON SECURITY
Cyberintelligence & Solutions

III. TIPOS

VECTORES DE ATAQUE PASIVOS

- Son aquellos mediante los cuales se accede al sistema o a su información, pero no afectan al propio sistema.
- Principalmente ataques de ingeniería social (phishing), captura de datos de red (sniffing), etc.

VECTORES DE ATAQUE ACTIVOS

- Aquellos que tienen como objetivo alterar el sistema y/o su correcto funcionamiento.
- Principalmente secuestros de información, ataques DDoS, etc.

JAYMON SECURITY
Cyberintelligence & Solutions

IV. TIPOS

VECTORES DE ATAQUE PASIVOS

PHISHING

"Técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico." (INCIBE, 2022)

SPEAR PHISHING

"Modalidad phishing dirigida contra un objetivo específico, en el que los atacantes intentan, mediante un correo electrónico, conseguir información confidencial de la víctima." (INCIBE,2022)

JAYMON SECURITY
Cyberintelligence & Solutions

V. TIPOS

VECTORES DE ATAQUE ACTIVOS

RAMSOMWARE

"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." (INCIBE, 2022)

Wannacry

DENEGACIÓN DE SERVICIOS

"Ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones. " (INCIBE, 2022)

Fuente: Avast

JAYMON SECURITY
Cyberintelligence & Solutions

CICLO DE VIDA

JAYMON SECURITY
Cyberintelligence & Solutions

I. CICLO DE VIDA

Herramientas a utilizar

Explotación

Borrado huellas

Análisis e inspección del objetivo

Instalación de malware

Persistencia

JAYMON SECURITY
Cyberintelligence & Solutions

PRINCIPALES VÍAS DE ATAQUE A EMPLEADOS

I. PRINCIPALES VÍAS DE ATAQUE

Podemos diferenciar:

1. **Correo electrónico malicioso**

Correos o SMS phishing, mediante los cuales se suplantan a organizaciones conocidas por el receptor (bancos, Agencia Tributaria, empresas de paquetería, etc.).

2. **Endpoints**

Dispositivo que proporciona un punto de entrada a los activos y aplicaciones de una empresa.
Bring Your Own Device (BYOD): Uso de dispositivos propios para trabajar.

II. PRINCIPALES VÍAS DE ATAQUE

JAYMON SECURITY
Cyberintelligence & Solutions

3 Navegación web

Los ataques de navegación se deben principalmente a la falta de actualizaciones o por haber instalado plugins maliciosos.

Drive-by download: Se descarga el malware sólo con visitar una página web o ver un correo.

Browser in the browser: Se abre una ventana emergente de autenticación, en la cual nos solicitan las credenciales.

III. PRINCIPALES VÍAS DE ATAQUE

JAYMON SECURITY
Cyberintelligence & Solutions

4

Software y sistemas mal configurados o desactualizacos

Al no seguir los procedimientos adecuados (tanto en su configuración como protección).
Ejemplo: Ataques contra el router, ataques DDoS o DNS hijacking.

5

Credenciales de usuarios comprometidas

Se debe normalmente por ataques de ingeniería social, dispositivos maliciosos, o bases de datos hackeadas y publicadas en la Deepweb.
Ejemplo: Uso de software malicioso que registra todas las pulsaciones sin consentimiento de usuario (keylogger), o base de datos de usuarios hackeada a la Policía y publicada en la Deepweb.

JAYMON SECURITY
Cyberintelligence & Solutions

IV. PRINCIPALES VÍAS DE ATAQUE A EMPLEADOS

ATAQUES DE FUERZA BRUTA

Consiste en probar todas las combinaciones posibles hasta encontrar las credenciales de acceso.

Con el aumento del teletrabajo se han convertido en el objetivo preferido de los ciberdelincuentes debido a las contraseñas débiles y conexiones inseguras.

EJEMPLO

La utilización de contraseñas tipo “1234” es muy habitual y son muy fáciles de romper. Por eso es aconsejable utilizar contraseñas alfanuméricas y con caracteres especiales cómo mayúsculas y guiones.

JAYMON SECURITY
Cyberintelligence & Solutions

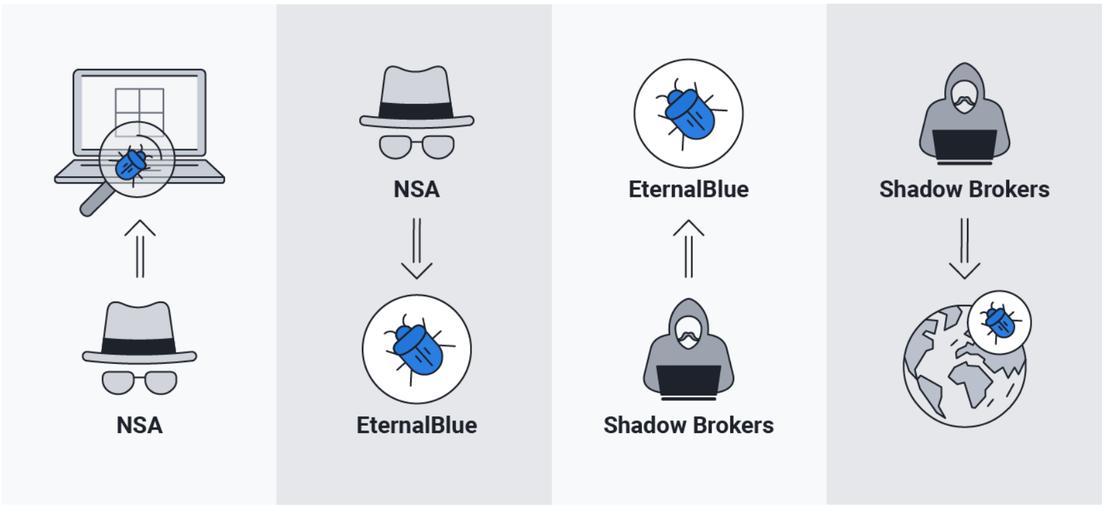
IV. PRINCIPALES VÍAS DE ATAQUE A EMPLEADOS

EXPLOTACIÓN DE VULNERABILIDADES

Proceso por el que un atacante identifica y aprovecha fallos en un sistema para obtener acceso no autorizado o realizar acciones maliciosas.

Estas vulnerabilidades pueden estar en el software y hardware. Los atacantes utilizan estas brechas de seguridad para infiltrarse en los sistemas, robar datos, instalar malware o interrumpir operaciones.

EJEMPLO



Fuente: 1000 marcas

JAYMON SECURITY
Cyberintelligence & Solutions

IV. PRINCIPALES VÍAS DE ATAQUE A EMPLEADOS

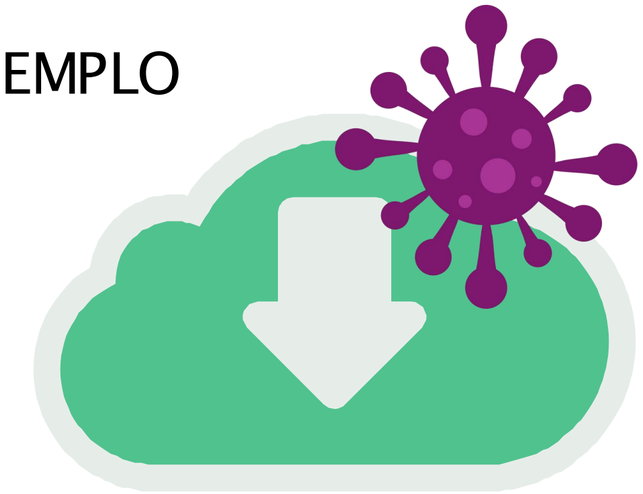
DRIVE - BY COMPROMISE

Vector de ataque usado para amenazas avanzadas persistentes (APT).

Son descargas automáticas en el dispositivo sin el consentimiento del usuario.

Puede ocurrir cuando el usuario navega en sitios ilegítimos o través de anuncios maliciosos.

EJEMPLO



Los ciberdelinceuntes aprovechan las vulnerabilidades de navegadores web y sistemas operativos.

JAYMON SECURITY
Cyberintelligence & Solutions

IV. PRINCIPALES VÍAS DE ATAQUE A EMPLEADOS

CORREO ELECTRÓNICO MALICIOSO

Correos phishing con archivos maliciosos adjuntos. Constituye la principal puerta de entrada para atacantes que se aprovechan de la falta de formación en ciberseguridad de las personas.

Evitar estos ataques es relativamente sencillo. Se requiere precaución y seguir unas normas básicas de ciberseguridad para evitarlos.

EJEMPLO

Fuente: www.amazon.es
Fuente: App Store - Apple

JAYMON SECURITY
Cyberintelligence & Solutions

IV. PRINCIPALES VÍAS DE ATAQUE A EMPLEADOS

UNIDADES DE MEMORIA EXTERNA

Consiste en la infección de memorias externas por un malware.

Es un vector de ataque utilizado para tener acceso a equipos y redes internas.

EJEMPLO

JAYMON SECURITY
Cyberintelligence & Solutions

MÉTODOS DE DEFENSA

JAYMON SECURITY
Cyberintelligence & Solutions

IV. MÉTODOS DE DEFENSA

Formación de toda la plantilla.

No descargar archivos o abrir enlaces dudosos.

Parchear vulnerabilidades y actualizar de forma periódica el software.

No permitir el acceso a la red interna de la organización desde redes públicas o no seguras.

Tener políticas de seguridad actualizadas y completas que contemplen la seguridad de los equipos y el uso de los dispositivos.

Instalar soluciones antivirus y herramientas antiphishing (filtros de spam, listas negras y blancas, etc.).

JAYMON SECURITY
Cyberintelligence & Solutions

FIN PRESENTACIÓN

info@jaymonsecurity.com

Jaymonsecurity.com

Jaymonsecurity.es