Ciberseguridad

Guía sobre seguridad informática en Lectura Fácil

JAYMON SECURITY
Cyberintelligence & Solutions

Desenreda
Afanias

Autor de los contenidos:

Afanias, Asociación pro-personas con discapacidad intelectual
en colaboración con Jaymon Security
Septiembre de 2023.

Adaptación a lectura fácil:

Javier Alonso Henar
Desenreda Afanias

Validación a lectura fácil:

Equipo de validación de lectura fácil de Afanias Canillejas

Diseño y maquetación:

Sandra López Mellado
Desenreda Afanias

Ilustraciones tomadas de:

https://elements.envato.com
https://www.canva.com/
https://www.freepik.es/

Para más información visita nuestra web: https://www.afanias.org

Índice

1. Palabras que debes conocer

Ciberseguridad:
son las medidas y los aparatos dirigidos a controlar
la seguridad informática.

Disco duro:
parte del dispositivo electrónico
donde se almacenan tus contenidos digitales,
por ejemplo, tus documentos, fotos o música.

Hacker o pirata informático:
persona con muchos conocimientos de informática
que se dedica a acceder de forma ilegal
a sistemas informáticos de otras personas.

Navegar:
desplazarse por internet.

Robo de identidad:
hacerse pasar por otra persona.
Las personas que roban la identidad a otras
buscan conseguir ciertos recursos,
por ejemplo, información o dinero.

Phishing:
es un tipo de engaño
que consiste en el envío de e-mails falsos
intentando que hagas clic o pinches en un enlace maligno
o escribas tus datos en una página falsa.

Virus:
son programas malignos
que se almacenan en el ordenador y lo dañan.

2. Objetivos de esta guía

Con esta guía de ciberseguridad y seguridad informática conseguirás los siguientes objetivos:

- Entender de manera básica lo que es la ciberseguridad y la seguridad informática.
- Mejorar nuestra ciberseguridad y seguridad informática.
- Aprender a aplicar algunas medidas de ciberseguridad.
- Entender cómo nuestro comportamiento mejora la Ciberseguridad en nuestro día a día.

3. ¿Por qué es importante la Ciberseguridad?

¿Qué es seguridad de la información?

La seguridad de la información consiste en proteger
nuestra privacidad y la de nuestros datos.

La tecnología ha hecho nuestras vidas
más fáciles en muchos aspectos,
pero al utilizarla aumentan nuestros riesgos o peligros.

¿Por qué debe preocuparte la seguridad informática?

En el mundo digital hay cada vez más robos.
Normalmente los ladrones digitales buscan robar:

- La identidad de una persona.
- Tus datos para hacerse pasar por ti.
- Tu cuenta bancaria.
- Tu usuario o tus contraseñas.

Cuando no tienes seguridad informática
pueden verse afectadas personas de tu alrededor.
Como, por ejemplo: compañeros de trabajo, amigos y familiares.

4. Conceptos que debes saber

Robo de identidad

La identidad son las características
de una persona que la hacen distinta de otra.
Robar la identidad es hacerse pasar por otra persona.

Las personas que roban la identidad a otras
buscan conseguir algunos recursos,
como información o dinero.

Desde el año 2018
aumentaron las amenazas de robo de identidad.

Normalmente el robo de identidad ocurre
por falta de seguridad en las bases de datos.
Las bases de datos son archivos electrónicos
que guardan la información o los datos.

4. Conceptos que debes saber

Virus

Los virus son programas malignos
que se meten en el ordenador y lo dañan.

Pueden destruir:

- Documentos.
- Fotos.
- Programas del ordenador.
- Borrar la información de tu disco duro.
- Enviar correos electrónicos desde tu ordenador.
- Robar tus datos bancarios.

Los virus informáticos
son como los virus que provocan enfermedades,
se contagian a otros ordenadores o dispositivos.

4. Conceptos que debes saber

Troyanos, gusanos y rootkits

Los troyanos son virus que parecen programas legales.
Este tipo de virus necesita que la persona abra el programa.
Una vez abierto comienza a infectar al ordenador.

Los gusanos son virus que se multiplican solos
y buscan más ordenadores que infectar.

Los rootkits son programas
que se instalan en secreto en los ordenadores
y permiten que la persona que envió el virus
pueda controlar tu ordenador.

Spyware

Spyware es una palabra en inglés que significa programa espía.
Son programas diseñados para reunir información
sobre tus hábitos, normalmente sin que te des cuenta.
Por ejemplo, mediante:

- Las páginas web que visitas
  y durante cuánto tiempo.
- Lo que has comprado por internet.
- El uso que haces del ordenador.

Habitualmente este virus
se instala mediante programas gratuitos.
Puede no causar daño y solo ser molesto.

4. Conceptos que debes saber

Cifrado

El cifrado es un proceso que permite que los datos
no puedan leerse cuando se guardan
o cuando se envían a través de internet.
De esta forma impedimos que los datos
puedan ser vistos por otras personas.
Es importante usar el cifrado para almacenar
o enviar información privada.
Para saber que está cifrado busca el candado en el navegador.

Muchos servicios, como la web y el correo electrónico,
pueden ser poco seguros si no utilizas el cifrado.

No todo es digital

No toda la información que los hackers roban
es digital y a través del ordenador.
Estas personas pueden encontrar información
muy valiosa en nuestra basura.

Los ladrones pueden encontrar en la basura:

- Información de clientes.
- Tarjetas de crédito.
- Recibos de compras y servicios
  como la luz, el agua o el gas.
- Documentación interna o técnica de tu trabajo.
- Solicitudes de préstamos de dinero.
- Planos del edificio de una empresa.

5. ¿Como protegerse ante las amenazas?

Para estar protegidos sigue los siguientes consejos:

- No compartas con nadie
  tus claves de acceso o contraseñas.
  Tampoco con tus compañeros de trabajo y amigos.

- La información privada que no necesites
  destrúyela o guárdala bajo llave.

- Bloquea siempre tu ordenador cuando te alejes.

  Para bloquear tu ordenador
  aprieta estos 2 botones + L.

- Ten siempre activado el antivirus.

- Nunca descargues archivos informáticos extraños.

- No abras archivos que no esperas
  en el correo electrónico.
  Asegúrate que es de alguien conocido.

5. ¿Como protegerse ante las amenazas?

- Nunca envíes información privada o datos de clientes por canales inseguros.
- Si sospechas que has sufrido un robo, o intento de hackeo, avisa a tu supervisor inmediatamente.
- En el trabajo no permitas que entren extraños en tu oficina y no dejes las puertas abiertas.
- En el trabajo cuando notes actividades o personas sospechosas avisa a tu responsable.

Recuerda:

estos consejos sirven para estar seguros en nuestro puesto de trabajo y para nuestros ordenadores o moviles personales.

5. ¿Como protegerse ante las amenazas?

Contraseñas

La contraseña es un código secreto
que se introduce para acceder a tu ordenador,
móvil o cuentas personales.
Para que tus contraseñas ayuden a evitar robos,
tienes que tener en cuenta lo siguiente:

- Tu usuario y contraseña son muy importantes,
  es lo primero que te defiende de las amenazas informáticas.

- Nunca compartas tu usuario y tu contraseña.

- Si la contraseña es muy corta o muy sencilla,
  los delincuentes pueden conseguirla fácilmente.

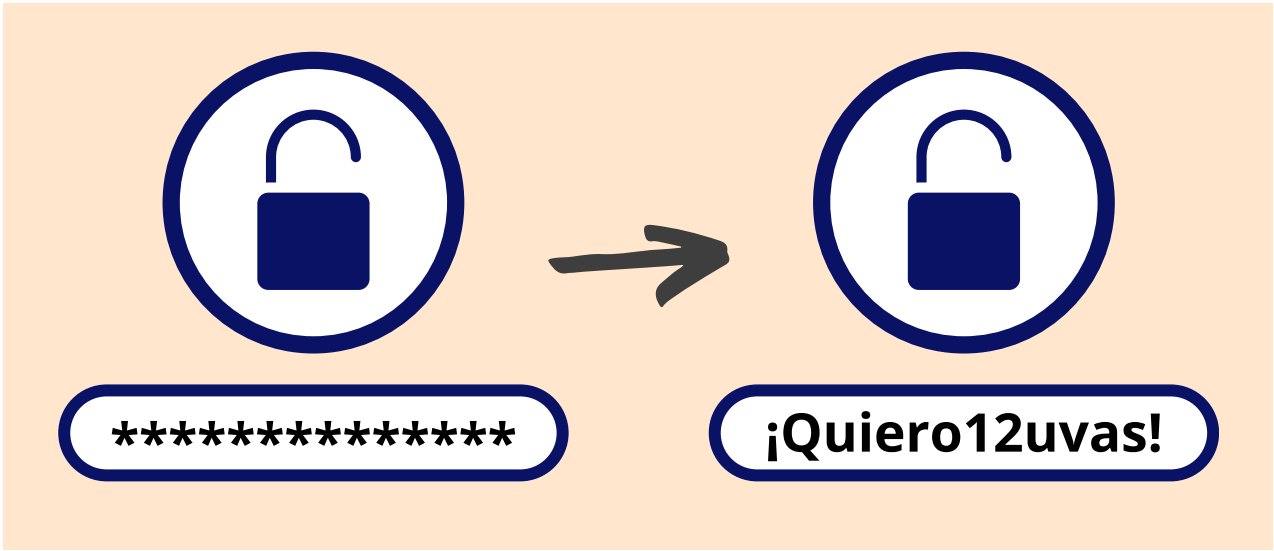
- Los delincuentes prueban diferentes combinaciones
  que pueden ser habituales,
  para conseguir tu contraseña.

- Cuanto más segura es la contraseña,
  más difícil es que los delincuentes la consigan.

5. ¿Como protegerse ante las amenazas?

Una contraseña segura debe:

- Tener como mínimo 14 caracteres.
  Los caracteres son los diferentes elementos
  que componen nuestra contraseña,
  por ejemplo, letras, números o símbolos.
- Incluir números, mayúsculas y minúsculas
  o símbolos, como @, &, +,...
- No repitas la misma contraseña.
- No incluyas información personal,
  como el nombre, fechas especiales
  o el número del DNI.



6. Ingeniería social

La ingeniería social es un engaño.
El delincuente quiere engañarte
intenta que le des tu usuario y contraseña
o hagas algo que no debes.

Este delincuente puede intentar:

- que abras un programa de tu dispositivo.
- que pagues facturas.
- que modifiques datos.
- que permitas accesos.

Sacar información a las personas es muy sencillo,
por eso los delincuentes se aprovechan.
Aprovechan la amabilidad
y las ganas de ayudar de las personas.

Los delincuentes actúan de diferentes formas:

· En persona.
· A través de un email.
· A través de llamadas, WhatsApp o mensajes móviles.
· Por correo postal.

6. Ingeniería social

Ataques más habituales

Los delincuentes para engañarte se hacen pasar por:

- El jefe de algún departamento de tu trabajo o decir que viene de parte de un jefe.
- Un profesional de algún servicio contratado, por ejemplo, gas, luz o teléfono.
- Por un cliente.
- Por policía, Guardia Civil o trabajador público.

Importante

En el trabajo, confirma con tu responsable cuando un desconocido te pide hacer alguna tarea que no es habitual.
No dar nunca información tuya o de tu trabajo a un desconocido.

7. Phishing

El phishing es otro tipo de engaño,
el delincuente envía emails falsos a sus víctimas.

Quieren que pinches en un enlace maligno
o que escribas tus datos en una página falsa.
Los emails falsos pueden parecer iguales
que un email oficial.
Por ejemplo, de tu jefe, del banco o de correos.
Desconfía siempre de correos mal escritos.

Importante

· Aunque esté bien escrito,
recuerda que tu banco no envía este tipo de emails.

· Ante la duda, pregunta siempre.

· No descargues nada que te envíen desde estos correos
ni pinches en sus enlaces.

8. Redes sociales

Una red social es un espacio de internet
que pone en contacto a muchas personas.
Instagram, Facebook o Tiktok son redes sociales.
Las redes sociales te permiten publicar información
en tu perfil y tus fotos.

Normalmente se ponen datos personales como:

- Nombre
- Edad
- Ubicación
- Fotos
- Lugar de trabajo

Los delincuentes utilizan la información
personal y laboral
que publicas en estas redes sociales,
para atacarte a ti y a tus conocidos.
Para ello el delincuente:

- Identifica los nombres de amigos,
  familiares y compañeros de trabajo.
- Con esta información
  se hacen pasar por alguien conocido.
- Un ejemplo habitual es publicar un artículo
  diciendo que te vas de vacaciones
  y el delincuente aproveche
  para robar en tu casa.

9. Navegación segura

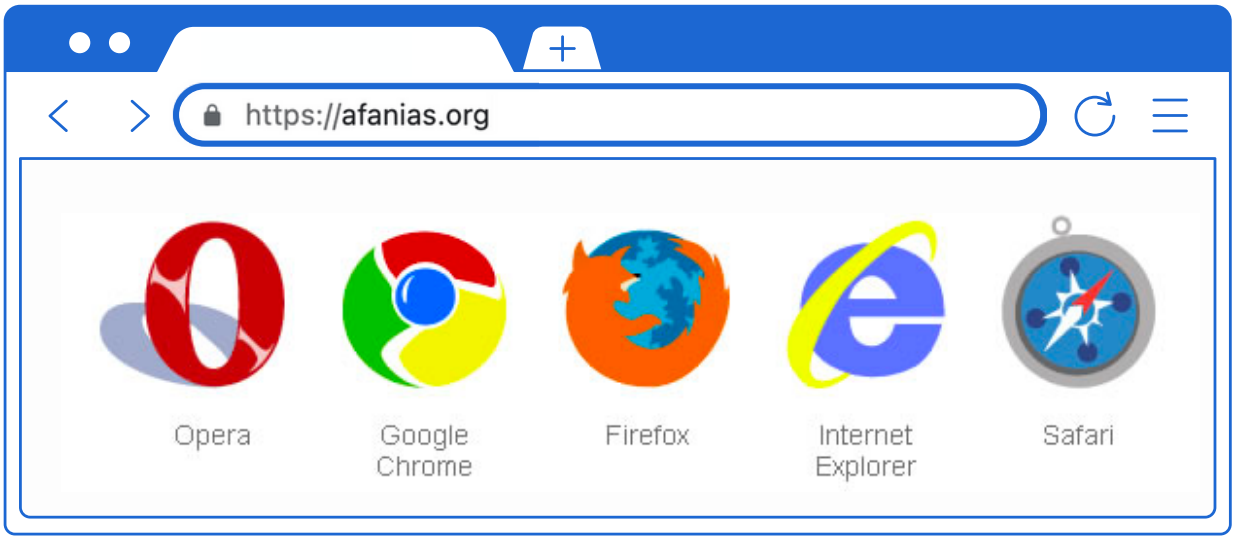
Para navegar por las páginas web
de manera segura,
hay que tener en cuenta lo siguiente:

• Es importante atender
a los mensajes de seguridad del navegador.
Un navegador es un programa que permite
ver la información que contiene una página web.
Ejemplos de navegadores: Google, Firefox o Internet explorer.

• Al realizar compras online o transferencias bancarias,
debes utilizar conexiones seguras:

- Las páginas web que son seguras comienzan
con HTTPS:// o muestran un candado cerrado
al lado de la dirección.

- La mayoría de navegadores
te muestran si la conexión es segura o no.
Cuidado con las advertencias.



9. Navegación segura

Consejos para navegar de manera segura

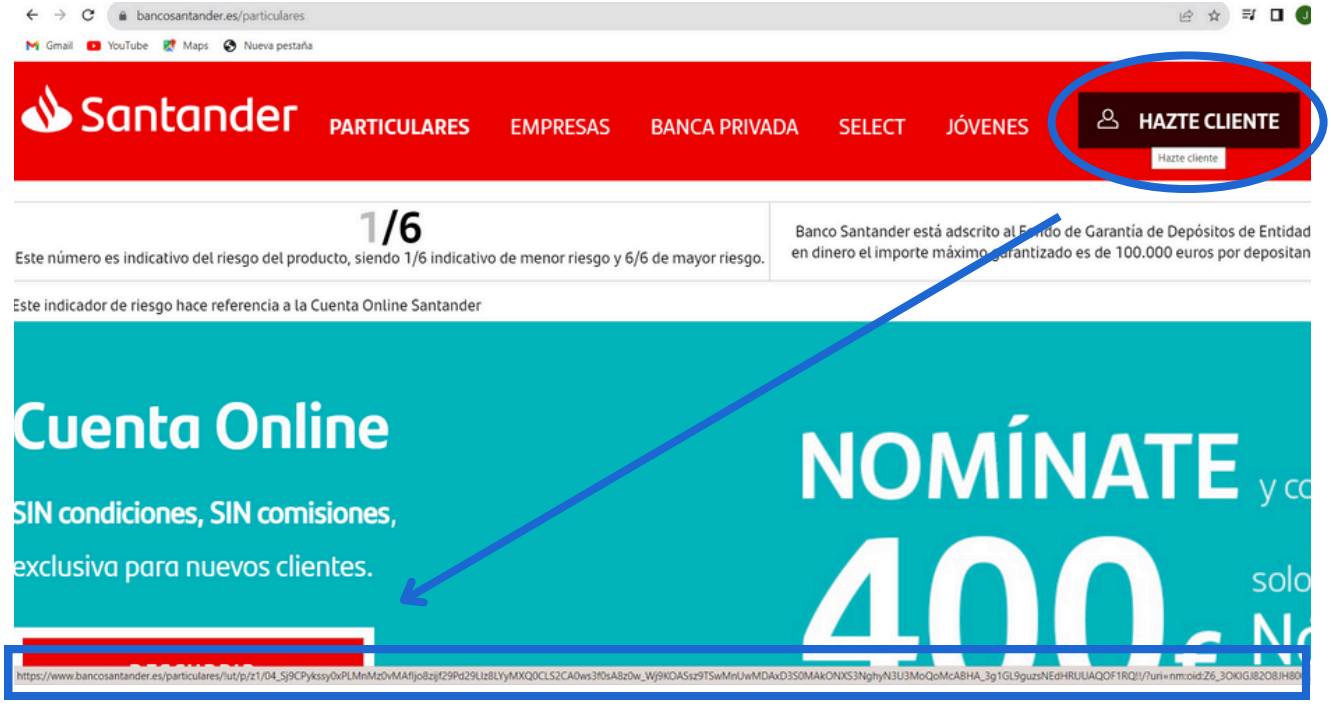
Consejos para navegar por internet de manera segura:

- Fíjate en la dirección de la página Web.
- Ten cuidado con los nombres
  que te suenen raros, desconocidos
  o que se parezcan al original.

Por ejemplo (www.bancosantander.es en lugar de www.bancosantanderr.es).

- Comprueba dónde te llevan los enlaces que te envíen,
  para ello pon la flecha del ratón encima del enlace
  y comprueba la dirección que aparece debajo.

La imagen nos enseña que al colocar la flecha en el enlace coincide la dirección.



10. Dispositivos portátiles

Los **dispositivos portátiles** son aparatos electrónicos
que llevamos encima.
Como, por ejemplo: los móviles, ordenadores portátiles
o tablets.

1. Los dispositivos portátiles
son fáciles de perder o de robar:
· Mantenlos siempre a la vista,
o guárdalos bajo llave cuando no los uses.
· Ten mucho cuidado cuando estés
en zonas con mucha gente.
· Denuncia a la policía inmediatamente
sí pierdes o te roban algún aparato electrónico.

2. Los dispositivos portátiles
suelen contener información privada,
por eso debes:
· Utilizar contraseñas seguras.
Recuerda, tienes que utilizar mínimo 14 caracteres.
Utiliza alguna frase que te sea fácil de recordar.
Por ejemplo: ¡Quiero12uvas!
· Configura tu dispositivo
para que se bloquee cuando no lo uses.
· Realiza siempre un borrado seguro
antes de tirar o vender tus dispositivos.

3. Normalmente los dispositivos son muy valioso.
Vigila para no perderlo.
la información que contiene es mucho más valiosa.
Por ejemplo: Fotos de tu familia, nóminas,
el libro que estoy escribiendo, etc.

11. Recuerda

10 recomendaciones para recordar

1. No pinches en los enlaces
   o abras archivos adjuntos al email.

2. Usa antivirus y no lo desinstales nunca.

3. No envíes datos importantes
   a través de canales o medios no seguros.

4. Destruye los datos en papel o tarjetas
   de manera adecuada.

5. Borra los datos de los dispositivos electrónicos
   de forma segura o destruye el disco duro
   antes de tirar tu dispositivo.

6. No abras programas de los que desconfíes.

7. Bloquea tu dispositivo si no lo utilizas o te alejas.

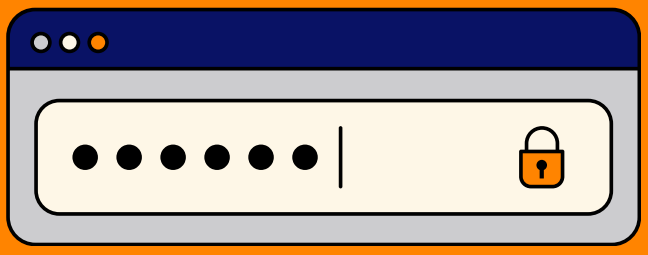
8. La información debe estar siempre segura,
   para ello utiliza:

   · Cajas fuertes o cajones cerrados para documentos físicos.
   · Cifrado para la información digital.

9. Comprueba que la identidad de la persona es real
   o que el sitio web es seguro.

10. Si algo parece demasiado bueno para ser verdad,
    probablemente es mentira.

Ciberseguridad



JAYMON SECURITY
Cyberintelligence & Solutions

Desenreda
Afanias

Desenreda, Servicio de Accesibilidad Cognitiva de Afanias
Afanias, Asociación pro-personas con Discapacidad Intelectual
Jaymon Security Ciberintelligence & Solutions