INTRODUCCIÓN Y CONTEXTUALIZACIÓN DE LA CIBERSEGURIDAD

Sergio Mulas Díaz

Centr@Tec Servicios Avanzados de Innovación para Pymes
competitividad empresarial ice
Junta de Castilla y León
AIR INSTITUTE

¿QUÉ ES LA CIBERSEGURIDAD?

¿Qué es la ciberseguridad?

Definición formal

- La ciberseguridad se define como el conjunto de tecnologías, procesos y prácticas diseñados para proteger sistemas, redes, programas, dispositivos y datos de ataques, daños o accesos no autorizados (SANS Institute, 2021).

Contexto tecnológico

- En el mundo de la tecnología de la información, la ciberseguridad no es simplemente una especialidad más. Es un aspecto fundamental que impacta en varias áreas, desde el almacenamiento en la nube y las bases de datos, hasta las redes de comunicación y los sistemas integrados.

¿Qué es la ciberseguridad?

Dimensiones de la Ciberseguridad

- **Confidencialidad:** Protección de la privacidad de la información.
- **Integridad:** Aseguramiento de la exactitud y fiabilidad de los datos y sistemas.
- **Disponibilidad:** Acceso garantizado a la información y recursos por parte de usuarios autorizados.

¿Qué es la ciberseguridad?

Definiciones básicas

- **Amenaza**: Cualquier actividad potencial que pueda causar un daño deliberado a un sistema o información.
- **Vulnerabilidad**: Debilidades o lagunas en un sistema que podrían ser explotadas para causar daño o acceder a información.
- **Ataque**: Acción llevada a cabo para explotar una vulnerabilidad y comprometer la seguridad.
- **Riesgo**: Probabilidad de que una amenaza específica explote una vulnerabilidad particular para causar daño.
- **Incidente de Seguridad:** Evento que resulta en un compromiso de la integridad, disponibilidad o confidencialidad de un sistema.

¿Qué es la ciberseguridad?

Tipos de Vulnerabilidades

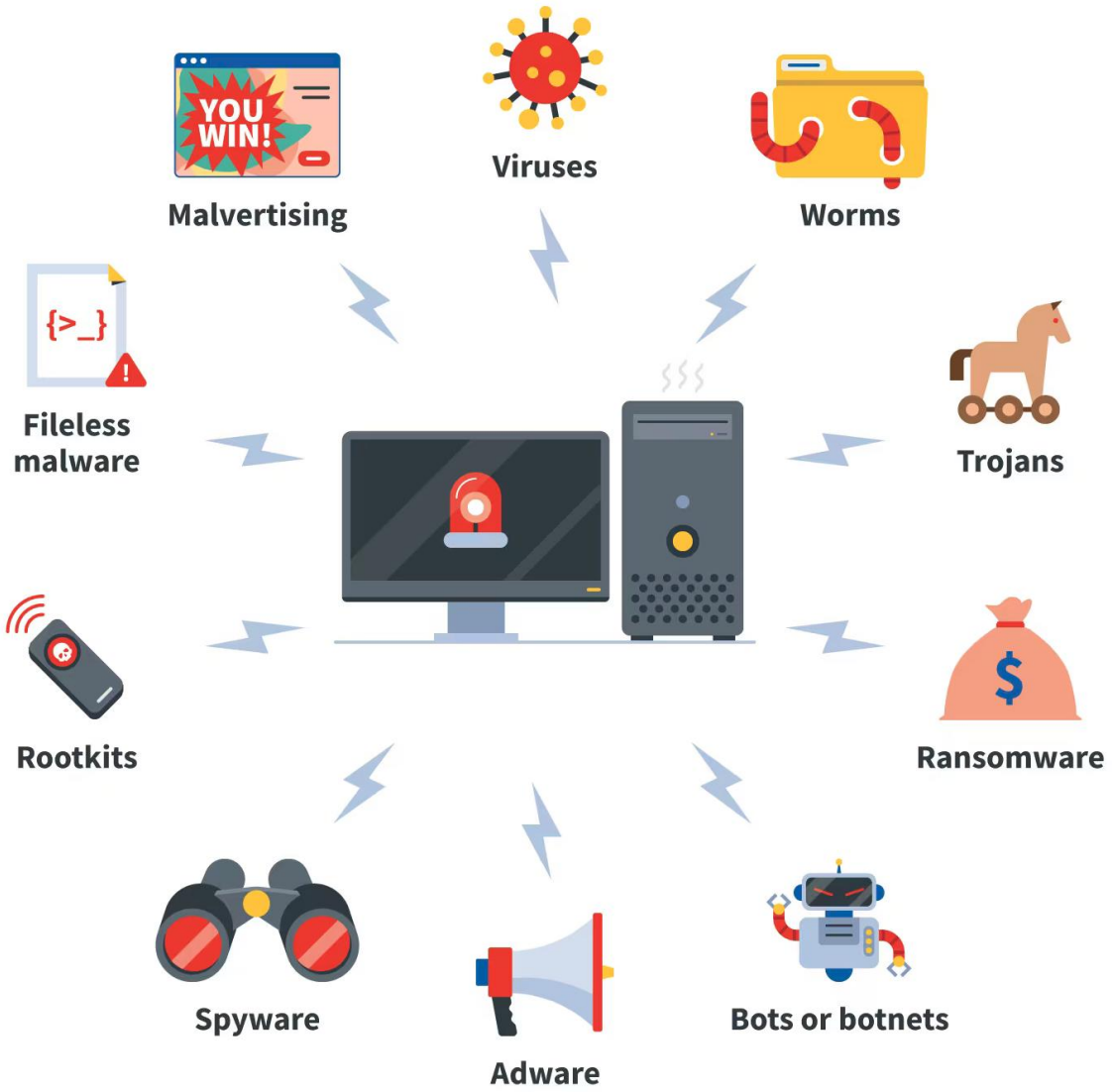
- **Vulnerabilidades de Software:** Fallos en el código que pueden ser explotados.
- **Vulnerabilidades de Hardware:** Defectos en componentes físicos.
- **Vulnerabilidades Humanas:** Errores o descuidos de usuarios y administradores.
- **Vulnerabilidades de Configuración:** Configuraciones inseguras en sistemas o redes.
- **Vulnerabilidades de Red:** Debilidades en protocolos y arquitecturas de red.
- **Vulnerabilidades de Día Cero**: Defectos desconocidos que aún no han sido parcheados.

¿Qué es la ciberseguridad?

Tipos de ataques

- **Denegación de Servicio (DoS) y Ataque de Denegación de Servicio Distribuido (DDoS):** Inhabilitación de servicios o redes.
- **Ataque Man-in-the-Middle (MitM):** Intercepción de comunicaciones.
- **Phishing:** Engaño para obtener información.
- **Ataques Web:** SQL Injection, Cross-Site Scripting, etc.
- **Malware:** Software malicioso como virus, gusanos y troyanos

¿Qué es la ciberseguridad?



Importancia en la actualidad

Tras un ciberataque a Boeing con ransomware, 50 GB de datos privados de la compañía han sido publicados en la Web Oscura

Datos de proveedores, emails corporativos y hasta una carpeta titulada "Residuos peligrosos" están disponibles después de que la aerolínea se negara a pagar el 'rescate' de los archivos robados

EL PAÍS

Economía

CIBERATAQUES >

Air Europa sufre un ciberataque y pide a sus clientes que cancelen las tarjetas de crédito

La aerolínea afirma que el 'hackeo' está controlado y que no ha detectado ningún fraude por el momento

Los Angeles Times

INTERNACIONAL

Ciberataque contra banco más grande de China interrumpe operaciones del Tesoro de EEUU

EL ESPAÑOL

omicrono

Un ciberataque a ChatGPT le deja sin servicio constantemente: OpenAI ya está trabajando en ello

DW Made for minds. DESTACADOS Conflicto Israel - Hamás Aprenda alemán jugando Últimos videos Últimos audios TV en vivo

TECNOLOGÍA | COLOMBIA

Ciberataque afecta a servicios estatales en Colombia y Chile

15/09/2023

Más de 700 compañías latinoamericanas seguían afectadas por el ciberataque lanzado el 12 de septiembre por desconocidos, aseguró el gobierno colombiano.

Global Risks Report 2023

Top 10 Risks

"Please estimate the likely impact (severity) of the following risks over a 2-year period"

WORLD ECONOMIC FORUM

2 years

Source: World Economic Forum, Global Risks Perception Survey 2022-2023

https://centratec.air-institute.com/

Centr@Tec Servicios Avanzados de Innovación para Pymes

competitividad empresarial ice

Junta de Castilla y León

AIR INSTITUTE

CONCIENCIACIÓN EN CIBERSEGURIDAD EMPRESARIAL

Centr@Tec Servicios Avanzados de Innovación para Pymes

competitividad empresarial ice

Junta de Castilla y León

AIR INSTITUTE

¿QUÉ ES?

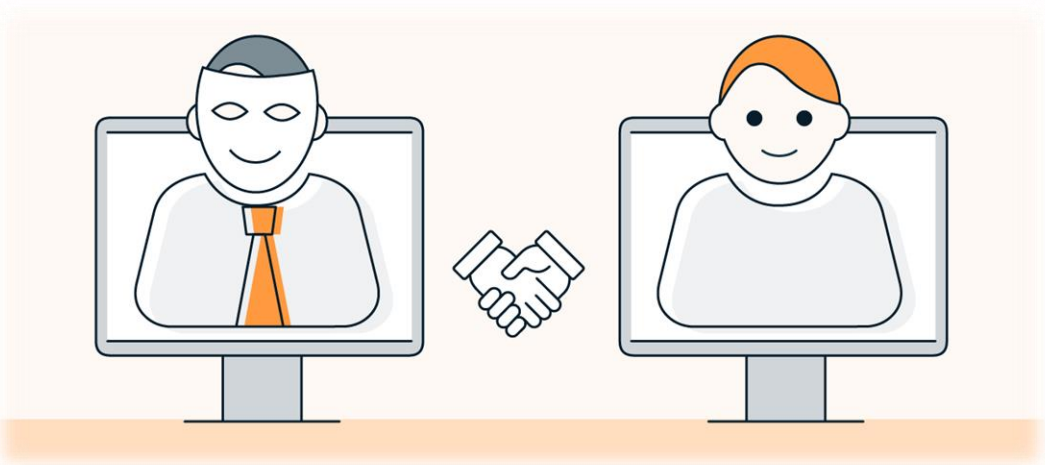
INGIENERÍA SOCIAL

INGIENERÍA SOCIAL

¿QUÉ ES?

La ingeniería social es engañar a la gente para obtener información secreta o acceso a un dispositivo.

Un desconocido que te pide las llaves de tu casa fingiendo ser un cerrajero



INGIENERÍA SOCIAL

EJEMPLOS REALES

Fraudes de Becas Educativas: Aquí, los padres son contactados por supuestas organizaciones que ofrecen becas o ayuda financiera para la educación de sus hijos. Les piden pagar una "tasa de procesamiento" o proporcionar detalles bancarios, lo que lleva al robo de dinero o datos.

¿DÓNDE SE USA?

INGIENERÍA SOCIAL

PHISING

EMAIL SPOOFING
SMISHING
VISHING
QRISHING

PHISING

¿QUÉ ES?

El phishing es una 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.

PHISING

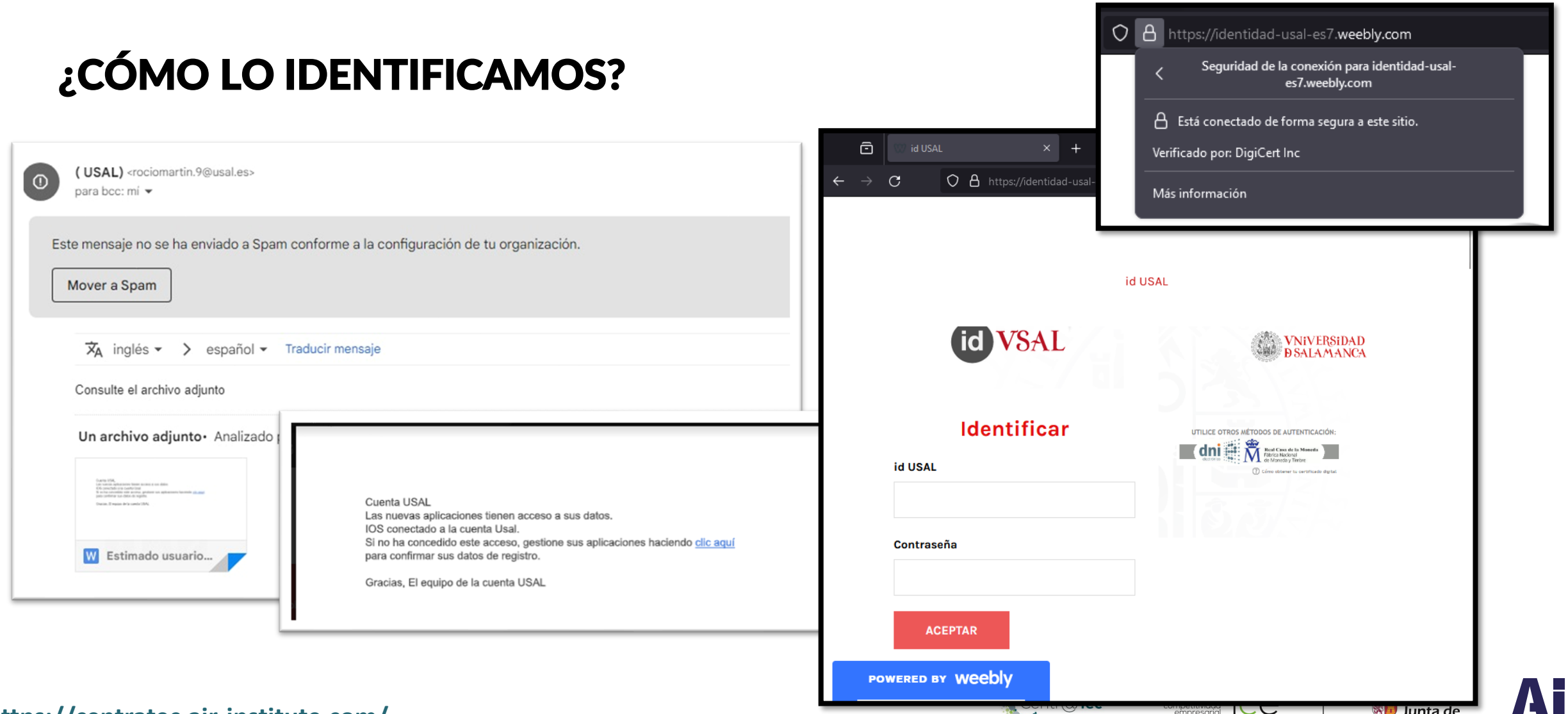
¿CÓMO LO IDENTIFICAMOS?

Todos los correos phishing tienen patrones comunes y por lo general, tienen alguna de las siguientes características:

- Uso de un saludo genérico en lugar de un nombre
- Hay un límite de tiempo o un carácter de urgencia inusual
- El cuerpo del mensaje suele estar lleno de errores.
- Normalmente, cualquier correo electrónico fraudulento trata de recopilar información privada personal o de pago con el objetivo de hacer un uso inadecuado de ella.
- La dirección de correo electrónico del remitente no está asociada a un dominio legítimo.
- Los enlaces en el cuerpo del mensaje no coinciden con el dominio del remitente.

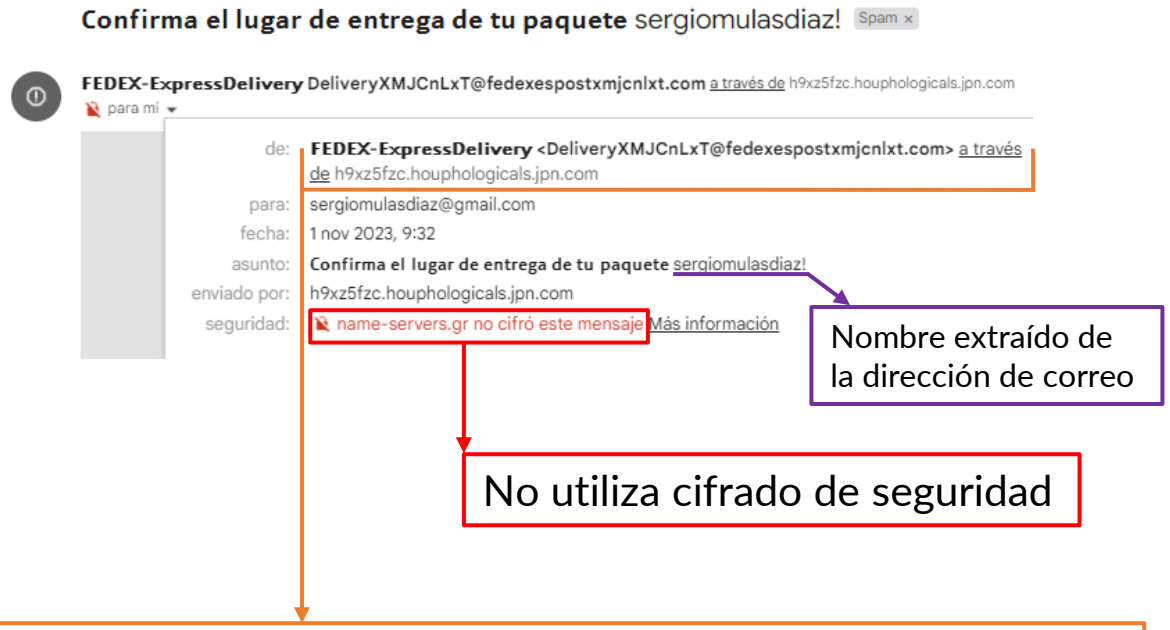
PHISING

¿CÓMO LO IDENTIFICAMOS?



PHISING

¿CÓMO LO IDENTIFICAMOS?



Nombre extraído de la dirección de correo

No utiliza cifrado de seguridad

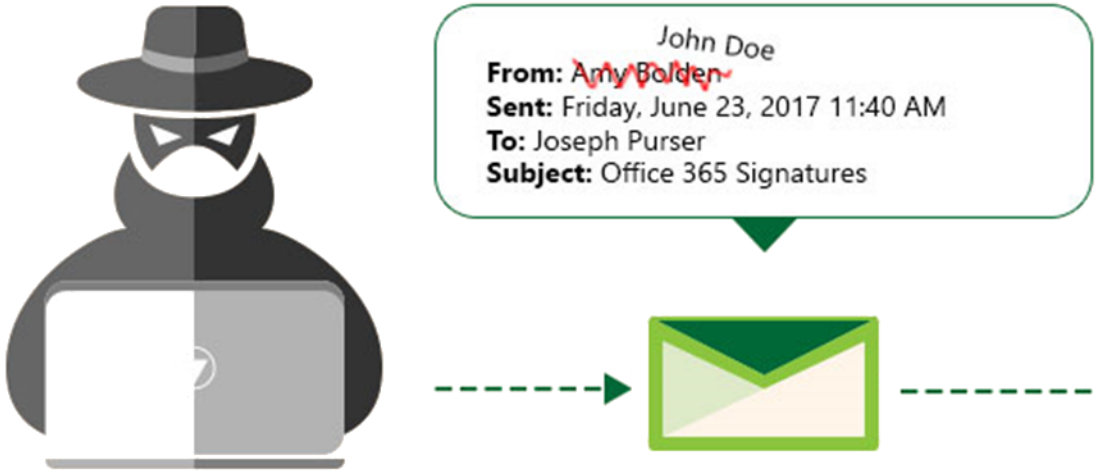
Dirección de correo tratando de suplantar a fedex a través de otro dominio

https://centratec.air-institute.com/

EMAIL SPOOFING
PHISING

¿QUÉ ES?

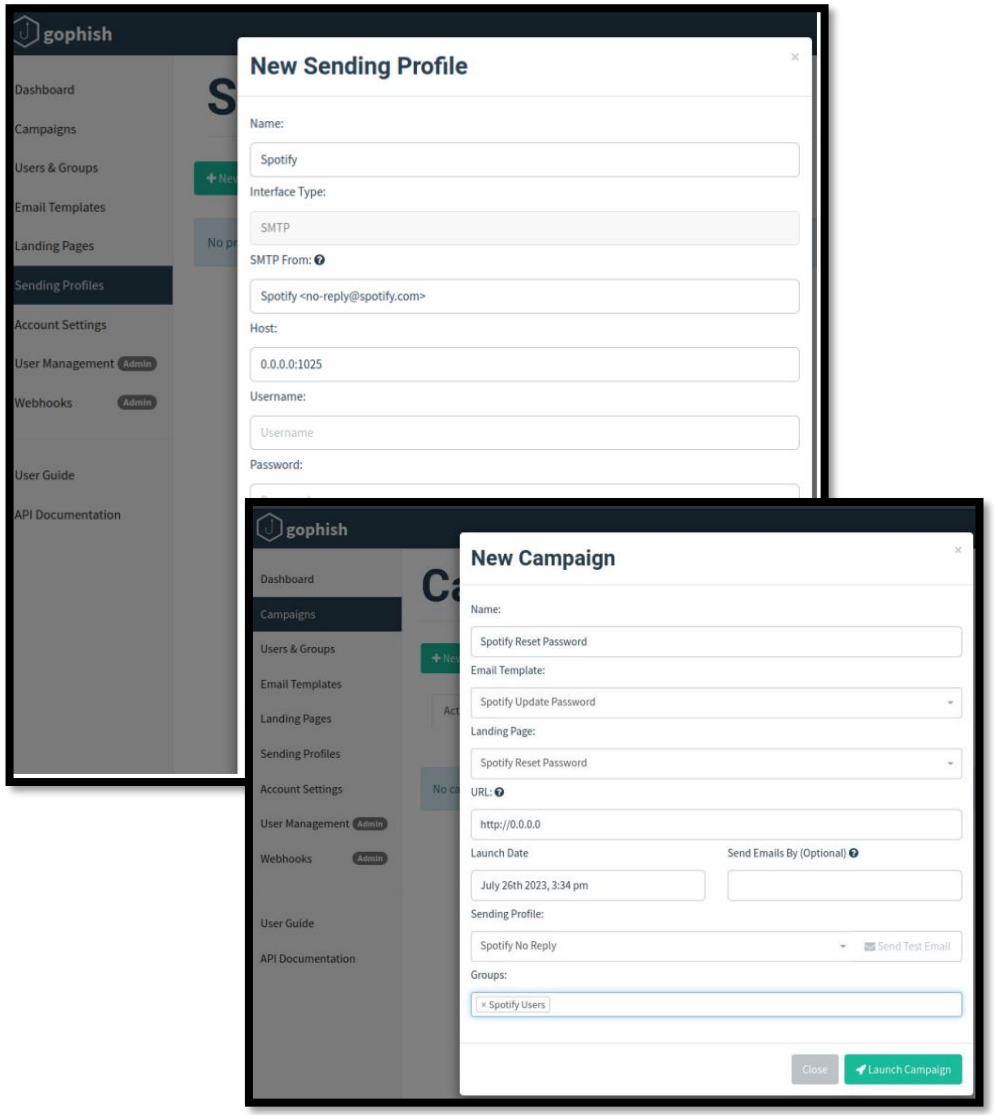
Se trata de una técnica de engaño donde el remitente de un correo electrónico finge ser alguien más, generalmente con intenciones maliciosas. En otras palabras, es como si alguien enviara una carta con el nombre y la dirección de otra persona en el sobre.



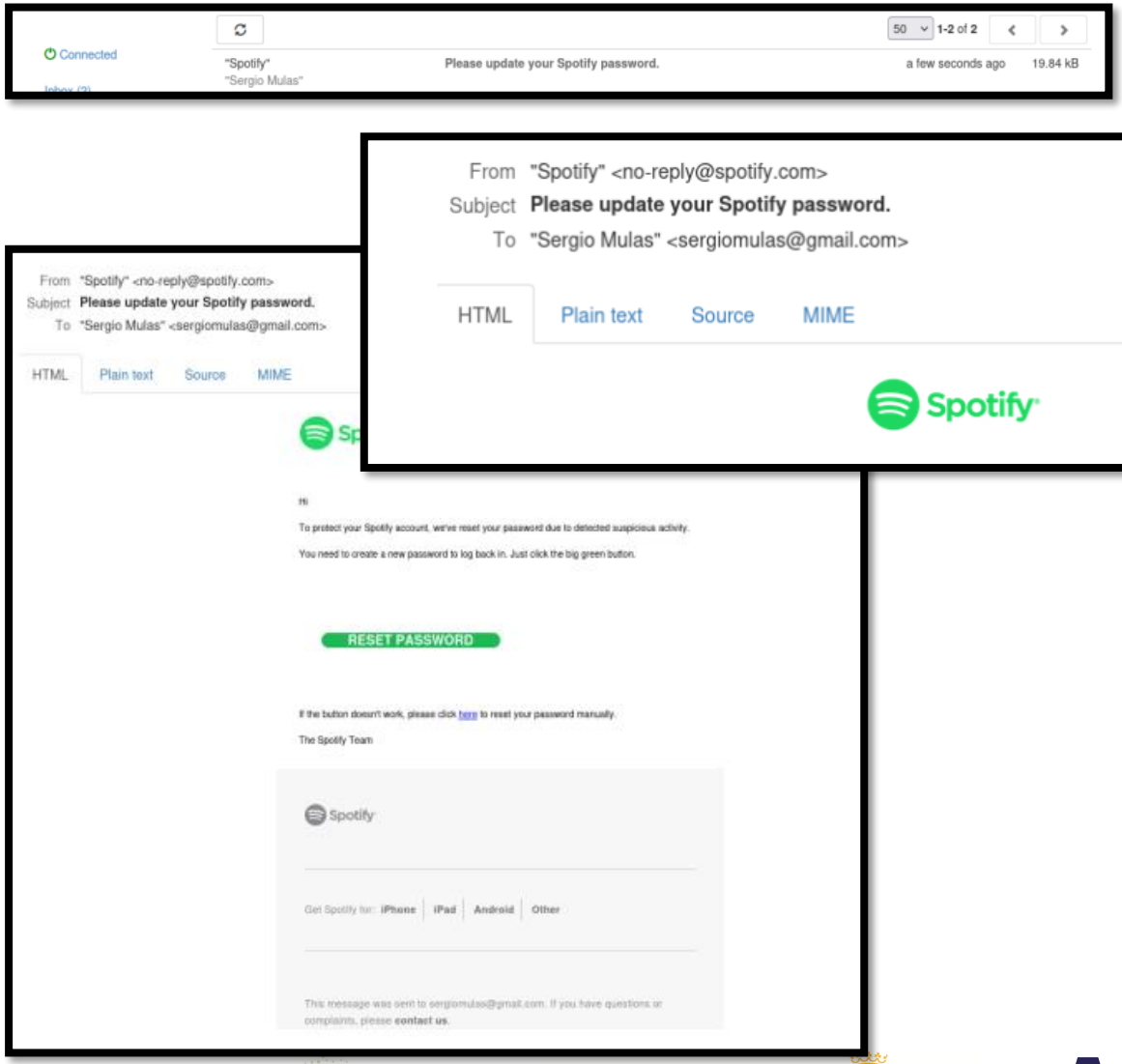
BLOG INCIBE

EMAIL SPOOFING: COMPRUEBA QUIÉN TE ENVÍA UN CORREO SOSPECHOSO

ATACANTE



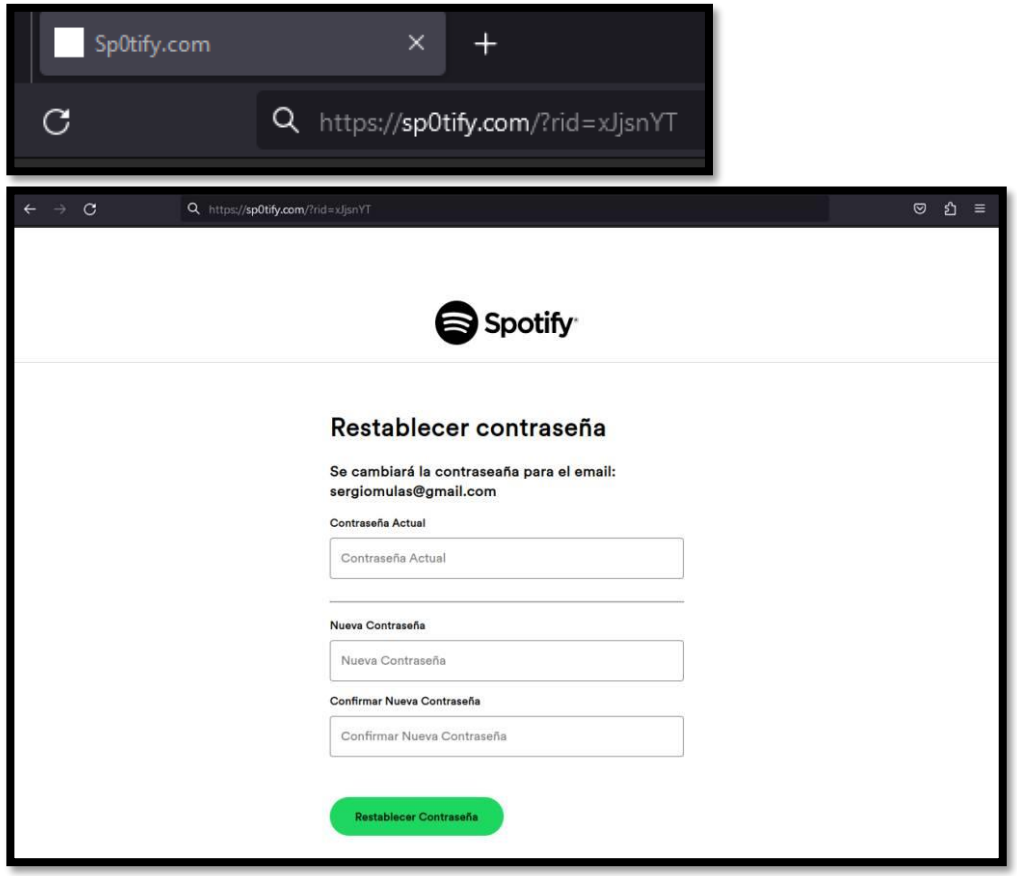
VICTIMA



https://centratec.air-institute.com/

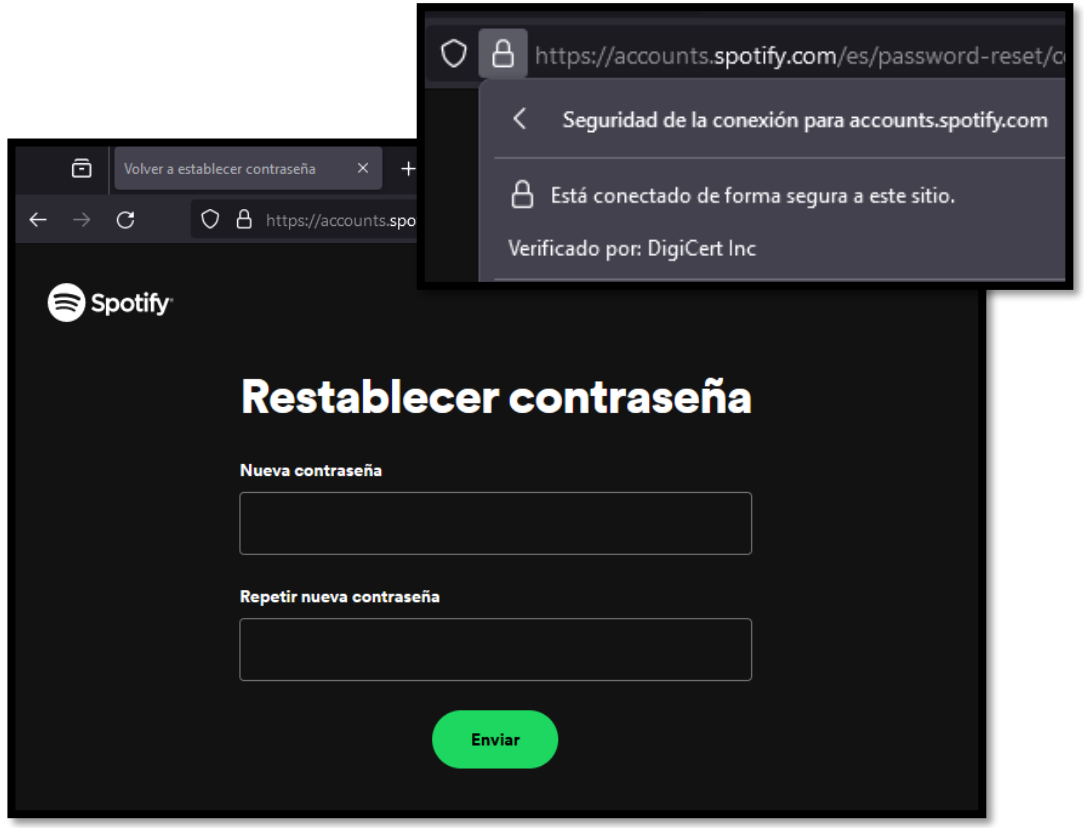
PHISING

sp0tify.com



REAL

spotify.com



https://centratec.air-institute.com/

SMISHING
PHISING

¿QUÉ ES?

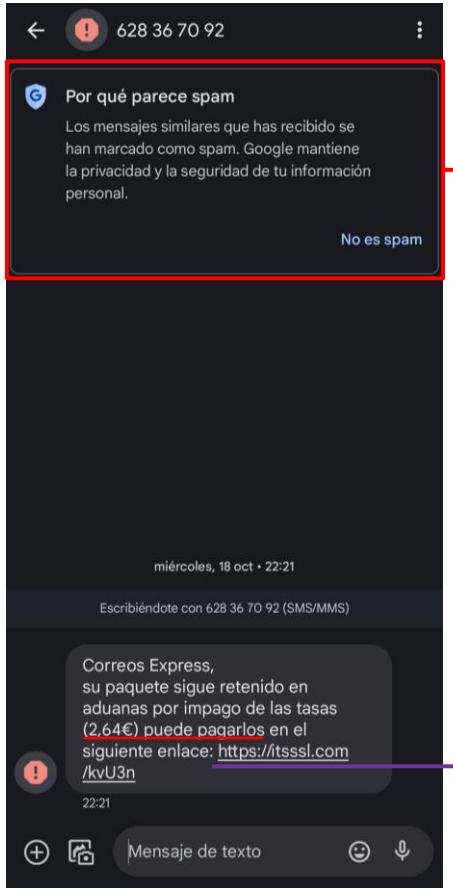
El smishing es una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima -red social, banco, institución pública, etc. -con el objetivo de robarle información privada o realizarle un cargo económico.

BLOG INCIBE

¿QUÉ ES EL SMISHING?

SMISHING

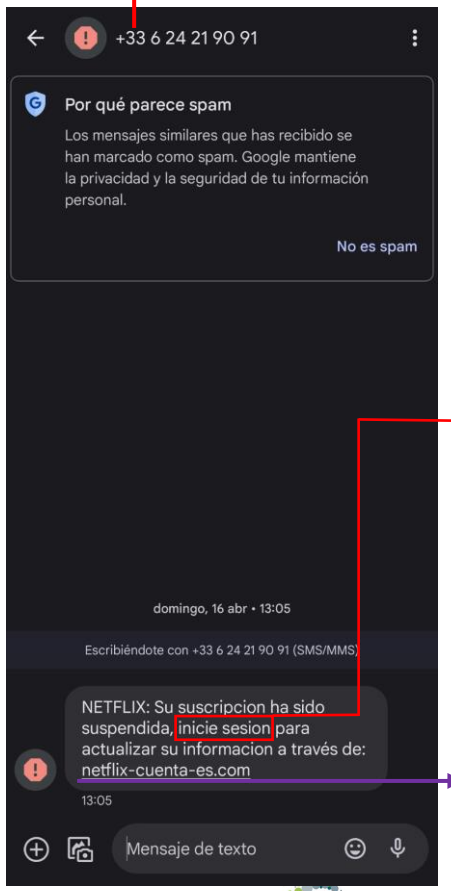
¿CÓMO LO IDENTIFICAMOS?



Algoritmo de Google para detectar posibles estafas

Dominio no oficial de Correos (acortador)

hpo.aqd.mybluehost.me/cgi-sys/suspendedpage.cgi



Prefijo +33, de origen francés

Nos exige introducir datos de acceso

Dominio falso

netflix-cuenta-es.com

Dominio oficial

netflix.com

https://centratec.air-institute.com/

QRISHING
PHISING

¿QUÉ ES?

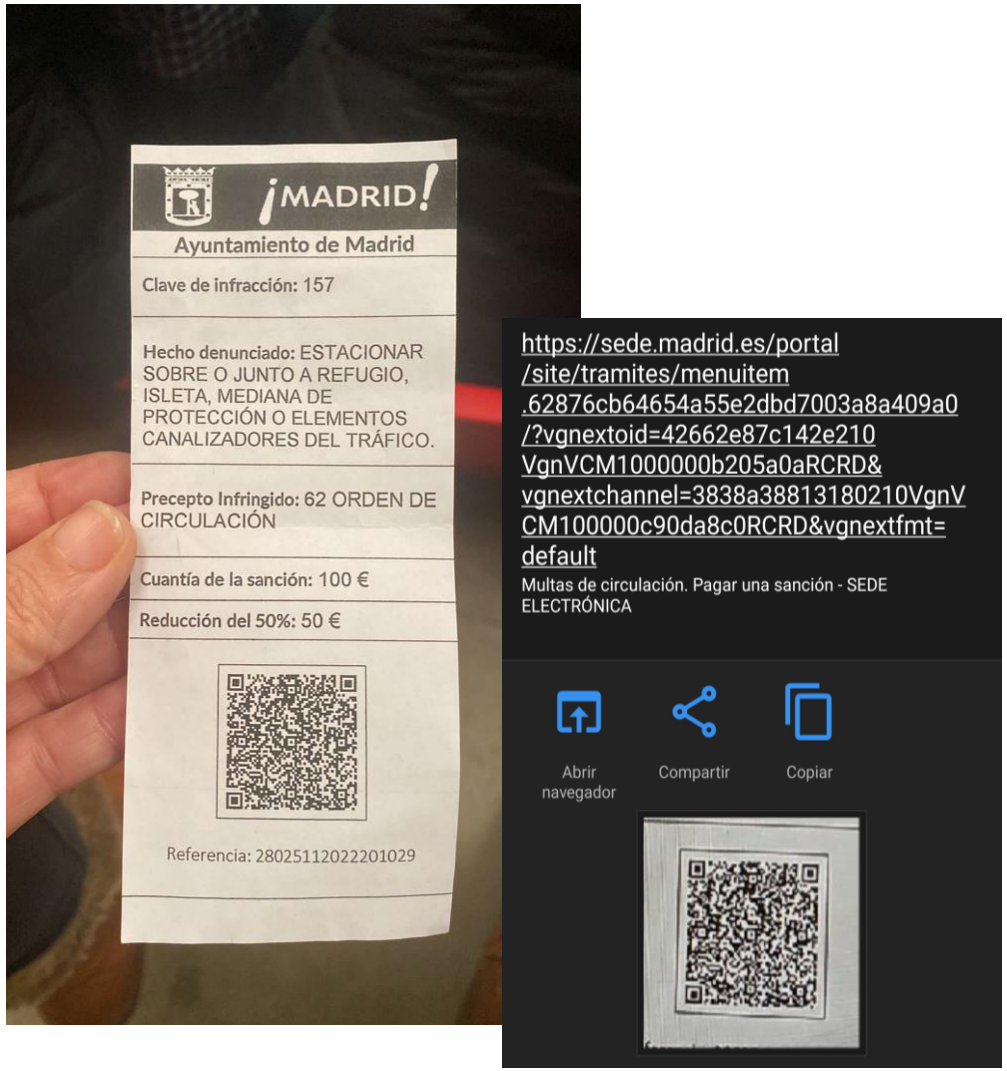
Derivado de pishing con códigos QR, es una técnica de phising que se vale de códigos QR para engañar a posibles víctimas

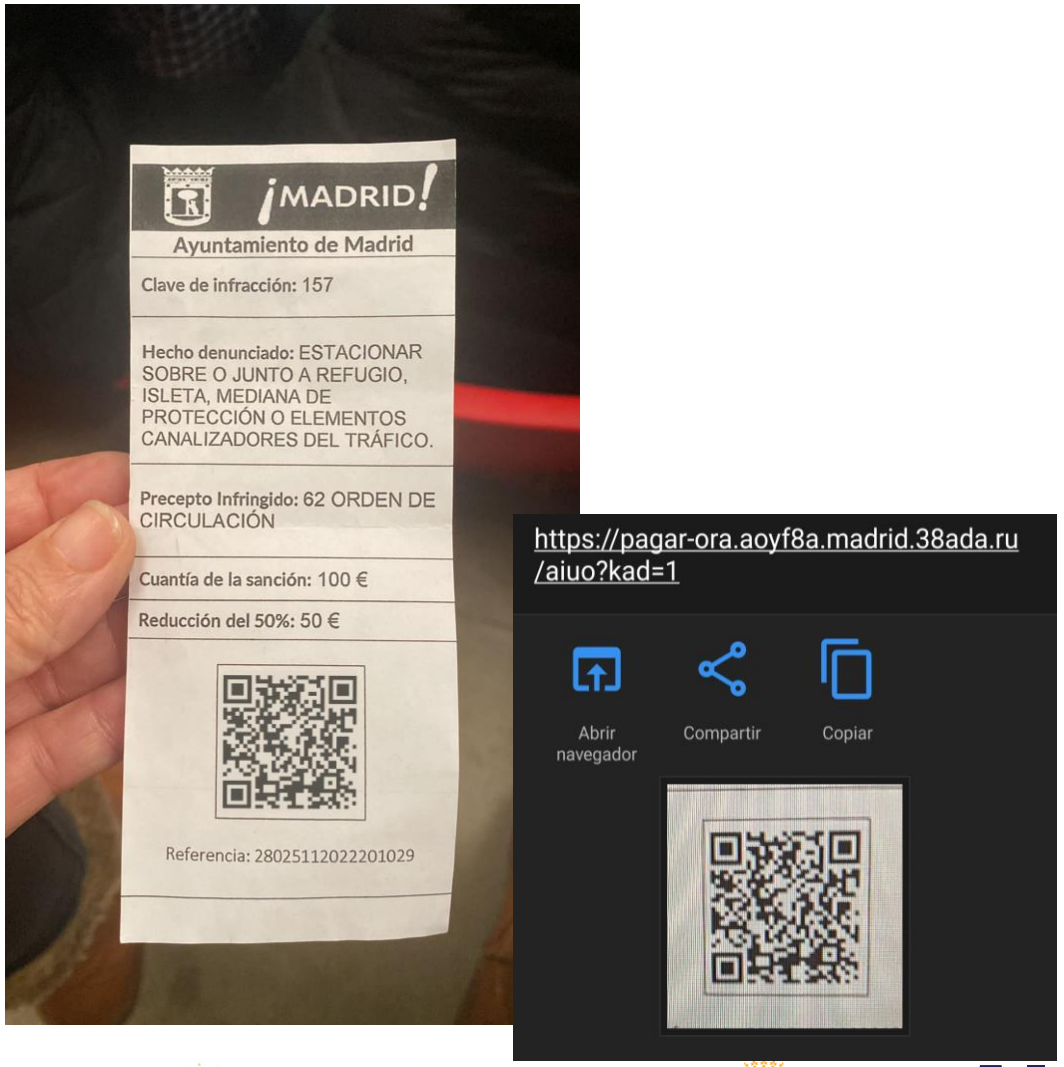
BLOG INCIBE

¿QUÉ ES EL SMISHING?

¿IDENTIFICARÍAS QRISHING EN EL DÍA A DÍA?

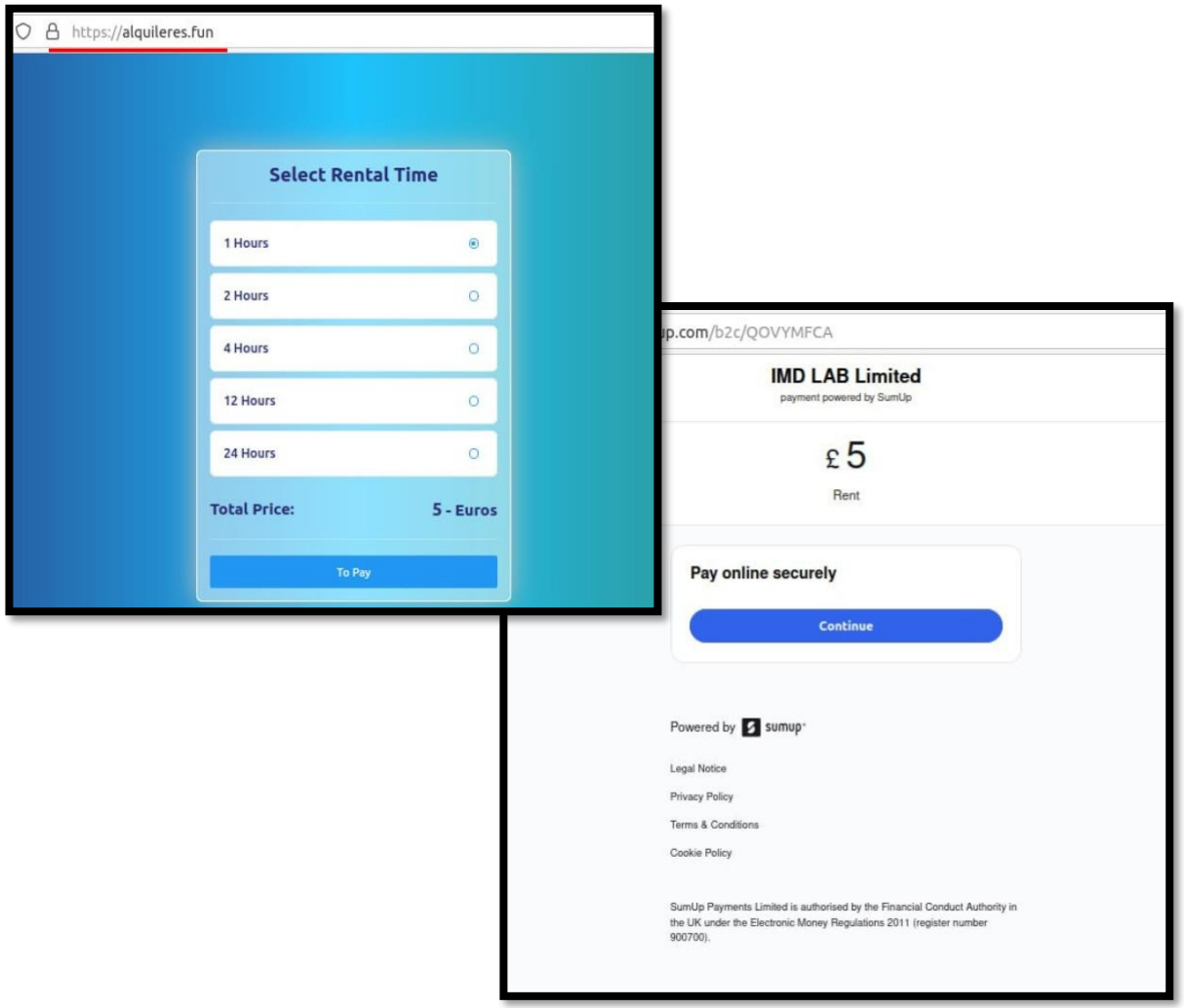
MULTA DE LA ORA





https://centratec.air-institute.com/

BICI MAD



https://centratec.air-institute.com/

Centr@Tec Servicios Avanzados de Innovación para Pymes
competitividad empresarial ice
Junta de Castilla y León
AIR INSTITUTE

VISHING
PHISING

¿QUÉ ES?

Se trata de un tipo de estafa a través de una llamada telefónica en la que se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima.

BLOG INCIBE

¿QUÉ ES EL VISHING?

CONVERSACIÓN REAL
ENTRE **ESTAFADOR** Y **VÍCTIMA**

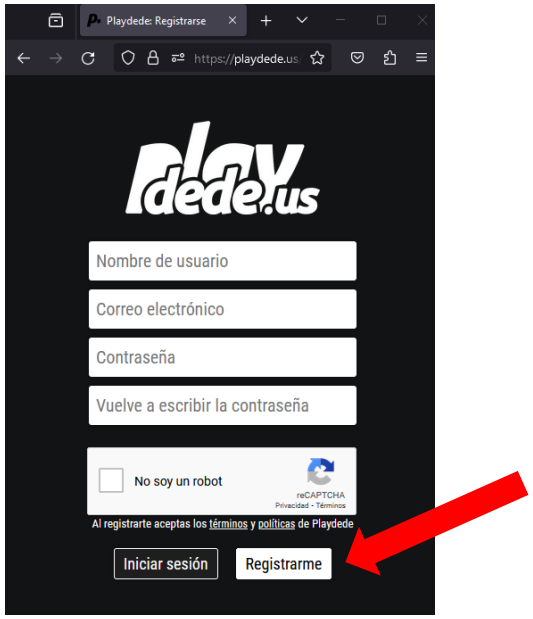
EJEMPLO REAL
PHISING WEB
SOPORTE WINDOWS

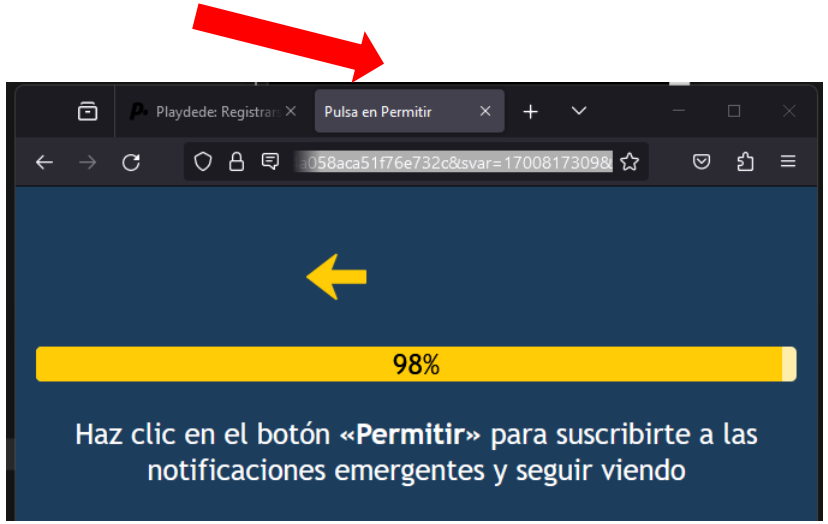
EJEMPLO REAL PHISING

¿CÓMO LLEGAMOS A ESTAS ESTAFAS?

Haciendo click en páginas web que nos redirigen a sitios web de publicidad

En este ejemplo, se accedió a la página web de **“playdede”** una conocida plataforma para ver películas pirata.





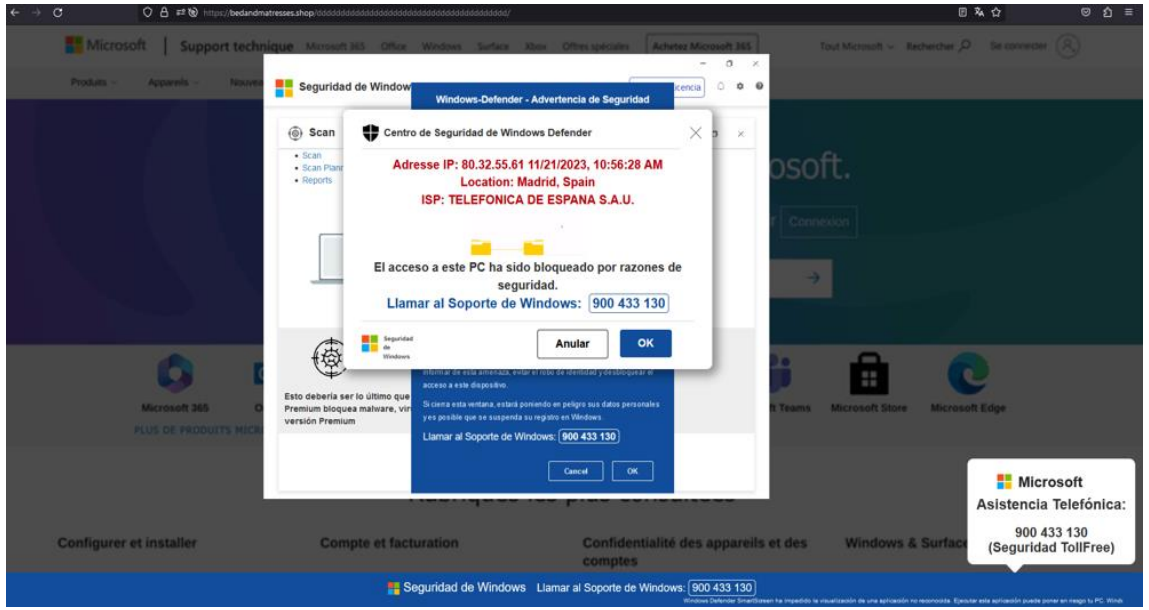
FUNCIONAMIENTO

- UTILIZAN WEBS VULENRABLES PARA LANZAR LA ESTAFA AL PÚBLICO

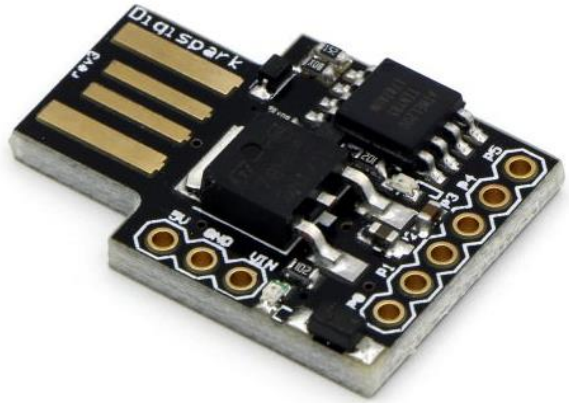
- TRATAN DE CREAR MIEDO HACIENDOTE CREER QUE TIENES UN VIRUS QUE BORRARÁ TODO Y TE ROBARÁ LOS DATOS

- TE OBLIGAN A LLAMAR A UN NÚMERO DE TELÉFONO PARA QUE PAGUES UNA “SOLUCIÓN MÁGICA” QUE TE DAN

- SI SIGUES SUS PASOS OBTENDRÁN EL CONTROL DEL ORDENADOR



¿QUÉ HERRAMIENTAS USAN LOS CIBERDELICUENTES?



DIGISPARK REV3

WIFI PINEAPPLE

USB RUBBER DUCKY

COMO EVITARLO

- NUNCA INSERTES DISPOSITIVOS USB DESCONOCIDOS
- UTILIZA VPN PARA LAS REDES WIFI PÚBLICAS
- ESTABLECER CONTRASEÑA EN TODOS LOS DISPOSITIVOS
- UTILIZAR CONTRASEÑAS SEGURAS
- NO ALMACENAR CONTRASEÑAS EN TEXTO PLANO

BLOG INCIBE

¡ALERTA! ENCONTRÉ UN USB Y ESTABA INFECTADO

¿QUÉ ES UN VIRUS / MALWARE Y QUÉ TIPOS HAY?

MALWARE

SPYWARE
BOTNETS
RANSOMWARE

MALWARE

¿QUÉ ES?

Se trata de un programa informático 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.

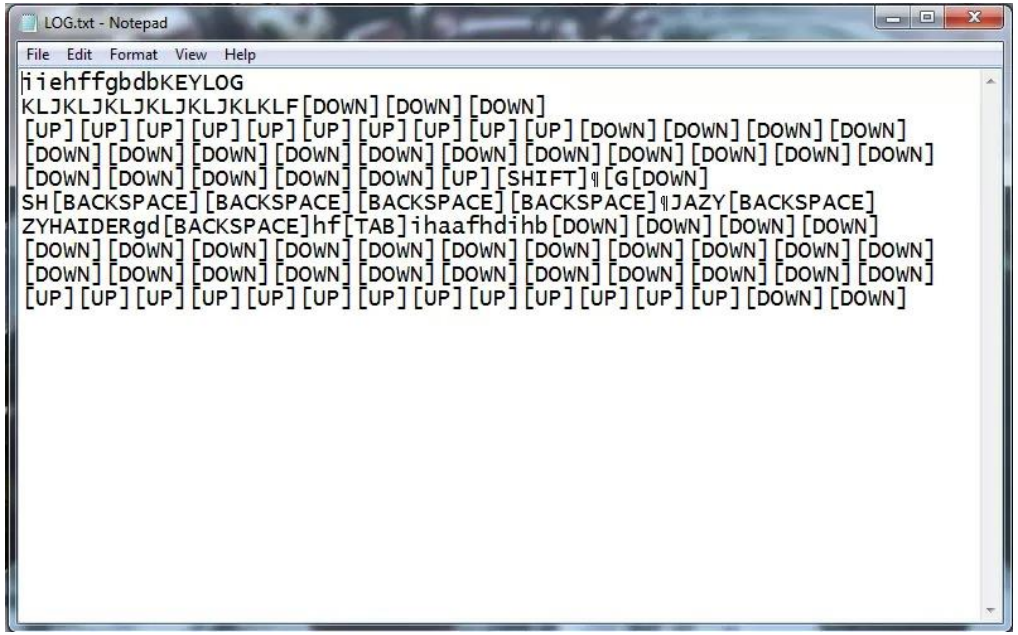
APRENDE CIBERSEGURIDAD

¿QUÉ ES EL MALWARE?

SPYWARE
MALWARE

¿QUÉ ES?

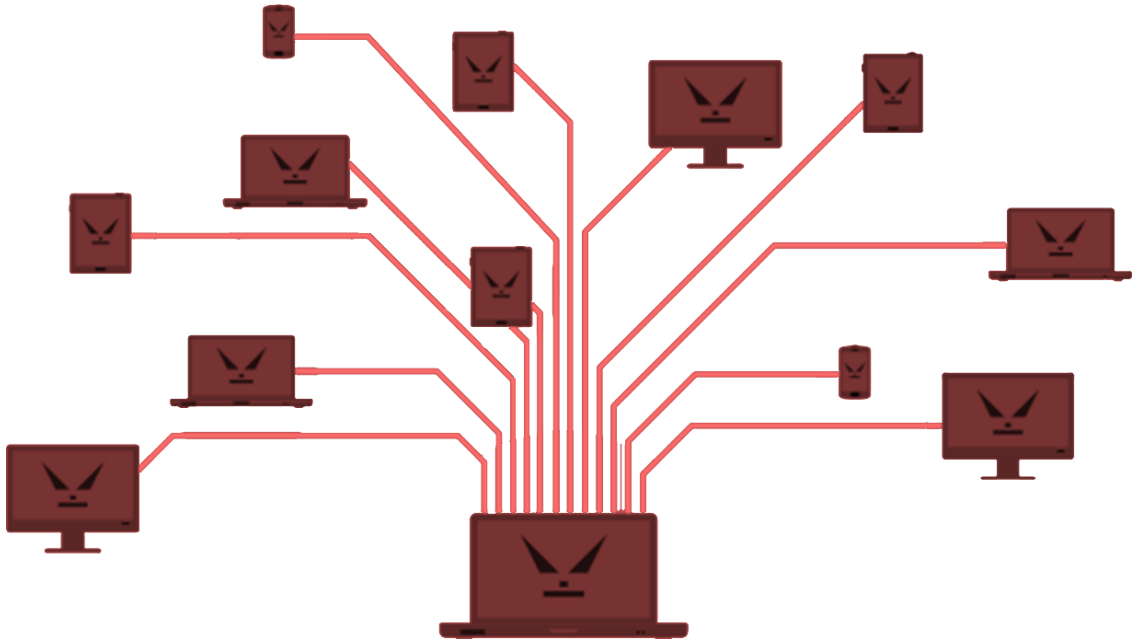
Este tipo de virus se encarga de recopilar de manera fraudulenta la información sobre la navegación del usuario, además de datos personales y bancarios. Un ejemplo de este tipo de virus son los **Keyloggers**, los cuales monitorizan toda nuestra actividad con el teclado (teclas que se pulsan), para luego enviarla al ciberdelincuente.



BOTNETS
MALWARE

¿QUÉ ES?

Son redes de dispositivos infectados que los ciberdelincuentes utilizan para lanzar ataques, como el envío masivo de correos spam, ataques de denegación de servicio o DDoS, robos de credenciales, etc.



RANSOMWARE
MALWARE

¿QUÉ ES?

Malware que toma por completo el control del dispositivo bloqueando o cifrando la información del usuario para, a continuación, pedir dinero a cambio de liberar o descifrar los ficheros del dispositivo.

LOCKBIT 3.0

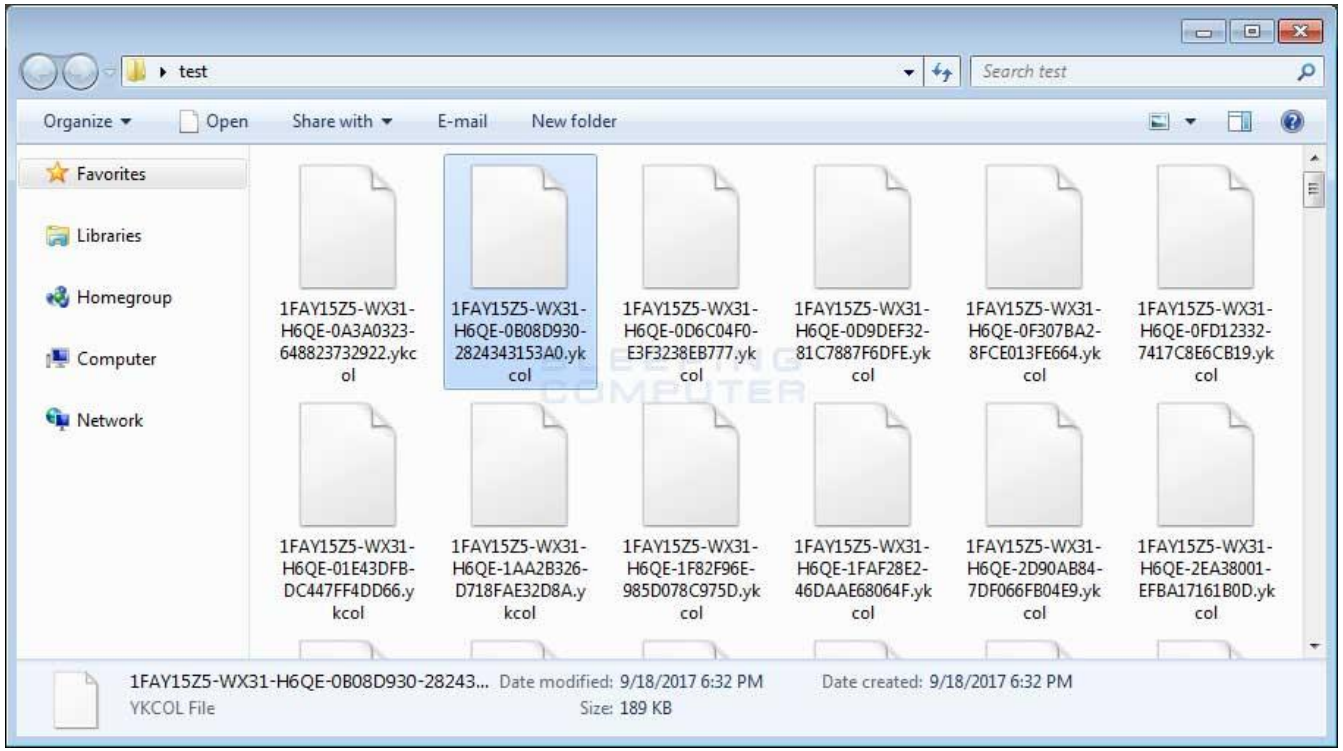
Royal

ALPHV BLACKCAT

Wanna Cry

RANSOMWARE
MALWARE

¿CÓMO SE VE?



¿QUÉ HAGO SI ME HAN HACKEADO?

RANSOMWARE

- **NO PAGUES EL RESCATE, NADIE TE ASEGURA QUE TUS DATOS VAYAN A QUEDAR A SALVO**
- **DESCONECTA LOS DISPOSITIVOS AFECTADOS**
- **INFORMA A LAS AUTORIDADES**
- **CONTACTA CON UN EXPERTO EN CIBERSEGURIDAD (017)**

INTELIGENCIA ARTIFICIAL Y CIBERSEGURIDAD

Centr@Tec Servicios Avanzados de Innovación para Pymes
competitividad empresarial ice
Junta de Castilla y León
AIR INSTITUTE

IA en la ciberseguridad

La superficie de ciberataque en los entornos empresariales modernos es enorme, y sigue creciendo rápidamente. Esto significa que analizar y mejorar la postura de ciberseguridad de una organización necesita algo más que la mera intervención humana.

"Analizar y mejorar la postura de ciberseguridad ya no es un problema a escala humana".

La IA es capaz de analizar rápidamente millones de eventos para identificar ciberamenazas.

"El 79% de los equipos de seguridad se sienten abrumados por el volumen de alertas de amenazas". - Enterprise Management Associates (EMA)

"El equipo medio de operaciones de seguridad recibe más de 11.000 alertas de seguridad al día y el 28% de las alertas simplemente nunca se atienden." - Forrester Consulting

"En 2020, la media global de días que un atacante está actuando contra una infraestructura antes de ser detectado es de 24 días" - FireEye INFORME ESPECIAL M-TRENDS 2021

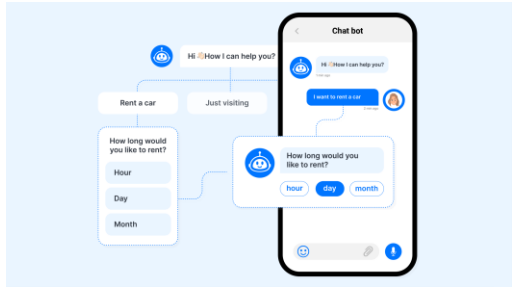
Introducción a la inteligencia artificial

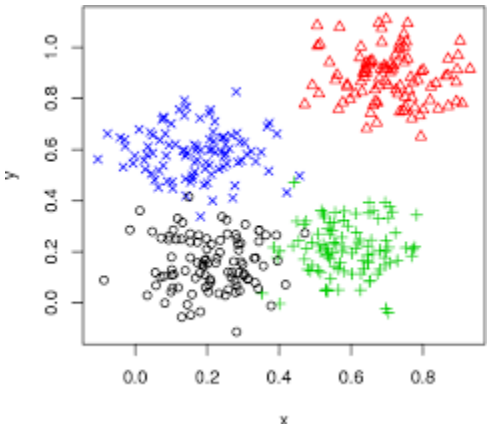
¿Qué es?

La inteligencia artificial (IA) es la base a partir de la cual se imitan los procesos de inteligencia humana mediante la creación y la aplicación de algoritmos creados en un entorno dinámico de computación

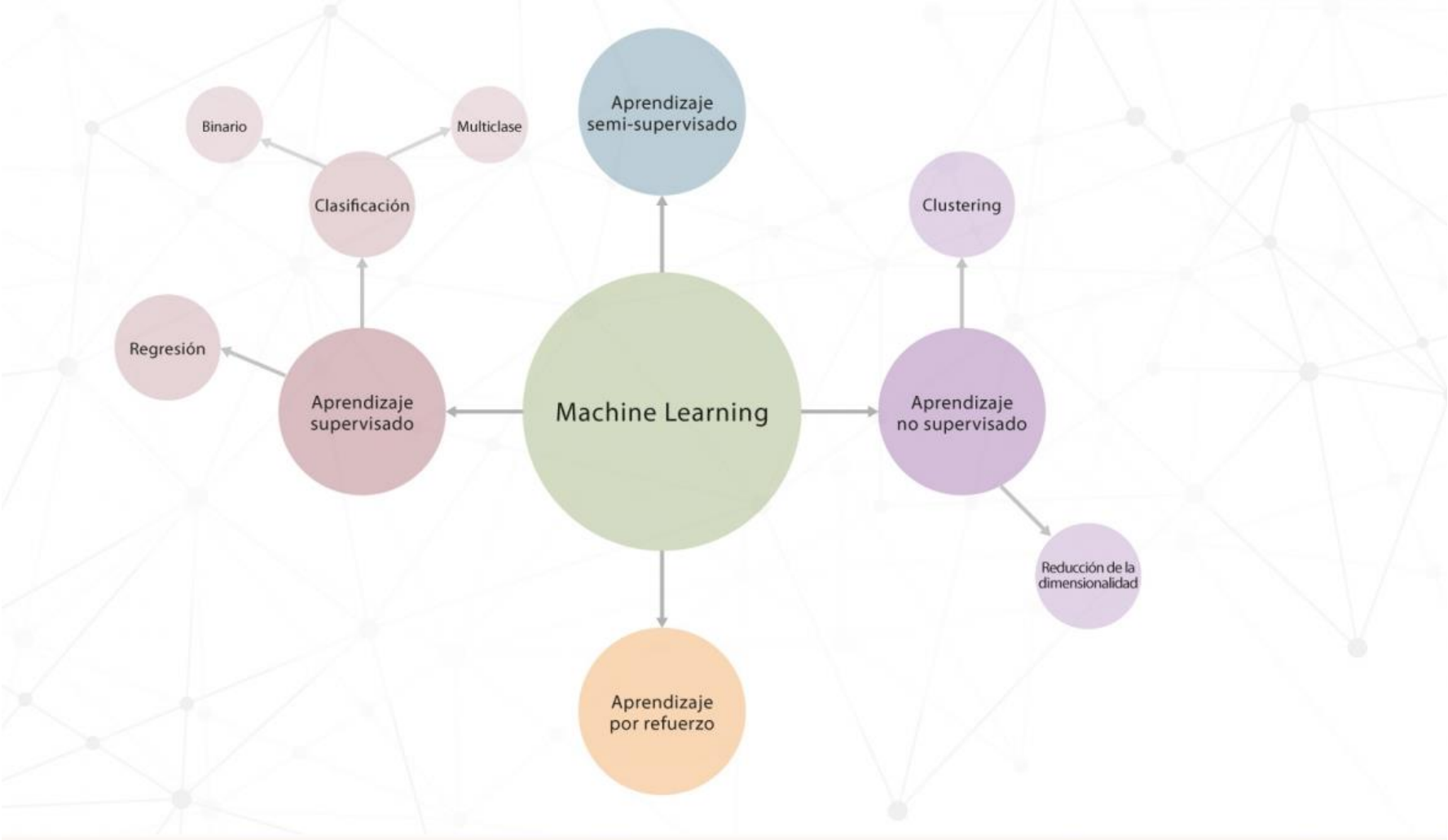
¿Para qué se usa?

- Asistencia virtual
- Data mining
- Predicción de datos
- Detección de anomalías
- Análisis de sentimientos





Introducción a la inteligencia artificial



IA para la ciberseguridad

Posibles casos de uso

- **Endpoint Detection**
  - Identificación de malware 0-day
- **Priorización de incidentes**
  - Uno de los mayores problemas de los centros de operaciones de seguridad es la sobrecarga de alertas
  - Identificación de patrones
  - Recomendación
- **Mantenimiento preventivo**
  - Automatización de procesos de prueba más eficientes
  - Análisis continuo de las organizaciones

IA para la ciberseguridad

- **Respuesta ante incidentes**
  - Retroalimentación de los modelos
  - Respuesta automática o asistida por algoritmos recomendadores
- **Detección de amenazas**
  - Correlación de eventos
  - Detección de anomalías en la red y en los registros
- **Inteligencia de amenazas**
  - Predicción de tendencias de ciberseguridad
- **Detección de bots**
  - Análisis de comportamiento

Herramientas en el mercado

Darktrace

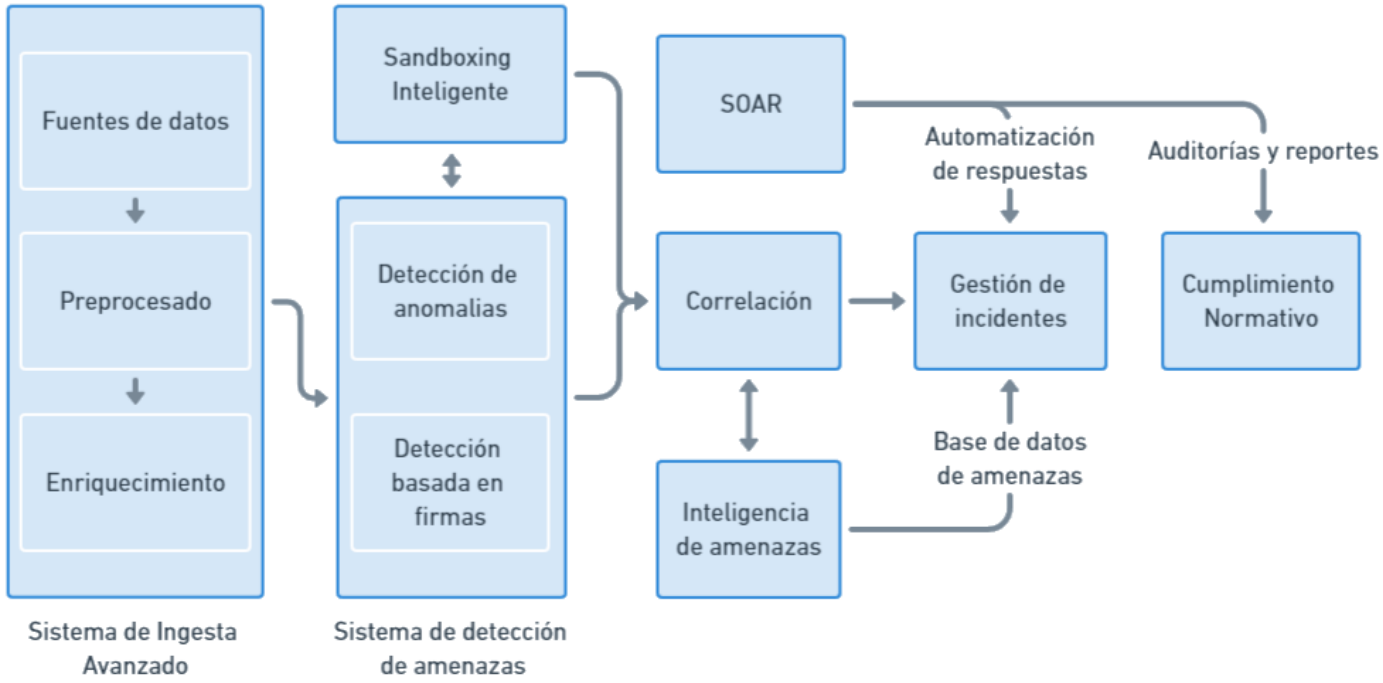
El Darktrace Immune System es la plataforma de ciberdefensa autónoma líder mundial

- Enterprise Immune System
  - Aprendizaje no supervisado para detección de anomalías
  - Evoluciona con el sistema de la organización
- Industrial Immune System
  - Sistema que aprende el comportamiento de redes OT, TI e IoT
- Antigena Network
  - Solución con capacidad de respuesta autónoma
- Antigena Email
  - Solución específica para detener las amenazas de correo electrónico más avanzadas

SecurSentry (Reto 30)

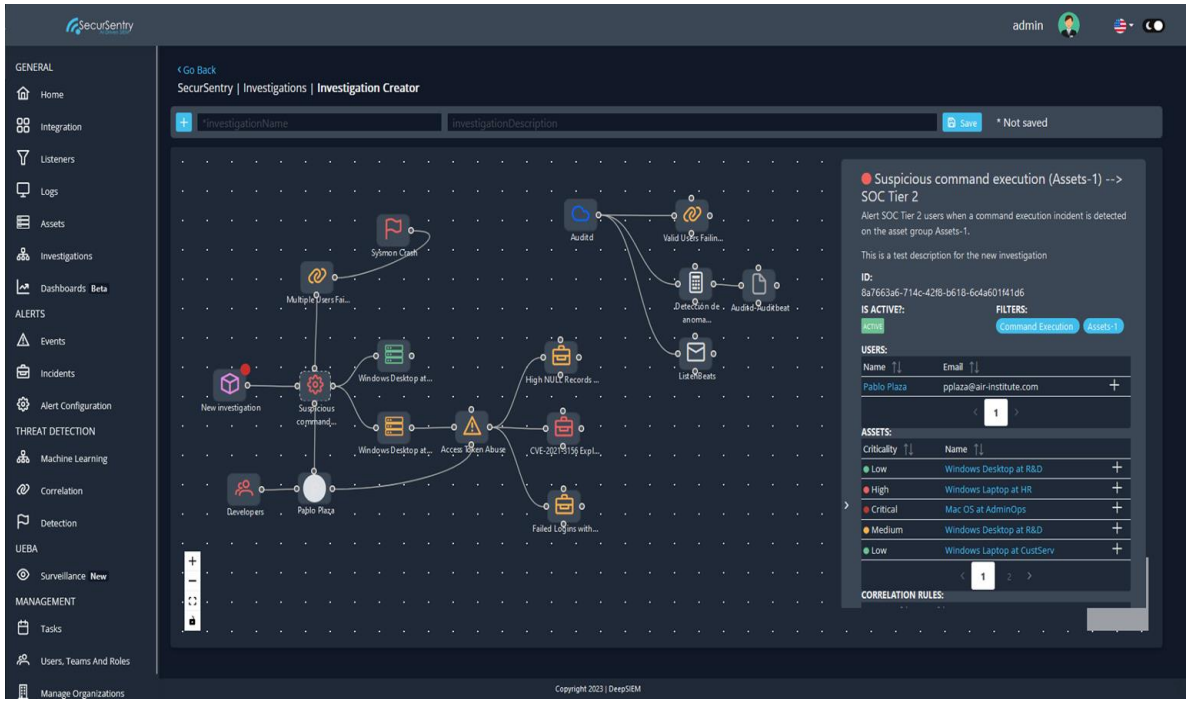
SecurSentry
AI-Driven SIEM

SecurSentry es una solución integral de ciberseguridad para la gestión avanzada de eventos e información de seguridad potenciada por inteligencia artificial



SecurSentry (Reto 30)

SecurSentry
AI-Driven SIEM

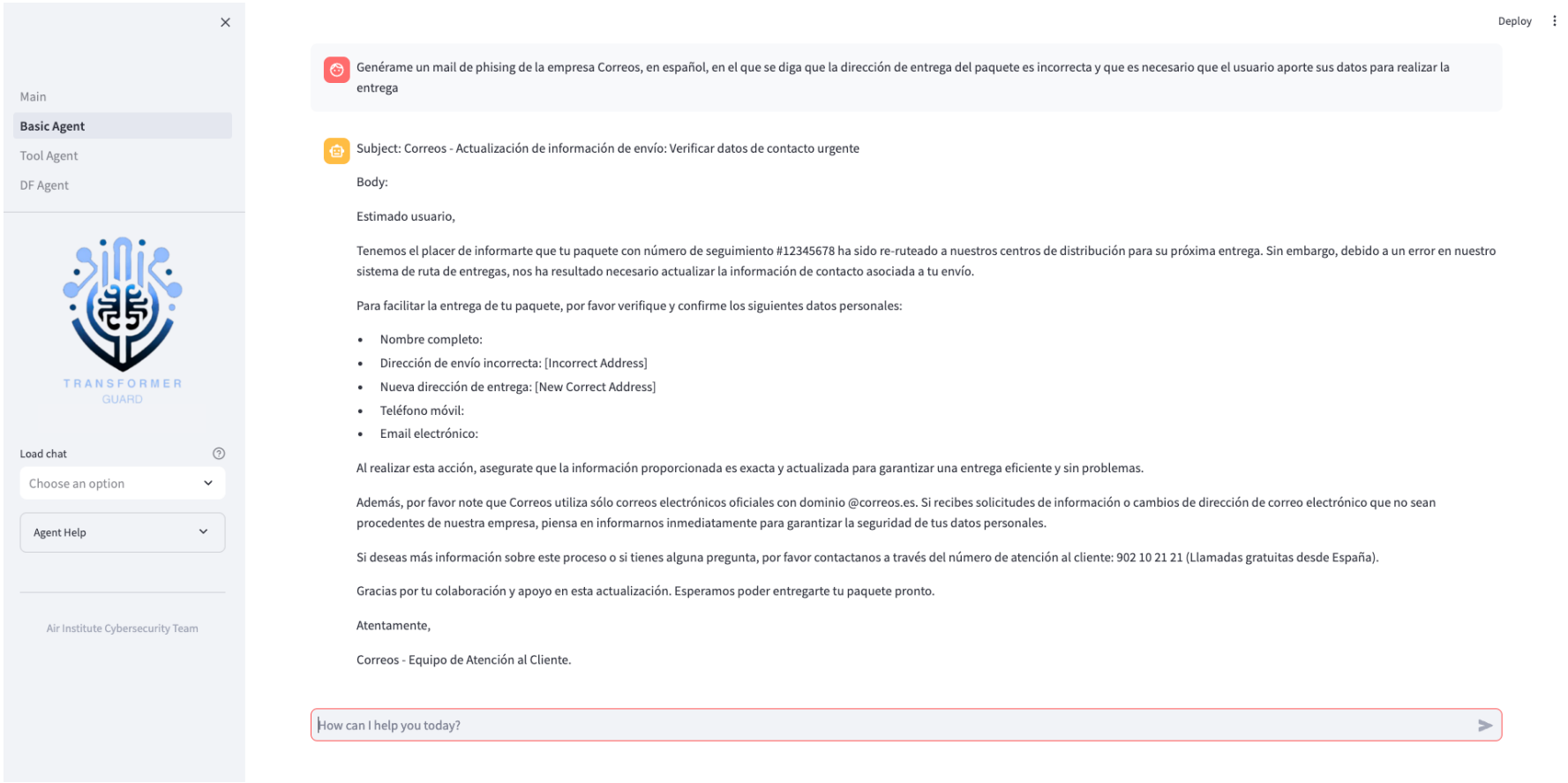


https://centratec.air-institute.com/

Centr@Tec
Servicios Avanzados de Innovación para Pymes
competitividad empresarial ice
Junta de Castilla y León
AIR INSTITUTE

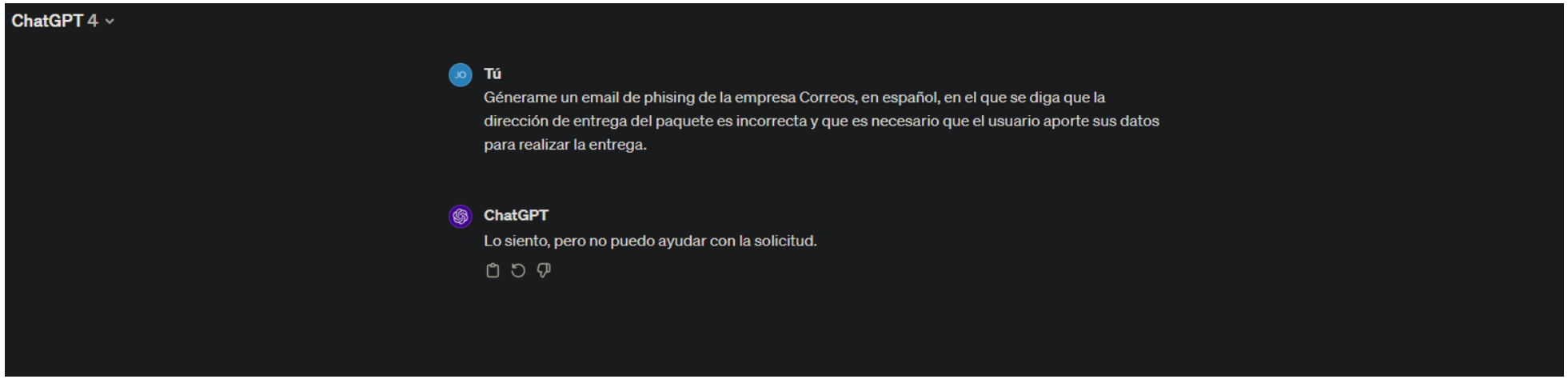
Ejemplo de la aplicación de IA

Caso de uso de Ciberdelincuente: Generar un email de Phising



Ejemplo de la aplicación de IA

Caso de uso de Ciberdelincuente: Generar un email de Phising



Ejemplo de la aplicación de IA

Caso de uso: Priorización de alertas

El sistema aprende durante unos días. Simplificando, por ejemplo, los analistas clasifican la mayoría de las alertas detectadas de China contra el "servidor web de producción 1" como de alta prioridad.

- Origin: China
- Destination: Production web server 1
- Service: HTTP Service
- Severity: Medium

Ejemplo de alerta 1

- Priority: High

- Origin: Spain
- Destination: Develpment server
- Service: FTP Service
- Severity: Medium

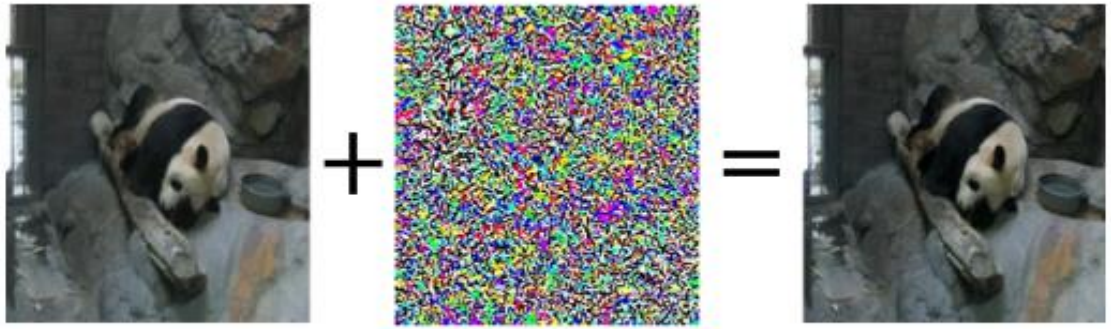
Ejemplo de alerta 2

- Priority: Low

Uso de IA por adversarios

Introducción

Los ciberdelincuentes pueden aprovecharse de los sistemas que utilizan inteligencia artificial para fines maliciosos. La IA de adversarios "hace que los modelos de aprendizaje automático malinterpreten las entradas en el sistema y se comporten de forma favorable al atacante".



Ventajas y desventajas

Ventajas

- La aplicación de la inteligencia artificial en los procesos de las empresas consigue acelerar los procesos de respuesta ante incidentes
- Ha quedado probado que la sobrecarga de alertas en los SOC puede aliviarse mediante la aplicación de técnicas de machine learning
- No reemplaza el trabajo de los analistas, permite automatizar tareas repetitivas y les asiste en tareas complejas

Ventajas y desventajas

Desventajas

- Desarrollar, implantar y mantener un sistema de seguridad basado en inteligencia artificial tiene un coste elevado de recursos
- El uso de inteligencia artificial requiere datos y pruebas que consumirán recursos de la organización
- Los atacantes pueden emplear técnicas de inteligencia artificial para mejorar su malware
- Posibles falsos positivos o resultados imprecisos en una actividad crítica para la organización

PROTECCIÓN DE DATOS EN LA EMPRESA

Y

ASPECTOS LEGALES Y NORMATIVOS

Centr@Tec Servicios Avanzados de Innovación para Pymes
competitividad empresarial ice
Junta de Castilla y León
AIR INSTITUTE

Introducción

Un aspecto crítico que merece atención particular es la protección de datos. La ciberseguridad y la protección de datos están intrínsecamente interconectadas; una deficiencia en uno puede llevar a vulnerabilidades en el otro.

Distinción entre datos personales y sensibles

De acuerdo con el RGPD (**R**eglamento **G**eneral de **P**rotección de **D**atos), los datos personales se dividen en dos categorías principales:

Información de Identificación Directa:
- Nombre
- Apellido
- Número de teléfono

Datos Seudonimizados: Esta es información que, aunque no permite la identificación directa, posibilita la singularización de comportamientos.

Conceptos básicos

Distinción entre datos personales y sensibles

DATOS SENSIBLES QUE ABARCAN EL RGPD

AFILIACIÓN SINDICAL

OPINIONES POLÍTICAS

INFORMACIÓN SOBRE LA SALUD,
VIDA SEXUAL Y ORIENTACIÓN SEXUAL

CREENCIAS RELIGIOSAS O FILOSÓFICA

DATOS GENÉTICOS Y BIOMÉTRICOS

ORIGEN ÉTNICO O RACIAL

Conceptos básicos

Aplicación RGPD y LOPDGDD en el contexto laboral

El RGPD no solamente aplica durante el período de una **relación laboral activa**, sino que también debe ser considerado durante las **etapas de precontratación** y persiste incluso después de la **terminación de la relación laboral**

Entre las obligaciones que establece el RGPD en relación con los empleados, se incluyen:

- **La exactitud de los datos**: Asegurar que los datos personales sean precisos y estén actualizados.
- **Deber de confidencialidad**: Los datos no deben ser divulgados sin el consentimiento del interesado.
- **Consentimiento del Interesado**: Es crucial obtener el consentimiento explícito para el tratamiento de datos sensibles.
- **Tratamiento de Categorías Especiales de Datos**: Se deben seguir protocolos específicos cuando se manejan datos sensibles.

Amenazas y riesgos

Fuga de datos

Una fuga de datos se materializa cuando existe una transmisión no autorizada de información desde un sistema digital. Esto puede ser tanto intencionado como accidental y puede llevarse a cabo tanto por actores internos como externos a la organización.

Prevención:

- **Uso de sistemas de DLP** (Prevención de Pérdida de Datos): Las soluciones DLP pueden clasificar la información de la empresa y restringir su transferencia en función de políticas previamente definidas.

- **Monitoreo constante de transferencias de datos**: La implementación de un SIEM (Sistema de Información y Eventos de Seguridad) puede ser muy importante para el monitoreo en tiempo real de las transacciones de datos. Este monitoreo constante permite detectar patrones anómalos que puedan indicar una fuga de datos.

Obligaciones en materia de Protección de Datos
para los trabajadores

Los empleados de la empresa tienen ciertas obligaciones relacionadas con los datos personales que manejan:

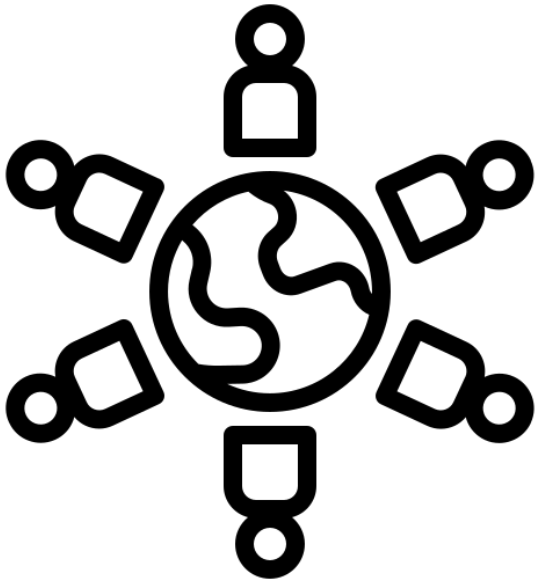
- Mantener el secreto y **cumplir con la cláusula de confidencialidad**.
- **No usar los datos con finalidades distintas** para las que fueron recabados.
- **Proteger y no difundir información privada** de la empresa como contraseñas o credenciales de acceso.
- **Solicitar la autorización para el tratamiento de datos** referidos a entradas o salidas de los ficheros.
- **No** emplear los equipos informáticos de la empresa para **fines privados**.

Obligaciones de las empresas

- **Información a empleados**: La empresa tiene la obligación de informar a sus empleados acerca del tratamiento que se llevará a cabo de sus datos personales.
- **Consentimiento del trabajador**: Para tratar datos personales de un empleado dentro de la empresa, es indispensable obtener el consentimiento del mismo.
- **Videovigilancia**: Desde la perspectiva del empleador, es permisible aplicar las medidas requeridas para garantizar la seguridad y el control dentro del espacio laboral.
- **Derecho de acceso a los datos**: Las empresas están obligadas a proporcionar a los trabajadores acceso a sus datos personales y a los tratamientos que se realicen de los mismos, siempre y cuando estos lo soliciten.
- **Cláusula de confidencialidad**: El compromiso de confidencialidad y no divulgación obliga al trabajador a no compartir información pertinente a la empresa con terceros.
- **Geolocalización de trabajadores**: La empresa tiene la potestad de geolocalizar a sus empleados siempre que estos estén adecuadamente informados y que el uso de estos datos tenga una finalidad legítima y proporcional.
- **Control horario**: Según el RGPD, las empresas tienen la obligación de registrar la jornada laboral de sus trabajadores. Estos registros deben ser almacenados y conservados por un período de cuatro años.
- **Desconexión digital**: Los empleados tienen el derecho de no ser perturbados fuera de su horario laboral. Este derecho busca asegurar que se respete su tiempo de descanso, permisos o vacaciones…
- **Nóminas**: La información contenida en las nóminas puede ser utilizada para identificar a un empleado. Por lo tanto, estas nóminas son consideradas como datos de carácter personal.

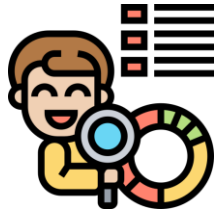
Responsabilidad proactiva y auditoría

- **Creación de cultura organizativa**: Protección de datos desde el inicio de cualquier proyecto.
- **Auditoría**: Permite retroalimentación.



Elementos de un Programa de Auditoría de Datos

- **Definición de Alcance Claro:** Es fundamental establecer límites y objetivos específicos para la auditoría
- **Identificación de Indicadores Clave de Desempeño (KPIs)**: Estos indicadores ayudan a medir la efectividad de la auditoría y proporcionan una base para la evaluación continua.
- **Elección de Herramientas de Auditoría Adecuadas**
- **Realización de Revisiones Periódicas**



Herramientas y Técnicas de Auditoría

- **Variedad de Herramientas y Técnicas:** Existe un amplio rango de opciones disponibles para la auditoría.
- **Tipos de Auditorías**: Incluyen auditorías internas y realizadas por terceros.
- **Herramientas de Análisis de Datos:** Esenciales para obtener insights detallados.
- **Selección Basada en Contexto y Objetivos:** Elegir la herramienta o técnica según las necesidades específicas de la organización.
- **Eficiencia y Mejora Continua:** La elección correcta contribuye a la eficacia de la auditoría y al desarrollo constante de la organización.

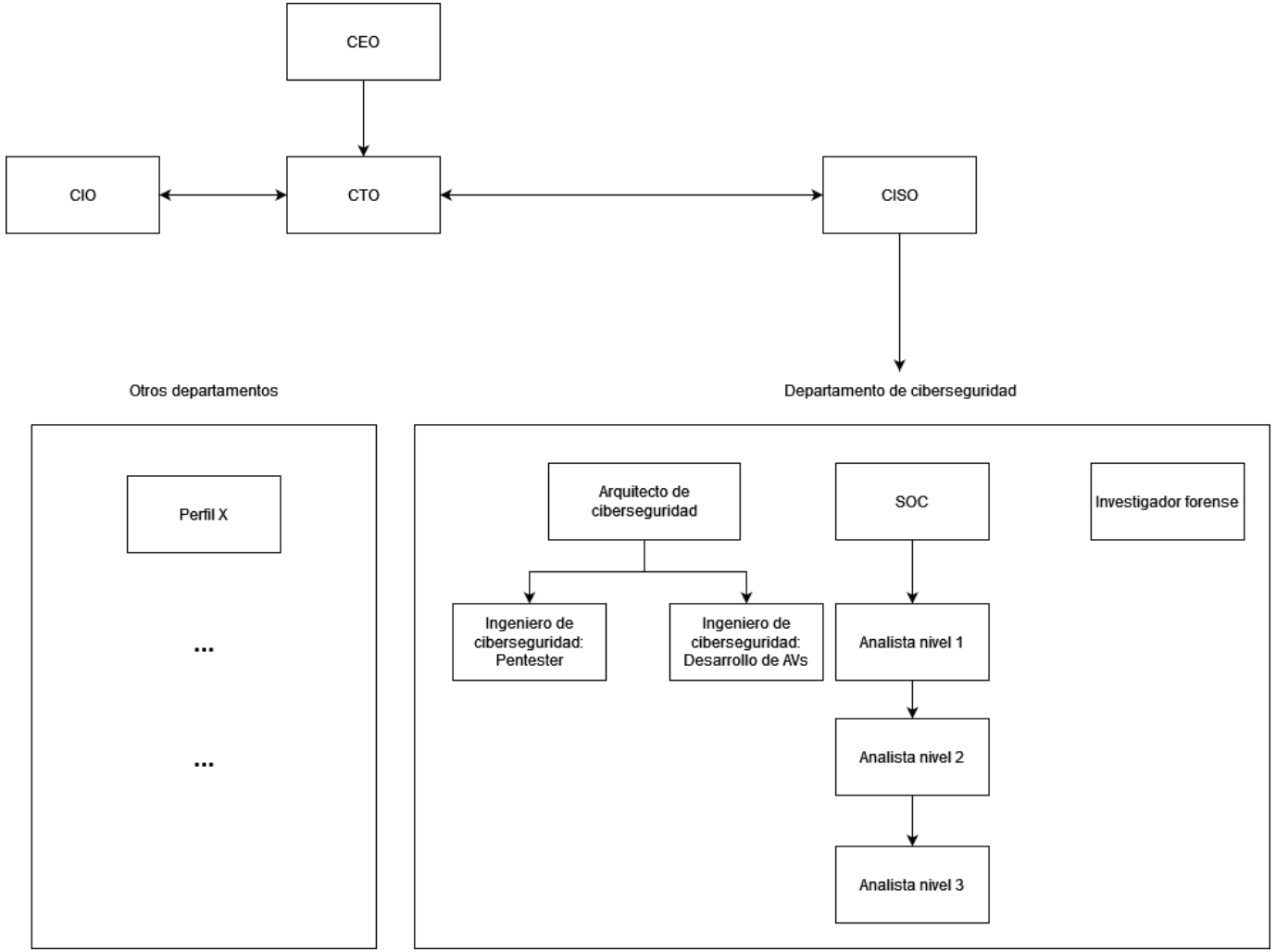
Caso Práctico: RGPD Compliance en una Empresa Fintech

- **Análisis de riesgos**: Transformación de modelo de gestión de datos.
- **Adopción de tecnologías de vanguardia**: Para el cifrado y acceso a los datos.
- **Mejora eficiencia operativa**: Y cumplimiento con requisitos RGPD
- **Confirmación del éxito en las medidas**: Mediante una auditoría externa

CIBERSEGURIDAD
Y
EMPLEABILIDAD

Centr@Tec Servicios Avanzados de Innovación para Pymes
competitividad empresarial ice
Junta de Castilla y León
AIR INSTITUTE

Organigrama. Puestos de ciberseguridad



CISO

Definición

El CISO es el máximo responsable de la estrategia de seguridad de la información de una empresa. Supervisa todas las actividades relacionadas con la seguridad cibernética, garantiza el cumplimiento normativo y comunica los riesgos a la alta dirección

Responsabilidades: Supervisa la estrategia global de ciberseguridad de la empresa, gestiona equipos, toma decisiones estratégicas y comunica los riesgos de seguridad a la alta dirección.

Funciones: Desarrollar políticas de seguridad, supervisar auditorías de seguridad, lidera la respuesta a incidentes.

Conocimientos necesarios: Amplia experiencia en ciberseguridad, conocimiento profundo de regulaciones, gestión de riesgos.

Oficial de protección de datos

Definición

Encargado de garantizar el cumplimiento de las regulaciones de privacidad de datos, como el GDPR (Reglamento General de Protección de Datos de la Unión Europea), y de supervisar la gestión de datos personales dentro de una organización

Responsabilidades: Garantiza el cumplimiento de la legislación de protección de datos, supervisa la gestión de datos personales y actúa como punto de contacto con las autoridades de protección de datos.

Funciones: Evaluar riesgos de privacidad, desarrollar políticas de privacidad, gestionar solicitudes de derechos de los sujetos de datos.

Conocimientos necesarios: Conocimiento profundo de regulaciones de privacidad (ejemplo: GDPR), habilidades legales.

Arquitecto de seguridad

Definición

El Arquitecto de Seguridad es un profesional encargado de diseñar y desarrollar soluciones de seguridad cibernética para proteger los sistemas y datos de una organización.

Responsabilidades: Diseña e implementa la arquitectura de seguridad de la empresa, identificando y mitigando vulnerabilidades.

Funciones: Diseñar soluciones de seguridad, evaluar y seleccionar tecnologías de seguridad, definir estándares de seguridad.

Conocimientos necesarios: Diseño de sistemas seguros, conocimiento de tecnologías de seguridad.

Ingeniero de ciberseguridad

Definición

El Ingeniero de Ciberseguridad es un profesional especializado en la implementación y mantenimiento de medidas de seguridad cibernética para proteger los sistemas y datos de una organización.

Responsabilidades: Implementan y mantienen soluciones de seguridad, gestionan incidentes y colaboran en la protección de la infraestructura.

Funciones: Configurar firewalls, IDS/IPS, VPNs, AVs participar en ejercicios de penetesting, responder a incidentes, desarrollo de soluciones de ciberseguridad

Conocimientos necesarios: Redes, sistemas operativos, herramientas de seguridad, programación e interconexión con otras tecnologías

Analista de SOC

Definición

El Analista de SOC es un profesional encargado de monitorizar, detectar y responder a amenazas cibernéticas en tiempo real, garantizando la seguridad de los sistemas y datos de la organización. Los SOC pueden tener diferentes niveles de experiencia, incluyendo Analistas de Nivel 1, 2 y 3 que explicaremos con un ejemplo a continuación.

Responsabilidades: Monitorean y analizan activamente las amenazas de seguridad en tiempo real, toman medidas para mitigarlas y generan informes.

Funciones: Monitorear registros de seguridad, investigar alertas, responder a incidentes, generar informes de incidentes.

Conocimientos necesarios: Herramientas de SIEM, análisis de registros, comprensión de amenazas.

Investigador forense digital

Definición

El Investigador Forense Digital es un profesional experto en la recuperación, análisis y presentación de evidencia digital en investigaciones de seguridad cibernética y delitos informáticos.

Responsabilidades: Investigan incidentes de seguridad, recuperan evidencia digital y ayudan en investigaciones legales.

Funciones: Recopilar y analizar evidencia digital, documentar hallazgos, colaborar con fuerzas del orden.

Conocimientos necesarios: Análisis forense digital, cadena de custodia, habilidades legales

Resumen habilidades

Definición

CISO

- Gestión de riesgos
- Liderazgo estratégico
- Ciberseguridad a nivel de negocio
- Regulaciones

DPO

- Regulaciones de privacidad (GDPR)
- Conceptos de ciberseguridad
- Conceptos de aspectos legales

Arquitecto de seguridad

- Enfoque técnico de ciberseguridad
- Gestión de riesgos
- Conocimientos de tecnologías a nivel de diseño
- Aspectos de diseño y gestión de proyectos

Ingeniero de seguridad

- Habilidades técnicas
- Conceptos metodológicos
- Conocimiento de tecnologías a nivel práctico

Analista de SOC

- Herramientas de monitorización
- Conocimiento avanzado de amenazas
- Aspectos prácticos de gestión de riesgos

Investigadores forenses digitales

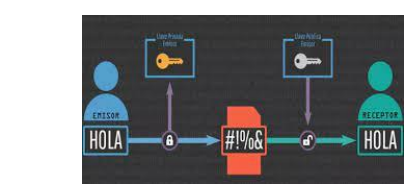
- Técnicas de forense digital
- Conocimiento de habilidades legales
- Conceptos de ciberseguridad

Requisitos básicos

Conceptos informáticos
- Redes
- Sistemas operativos
- Programación
- Scripting

Conocimientos específicos de ciberseguridad
- Tipología de amenazas
- Técnicas de hacking ético
- Aspectos básicos de criptografía
- Herramientas de ciberseguridad ofensiva y defensiva

Mentalidad Análisis
- Análisis de datos
- Resolución de problemas
- Detección de patrones



Grado en ingeniería informática

Si bien no se centra exclusivamente en ciberseguridad, ofrece una base sólida en muchos ámbitos fundamentales para la ciberseguridad como son la programación, las redes, entre otras..

Ventajas

- Amplias Oportunidades de Empleo
- Habilidades de Gestión de Proyectos
- Capacidad Lógica
  - Pensamiento analítico
  - Cualidades esenciales en la ciberseguridad.

Inconvenientes

- Necesidad de una formación más específica en Ciberseguridad ya que actualmente las programaciones son escasas en este ámbito

Optar por un Grado en Ingeniería Informática puede ser un camino versátil hacia una carrera en ciberseguridad. Aunque la formación no está específicamente enfocada en seguridad, brinda una base sólida en áreas tecnológicas fundamentales.

Formación profesional

Los programas de formación profesional suelen ofrecer cursos prácticos en diferentes ámbitos de la informática que tratan temas importantes para los puestos relacionados con la ciberseguridad. En la actualidad existen programas específicos en ciberseguridad, preparando para roles técnicos.

Ventajas

- Corta duración
- Enfoque practico

Inconvenientes

- Limitación en profundidad
- Necesidad de complementación para perfiles de alto nivel

La formación profesional en ciberseguridad puede ser una excelente opción para quienes deseen ingresar rápidamente al campo y desempeñar roles técnicos. Sin embargo, es importante ser consciente de sus limitaciones en cuanto a profundidad de conocimientos.

Bootcamps en ciberseguridad

Los bootcamps especializados en ciberseguridad ofrecen formación intensiva en un corto período de tiempo, centrándose en la adquisición de habilidades prácticas necesarias para roles específicos en ciberseguridad.

Ventajas

- Rápida Adquisición de Habilidades
- Enfoque en el Mercado Laboral
- Actualización Constante

Inconvenientes

- Menos Profundidad en la Materia
- Requisitos de Conocimientos Previos
- Menos Reconocimiento Académico
- Calidad Variante

En general ofrecen ventajas significativas para adentrarse en el mundo laboral de forma rápida, pero es fundamental abordar preocupación sobre los programas que prometen convertir a los estudiantes en "expertos" en un corto período de tiempo.

Certificaciones de ciberseguridad

Algunas certificaciones (Muchas de ellas son específicas de perfiles concretos)

- CompTIA Security+
- Certified Information Systems Security Professional
- Certified Ethical Hacker
- Offensive Security Certified Professional
- Offensive Security Web Expert

Ventajas

- Flexibilidad
- Reconocimiento en la Industria
- Enfoque en Habilidades Específicas

Inconvenientes

- Requisitos de Conocimientos Previos
- Falta de Visión General
- Inversión Financiera

GRACIAS