AGOSTO **2023**

CURSO

CIBER SEGURIDAD

MARTÍN ROUSSEAUX

CURSO
CIBER SEGURIDAD

MARTÍN ROUSSEAUX

CONTENIDO

INTRODUCCIÓN
Ciberseguridad
Incidentes
Estadisticas

COMPAÑIAS NAVIERAS
Sistemas y vulnerabilidades
TMSA3

TIPOS DE ATAQUES MÁS COMUNES
Mensajes malisiosos
Software malicioso (malware)

COMO PROTEGER MIS DATOS
Autenticación segura
Copias de seguridad y cifrado de datos
Herramientas

RECOMENDACIONES
Espacios públicas y accesos remotos
Escritorio seguro
Por último

CURSO

CIBER SEGURIDAD

INTRODUCCIÓN

MARTÍN ROUSSEAUX

MARTÍN ROUSSEAUX

- # CIBERSEGURIDAD

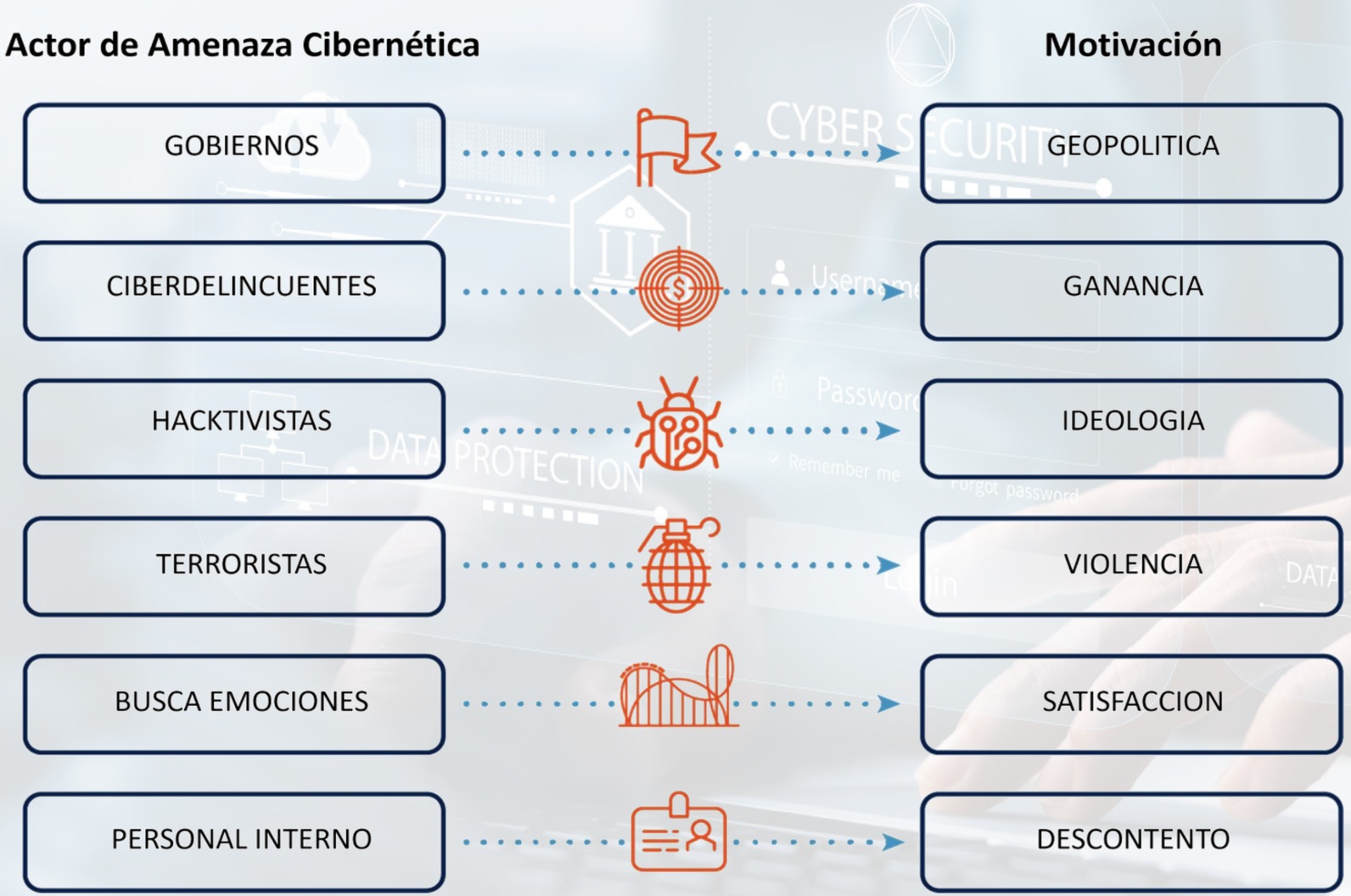
¿Qué es?

La ciberseguridad es el proceso de protección de la información en el ciberespacio. Se trata de proteger los datos o la información que reside en un sistema informático o en una red para que no se vean comprometidos por piratas informáticos, virus y otros programas maliciosos.

MARTÍN ROUSSEAUX

- # CIBERSEGURIDAD

¿Qué es?



MARTÍN ROUSSEAUX

- **CIBERSEGURIDAD**

CAUSAS

INTERNAS

Son aquellas en las que la pérdida se produce por parte del propio equipo de la compañía, ya sea por desconocimiento, error o a propósito por alguna motivación.

EXTERNAS

Los motivos externos son intencionados, en el que se trabaja por conseguir vulnerar la seguridad de la compañía para adquirir la información. Esta accion puede estar motivada por obtener un beneficio económico, venganza, dañar la imagen de la empresa...

ÁMBITO ORGANIZATIVO

- Falta de clasificación de la información
- Falta de conocimiento y formación
- Falta de procedimientos
- Falta de acuerdos de confidencialidad

ÁMBITO TÉCNICO

- Falta de soluciones ante ataques
- Falta de seguridad en accesos a infraestructuras
- Falta de seguridad o control en sistemas de la nube
- Uso de BYOD sin control por parte de la empresa

MARTÍN ROUSSEAUX

- **CIBERSEGURIDAD**

CONSECUENCIAS

DAÑOS DE IMAGEN

La fuga de datos genera un impacto negativo en la imagen de la empresa. La falta de seguridad dentro de la misma provoca la desconfianza de clientes, clientes potenciales y otras empresas.

CONSECUENCIAS ECONÓMICAS

Ligada al daño de imagen, la pérdida de reputación y clientes deriva en disminución de la inversión así como de proyectos. En pequeñas y medianas empresas esto puede suponer la limitación de la continuidad de negocio, pudiendo llegar hasta la bancarrota.

CONSECUENCIAS LEGALES

En cuanto a las consecuencias legales, se debe valorar el tipo de información. En el caso de que la información extraída sean **datos personales** se denomina **"brecha de seguridad"** y, exige ciertos deberes para cumplir con la legislación vigente:

- INCIDENTES

SECCIONES | Clarín TECNOLOGÍA

CLARÍN > TECNOLOGÍA | POLITICA SOCIEDAD DEPORTES ESPECTÁCULOS MUNDO ECONOMÍA OPINIÓN POLICIALES

Bajo amenaza: hackean 32 millones de cuentas de Twitter

Te contamos cómo verificar si tu cuenta fue atacada.

New Massive Security Breach Exposes 773 Million Passwords

By Joel Hruska on January 17, 2019 at 3:45 pm | 20 Comments

Alaska notifies 87,000 people after computer security breach

Originally published January 23, 2019 at 9:29 pm | *Updated January 24, 2019 at 6:45 am*

Cryptopia cryptocurrency exchange pulled offline due to security breach

Reports suggest that cryptocurrency may have been lost by the exchange.

By Charlie Osborne for Zero Day | January 15, 2019 -- 15:40 GMT (07:40 PST) | Topic: Security

Humana notifies members of 2018 security breach

Written by Julie Spitzer | January 07, 2019 | Print | Email

Firms fined $1M for SingHealth data security breach

SingHealth and Singapore's public healthcare sector IT agency IHIS have been slapped with S$250,000 and S$750,000 financial penalties, respectively, for the July 2018 cybersecurity attack that breached the country's personal data protection act. The fines are the highest dished out to date.

By Eileen Yu for By The Way | January 15, 2019 -- 10:41 GMT (02:41 PST) | Topic: Security

DailyMotion discloses credential stuffing attack

DailyMotion falls to credential stuffing attack two weeks after Reddit had the same fate.

By Catalin Cimpanu for Zero Day | January 27, 2019 -- 12:02 GMT (04:02 PST) | Topic: Security

Massive data breach involving millions of mortgage documents just got much worse

Original mortgage documents found on separate exposed server

January 24, 2019 *Ben Lane*

German data breach: agencies 'failing to take security seriously'

Bavarian interior minister 'astonished' at handling of biggest data leak in German history

- INCIDENTES

INDEPENDENT SUBSCRIBE REGISTER LOGIN

INDY/LIFE

50,000 SHIPS WORLDWIDE ARE VULNERABLE TO CYBERATTACKS

Vulnerabilities in shipping show how far the industry has to go but proper cyber security is more complex than you might initially think

Keith Martin Rory Hopcraft |
Wednesday 20 June 2018 23:15 |

Shipping Industry Cybersecurity: A Shipwreck Waiting to Happen

Author:
Tara Seals
June 7, 2018 / 2:46 pm

5 minute read

Share this article:

Pen Test Partners demonstrates how to send vessels off-course or even onto a path to collision — fairly easily.

Cyber Security at Sea: The Real Threats

BY DAVID RIDER (HTTPS://WWW.MARITIME-EXECUTIVE.COM/AUTHOR/DAVID-RIDER)
2018-03-10 22:05:14

The maritime cyber security landscape is a confusing place. On the one hand, you have commercial providers suggesting the risks of everything from a hostile attack on ship's systems which allows the vessel to be remotely controlled by pirates and direct it to a port of their choice, or causing a catastrophic navigation errors, a phishing attack or ransomware on the Master's PC. While on the other, you have sensible people who point out that this notion is nonsense due to the number of fail safes and manual overrides and

ESTADÍSTICAS

- Se estima que el costo mundial anual del delito cibernético supera $ 20 trillón por 2026 (Empresas de ciberseguridad)
- Hubo 2,244 ciberataques por día, lo que equivale a más de 800,000 ataques por año. Eso es casi un ataque cada 39 segundos. (Universidad de Maryland)
- Hubo 236.1 millones de ataques de ransomware en el primer semestre de 2022. (Statista)
- 71% de las organizaciones en todo el mundo han sido víctimas de ataques de ransomware en 2022. (Empresas de ciberseguridad)
- Crimen organizado es responsable del 80% de todas las violaciones de seguridad y datos. (Verizon)
- Los ataques de ransomware ocurren cada 10 segundos (Grupo de InfoSeguridad)
- 71% de todos los ataques cibernéticos están motivados económicamente (seguidos por el robo de propiedad intelectual y luego el espionaje). (Verizon)

ESTADÍSTICAS

> **En promedio, se publicó una aplicación de Android maliciosa cada 23 segundos en 2022.**

Fuente: G-Data

> **En 2022, el coste medio de un ataque de filtración de datos alcanzó los 4.35 millones de dólares. Este es un aumento del 2.6% con respecto al año anterior.**

Fuente: IBM

> **El 83% de las empresas estuvieron expuestas al phishing en 2022.**

Fuente: Cybertalk

> **Los correos electrónicos de malware en el tercer trimestre de 3 aumentaron a 2022 millones y representaron un aumento del 52.5 % en comparación con el mismo período del año anterior (217 millones).**

Fuente: Vadesecure

> **Más del 90 % del malware llega a través del correo electrónico.**

Fuente: CSO Online

> **En julio de 2022, Twitter confirmó que se habían robado los datos de 5.4 millones de cuentas.**

Fuente: CS Hub

CURSO

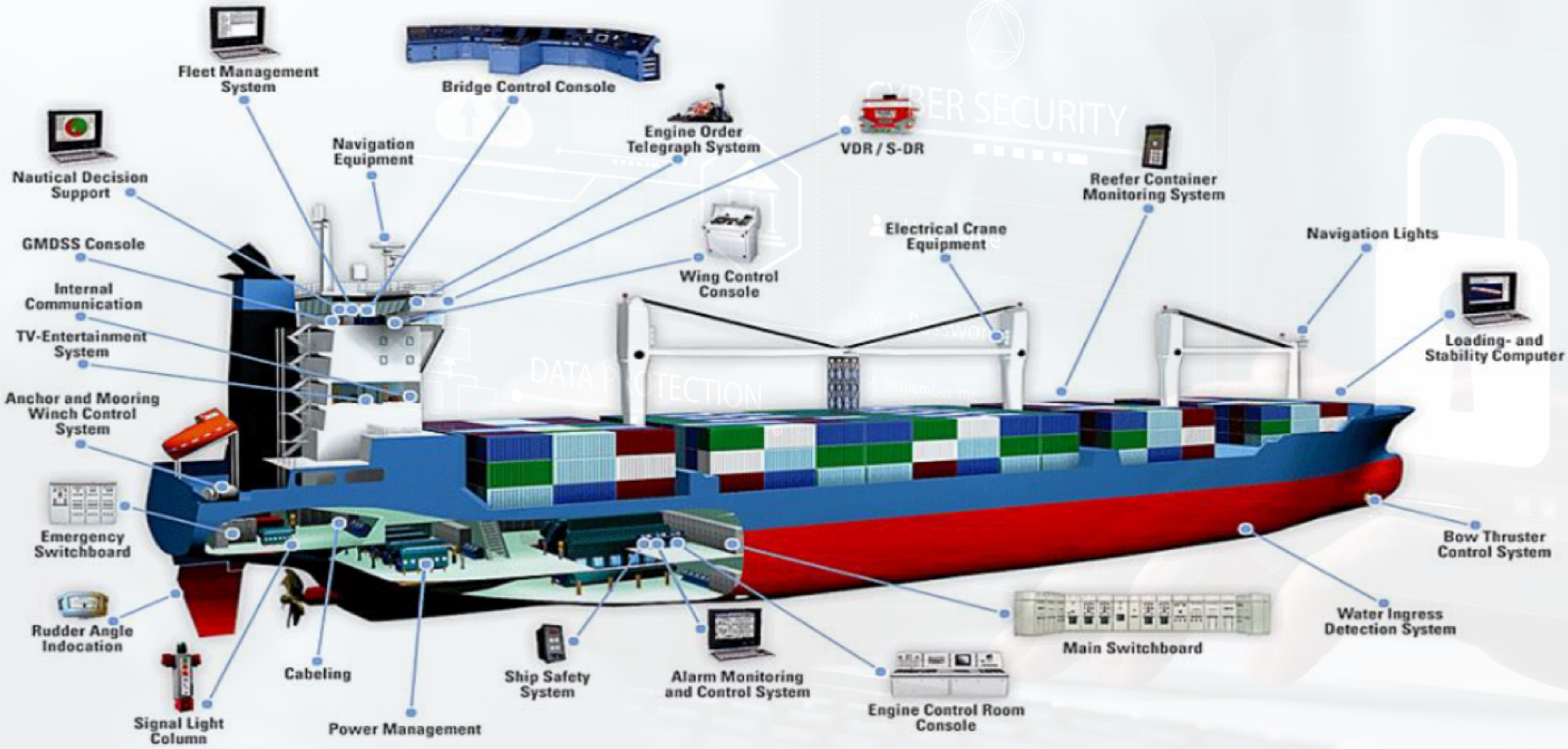
CIBER SEGURIDAD

COMPAÑIAS NAVIERAS

MARTÍN ROUSSEAUX

MARTÍN ROUSSEAUX

- SISTEMAS Y VULNERABILIDADES

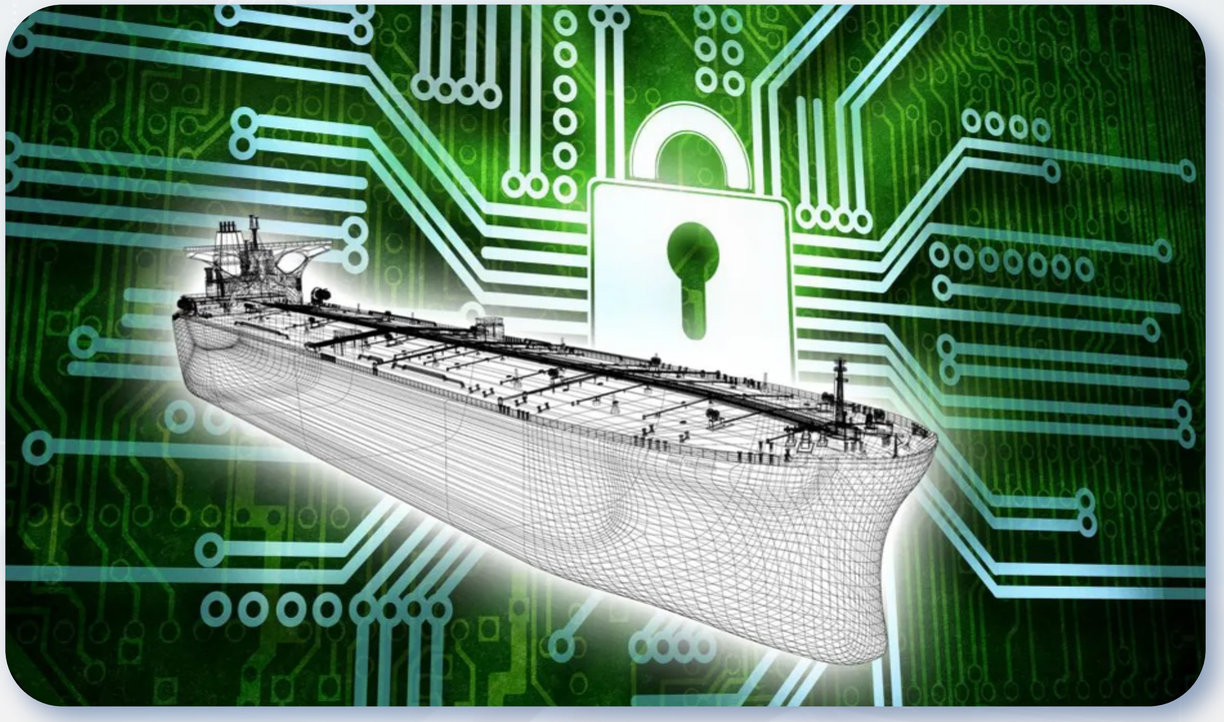


MARTÍN ROUSSEAUX

SISTEMAS Y VULNERABILIDADES

Los Ciber Incidentes están divididos en 5 grandes categorías:

- Sistemas de Ayuda a la Navegación (ECDIS y GPS)
- Sistemas de Seguimiento de Carga (Cargo Tracking)
- Automatic identification systems (AIS)
- Comunicaciones Satelitales
- Sistemas de Radar



Tecnologías que los Hackers han logrado explotar en buques en navegación:

- GPS (GPS Spoofing)
- Automatic Identification System (AIS)
- Electronic Chart Display and Information System (ECDIS)
- Mandatorio para los buques en navegación desde Julio 2018

MARTÍN ROUSSEAUX

TANKER MANAGEMENT AND SELF ASSESSMENT (TMSA)

- TMSA3 pone foco en los problemas de seguridad frecuentemente detectados en buques tanqueros marítimos.
- El Elemento 7 (Manejo del cambio) y el 13 (Seguridad Maritima) requieren que cada compañía marítima tenga desarrollados planes que consideren la Ciber Seguridad a bordo de los buques, en oficinas de tierra y en las comunicaciones entre ellos.
- El Plan de Ciber Seguridad debe atender las amenazas informáticas y las medidas de contención, procedimientos de respuesta y contingencia, manejo del cambio y análisis de riesgo

MARTÍN ROUSSEAUX

- **TMSA3 – ELEMENTO 13**

PROCESOS

sistemas de gestión
políticas, procedimientos
Manejo del proveedor / terceras partes
Régimen de simulacros y auditorías

GENTE

Higiene cibernética
Formación y concientización
Habilidades y calificaciones profesionales
Procedimientos escritos
Control de autorización
Seguridad física

TECNOLOGÍA

Antivirus
Cortafuegos
Sistemas de detección de intrusión
Actualizaciones de software, parches
Pruebas
Pruebas funcionales
Escaneo de vulnerabilidades
Prueba de penetración

CURSO

CIBER SEGURIDAD

TIPOS DE ATAQUES MÁS COMUNES

MARTÍN ROUSSEAUX

- TIPOS DE ATAQUES MÁS COMUNES

CIBERAMENAZAS

MENSAJES MALICIOSOS

CORREO NO DESEADO

- SPAM
- SPIM

FRAUDES Y EXTORSIONES

- HOAX
- PISHING
- INGENIERÍA SOCIAL

SOFTWARE MALICIOSO (MALWARE)

- VIRUS
- GUSANOS
- TROYANOS
- ADWARE
- SPYWARE
- RANSOMWARE

MARTÍN ROUSSEAUX

- **SPAM**

Correos enviados de manera masiva a muchos destinatarios. Contenido publicitario o comercial.

Consejos básicos y prevención

NUNCA responder al spam,
sólo les confirmas tu dirección

NO abrir ningún enlace,
pueden llevar a webs falsas
que recopilan información
sobre nosotros

Valorar bien dar nuestra
dirección a un concurso o sorteo

OJO al cancelar la suscripción

Buenas prácticas

No utilizar la misma dirección de correo
para todo

En caso de tener que hacer pública nuestra
dirección de correo evitar ser indexados
por los buscadores

- **SPIM**

Mensajes enviados de manera masiva a muchos destinatarios, pero a través de nuestros teléfonos.

Consejos básicos y prevención

Evita hacer público tu número de teléfono en redes sociales, foros o páginas web

No acceder a los enlaces que puedan aparecer en el mensaje

Buenas prácticas

Mantener actualizada la app de mensajería

Advertir a quien te lo ha mandado ya que su dispositivo puede estar infectado.

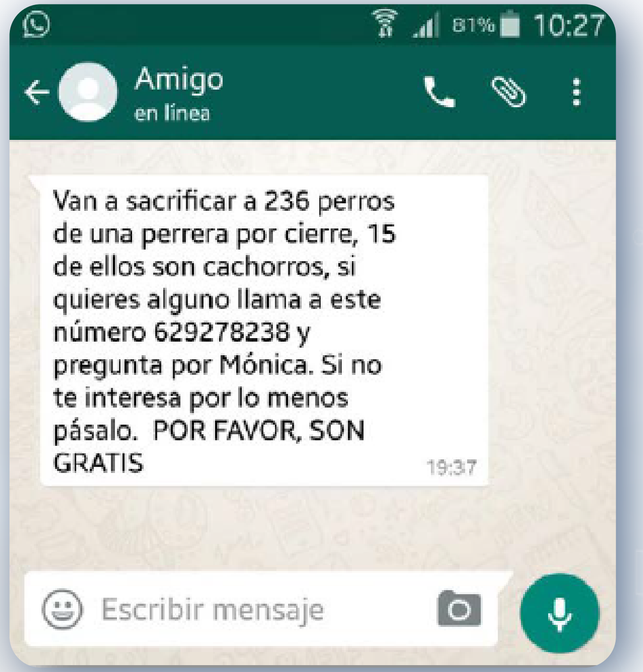
MARTÍN ROUSSEAUX

- **FRAUDES Y EXTORSIONES**

Técnicas de engaño con contenido falso y ventajoso que sirve de gancho para robarnos datos y/o dinero.

MARTÍN ROUSSEAUX

- **HOAX**



Señales de alarma

Se solicita reenviar el mensaje a tantas personas como sea posible
Se amenaza con consecuencias si se ignora esta solicitud
No se nombra la fuente que añadiría credibilidad a la noticia
o se da una fuente falsa.
No se citan detalles acerca del autor y el origen de la información
Información sobre el tiempo, como "la semana pasada" o "el día de ayer",
nunca se menciona un claro momento en el tiempo

En muchos casos de correo electrónico, la estructura del mensaje indica que se ha copiado y reenviado en numerosas ocasiones. Esto se puede reconocer porque el texto ya no tiene ningún formato o en el correo electrónico aparecen numerosos destinatarios.
Un hoaxes fácil de reenviar, pero no siempre es sensato hacerlo a ciegas.
Piénsatelo primero antes de reenviarlo, los engaños aprovechan la tendencia de los usuarios a preocuparse o a empatizar...

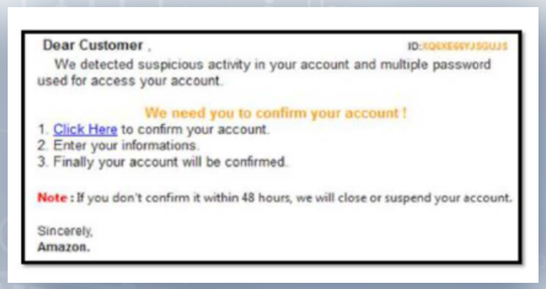
MARTÍN ROUSSEAUX

PHISING

El phishing es una amenaza en la que los atacantes utilizan mecanismos de ingeniería social con intención de engañarnos para que les revele mis datos confidenciales y puedan suplantar mi identidad en sitios web o transacciones financieras.

MARTÍN ROUSSEAUX

- **PHISING**



MARTÍN ROUSSEAUX

PHISING

El phishing es una amenaza en la que los atacantes utilizan mecanismos de ingeniería social con intención de engañarnos para que les revele mis datos confidenciales y puedan suplantar mi identidad en sitios web o transacciones financieras.
El objetivo del phishing es obtener datos (credenciales) o engañar al usuario para infectarlo.

MARTÍN ROUSSEAUX

INGENIERÍA SOCIAL

Se basa en interactuar con la víctima para ganarse su confianza. El fraude y el phishing utilizan técnicas de ingeniería social.

Los objetivos de la ingeniería social son:
Claves de acceso a cuentas y servicios (usuari@ y contraseña)
Datos personales o sensibles
Información bancaria: acceso a cuentas online, datos de tarjetas de crédito
Infectar un ordenador o dispositivo, para acceder a su información de forma remota.

Ejemplos:

- e mail para reactivar un servicio, una llamada mediante un sistema automático (una máquina que nos dice que nuestra tarjeta ha sido bloqueada y nos dan los pasos para desbloquearla)
- larga encuesta en la que se nos van preguntando datos personales
- memoria USB abandonada a posta en un lugar estratégico para infectar un ordenador y controlarlo de forma remota (BAITING)
- ventana que alerta sobre un fallo de seguridad en nuestro pc y ofreciendo la descarga de un software o un número al que llamar, además de pagar una cantidad de dinero para solucionarlo (timo del servicio técnico)

MARTÍN ROUSSEAUX

INGENIERÍA SOCIAL

Tácticas

Comportamiento agresivo o autoritario.
Comportamiento excesivamente amistoso
Intentos inusuales de establecer una relación.
No quieren que les devuelvas la llamada o que quieran verificar la identidad
Gente que está “apurada” o quiere información de manera “urgente”.
Gente que se hace pasar por proveedor, o empleados temporales, o contratistas.
Piezas incompletas de información y que intentan que Ud. complete el resto...
Afirmar algo que sabemos que es erróneo, con el afán de que los “corrijamos” para tomar esa información (conocido como “Mentira-Verdad”).

MARTÍN ROUSSEAUX

- # SOFTWARE MALICIOSO

Tipos de código dañino

Cuando se habla de código dañino o malware se está haciendo referencia a programas que se instalan en un sistema informático, normalmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los sistemas operativos, aplicaciones y datos de dicho sistema, o bien simplemente para molestar o perjudicar al usuario.

Cada día surgen nuevas muestras de malware susceptibles de mutar o transformarse adquiriendo nuevas funcionalidades y capacidades de ocultación. Aun así, se establece a continuación una clasificación básica sobre los tipos de malware más comunes que se pueden encontrar en el panorama actual

MARTÍN ROUSSEAUX

SOFTWARE MALICIOSO

VIRUS

- Código malicioso que tiene la capacidad de propagarse haciendo copias de si mismo.
- Efectos diversos según el tipo de virus que sea (ralentización del dispositivo, acciones inesperadas y autónomas en ellos o aplicaciones que se bloquean...)
- La fuente de infección puede ser a través de Internet o mediante un dispositivo externo.

GUSANOS

- Programa malicioso que también es capaz de replicarse a sí mismo y difundirse a través de la Red rápidamente.
- A diferencia de los virus no necesitan ser ejecutados por una persona.
- Su objetivo es infectar el mayor número de dispositivos posibles.
- Se utilizan para crear botnets(redes zombiesde dispositivos que se activan de manera simultanea para cometer ciberataques).

- # SOFTWARE MALICIOSO

TROYANO

Caballo de Troya, o troyano, es un malware que se presenta como un programa legítimo, pero que, al ejecutarlo, abre un acceso remoto a nuestro dispositivo. Es decir, no es algo que se acopla a algo nuestro sino que, directamente lo descargamos como un programa legítimo (parches, juegos, películas, etc...son su camuflaje perfecto).

Los datos que recoge se envían al atacante mediante el correo electrónico o se almacenan en un servidor en espera de ser utilizados para tomar el control de nuestro dispositivo (archivos, micrófono, teclado, webcam...)

Los troyanos se clasifican según el tipo de acciones que pueden realizar en nuestros dispositivos:

Backdoors
Keyloggers
Banker
PasswordStealer
Dialer
Cementery
Downloader
Botnets
Proxy

MARTÍN ROUSSEAUX

- # SOFTWARE MALICIOSO

ADWARE

Software malicioso que muestra publicidad no deseada. Además de molesto el peligro real del adwareestá en que puede cambiar los resultados de nuestras búsquedas con el propósito de llevarnos a sitios no legítimos o incluso infectadas con otros tipos de malware. Puede instalar barras de herramientas y manipular la configuración de nuestro navegador cambiando incluso la página de inicio.

Prevenirlo y eliminarlo:
Revisar periódicamente las extensiones instaladas en nuestros navegadores y tenerlo actualizado a las últimas versiones disponibles.
Revisar los últimos programas instalados y desinstalarlos
Si se cambia la lista de buscadores predeterminados eliminarlos y restaurar el nuestro.

MARTÍN ROUSSEAUX

- # SOFTWARE MALICIOSO

SPYWARE

Software malicioso creado pararecopilar información de nuestros dispositivos y enviársela a una tercera persona sin nuestro consentimiento (hábitos de navegación, historial y otros datos sensibles...)
bien para suplantar nuestras identidades o para utilizarlos con fines comerciales.
Actúa de forma silenciosa porque su finalidad es recoger cuanta más información mejor.
Llegan a través de mensajes de correo, de descargas de la Web, ocultos en otros programas
o tras hacer click en ventanas de publicidad.

Prevenirlo y eliminarlo:

Revisar periódicamente los iconos de nuestra bandeja del sistema.
Revisar los últimos programas instalados y desinstalarlos.
Si se cambia la lista de buscadores predeterminados eliminarlos y restaurar el nuestro.
Utilizar programas de confianza y actualizarlos periódicamente.

MARTÍN ROUSSEAUX

• SOFTWARE MALICIOSO

	Qué es	Daños provocados	Prevención
VIRUS	Infecta a otros archivos o programas.	Daños en el equipo, borrado o manipulación de archivos.	Cuidado a la hora de usar USB externas o descargar archivos.
GUSANOS	Se replican a sí mismos y se propagan solos.	Usados para crear botnets, redes de dispositivos zombies.	Evitar descargar adjuntos no solicitados.
TROYANOS	Crean puertas traseras por donde entrar y controlar el equipo en remoto.	Robo de información y control de webcam, teclado, micrófono...	Instalar antimalware que pueda deterctarlos y realizar análisis periódicos.
ADWARE	Muestra publicidad no deseada y altera búsquedas.	Manipula resultados de búsquedas y lleva a págs. alteradas o a la descarga de malware.	Evitar instalar programas de páginas o tiendas no oficiales.
SPYWARE	Recopila información de las personas usuarias.	Recopila información sobre hábitos de navegación, programas instalados o datos sensibles.	No aceptar cuadros de diálogo que aparezcan al navegar.

MARTÍN ROUSSEAUX

- # SOFTWARE MALICIOSO

RANSOMWARE

Software malicioso capaz de “secuestrar” nuestros dispositivos y/o archivos mediante del cifrado de datos, y solicita un rescate para descifrarlos.
Es un tipo de extorsión económica que afecta a todo tipo de dispositivos; ordenadores, smartphones,
Tablets e incluso a los que incorporan el llamado “Internet de las cosas” (wearables, electrodomésticos, coches...)
Los ganchos son entidades o empresas destacadas (Correos, Amazon, entidades bancarias...)
que nos ofrecen campañas y acciones que bien pudieran ser lícitas. Es decir, se basa en una combinación
de correo electrónico malicioso, phishing y mucha ingeniería social.

MARTÍN ROUSSEAUX

- **SOFTWARE MALICIOSO**

CURSO

CIBER SEGURIDAD

COMO PROTEGER MIS DATOS

MARTÍN ROUSSEAUX

MARTÍN ROUSSEAUX

COMO PROTEGER MIS DATOS

Gran parte de las amenazas que pueden afectar a la seguridad de nuestros datos y dispositivos depende de la precaución (actitud + aptitud) que tengamos mientras realizamos las tareas más comunes; correo electrónico, navegar por internet, banca electrónica, redes sociales, etc...

Acciones que podemos realizar las personas para reforzar esa actitud de cautela y precaución:

Autenticación Segura
Copias de seguridad y Cifrado de Datos
Herramientas específicas

AUTENTICACIÓN SEGURA

Algo que tú sabes (nombre de usuari@ y la contraseña).

Doble autenticación:

- Me envíe un SMS al móvil
- Me envíe una clave por email

Aplicaciones de terceros:

- Google Autenticator
- Microsoft Autenticator, ...

Algo que tú tienes; llaves criptográficas (TitanKeys)

Algo que tú eres

- Huella dactilar
- Reconocimiento facial
- Iris, ...

MARTÍN ROUSSEAUX

- # AUTENTICACIÓN SEGURA

Contraseñas seguras

Las contraseñas son las llavesque dan acceso a nuestros servicios, y por ende a nuestra información personal,por lo que si alguien las consigue puede comprometer nuestra privacidad, pudiendo, entre otras cosas; publicar en nuestro nombre en redes sociales, leer y contestar a correos electrónicos haciéndose pasar por nosotros, acceder a nuestra banca online, etc.

SEGURAS Y ROBUSTAS

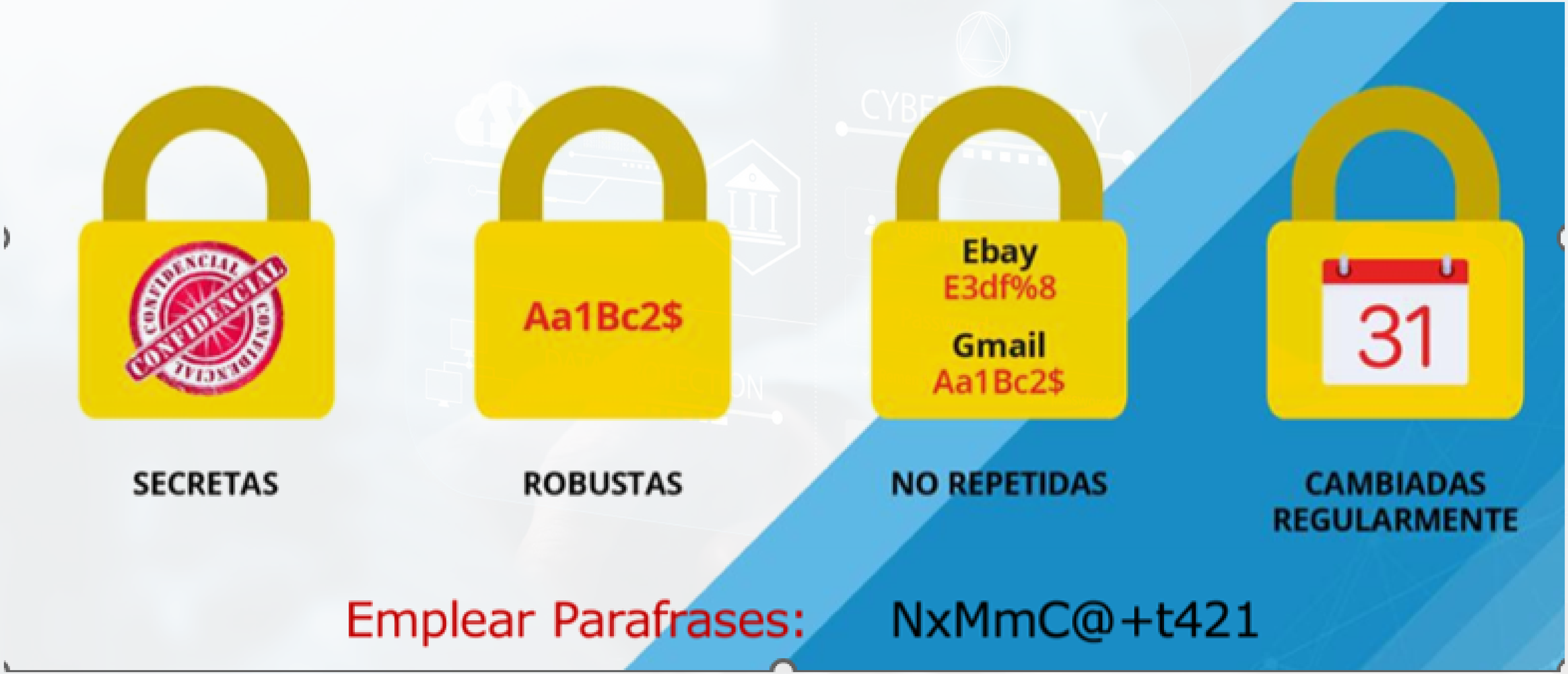
DOBLE AUTENTICACIÓN

GESTORES DE CONTRASEÑAS

KeePass
LastPass
1Password
bitwarden

MARTÍN ROUSSEAUX

- **AUTENTICACIÓN SEGURA**



MARTÍN ROUSSEAUX

CONTRASEÑAS COMPLEJAS

Las contraseñas complejas poseen las siguientes características:

- No contienen información personal (como ser nombres de familiares, mascotas, hobbies, o intereses personales, etc.)
- Contienen tanto letras mayúsculas (AABBCC...) así como minúsculas (aabbcc...) del alfabeto en cualquier combinación (Ej. ABftDaL)
- Tienen al menos un numero (0-9) y un carácter especial (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./), adicional a las letras mayúsculas y minúsculas mencionadas anteriormente.
- No contienen palabras ofensivas en ningún lenguaje (incluidos lunfardos, dialectos, términos obscenos, etc.)

MARTÍN ROUSSEAUX

ACTIVIDADES PROHIBIDAS RELACIONADAS A LAS CONTRASEÑAS

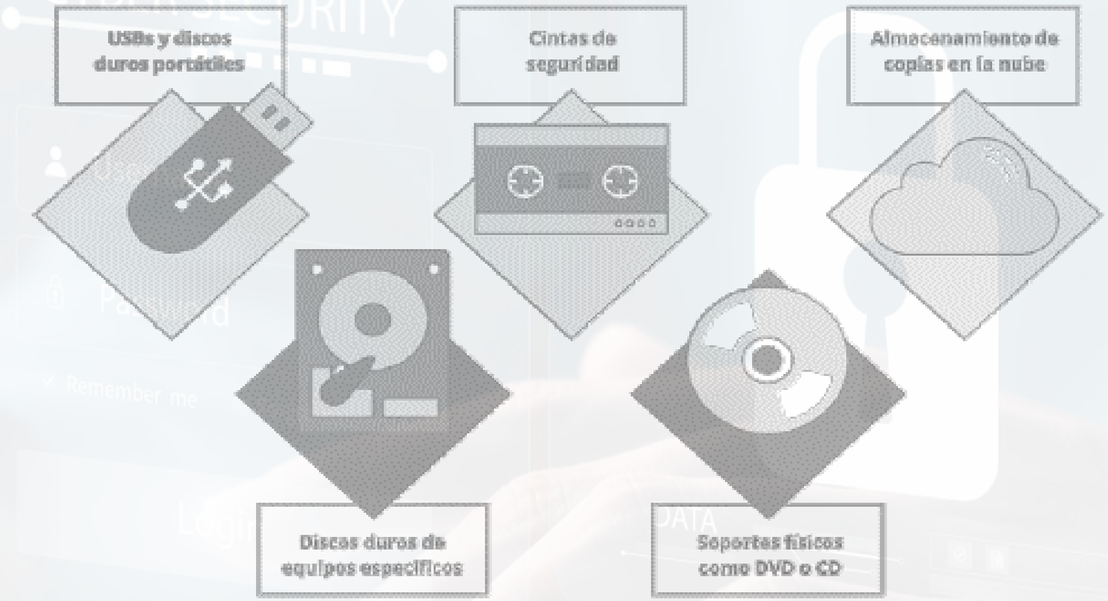
- Revelar o compartir contraseñas por teléfono con otras personas, incluidas personas que se declaren o pertenezcan al departamento de Soporte Técnico o HelpDesk.
- Revelar o compartir contraseñas por mensajes de correo electrónico.
- Hablar de contraseñas propias en frente de otras personas.
- Insertar contraseñas en mensajes de correo electrónico u otros con formato de formularios electrónicos u otras formas de comunicación.
- Crear contraseñas utilizadas en la Compañía que sean las mismas utilizadas en las cuentas de acceso en la vida personal.
- Revelar contraseñas en cuestionarios o formularios de seguridad.
- Revelar contraseñas a compañeros laborales en periodos de ausencia o vacacionales.
- Utilizar la funcionalidad de “recordar contraseña” disponible en aplicaciones (por ejemplo, Internet Explorer, Yahoo, Gmail, Outlook, etc..).
- Escribir contraseñas en papel o recordatorios visibles.
- Guardar contraseñas en archivos o en CUALQUIER dispositivo electrónico (PDA, Palms, Teléfonos inteligentes, entre otros) sin utilizar un método de encriptación adecuado.

MARTÍN ROUSSEAUX

COPIAS DE SEGURIDAD

Los datos son nuestro gran tesoro y el objetivo último de todos los ataques en Internet, es lógico que tengamos especial cuidado en "tenerlos a buen recaudo".

Existen soluciones mediante programas específicos para automatizar las copias de seguridad de nuestros dispositivos. También podemos hacerlas a mano, pero siempre debieran de ser en dispositivos o soportes externos ya que si, sufrimos un ataque o el dispositivo electrónico se pierde o inutiliza, nuestros preciados datos seguirán bajo nuestra custodia.



MARTÍN ROUSSEAUX

CIFRADO DE DATOS

Cifrar o encriptar información supone ocultar el contenido a simple vista, de modo que para acceder a esos archivos, carpetas, unidades, mensajes, etc...sea necesario realizar una interacción concreta.

Se hace mediante la aplicación de un algoritmo matemático. Esto no es nuevo y ya existía desde hace 2.500 años

El cifrado, por tanto, es el elemento más importante de la seguridad de datos y la manera mas simple de impedir que alguien robe o lea la información de un sistema digital con fines malintencionados.

MARTÍN ROUSSEAUX

- # HERRAMIENTAS

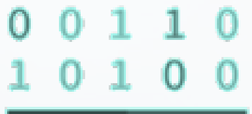
Existen también herramientas que nos ayudan a proteger nuestros dispositivos (ordenador, smartphone, tablet) para que nuestras vidas digitales sean lo más seguras posibles.

La instalación de programas puede afectar al rendimiento y la seguridad de los dispositivos/equipos ya que, de hecho, son la vía de entrada de malware. Por ello, se recomienda:

Utilizar software legal y actualizado,
no ejecutar a la ligera programas de origen desconocido, y trabajar habitualmente en el sistema como usuari@ sin privilegios, no como “Administrador”

MARTÍN ROUSSEAUX

- HERRAMIENTAS



FILTRADO

Entrante y saliente de contenidos maliciosos

PROTECCIÓN

Protección en el correo electrónico, en la navegación y en las conexiones de todo tipo, en redes profesionales o domésticas

ANÁLISIS

Análisis de los ficheros en dispositivos extraíbles como discos externos o memorias USB, y permitir programar análisis exhaustivos cada cierto tiempo

Malwarebytes

AdwCleaner

Spybot Search & Destroy

kaspersky

ESET

CURSO

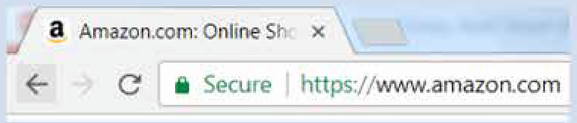
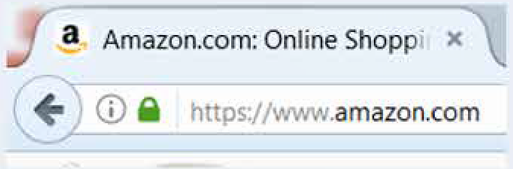
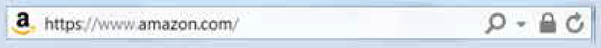
CIBER SEGURIDAD

RECOMENDACIONES

MARTÍN ROUSSEAUX

MARTÍN ROUSSEAUX

- # NAVEGACIÓN SEGURA

	Secure	Insecure
Chrome		
Firefox		
Internet Explorer		

MARTÍN ROUSSEAUX

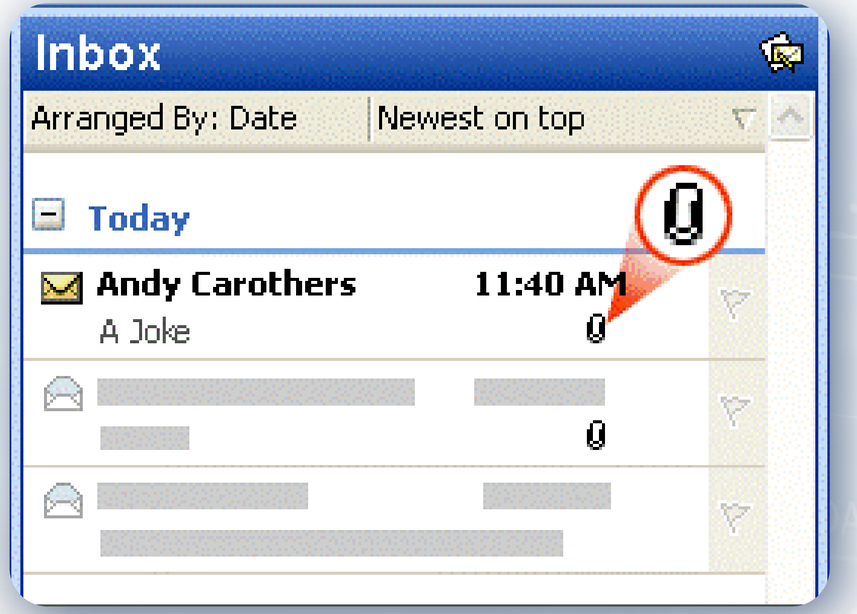
NAVEGACIÓN SEGURA

RECOMENDACIONES

- Acceder únicamente a sitios de confianza.
- Descargar los navegadores y programas desde los sitios oficiales. Mantenerlo actualizado.
- Personalizar la configuración por defecto del navegador; nivel de seguridad, permisos para notificaciones, ventanas emergentes, autocompletados,
- Borrar las ‘cookies’, historial de navegación y archivos temporales SIEMPRE en equipos ajenos y periódicamente en los nuestros.
- Evitar, en la medida de lo posible, las redes wifi públicas y abiertas son puntos peligrosos y con potenciales amenazas para la seguridad de nuestros datos. Borra los datos de la red tras utilizarla para evitar una conexión automática.
- En caso de necesidad, utilizar una red virtual privada (VPN), donde los paquetes de información van cifrados

MARTÍN ROUSSEAUX

- # EMAIL CORPORATIVO



Los archivos attachados a los mails son uno de los medios mas comunes por los cuales su computadora puede ser infectada

Debe sospechar y tener cuidado si:

El remitente es desconocido o incoherente
El titulo del mensaje es incohrente o extraño.

Si ud. tiene la sospecha que el mensaje esta infectado, deberia pedir confirmacion al remitente antes de abrirlo.

EN CAMBIO SI TIENE LA CERTEZA QUE EL MENSAJE CONTIENE UN VIRUS, DEBE ELIMINARLO Y LUEGO VACIAR LA CARPETA DE ELEMENTOS ELIMINADOS.

MARTÍN ROUSSEAUX

POLÍTICA DE UTILIZACIÓN DE LAS COMPUTADORAS E INTERNET

Uso aceptable de computadoras personales e internet:

- El acceso a Internet está específicamente limitado a las actividades correspondientes al negocio oficial de la Compañía.
- Adicionalmente al uso corporativo, la conexión a Internet puede ser utilizada para propósitos educacionales, entrenamiento o de investigación.
- Si algún usuario tiene dudas acerca del uso permitido por la Compañía deberá ser presentada al supervisor directo. De ser necesario, el Gerente o supervisor deberán consultar al Gerente de Sistemas acerca de los lineamientos de acceso.

MARTÍN ROUSSEAUX

POLÍTICA DE UTILIZACIÓN DE LAS COMPUTADORAS E INTERNET

Uso inapropiado de computadoras personales e internet:

- El acceso a Internet no debe ser utilizado para propósitos ilegales e ilícitos. Por ejemplo, la transmisión de contenidos amenazantes, violentos, fraudulentos, pornográficos, obscenos u otro material ilícito.
- El uso del e-mail de la Compañía u otro servicio de mensajería está limitado a actividades del negocio de la Compañía. Los servicios mencionados no deben ser utilizados para hostigar, intimidar o molestar a otra persona.
- No se permite el acceso a Internet con propósitos personales, de recreación, o alguna otra actividad no relacionada con la Compañía.
- La Intranet de la Compañía o el servicio de Internet no deben ser utilizadas para propósitos comerciales o políticos no referidos al negocio de esta.
- Los usuarios no deben intentar sortear o atentar contra las medidas de seguridad en la red de la Compañía o en alguna aplicación conectada o accesible a través de Internet.
- Los usuarios de la Compañía no deben hacer o utilizar copias ilegales del material de la Compañía, almacenar dichas copias en equipos de la Compañía o transferirlos electrónicamente por la red.

MARTÍN ROUSSEAUX

POLÍTICA DE UTILIZACIÓN DE LAS COMPUTADORAS E INTERNET

Formalidades en el uso de internet y e-mail:

- Los empleados de la Compañía deben asegurarse de que todas las comunicaciones por medio del e-mail de la Compañía son realizadas de manera profesional. El uso de lenguaje vulgar, obsceno o sugestivo está prohibido.

- Los usuarios de la Compañía no deben comunicar información privada por medio del correo electrónico de la Compañía sin la autorización pertinente y por escrito de la Gerencia.

- Los usuarios deben asegurarse de que los correos electrónicos son enviados únicamente a las personas que lo necesitan. La transmisión de e-mails a grupos, utilización de listas de distribución o el envío de mensajes con archivos adjuntos grandes (con tamaño superior a 5Mb) deberá ser evitada.

- Computadoras personales y uso de internet – seguridad:

- Los usuarios de la Compañía que identifiquen o perciban un problema de seguridad deberán contactarse inmediatamente con el Gerente de Sistemas.

- Los usuarios de la Compañía no deben revelar sus contraseñas o permitir la utilización de sus cuentas a otras personas. Asimismo, los usuarios no deberán utilizar cuentas de otros empleados de la Compañía.

El acceso a los recursos en la red de la Compañía deberá ser removido para los usuarios que hayan sido identificados en un problema de seguridad informática o que hayan demostrado un historial de problemas de seguridad informática.

MARTÍN ROUSSEAUX

REDES SOCIALES

Personalizar siempre nuestro perfil y la configuración de privacidad de todas las redes sociales.

No aceptar todo tipo de solicitudes de amistad. Ni permitir a las redes sociales que accedan a nuestra libreta de direcciones. Hemos de proteger también las direcciones de nuestros contactos.

Reflexionar sobre todo lo que publicamos; ahí queda.

No utilizar ni permitir apps de terceros dentro de ellas.

Ojo a los servicios basados en la localización y la información de nuestros Smartphone.

Precaución con los enlaces. Analízalos en caso de duda.

Escribir directamente la urlen el navegador para evitar que un sitio falso pueda robar nuestra información personal..

Utilizar contraseñas robustas y añadir un segundo factor de autenticación (2FA).

MARTÍN ROUSSEAUX

• ESPACIOS PÚBLICOS

Desactivar la sincronización: Son tareas que se desarrollan en segundo plano, sin la intervención del usuario. Es recomendable deshabilitar estos servicios cuando nos encontramos conectados a una red no segura.

Limpiar la lista de puntos de acceso guardados: Es conveniente revisar la lista de puntos de acceso memorizados para dejar únicamente aquellos que son confiables.

Navegar en páginas HTTPS: Siempre que estén disponibles, conectarse a páginas con certificado de seguridad.

Proteger la privacidad: Evitar realizar transacciones bancarias ni exponer datos de usuario y contraseña.

Desactivar la conexión WIFI: Una vez fuera del alcance de nuestras redes WIFI de confianza, se debe deshabilitar la opción de conexión automática.

Antivirus: Instalar un software antimalware que pueda detectar y bloquear intentos de ataques.

Parches de seguridad: Las aplicaciones y los servicios pueden contener fallos de seguridad que un atacante utilizará para ganar acceso a nuestro equipo. Los fabricantes de software están constantemente lanzando actualizaciones que deben ser instaladas lo antes posible.

CURSO

CIBER SEGURIDAD

MARTÍN ROUSSEAUX

• ESCRITORIO SEGURO

Se trata de que el escritorio sea SEGURO, no sólo limpio.
Clean Desk significa que cuando el mismo no está en uso, toda la documentación y equipamiento esté guardada en un lugar seguro.

Qué proteger:

Material impreso. Papeles importantes con datos confidenciales.

No guarde nunca sus contraseñas en cuadernos
o Post-it pegados en el monitor!

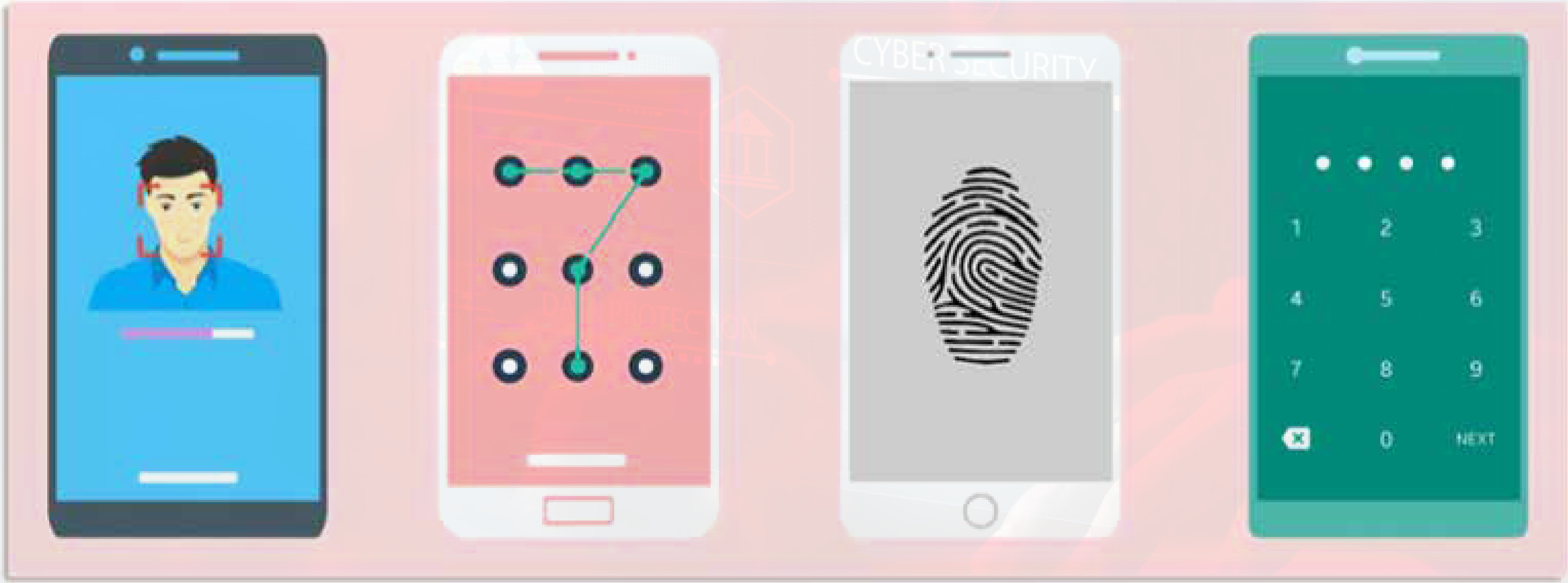
Medios electrónicos (USB, CD-ROM, discos rígidos externos, etc.)

Dónde:

En armarios, gabinetes, cajones, en cualquier lugar
QUE TENGA LLAVE.

MARTÍN ROUSSEAUX

- # DISPOSITIVOS MÓVILES



MARTÍN ROUSSEAUX

CONTROL DE ACCESO A PUERTOS USB

A fin de mitigar el riesgo por el uso no controlado y/o no autorizados de dispositivos USB, se bloquearán los accesos a todas las computadoras instaladas a bordo por medio de dispositivos mecánicos y/o por software.

Esta medida alcanza a las computadoras conectadas en red, a las que dan soporte a sistemas operativos y a todo dispositivo o sistema operativo que cuente con puertos USB (ejemplo: ECDIS)

Responsabilidades:

- El Capitán será el responsable por velar que todos los puertos USB se encuentren debidamente bloqueados (sea por bloqueo físico o por software).
- Los Oficiales de Guardia son responsable por verificar que los puertos USB de los equipos instalados en su área de trabajo se encuentren bloqueados (física o por software) durante su periodo de guardia. Deberá notificar al Capitán en caso de detectar un desvío.

MARTÍN ROUSSEAUX

CONTROL DE ACCESO A PUERTOS USB

Procedimiento:

- A bordo de dispondrá de una llave única para permitir el retiro de los dispositivos mecánicos de bloqueo de puertos USB cuando tareas de mantenimiento o actualización de los sistemas así lo requieran.
- La llave para retirar el bloqueo mecánico / físico siempre debe estar en poder del Capitán.
- Finalizada la tarea en curso, se deben bloquear físicamente los puertos USB o avisar al Departamento de IT para restaurar el bloqueo por Software (en caso de que aplique).

MARTÍN ROUSSEAUX

- POR ÚLTIMO

PREVENIR

ANALIZAR

DESINFECTAR

MARTÍN ROUSSEAUX

- POR ÚLTIMO

PREVENCIÓN

Mantener actualizados firmware, sistema operativo y aplicaciones (sobre todo navegadores y software de seguridad) de nuestros dispositivos.

Copias de seguridad periódicas en diferentes almacenamientos no internos.

Particionar el disco duro para mantener separado sistema operativo y datos almacenados.

Cifrado de carpetas y archivos en nuestros discos duros. Esta acción y la copia de seguridad cobra especial importancia en el Ransomware.

Atención especial para identificar posibles mensajes maliciosos, sobre todo phishing, en nuestro correo o apps de mensajería instantánea. No descargar cualquier adjunto no esperado ni abrir sin analizar.

Borrar periódicamente el historial y datos de navegación, así como los archivos temporales y, si detectas algo extraño...¡desconecta de internet y ANALIZA!.

MARTÍN ROUSSEAUX

- POR ÚLTIMO

ANÁLISIS

En todo dispositivo debemos tener unos programas básicos de seguridad; firewall o cortafuegos que impida conexiones no permitidas, antivirus actualizado para realizar diferentes tipos de análisis y un antimalware.

Si tenemos sospecha de algún tipo de ataque, realizar análisis online con alguna herramienta diferente a la que tenemos instalada (una segunda opinión...)

En caso de tener duda con algún enlace, analizar la URL para ver su legitimidad

MARTÍN ROUSSEAUX

- POR ÚLTIMO

DESINFECCIÓN

Si los análisis nos reportan infección por algún tipo de código malicioso proceder a su desinfección o puesta en cuarentena de los datos afectados.

Si, por el contrario, hemos sufrido algún tipo de ciberataque en el que nuestros datos personales, nuestra identidad digital o nuestros dispositivos se han visto afectados ponernos en contacto con el área de sistemas