MÓDULO

CIBERSEGURIDAD

ProtecCyL/CIM-BSE

Plan de promoción de la Autoprotección
Plano de promoção da Autoproteção

Junta de Castilla y León

Interreg
España – Portugal

Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia

SEGURIDAD DE LA INFORMACIÓN

- **¿Qué entendemos por seguridad de la información?:** Cuando hablamos de seguridad de la información nos referimos a **activos de información:** los datos, los equipos, las aplicaciones e incluso las personas que crean, gestionan, transmiten y destruyen la información.

- La **seguridad de la información** es un área que vela por el cumplimiento de los **parámetros que definen el nivel de seguridad** en una organización.

SEGURIDAD DE LA INFORMACIÓN

- ***La seguridad informática o ciberseguridad*** *se encarga de la protección de las infraestructuras TIC que soportan un negocio o sistema de información.* ***La seguridad de la información*** *abarca muchas mas áreas que las infraestructuras TIC.*

- *Por tanto, la* ***seguridad de la información abarca la*** ***seguridad informática o ciberseguridad***

SEGURIDAD DE LA INFORMACIÓN

- **Entonces, ¿Qué es la Ciberseguridad?:** Es la "**Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información interconectados**".

- La ciberseguridad pretende **proteger activos** como el software, hardware, redes, servicios o la propia infraestructura.

ProtecCyL/CIM-BSE
Plan de promoción de la Autoprotección
Plano de promoção da Autoproteção

Junta de Castilla y León

Interreg
España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia

EL PENTÁGONO DE LA SEGURIDAD DE LA INFORMACIÓN

Hay 5 parámetros que definen lo seguro que es un activo de la información.

Confidencialidad

A la información sólo pueden acceder las personas autorizadas para ello.

Disponibilidad

La información está lista para acceder a ella o utilizarse cuando se necesita.

Integridad

La información ha de estar completa y correcta en todo momento.

Trazabilidad

Poder asegurar en todo momento quien hizo que y cuándo lo hizo.

Autenticidad

La información es lo que dice ser o el transmisor de la información es quien dice ser.

CONFIDENCIALIDAD

- ***A la información sólo pueden acceder las personas autorizadas para ello:*** si una persona no autorizada accede a nuestra información podría hacer un mal uso de ella: la podría vender para obtener beneficios, denunciar a la organización ante la Agencia de Protección de Datos , dañar la imagen de la persona, distribuir información en redes sociales, etc..

INTEGRIDAD

- **La información ha de estar completa y correcta en todo momento:** La integridad garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea accidental o intencionada.

- Por ejemplo: Si se envían facturas a clientes con datos erróneos se genera confusión y queja de los usuarios lo que supone mas trabajo y tiempo para corregir los errores.

DISPONIBILIDAD

- **La información está lista para acceder a ella o utilizarse cuando se necesita:** En la actualidad el acceso a datos cada vez tiene que ser mas inmediata debido a las necesidades que se están creando. Un fallo de disponibilidad siempre tiene un impacto económico en una organización ya que afecta directamente al trabajo de los usuarios.

- Por ejemplo: Si una organización no tiene acceso a su programa de gestión en la nube no podrá gestionar pedidos, realizar ventas o consultar clientes propios para hacer gestiones.

AUTENTICIDAD

- **La información es lo que dice ser o el transmisor de la información es quien dice ser:** Es muy importante porque permite asegurar que la información, los datos y las transacciones en línea se realicen entre partes legítimas y confiables.

- Por ejemplo: Si tenemos documentos guardados con nombres erróneos o que indican que el documento es de un tipo y luego es de otro, generará confusión, pérdidas de tiempo y dinero, incluyo mala imagen ante clientes y proveedores.

TRAZABILIDAD

- **Poder asegurar en todo momento quien hizo que y cuando lo hizo:** Nos garantiza la posibilidad de conocer el origen, uso, recorrido y localización del dato. Muy Importante para el tratamiento de datos personales pudiendo saber que datos son tratados, quien participa en el proceso y quienes tienen acceso a ellos.

- Por ejemplo: En ocasiones una persona crea la información, otra la modifica y un tercero la envía, si se genera un error importante saber en que fase del proceso ha sucedido.

¿QUÉ ES UN CIBERATAQUE?

- **¿Qué entendemos por un ciberataque?: Cualquier tipo de acto delictivo** para cusar un daño, realizado a través de **sistemas informáticos o internet** contra entidades, instituciones o personas físicas.

- Las **Principales intenciones de un ciberataque** son robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital.

ProtecCyL/CIM-BSE
Plan de promoción de la Autoprotección
Plano de promoção da Autoproteção

Junta de Castilla y León

Interreg
España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia

VIRUS INFORMÁTICOS

Son programas maliciosos cuya finalidad es infectar archivos para causar daños. El virus introduce un código malicioso en los archivos que han sido infectados, el cual se propaga cada vez que se ejecutan estos.

SPAM O CORREO NO DESEADO

Son mensajes que el usuario no solicita, normalmente con un remitente desconocido y que suelen realizarse de forma masiva.

KEYLOGGERS
(INSTALACIÓN DE FICHEROS ESPÍAS)

Son programas que funcionan registrando la pulsación de las teclas o del ratón.

ARCHIVOS BOT

Su funcionamiento se hace de forma remota, sin que el usuario tenga conocimiento. Se utiliza en chats que suelen estar siempre abiertos y donde el usuario cree estar hablando con una persona real.

¿Cómo se realiza un ciberataque?

Hay múltiples maneras de realizar un ciberataque, estas son las más comunes.

SPOOFING
(SUPLANTACIÓN DE LOS REMITENTES DE CORREO)

Se realiza simulando la identidad de otro equipo para poder tener acceso a un tercero de la misma red.

TROYANOS (CABALLO DE TROYA):

Es un tipo de virus que funciona infectando al sistema a través de programas o archivos utilizados habitualmente.

ROOTKITS

Son un conjunto de herramientas que no pueden ser detectadas y que permiten al delincuente tener acceso al sistema, ocultando los procesos mostrando información falsa.

¿Cuáles son los efectos de un ciberataque?

ACCESOS NO AUTORIZADOS

Permite el acceso a personas no autorizadas a nuestro equipo pudiendo acceder a información confidencial o a la destrucción de datos.

ATAQUES POR DENEGACIÓN DE SERVICIO (DDoS)

Mediante este ataque el servidor es atacado desde uno (DoS) o múltiples equipos (DDoS), con el fin de que deje de dar servicio a toda la red.

SATURACIÓN DE CORREOS

Se realiza enviando emails de forma masiva para que el almacenamiento se sature y no puedan entrar los correos reales.

ROBO DE INFORMACIÓN

El objetivo es la sustracción de información personal y financiera. El más conocido es el llamado Phising, que veremos más adelante.

ANULACIÓN DE EQUIPOS

A través del envío de virus, el equipo puede quedar inutilizado para su funcionamiento.

EL FACTOR HUMANO

- **¿Qué es la ingeniería social?.:** Es el método utilizado por los **ciberdelincuentes**, para **acceder a información confidencial del usuario**, utilizando la manipulación, la persuasión y la confianza, y obtener acceso a los sistemas informáticos.

- Los **ciberdelincuentes** usan tácticas de ingeniería social para obtener datos personales, información financiera (credenciales de inicio de sesión, número de tarjeta de crédito, numero de cuentas bancaria). Usan esta información para la suplantación de identidad y realizar compras, o retirar dinero de las cuentas

ProtecCyL/CIM-BSE
Plan de promoción de la Autoprotección
Plano de promoção da Autoproteção

Junta de Castilla y León

Interreg
España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia

¿Cuáles son las técnicas mas utilizadas por los ciberdelincuentes?

PHISING:
Emails en los que se adjuntan archivos con malware o enlaces a una web falsa, para tener el control sobre el ordenador o establecer una falsa relación.
Pueden hacerse pasar por una entidad bancaria, alguna asociación a la que pertenezcamos o la policía.

CARTAS NIGERIANAS:
Mensajes falsos que, haciéndose pasar por alguien conocido, prometen una gran cantidad de dinero a cambio de ingresar una pequeña cantidad por adelantado.

CORREO ELECTRÓNICO:
Podemos recibir mensajes de remitentes conocidos, que han sido previamente suplantados por el atacante, y que confiando en ellos los abrimos. Por ejemplo, de la Policía o de Correos.

BAITING:
El delincuente deja en un sitio estratégico un dispositivo USB para que alguien lo encuentre y lo conecte a su equipo, produciéndose en ese momento la infección.

ATAQUE TELEFÓNICO:
El delincuente realiza una llamada a la víctima haciéndose pasar por otra persona, como puede ser un técnico de telefonía que nos solicita que le facilitemos la clave de nuestra wifi.

REDES SOCIALES:
Se puede obtener mucha información sobre una persona a través de sus perfiles sociales, pudiendo ser utilizada por un atacante.

BUENAS PRÁCTICAS

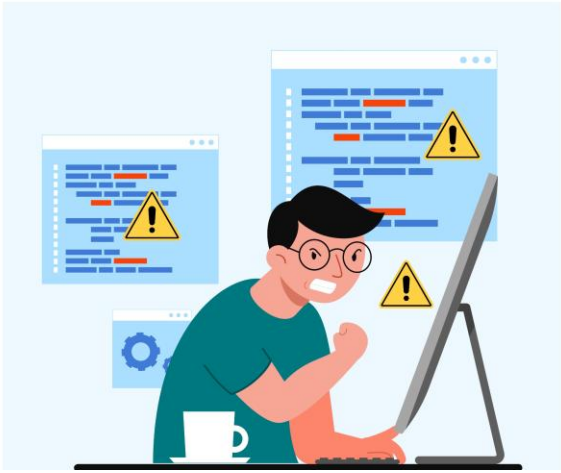
- **No revelar nunca por teléfono, email o RRSS ningún dato personal y confidencial** (números de tarjetas de crédito, claves de acceso, etc.)
- **Crear contraseñas difíciles de adivinar**. Es aconsejable que tengan al menos **8 caracteres alfanuméricos**, combinando mayúsculas, minúsculas, números y caracteres especiales.
- Utilizar **webs** que nos ayudan a crear contraseñas: **www.clavesegura.org**
- **No abrir ningún enlace a una página web en la que no confiemos**, (nos pueden redirigir) a otro enlace no deseado.
- **No abrir enlaces enviados desde un correo desconocido** (podría contener un virus).

BUENAS PRÁCTICAS

- **Asegurarse** de que la **web** a la que estamos accediendo es la correcta, especialmente en casos de banca electrónica.
- **Tener instalado en el equipo alguna medida de seguridad**, (antivirus y antimalware).
- **No confiar en correos** que nos indiquen que **hemos ganado algún premio** o que permiten hacer ganar dinero de manera fácil.
- **No dejarse intimidar por las amenazas** (es una técnica para manipular).
- Y por último, pero no menos importante, **usar siempre el Sentido Común**.

LA INGENIERÍA SOCIAL INVERSA

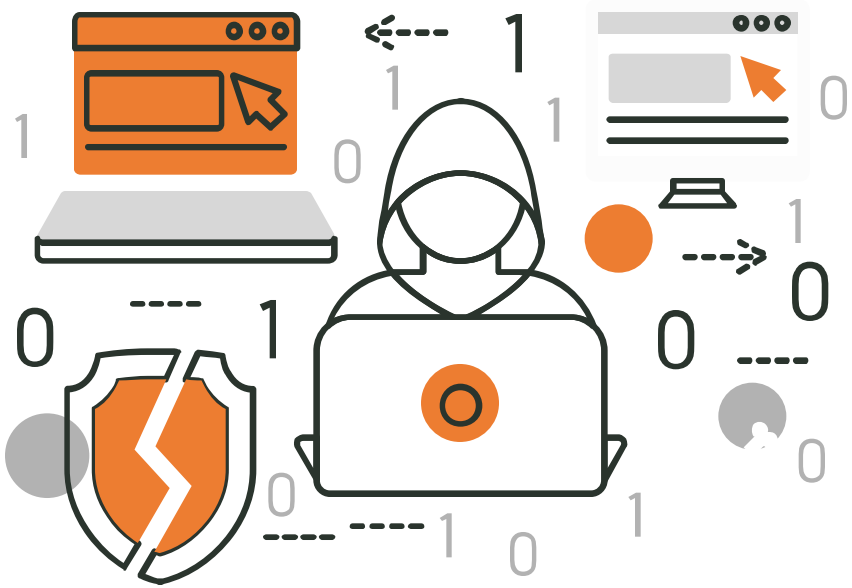
- Es una técnica **pasiva**, el atacante no actúa directamente sobre su víctima, sino que es **la víctima quien se pone en contacto con el delincuente** sin tener conocimiento de que está siendo estafada.
- El atacante va poco a poco consiguiendo la confianza de la víctima hasta que logra la información necesaria para obtener su fin.
- Por ejemplo: siendo un técnico que acude a ayudar cuando uno tiene un problema. Lo que la víctima no sabe es que el problema lo han causado a propósito para ganarse su confianza después yendo a repararlo.



MECANISMOS DE ATAQUE

- **HACKTIVISMO** o desobediencia civil electrónica es una forma de protesta no violenta que surgió en los ´80 y utiliza medios digitales no legales, con el fin de reivindicar algunos derechos como pueden ser ideas políticas, libertad de expresión o derechos humanos. .

- Su principal arma es el **ataque DDoS o de denegación de servicio** que consiste en atacar el servidor web de cualquier organización, provocando que deje de prestar servicio pudiendo llevar a la quiebra a la organización.



MECANISMOS DE ATAQUE

- **HOAXING** es el envío, de forma masiva, de mensajes sobre una broma o engaño sobre un falso virus o cualquier otro tipo de alerta. Su objetivo simplemente es molestar al mayor número posible de usuarios. Por ello solicitan que el mensaje sea compartido a nuestros contactos.

- Al no llevar ningún código malicioso no será detectado por el antivirus.

MECANISMOS DE ATAQUE

- **Phising Bancario** es la suplantación de la identidad del banco por el atacante. El usuario **recibe un correo electrónico fraudulento** solicitándole que realice alguna acción en su cuenta para hacerse con sus datos.

- Lo normal es incluir en el correo electrónico una URL del enlace donde indican hacer click, **no es a la que realmente nos dirigirá.**

- En la web en la que acabamos tendrá un aspecto casi idéntico a la original, pero al introducir los datos se los estaremos dando directamente a nuestro atacante.

MECANISMOS DE ATAQUE

- **Shoulder surfing:** Se trata de **espiar** a una persona mientras está introduciendo sus claves, ya sea bancaria, números PIN o cualquier otro dato personal con el fin de robar esa información confidencial y utilizarla de manera maliciosa. **El atacante se sitúa cerca de la víctima** ya sea en tiendas, al pagar por TPV, mientras usa su smartphone, al introducir sus claves etc.

MECANISMOS DE ATAQUE

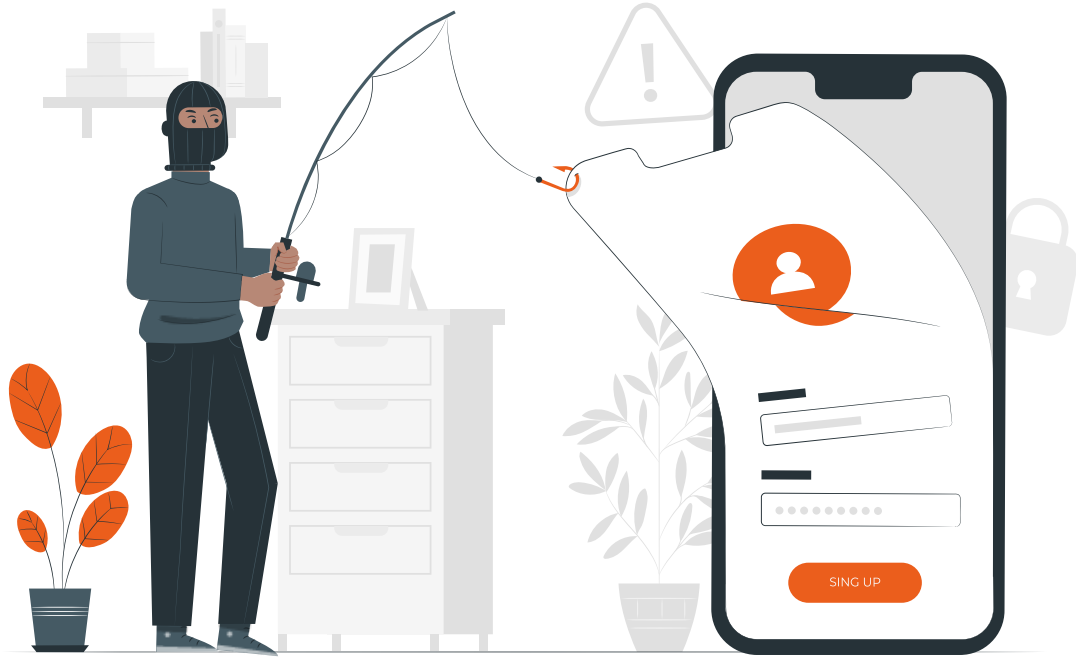
- **Tailgaiting: Violación de la seguridad**. Consiste en dejar **la puerta abierta** de una organización con el fin de que entren los atacantes y roben portátiles, dispositivos, discos duros, memorias USB etc.

- Debido al volumen de personal de muchas grandes empresas, no siempre se mantienen las medidas de seguridad adecuadas y los delincuentes se aprovechan acudiendo, por ejemplo, falsamente uniformados.

MECANISMOS DE ATAQUE

- **Vishing:** es una **variante del Phishing**, mediante el cual los atacantes conectan con el usuario por medio del **servicio VoIP**.

- La finalidad es la misma, engañar al usuario y, de esa manera, hacerse con información sensible



MALWARE Y OTRAS AMENAZAS

- Definimos **Malware o software malicioso** como un tipo de software que puede acceder a un dispositivo sin el consentimiento del usuario con la finalidad de infiltrarse o dañar el equipo.

- Desde que se creó hace más de 30 años, el malware se ha utilizado mediante varias formas de ataque: archivos adjuntos de correo electrónico, anuncios maliciosos en sitios web populares, instalaciones de software fraudulento, unidades USB y aplicaciones infectadas, correos electrónicos de phishing e incluso mensajes de texto.

Tipos de Malware

- **VIRUS INFORMATICOS:**
  - Son programas cuya finalidad es infectar el equipo a través de otro software que se instala al añadir el código malicioso.
- **GUSANO:**
  - Son programas que pasan de un equipo a otro como un gusano, a través de los correos electrónicos, chats, archivos P2P, redes locales, etc., propagándose a gran velocidad.
  - Una vez que el gusano está dentro del equipo intenta obtener las direcciones de otros equipos de la misma red, o de las listas de contactos de correo electrónico.
- **TROYANOS:**
  - Este malware no infecta los programas o datos del equipo, pero instala otros programas sin el conocimiento y consentimiento del usuario. Su objetivo es recolectar datos para alterar o destruirlos y usar el equipo para fines delictivos.

Tipos de Malware

- **SPYWARE:**
  - Capta la información sobre el usuario sin su autorización, como por ejemplo el contenido del disco duro, e instalan un código en el navegador de internet para redireccionar el tráfico abriendo páginas no solicitadas.
- **PHISIHG:**
  - Se propagan a través del correo electrónico donde se solicita al usuario datos confidenciales.
- **ADWARE:**
  - Se instalan en los softwares de distribución gratuita, y funcionan mostrando publicidad al usuario en la interfaz, pudiendo recoger datos personales del usuario.
- **ROOTKITS:**
  - Programas utilizados por los hackers para evitar ser detectados mientras intentan acceder a un equipo no autorizado. Acceden reemplazando archivos del sistema, o bien instalando un módulo kernel.

Otras amenazas:

- **GOOGLE HACKING:**
  - Técnica que explota la capacidad de almacenar información de Google mediante el uso de unos determinados operadores o palabras claves con el objetivo de encontrar información sensible.

- **INGENIERIA SOCIAL:**
  - Práctica de obtener información confidencial a través de la manipulación y el engaño de los usuarios. Mediante este estudio del comportamiento pueden obtener información que les permitan realizar algún acto perjudicial para la persona u organización.

- **ATAQUES POR DICCIONARIO:**
  - Es un método de cracking que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario.
  - Los ataques de diccionario tienen pocas probabilidades de éxito con sistemas que emplean contraseñas fuertes con letras en mayúsculas y minúsculas mezcladas con números (alfanuméricos) y con cualquier otro tipo de símbolos.
  - Sin embargo, se aprovechan de la dificultad de los usuarios para recordar tales y prueban con las más probables hasta dar con la correcta.

Otras amenazas:

- **METADATOS:**
  - Son datos que describen otros datos. Un grupo de metadatos se refiere a un grupo de datos, llamado recurso. Por ejemplo, en una biblioteca se usan fichas que especifican autores, títulos, casas editoriales y lugares para buscar libros. Así, los metadatos ayudan a ubicar datos.

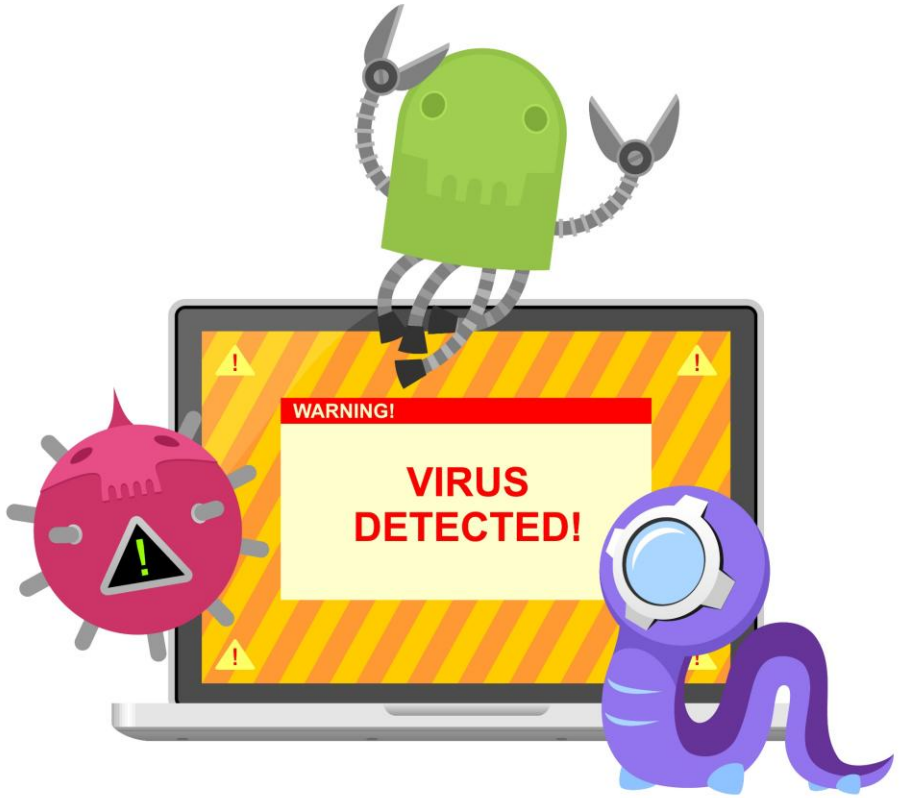
- **ATAQUES POR FUERZA BRUTA:**
  - Forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.
  - Un algoritmo que halla el juego de caracteres que se pueden utilizar en la clave. Estos ataques, dado que utilizan el método de prueba y error, son muy costosos en tiempo.
  - Esta técnica suele combinarse con un ataque de diccionario.

- **RED TOR:**
  - Proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones superpuesta sobre internet, en la que los mensajes entre usuarios son anónimos y que, además, mantiene la integridad y el secreto de la información que viaja por ella. Por este motivo se dice que esta tecnología pertenece a la llamada darknet (red oscura), deep web (web profunda).

COMO SUCEDE LA INFECCIÓN

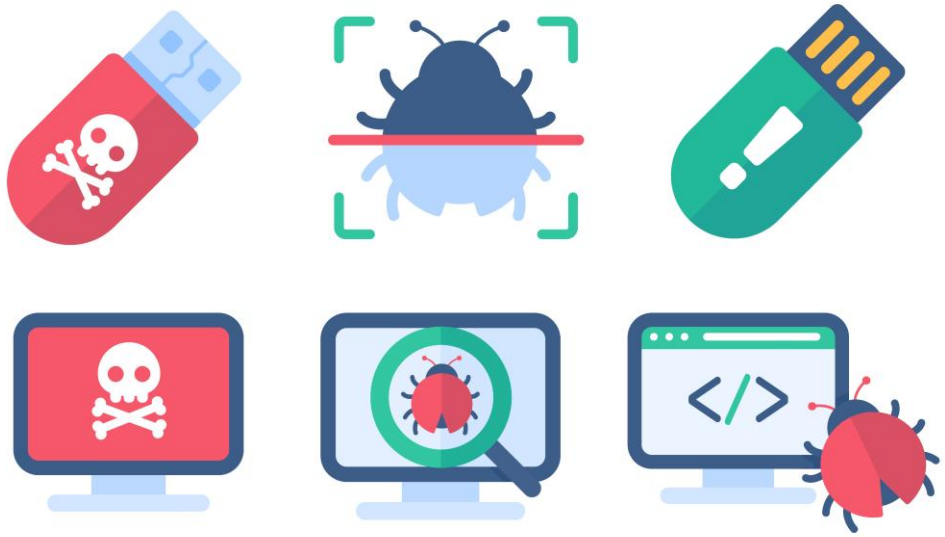
- Las dos grandes formas de propagación son los **virus** cuya instalación se hace por parte del usuario de forma inconsciente; y los **gusanos**, donde el programa malicioso se replica a través de las redes.

- En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos que dan la traza del problema y tienen que permitir la recuperación del mismo.



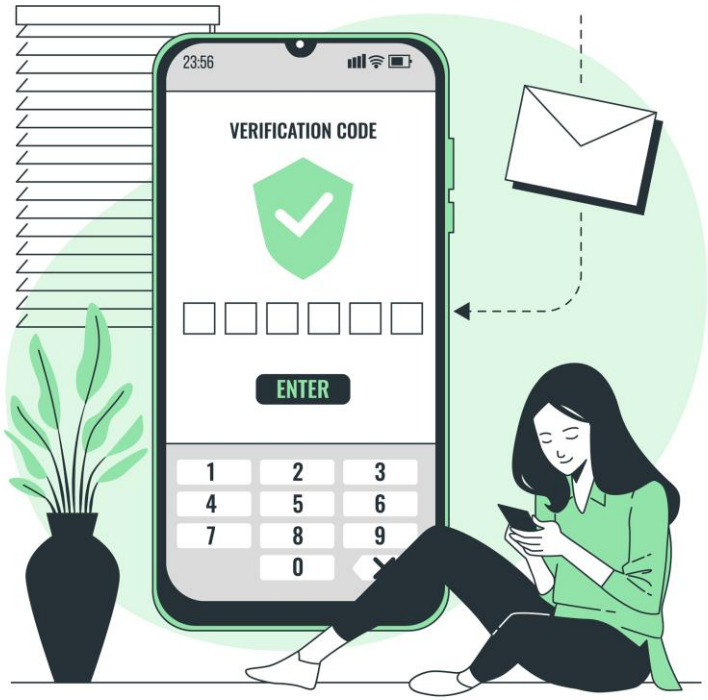
Contaminación por interacción del usuario:

- **Mensajes que ejecutan automáticamente programas,** como el programa de correo que abre directamente un archivo
- **Ingeniería social,** Mensajes como "ejecute este programa y podrá ganar un móvil última generación"
- **A través de unidades extraíbles de almacenamiento** de otros usuarios infectados
- **Instalación de software** que pueda contener uno o varios programas maliciosos



Tipos de códigos maliciosos para móviles:

- **TROYANOS SMS:**
  - Este tipo de amenaza busca suscribir a la víctima a números de mensajería SMS Premium sin su consentimiento.
- **TROYANOS TIPO BOOT:**
  - Buscan comprometer un dispositivo móvil para convertirlo en Zombie, de forma similar a los troyanos que lo hacen en los ordenadores.
- **TROYANOS QUE ROBAN INFORMACIÓN (SPYWARE):**
  - Roban información como fotografías, contactos, códigos de identificación MMC y MNC, mensajes de texto SMS, entre otro tipo de información.
- **PHISING O FRAUDES ELECTRÓNICO:**
  - Se suele propagar mediante un correo electrónico en el que se le indica al destinatario que deberá entregar determinados datos o su dispositivo tendrá problemas.
- **CÓDIGOS QR MALICIOSOS:**
  - Son un tipo de código de barras en dos dimensiones que facilitan el acceso a sitios web y otro tipo de información. Mediante su acceso el usuario aterriza en páginas maliciosas.



IMPACTO EN LAS EMPRESAS

- El impacto inmediato de las empresas es que un ataque puede **parar toda la producción** de la empresa en el momento y **por un tiempo largo** hasta que se limpian todos los equipos afectados.

- Si se filtra la información sobre clientes y usuarios, podemos tener problemas más serios: habría consecuencias legales, es decir, **sanciones** por incumplimiento de la Ley de Protección de Datos (acarrea duras sanciones económicas), pérdida de confianza de la organización y posibles **reclamaciones de terceros**.

- Muchas empresas se enfrentan a **pérdidas y desembolsos de dinero muy elevados después de un ataque de malware**: Ya sea por la extorsión de los ciberdelincuentes (robo de datos en los que se suele pedir un rescate para la recuperación de la información) por el coste de reparación de los dispositivos, por pérdidas de horas de trabajo, o por instalar nuevos sistemas de seguridad en la empresa.

ROBO DE CONTRASEÑAS

- El robo de contraseñas se refiere al robo de las **credenciales de inicio de sesión** de alguien, como nombres de usuarios y contraseñas. Los ciberdelincuentes utilizan esas credenciales para obtener **acceso a datos y cuantas bancarias**, lo que permite el robo de identidad y fraude financiero

- Actualmente el robo de contraseñas es una de las **principales causas** de la sustracción de datos en una empresa.

- Por este motivo es fundamental **usar contraseñas seguras y diferentes** para cada una de las cuentas de usuario que se tengan. Mucha gente usa variantes de la misma contraseña para así recordarlas con mayor facilidad, pero lo mejor es usar contraseñas siempre diferentes.

¿Qué es una contraseña robusta?

Una contraseña robusta es aquella que está creada para que sea difícil de descubrir por una persona o un programa, de manera que se asegure que solo el usuario autorizado puede acceder al equipo.

- **Consejos:**

- *Una longitud de al menos 8 caracteres. Cuanto mayor longitud, mas segura.*
- *Incluir letras mayúsculas y minúsculas, caracteres especiales y números.*
- *No aparecer el nombre, DNI, ni fechas relacionadas con el usuario.*
- *Utilizar doble factor de autenticación si es posible.*
- *Cambiar contraseñas cada cierto tiempo.*

- **Haz la prueba:**
- Entra en esta web (**www.clavesegura.org**) y prueba como de seguras son tus contraseñas.

Obligaciones a cumplir

Los usuarios tendrán una serie de obligación a cumplir:

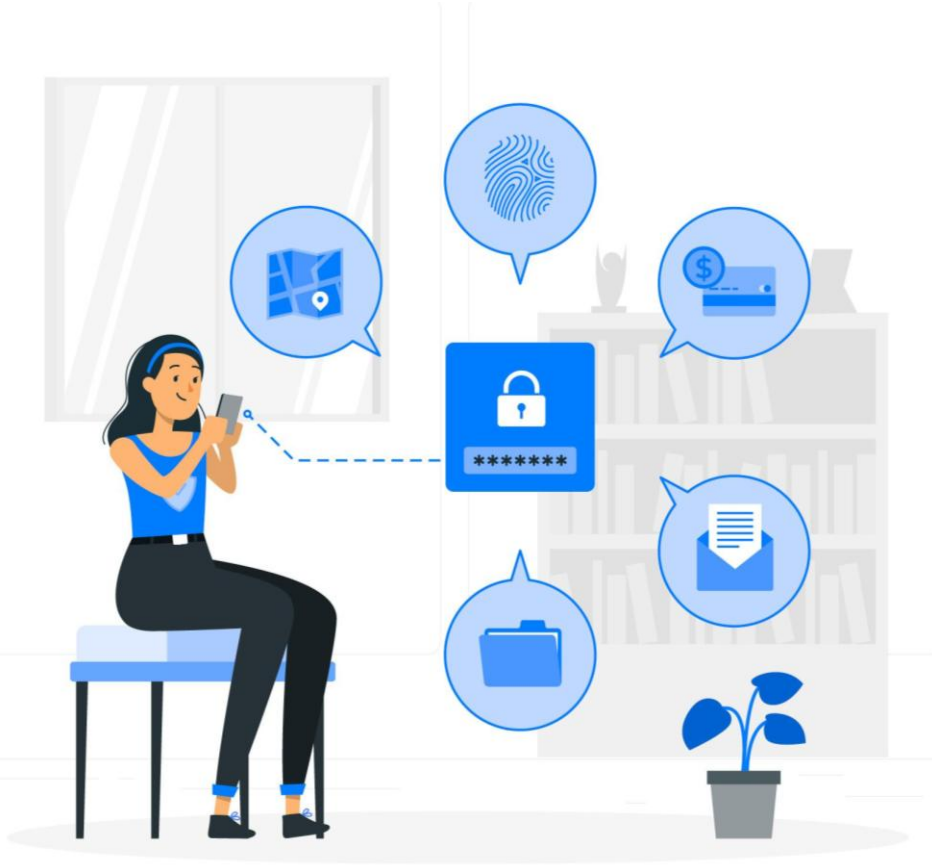
- Nunca tener apuntada la contraseña en lugares visibles (post-it en la pantalla, por ejemplo).
- No compartirla nunca con nadie.
- En caso de detectar que alguien pueda conocerla, cambiarla inmediatamente.

Reutilización de contraseñas

Es cómodo, de cara a memorizar, el utilizar la **misma contraseña** en todas o algunas de nuestras cuentas. El riesgo es que los ciberdelincuentes lo saben y, en caso de robo, intentarán utilizar esa contraseña en todas las cuentas y sitios web del usuario.

Algunos usuarios pueden pensar que sus cuentas **no son lo suficientemente importantes** como para ser atacadas por piratas informáticos. Por tanto, creen que reutilizar contraseñas no supone un riesgo importante.

Por lo tanto, es importante utilizar **una contraseña única y compleja para cada cuenta**. O bien, renuncie por completo al uso de contraseñas mediante el uso de otras soluciones de seguridad.



Consecuencia del robo de contraseñas

Cuando se produce el **robo de una contraseña** el delincuente puede acceder a la cuenta de la víctima y realizar diferentes actividades fraudulentas suplantando su identidad con las siguientes consecuencias:

- **Pérdida económica**: Podrán acceder nuestra cuenta bancaria y sustraer el dinero de la misma.
- **Suplantación de identidad**: Podrán cometer delitos en nombre de la víctima, como puede ser el ciberacoso.

Si se sospecha que hemos podido ser víctimas de un **robo de contraseñas bancarias** lo más importante es contactar con banco y solicitar el **bloqueo inmediato de las cuentas**.
También se recomienda **revisar el informe bancario** de forma habitual y comprobar que todos los movimientos realizados son correctos.

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- Un **Sistema de Gestión de Seguridad de la Información (SGSI)** permite gestionar de manera adecuada la información corporativa con la finalidad de hacer frente a las amenazas de ataques, errores o acciones fortuitas, entre otras acciones.

- Busca asegurar la **confidencialidad, la integridad y la disponibilidad** de los activos de información, es decir los dispositivos con los que trabajamos.

- Un SGSI comprende una serie de protocolos y de recomendaciones muy amplia y de las cuales sólo comentaremos algunas.

Bloquear la sesión del ordenador

Dejar una **sesión de trabajo abierta** es dejar que cualquiera pueda acceder a los datos de nuestro equipo. La mayoría de los sistemas, pasado unos minutos se bloquean automáticamente, pero puede no ser tiempo suficiente para evitar una fuga de información.

La forma más rápida de **bloquear un equipo** si te tienes que ausentar unos minutos y así forzar a que vuelva a pedir la contraseña seria esta:

LOGOTIPO DE WINDOWS + L

El navegador web

Un **navegador web** (web browser) es un software, aplicación o programa que permite el acceso a internet, interpretando la información de distintos tipos de archivos y sitios web para que estos puedan ser visualizados.

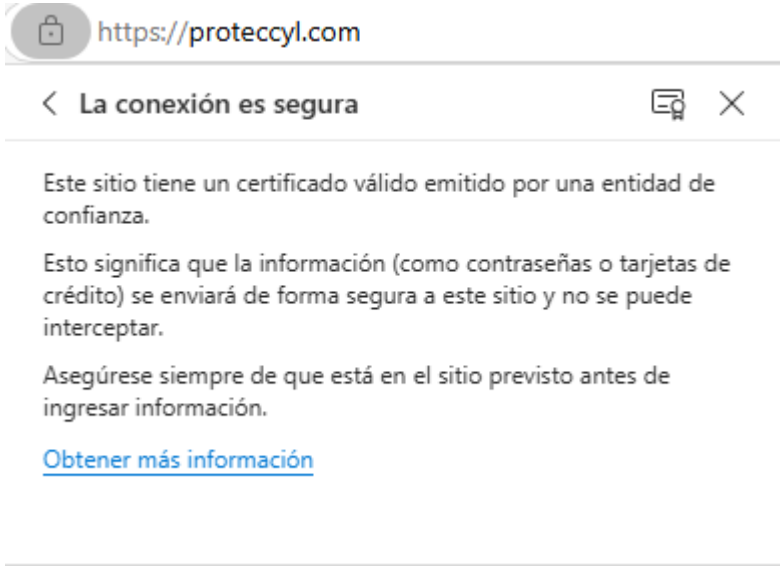
El navegador te permite acceder a páginas web que se encuentran en internet. Las páginas pueden estar alojadas en servidores del todo el mundo y el protocolo universal que se usa para todas estas páginas de la **Word Wide Web (www)** se llama **HTTP (Protocolo de Transferencia de Hipertexto).** Este protocolo es el que te traslada la página web a un ordenador

El navegador web

El **protocolo HTTP** realiza cada llamada a los servidores de manera independiente, por lo que no guarda información de solicitudes o sesiones anteriores. Por esto se dice que es un **protocolo sin estado**. Por este motivo se desarrollaron las **cookies**, que es información que el servidor guarda en el ordenador del usuario, permitiendo así saber si se ha iniciado sesión o no.

El navegador web

La versión segura del HTTP es el ***protocolo Seguro de Transferencia de Hipertexto o HTTPS.*** *destinado a la transferencia segura de datos. Este sistema es utilizado para la información sensible ya que cifra los datos y esto evita que un atacante pueda descifrarlos y usarlos.*



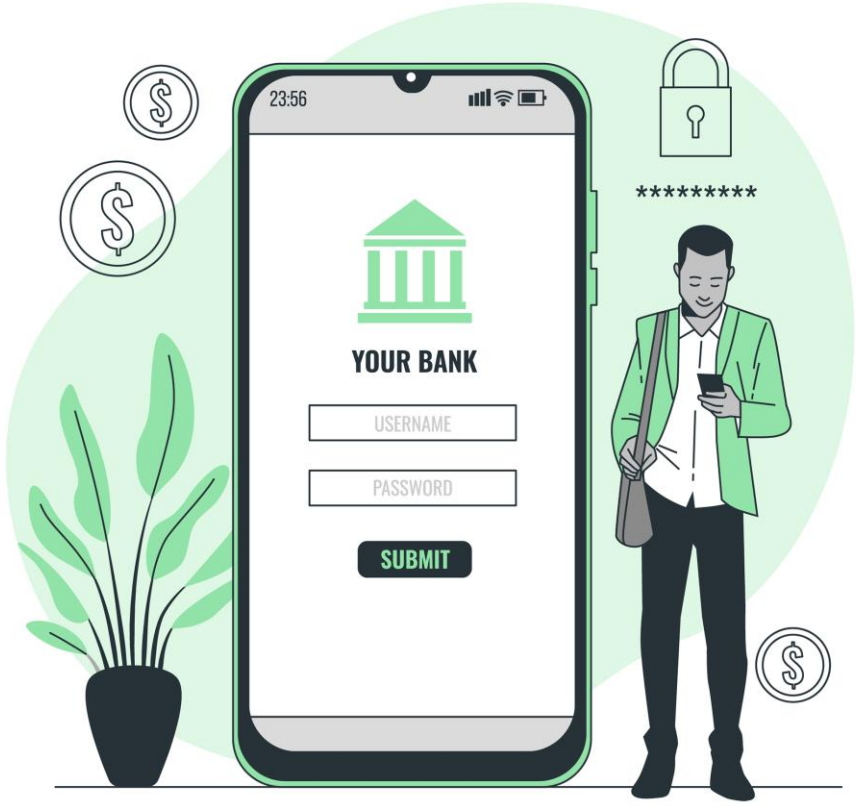
Aplicaciones bancarias

Actualmente la mayoría de las **operaciones bancarias** las realizamos a través de **internet** o de los **dispositivos móviles**. Por ello, cada vez son más los bancos que tienen su propia aplicación oficial para que los usuarios realicen sus gestiones cómodamente.

Aplicaciones bancarias

Como usar las aplicaciones bancarias de forma segura:

- Utilizar la aplicación oficial descargada directamente desde la página web del propio banco.
- Mantener la aplicación actualizada ya que aumenta la seguridad.
- Al finalizar siempre cerrar la sesión de la aplicación.
- No realizar gestiones conectados a wifis públicas o poco seguras.
- Asegurarse de que exista un límite en la cantidad de dinero a transferir o en su caso configurarlo.
- Tener instalado un antivirus.
- Proteger la entrada a la aplicación mediante validación biométrica o contraseña y activar el doble factor de autenticación para transacciones internas.



BANCA DIGITAL

- La **banca digital** es la versión que las entidades bancarias ofrecen de sus servicios y productos financieros **a través de plataformas en línea y aplicaciones móviles**, en lugar de las tradicionales sucursales u oficinas. La banca digital permite a los clientes realizar una amplia gama de transacciones y operaciones bancarias desde sus dispositivos electrónicos, como **smartphones, tablets u ordenadores.**

- Además, la evolución a **bancos digitales** implica que también puedan realizarse pagos a otras personas, empresas u organismos públicos, o pagar la adquisición de bienes o servicios a través de las tarjetas de crédito.

- La Banca digital tiene muchas ventajas: Disponible **24 horas, 365 días al año**, **comodidad** al no tener que desplazarte a una sucursal, **sostenibilidad** ya que se reduce mucho el uso de papel y ayuda a contribuir con la huella de carbono y a los bancos le supone un gran **ahorro de costes**.

Tipos de banca digital:

Banca Telefónica:

- Históricamente la relación con los bancos siempre ha sido presencial o mediante conversación telefónica debido a la escasez de medios que había.
- Aunque en la actualidad estos medios se han duplicado, se sigue usando el teléfono para ponerte en contacto con tu sucursal bancaria realizar determinados trámites.
- Lamentablemente, es una las vías por las que **más fraudes se producen**.
- El **fraude telefónico** tiene como objetivo engañar a la víctima para **obtener información confidencial** que posteriormente se usará para defraudarla (como puede ser datos personales o de acceso a la banca online). También es posible que durante la llamada insten a la victima a hacer un pago por unos supuestos servicios prestados.

Tipos de banca digital:

Banca Online:

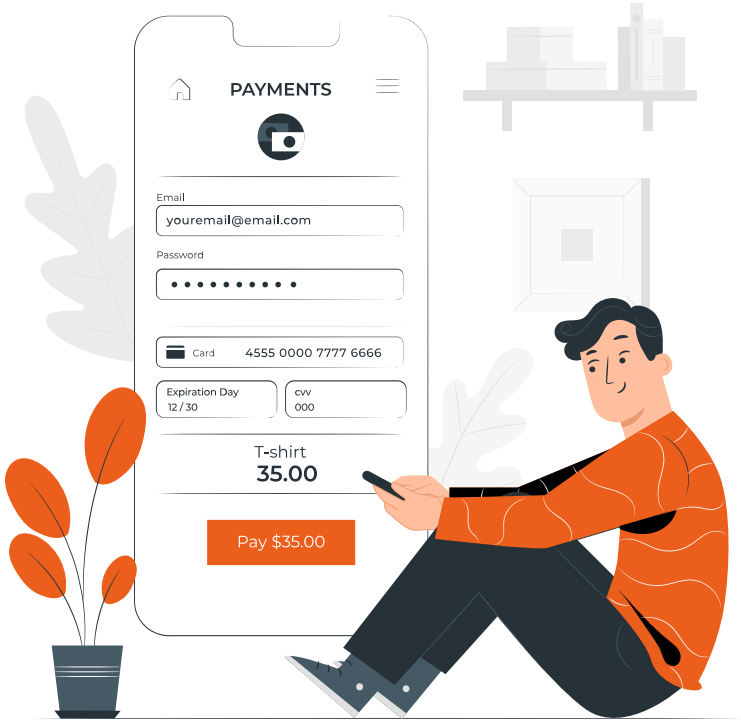
- Por banca online entendemos al servicio que las entidades financieras prestan a sus clientes al acceder por vía telemática para poder realizar cualquier operación financiera de forma segura y rápida, sin necesidad de tener que acudir a una sucursal.
- **Riesgos de la banca online:**
  - **Phishing o suplantación de identidad**. Método utilizad por los atacantes para engañar a los usuarios enviando emails falsos que simulan la identidad de la entidad bancaria. Así, les piden que verifiquen sus datos y obtienen las claves, número de cuentas bancarias, etc.
  - **Pharming**. El atacante redirige al usuario a páginas que no son las auténticas para conseguir datos confidenciales.
  - **Keyloggers o interceptación de teclado**. Inducen al usuario a la instalación de un programa que detecta las teclas que pulsa para obtener su información sensible una vez la marca.

Tipos de banca digital:

Banca Movil (APPS):

- En la actualizad es el método más usado para interactuar con tu banco.
- Suelen ser el objetivo principal de ciberdelincuentes, quienes aprovechan el descuido de los usuarios para acceder a sus cuentas.
- **El Peligro de tener la app de tu banco en la pantalla de inicio del móvil:**

    - Mantener la app de tu banco a la vista de todos puede ser una invitación para que alguien acceda a información confidencial si tu móvil cae en las manos equivocadas. Ya sea un robo, un descuido o un acceso no autorizado, la exposición directa facilita el acceso rápido a datos importantes.
    - **Es muy importante ocultarlas y protegerlas con sistemas extra de seguridad**.



TARJETAS DE CRÉDITO

- **Las tarjetas de crédito** son el medio más utilizado hoy en día para las compras tanto en establecimiento como a través de internet.

- **La tarjeta virtual** no lleva banda magnética y podemos utilizarlas para el pago a través de la red. Disponen de un número de control, número de tarjeta y la fecha de caducidad, pudiendo llevar incluso la confirmación de las operaciones a través de la recepción de un código por SMS o un PIN.

5 Escenarios de ataque:

- **Ataque por fuerza bruta**. El delincuente, teniendo el número de la tarjeta de crédito, probará diferentes combinaciones para llegar a averiguar el código de seguridad y la fecha de caducidad.
- **Keylogger**. Mediante un malware malicioso se puede detectar las pulsaciones del teclado obteniendo las claves de las cuentas bancarias.
- Modificar el **límite de obtención de efectivo**.
- **Explotar la vulnerabilidad en plataformas de compras virtuales**. Los atacantes instalan un código malicioso e interceptan las credenciales de las tarjetas de crédito de los clientes de tiendas virtuales.
- **Phishing o fraude en línea**. El delincuente obtiene información sensible del usuario y con ella hará uso de las tarjetas de débito para realizar transacciones o retirar efectivo.

TARJETAS CONTACTLESS

- Con estas **tarjetas de contacto**, se tramita el pago sin insertar la tarjeta en el datáfono, simplemente acercándola al dispositivo.

- Sin embargo, no son totalmente seguras por el riesgo de tener una aplicación maliciosa instalada en el móvil. Que lea los datos de forma inalámbrica.

6 Mecanismos de defensa:

- Llevar siempre la tarjeta en una **funda de aluminio** o en carteras específicas.
- **Limitar el importe** de las transacciones de pagos contactless. Necesidad de poner el PIN si se supera esa cifra.
- **Tener instalado un antivirus** en el dispositivo móvil.
- Tener activada la opción de notificaciones de movimientos bancarios por SMS.
- **Contactar con el banco** en caso de detectar irregularidad.
- Asegurarnos de que no pasamos nuestra tarjeta por ningún dispositivo no deseado.

REDES SOCIALES

- Una **red social** (en plural, redes sociales, abreviado como RR. SS.) es una **estructura social** compuesta por un conjunto de actores y uno o más **lazos o relaciones** definidos entre ellos.

REDES SOCIALES

- Las **redes sociales** son el medio de comunicación que más ha crecido en los últimos tiempos, y donde almacenamos más información privada.

- Cuando publicamos algo en una red social perdemos el control sobre el contenido ya que queda registrado para siempre en los servidores de dicha red social y cualquiera podrá usar esa información.

Consejos para unas RRSS seguras:

- Configurar la **privacidad de nuestro perfil** y protegerlas con **contraseñas robustas.**
- Leer la **política de privacidad** y condiciones del servicio.
- Ponerse en contacto con las **opciones de denuncia** de la red social si detectamos que podemos ser víctimas de robo o suplantación.
- **Controlar la información** que subimos a las redes sociales ya que puede ser utilizada en nuestra contra.
- Asegurarnos que nuestros **contactos** son realmente quien dicen ser.
- No compartir **videos ni fotos comprometidas**.

ProtecCyL/CIM-BSE
Plan de promoción de la Autoprotección
Plano de promoção da Autoproteção

Junta de Castilla y León

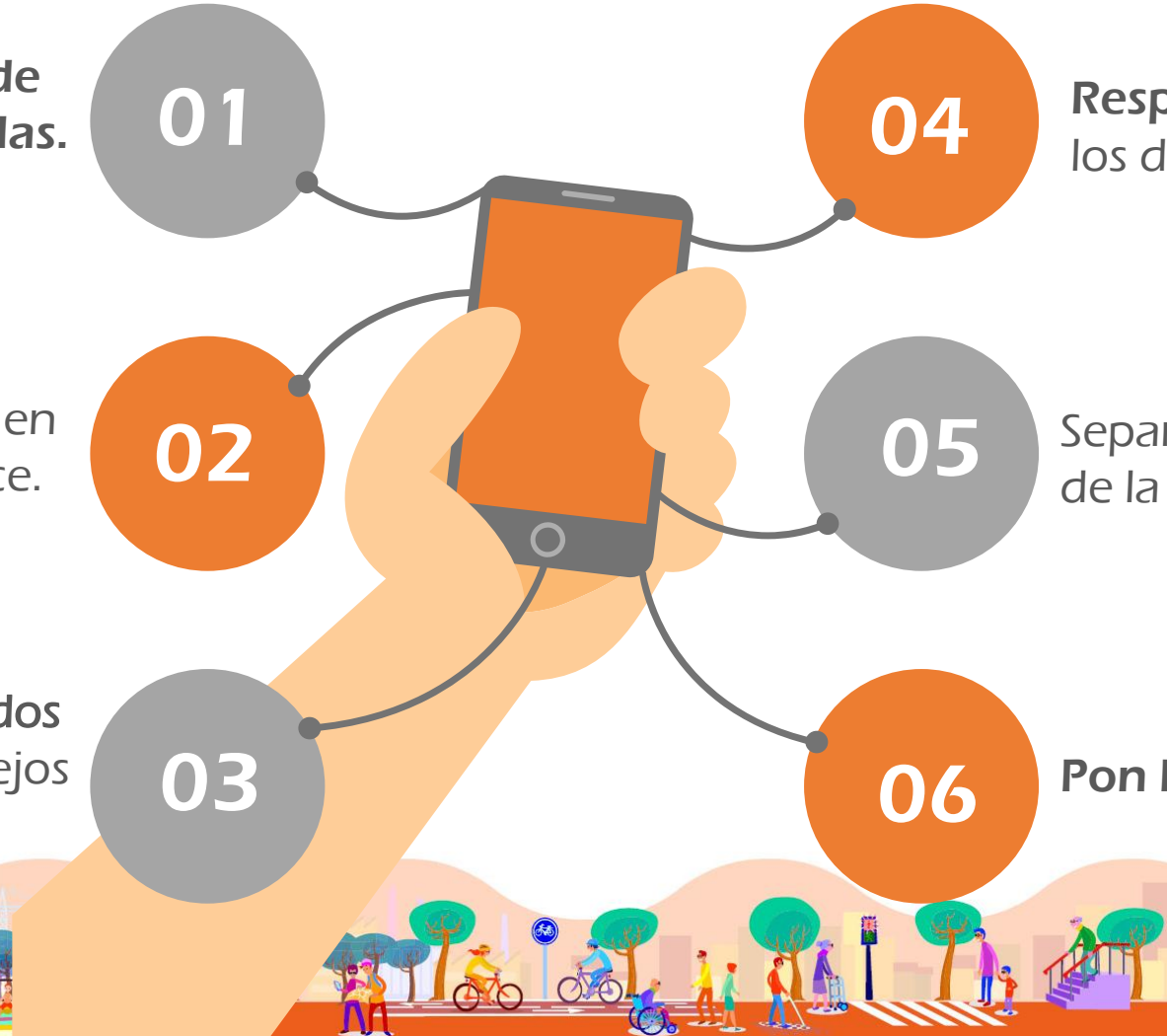
Interreg
España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia

Consejos para unas RRSS seguras

01 Mantén tus **aplicaciones de redes sociales actualizadas.**

02 **No hagas click** en cualquier enlace.

03 Educa a tus **seres queridos** dándoles apoyo y consejos de uso.



04 **Respeta la privacidad** de los demás.

05 Separa tu vida profesional de la vida personal.

06 **Pon límites a su uso.**

Configuración Privacidad:

- **Como pueden encontrarte y ponerse en contacto contigo los demás:**
  - Privacidad de las publicaciones.
  - Configuración de la privacidad.
  - Revisar etiquetas y menciones.
  -
  - Limitar la visibilidad del perfil.
  - Bloquear usuarios.

- **Tu actividad:**
  - Administrar aplicaciones y sitios web conectados.
  - Revisar y eliminar publicaciones antiguas.
  - Registro de actividad.

Configuración Privacidad:

- **Audiencia y etiquetas:**
  - Privacidad de los tweets.
  - Configuración de la cuenta.
  - Contenido que ves.
- **Mensajes Directos:**
  - Procedencia de mensajes.

- **Información de la ubicación:**
  - Detección de ubicación exacta.
  - Datos de interés.
- **Visibilidad y contactos:**
  - Contacto.

Configuración Privacidad:

- **Quién puede ver tu contenido:**
  - Privacidad de la cuenta.
  - Bloqueos.
- **Como pueden interactuar contigo los demás:**
  - Control de comentarios, mensajes y respuestas.
  - Etiquetas y menciones.
  - Permisos del sitio web

- **Centro de cuentas:**
  - Contraseñas y seguridad > Alertas de inicio de sesión.

Configuración Privacidad:

- **Visibilidad:**
  - Visibilidad de tu perfil y tu red.
- **Privacidad de los datos:**
  - Quién puede contactarte.
  - Mensajes.

- **Notificaciones:**
  - Mensajes, publicaciones y comentarios, asistencia a eventos.
- **Inicio de sesión y seguridad:**
  - Acceso a la cuenta.

Configuración Privacidad:

- **Visibilidad:**
  - Cuenta privada.
  - Servicios de ubicación.
  - Configuración de seguridad y privacidad
- **Interacciones:**
  - Comentarios, menciones y etiquetas, mensajes, story.
  - Cuentas bloqueadas.

Muchas gracias

ProtecCyL/CIM-BSE

Plan de promoción de la Autoprotección
Plano de promoção da Autoproteção

Junta de Castilla y León

Interreg
España – Portugal

Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia