Formación Ciberseguridad

Contenido

1. ¿Qué son los ciberataques y ciberdelincuentes?
2. Tipos de ataques
3. Qué es INCIBE
4. Concienciación ante esta nueva manera de agresión
5. Buenas prácticas para evitar ciberataques
6. Donde denunciar un ciberataque
7. Fake news
8. Compras online y otros tipos de fraudes
9. Protección de Irongate
10. Protección de Google Workspace

Ciberataques

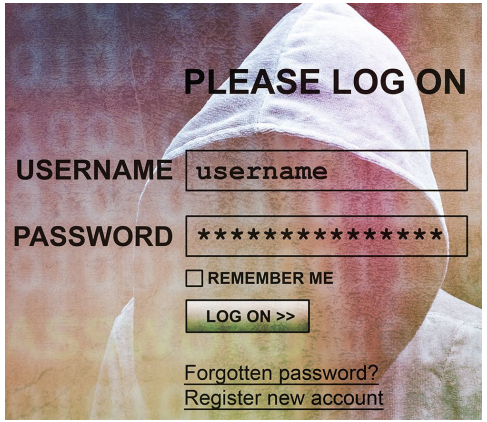
Los **ciberataques** son acciones malintencionadas llevadas a cabo por **ciberdelincuentes** que buscan acceder, dañar o controlar sistemas informáticos, redes y dispositivos electrónicos sin autorización. Como trabajadores, es crucial estar informados sobre los ciberataques y adoptar **buenas prácticas**, como el uso de **contraseñas seguras**, la **actualización de software** y la formación en **concienciación sobre ciberseguridad**, para mantener la seguridad de la información y proteger los activos digitales.

Ciberdelincuentes

Los **ciberdelincuentes** son individuos o grupos que realizan **acciones delictivas** en el entorno digital, como el robo de información o la manipulación de sistemas informáticos. Estos delincuentes pueden estar impulsados por diversos motivos, incluyendo **beneficios económicos, extorsión, venganza** o **ideologías políticas y religiosas**. Para enfrentar estos ataques, es esencial la formación y concienciación sobre ciberseguridad y la adopción de medidas preventivas.

Tipos de ataques

Ataques a contraseñas



- **Fuerza bruta:** los atacantes comienzan a hacer combinaciones de datos personales, nombres, números hasta que logran encontrar las contraseñas.

- **Por diccionario:** utilizan un conjunto predefinido de palabras o frases comunes y contraseñas comunes, para intentar averiguar una contraseña.

Tipos de ataques

Ingeniería Social

Técnicas dirigidas a los usuarios basadas en **engaños y manipulación** con el fin de **tomar el control de nuestros dispositivos**. Entre los más comunes, encontramos:

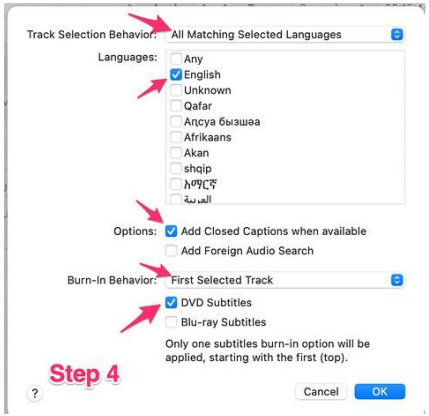
- Phishing, Vishing y Smishing
- Bating o Gancho
- Shoulder surfing o mirando por encima del hombro
- Dumpster Diving o rebuscando en la basura
- Spam o correo no deseado
- Fraudes online

Tipos de ataques

Ataques a conexiones

Son muy comunes y los ciberdelincuentes se sirven de softwares y herramientas con las que **saltarse las medidas de seguridad** e infectar o **tomar control de nuestros dispositivos**. Generalmente, este tipo de ataques se basan en interponerse en el intercambio de información entre nosotros y el servicio web para monitorizar y robar datos personales

- Redes trampa (Wifi falsas)
- Spoofing o suplantación
  - IP Spoofing y Web Spoofing
  - Email Spoofing y DNS Spoofing



Tipos de ataques

Ataques a cookies

Como sabemos las cookies son pequeños ficheros que contienen información de las páginas webs que hemos visitado. Las cookies nos ayudan a navegar de forma más rápida, recordando esta información para no tener que volver a procesarla. Estas son atacadas con el fin de **robar identidad y credenciales**, modificar datos y **robar datos sin nuestra autorización**. Aquí encontramos:

- Ataques DDos
- Inyección SQL
- Man in the middle o ataque de intermediario
- Sniffing

Tipos de ataques

Ataques por malware

Los ataques por malware se sirven de programas maliciosos cuya funcionalidad consiste en llevar a cabo **acciones dañinas en un sistema informático y contra nuestra privacidad**. Generalmente, buscan **robar información**, causar daños en el equipo, obtener un **beneficio económico** o **tomar el control** de su equipo.

- Virus, gusanos, troyanos
- Adware o anuncios maliciosos
- Spyware o software espía
- Apps maliciosas, Criptojacking y Rogueware o el falso antivirus

Fake news

Antes de todo:
Investiga la fuente de donde viene la noticia
Verifica quién es el autor del artículo.
Leé la noticia completa antes de compartirla
Realiza una búsqueda en Google para ver si la noticia está en otros medios de comunicación

Fake news (noticia falsa) es un **contenido pseudo periodístico** que se difunde a través de radio, prensa, rrss, televisión, etc con el objeto principal de **desinformar, manipular y desprestigiar a los implicados.**

¿Cómo se viralizan las noticias falsas?

- Medios de comunicación masivos
- RRSS
- Blogs, etc

Compras online

Otros tipos de fraudes:
Falsos préstamos
Falsos alquileres
Falsos soportes técnicos
Falsas ofertas de empleos
Sextorción, etc

Este tipo de fraude es cada vez más frecuente ya que realizar este tipo de compra nos da la libertad de realizarlas con comodidad, desde nuestra casa y sin agobios.
Sin embargo, debemos tener mucho cuidado al realizarlas, pues, podemos ser objeto de **estafas**.

Algunos tips a tener en cuenta:

- Desconfía de páginas que no son claras en los productos y servicios que ofrecen
- Accede a sitios seguros
- **Compra en páginas conocidas**

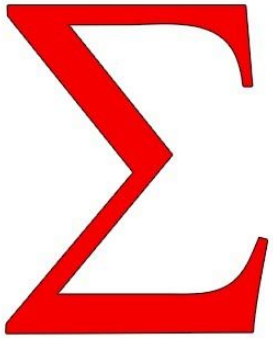
Algunas estadísticas

El cibercrimen crece en España y se profesionaliza en 2022

Los ciberataques aumentan en España y se especializan. El teletrabajo, la digitalización y el conflicto en Ucrania abren vías a los delincuentes para conseguir accesos en redes internas.

eadea

Algunas estadísticas



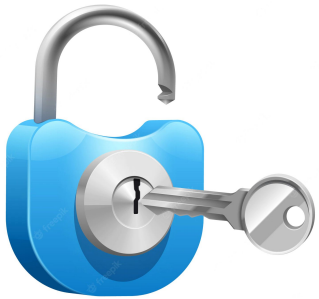
En los últimos 10 años, muchas empresas que forman parte de nuestra cotidianidad, han sido atacadas a nivel informático. Entre ellas podemos encontrar

- Facebook | Marzo 2019
- Cambridge Analytica | Marzo 2018
- Uber | Noviembre 2017
- Friend Finder | Noviembre 2016
- Elecciones en los Estados Unidos | Diciembre 2015

¿Qué es INCIBE?

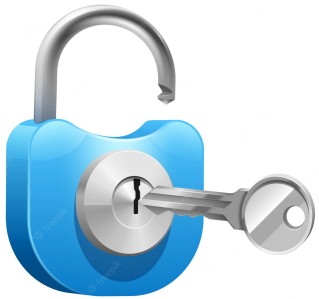
INCIBE es el Instituto Nacional de Ciberseguridad que trabaja para afianzar la confianza digital, elevar la ciberseguridad y la resiliencia y contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España.
Para mayor información, puedes consultar el siguiente enlace:
https://www.incibe.es

Concienciación ante esta nueva manera de agresión



Iniciamos este apartado comentando que la **ciberseguridad** es el conjunto de actividades que debemos llevar a cabo para **proteger** ordenadores, servidores, dispositivos móviles, **información confidencial**, redes, etc de fines maliciosos.

Sin embargo, podemos tener los mejores sistemas de protección, los más avanzados del mercado y podemos ser víctimas de un ciberataque… ¿Qué más podemos hacer? Aquí entra en juego **el usuario final que es nuestro último eslabón en la cadena de seguridad.**

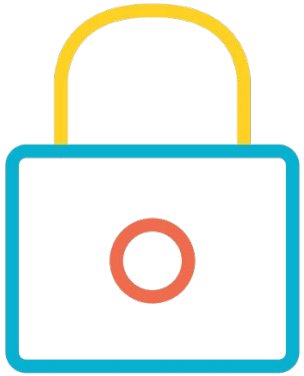


Debemos tomarnos muy en serio la ciberseguridad, pues, de esta manera, nos estamos protegiendo nosotros mismos y todo lo que nos rodea, además, **evitamos pérdidas económicas**, sobornos, chantajes y más.

Para que este eslabón sea lo suficientemente fuerte debe ser formado y concienciado de manera constante advirtiéndoles de los riesgos asociados a una mala praxis, tanto de dispositivos como de soluciones que se encuentren dentro de su alcance.

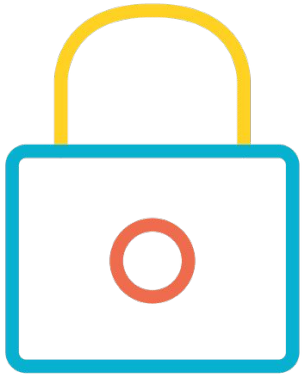
Afortunadamente, tenemos muchas maneras de protegerse de ciberataques y lograr una ciberseguridad óptima

Buenas costumbres para evitar ciberataques



Algunos puntos que tenemos que tomar en cuenta para evitar los ciberataques:

- Proteger todos nuestros equipos manteniendo sistemas operativos actualizados con las últimas versiones. Es sumamente importante la instalación de antivirus y programas de antimalware.
- Utiliza buenas contraseñas que tengan combinaciones de letras mayúsculas, minúsculas, números y caracteres especiales.



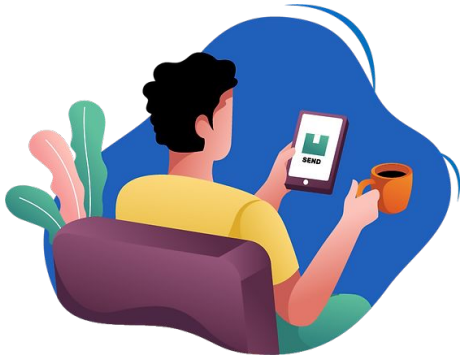
- No repitas las contraseñas entre gestión y gestión y cámbialas con frecuencia. No comentes a nadie de ellas.
- No descargues contenido de dudosa procedencia
- Haz copia de seguridad de tu información confidencial
- Comprobar que tus dispositivos están cifrados
- Si deseas descargar aplicaciones y programas sin riesgos hazlo siempre desde play store, app store y microsoft store, según sea tu caso.
- No hagamos uso de redes Wifi públicas o gratuítas. No son confiables.
- No abras ni email ni archivos adjuntos sospechosos.

¿Dónde denunciar un ciberataque?

- Se debe acceder al portal del Grupo de Delitos Telemáticos de la Guardia Civil.
- Llamar al 112
- Llamar a 091

Es importante denunciar este tipo de sucesos. De esta manera estamos siendo responsables como ciudadanos y evitaremos males mayores.

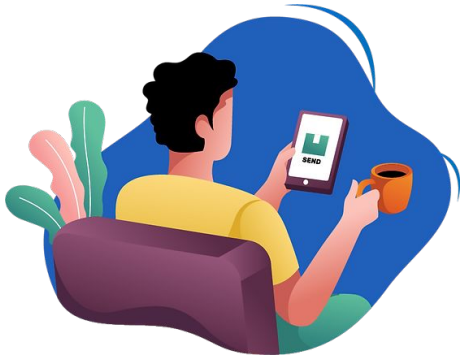
Ciberseguridad con Irongate



Irongate es un servicio proactivo que nos puede ayudar a proteger nuestros dispositivos y toda nuestra experiencia online.

Ellos en un conjunto de tecnologías de ciberseguridad dan un servicio MDR que proporciona prevención, detección y reparación de ataques avanzados, así como búsqueda de amenazas dirigida y basada en riesgos.

Esta protección está disponible tanto para ordenadores, servidores y dispositivos móviles.

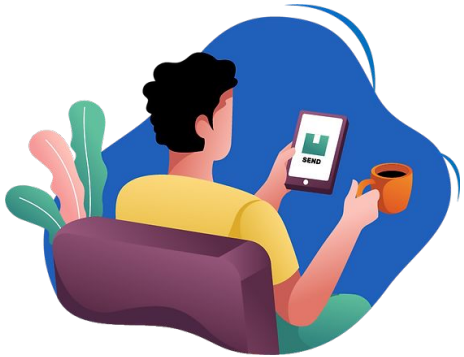


Irongate nos regala una guía de 10 pasos de ciberseguridad para vivir tranquilo.

1.- Activa el doble factor de autenticación. También llamado 2FA, es sin duda el mejor invento de seguridad de esta década y soluciona el 99% de los casos de robo de cuentas pero muy poca gente lo usa aún

2.- Instala un buen antivirus de pago tipo EDR (Endpoint Detection and Response) en móvil y ordenador. Los antivirus gratuitos, además de no ser fiables, realmente venden luego nuestros datos a otras empresas. No existe la "gratuidad".

3.- Si recibes un correo electrónico o llamada solicitando información personal o financiera, no facilitar ningún dato.

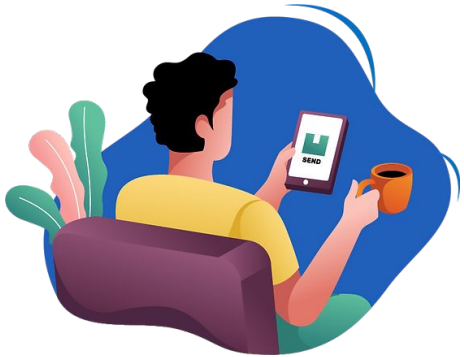


4.- Si el mensaje te invita a acceder a un sitio web, a través de un enlace adjunto, no entrar. El phishing es la entrada del 90% de las amenazas

5.- No acceder desde redes públicas. Todo lo que viaja por esa red puede ser visto por un delincuente en el medio de la comunicación.

6.- No descargar ni abrir archivos de fuentes no confiables. Evita el uso de aplicaciones bajadas de sitios no oficiales o piratas.

7.- Mantener actualizado el software de nuestros dispositivos, Tanto del sistema operativo como de las aplicaciones.



8.- Utiliza un gestor de contraseñas para crearlas complejas y no reutilizarlas en diferentes sitios.

9.- Date de alta en servicios de alerta de fuga de datos como https://haveibeenpwned.com/ o https://www.irongate.es/irongate-databreach y en cuanto te avisen cambia la contraseña de ese sitio. Si eres cliente de ironGate puedes estar tranquilo pues ya estás suscrito automáticamente. Todos nuestros servicios lo incluyen sin recargo.

10.- Cuando se trata de ciberseguridad la primera norma es “Estate tranquilo pero desconfía por defecto"

Si estas en entorno empresarial:

1.- Evita el BEC (Business Email Compromise) o Fraude del CEO donde una cuenta comprometida dentro de su propia empresa (del CEO o alguien similar en jerarquía) se usa para persuadir a alguien en el departamento de finanzas para que cambiar los detalles de la cuenta del destinatario justo antes de que venza un pago importante.

Cómo evitarlo:

Una de las mejores medidas que pueden tomar los individuos para evitar el engaño es confirmar telefónicamente que el supuesto remitente del correo electrónico sospechoso realmente envió la comunicación. Así de sencillo. Tu departamento financiero debe tener esa orden grabada a fuego.

2.- Nadie de la empresa, ni siquiera el departamento de IT, debería usar su equipo con derechos administrativos.

Cómo evitarlo:

El equipo de IT es el único que debería tener dos perfiles. El perfil de administrador para solo usarlo en momentos determinados donde se requiera de tareas de configuración y de mantenimiento de esa máquina y volver a su perfil de usuario restringido para el trabajo normal del día a día.

3.- Cifra el contenido del disco duro de los portátiles. Si te roban o pierdes tu portátil, por muy protegido que se encuentre mediante contraseñas, tiene sus datos accesibles. Solo es necesario sacar el disco duro y ponerlo como segundo disco de otro equipo

Cómo cifrarlo:

Tanto MacOS, Linux y Windows tienen sus propias utilidades de cifrado de disco. Solo debes activarlas y tus datos estarán a prueba de cualquiera que quiera leerlos. Ni las agencias gubernamentales son capaces de romper un cifrado estándar de 256 bits

Ciberseguridad con Google Workspace

Desde sus inicios Google Workspace ha trabajado activamente para garantizar que sus clientes estén bien protegidos. Su seguridad pasa por la encriptación de datos (información confidencial, fotos, mensajes de textos, y más). Además, posee una robusta infraestructura global, una cartera de profesionales expertos en seguridad y el constante afán innovador lo que hace que se mantenga a la vanguardia y ofrezca un entorno muy seguro, fiable y conforme con la normativa vigente.

Se nos hace importante resaltar la seguridad de Gmail y Drive, tomando en cuenta que son 2 de las herramientas que utilizamos con mucha frecuencia.

En cuanto a seguridad Gmail nos brinda:

- Protección de correos no deseados (spam)
- Protección en la suplantación de identidad (phishing)
- Navegación segura
- Gmail te advierte antes de que descargues un archivo adjunto que podría poner en riesgo tu seguridad.

- Seguridad de la cuenta. Supervisamos varias señales de seguridad a fin de proteger tu cuenta contra accesos sospechosos y actividad no autorizada
- Modo confidencial. Puedes hacer que tus mensajes caduquen después de cierto período de tiempo y quitar la opción que permite que los destinatarios reenvíen, copien, descarguen o impriman tu mensaje desde Gmail.

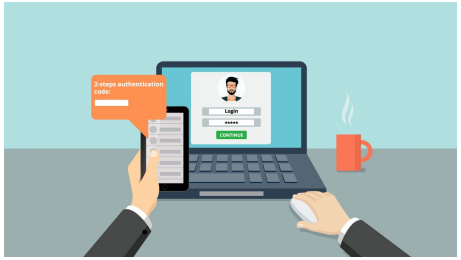
Drive nos brinda:

- Encriptación de tus archivos mientras se transfieren y cuando están almacenados en la nube.
- Realiza copias de seguridad automática

- Está relativamente a salvo del ransomware
- Y se de seguro está blindado contra robos
- Los archivos de Google Drive, se almacenan en los centros de datos seguros de Google. Google Drive cifra los datos en reposo en Drive y los datos en tránsito hacia y desde Drive.

Sin embargo, nosotros como usuarios también podemos ayudar a Google a asegurar aún más nuestras cuentas. Para esto debemos:

- Utiliza contraseñas únicas y seguras: es arriesgado utilizar la misma contraseña en varios sitios. Si te roban la contraseña de un sitio, podría usarse para acceder a tu cuenta en otros sitios



- Añade o actualiza las opciones de recuperación de la cuenta
- Activa la verificación en 2 pasos
- Activa los bloqueos de pantalla
- Mantén actualizado tu navegador, tus aplicaciones y el sistema operativo
- Evita correos, webs y solicitudes sospechosas
- En caso de que detectes actividad sospechosa en tu cuenta, sigue los pasos que necesarios para proteger tu cuenta
- No compartas tus contraseñas a nadie

Recuerda que nosotros como usuarios también podemos ser parte de la seguridad

Muchas gracias por formarte en ciberseguridad, si necesitas ayuda o tienes una pregunta contáctanos en www.eadea.net