

2. Comunicación y colaboración

2.5. Gestión de la identidad digital:

2.5.4. Riesgos para la identidad digital

Material elaborado por CRUE-REBIUN y adaptado por la Biblioteca de Mondragon Unibertsitatea

**Comunicación y
colaboración.
Gestión de la identidad
digital**

Riesgos para la identidad digital



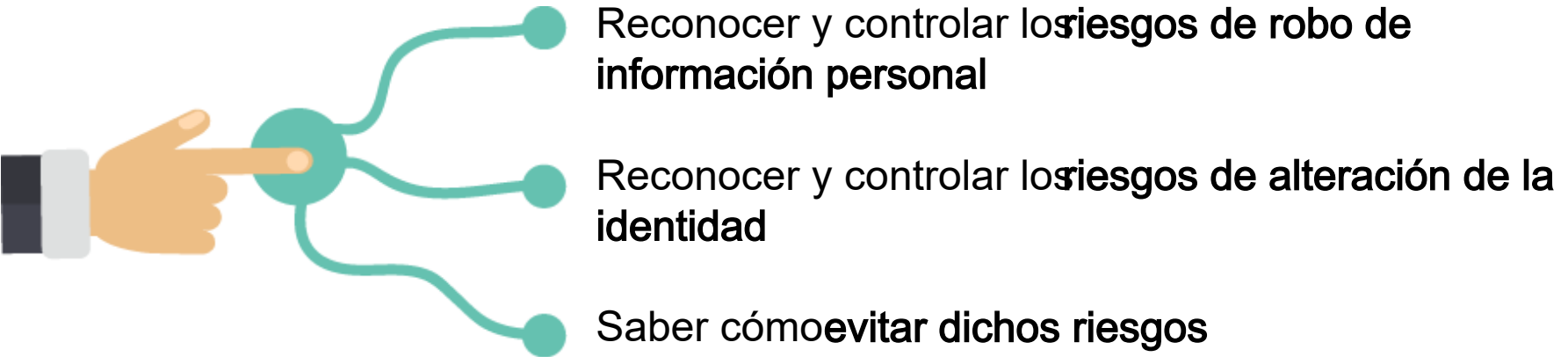
CRUE

REBIUN

Red de Bibliotecas Universitarias

OBJETIVO

Al finalizar esta actividad tienes que ser capaz de:



SUMARIO

- Robo de información personal
- Alteración de la identidad
 - Suplantación de identidad digital
 - Amenazas para la privacidad
 - Ataques a la imagen y a la reputación online
- Recomendaciones
- Para saber más...

RIESGOS FRECUENTES

1. ROBO DE INFORMACIÓN PERSONAL

Estos son algunos de los métodos para obtener datos de información personal:

- **Programas maliciosos (malware)** cuyo propósito principal es borrar, bloquear, modificar o copiar datos de los usuarios (virus, gusanos, troyanos...).
- **Phishing:** método utilizado para conseguir de forma engañosa (correo-e, llamadas telefónicas...) que se revele información personal (contraseñas, datos de tarjetas de crédito...).
- **Pharming:** práctica fraudulenta para redirigir un sitio web a otro falso, muy similar en apariencia, que instala software malicioso en el equipo del visitante o que inspecciona los datos personales del usuario.

RECOMENDACIONE

*Si no quieres
que te roben
información
personal...*



**Ante la mínima duda, sé prudente y
no te arriesgues**

- No abras ni lees correos electrónicos sin confirmar su procedencia y legitimidad.
- Introduce tus datos confidenciales solo en webs con protocolo seguro como https en lugar de http.
- No entres en webs con información privada (bancos...) a través de enlaces incluidos en correos electrónicos.
- No reveles tus claves y contraseñas a nadie y cámbialas con frecuencia.
- Mantén tu equipo protegido con antivirus.
- Evita utilizar redes Wi-Fi públicas para realizar operaciones privadas.

RIESGOS FRECUENTES

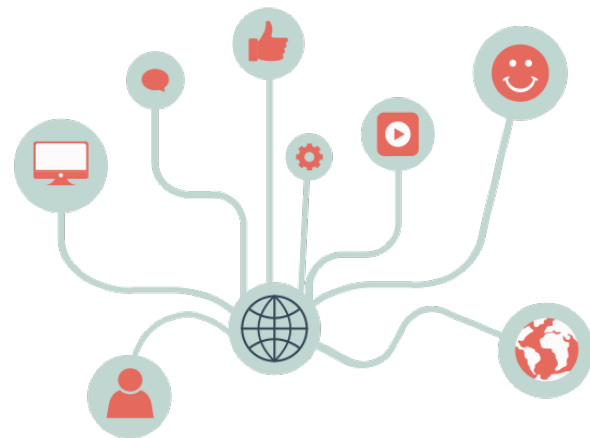
2. ALTERACIÓN DE LA IDENTIDAD

- 1 Suplantación de identidad digital
- 2 Amenazas para la privacidad
- 3 Ataques a la imagen y a la reputación online

1 SUPLANTACIÓN DE LA IDENTIDAD DIGITAL

Se produce cuando alguien malintencionado se apropia indebidamente de la identidad digital de otra persona y actúa en su nombre. Puede hacerlo de varias formas:

- ✓ Registrando un perfil falso, sin utilizar información personal de la persona suplantada. Por ejemplo, perfiles caricaturizados de personajes públicos.
- ✓ Creando un perfil falso con datos de otra persona.
- ✓ Accediendo de forma no autorizada al perfil de alguien en un servicio de Internet para hacerse pasar por él.



2

AMENAZAS PARA LA PRIVACIDAD

Al participar en medios sociales pierdes el control sobre la difusión de la información que publicas y otras personas pueden hacer un uso inadecuado de la misma.

Estas son las principales causas que pueden suponer una amenaza para la privacidad:

- Configuración insuficiente de las opciones de privacidad del medio que utilizas.
- Alteración de la privacidad derivada de la sincronización entre distintos medios.
- Etiquetado en las redes sociales

- Sexting (envío de contenidos de carácter sexual a través del móvil).
- Uso de cookies sin conocimiento del usuario.
- Compartir información que afecta a terceras personas.

3 ATAQUES A LA IMAGEN Y REPUTACIÓN

El riesgo a sufrir un ataque al honor o a la reputación aumenta en Internet, ya que la viralidad en la difusión de los contenidos dificulta el control de la información personal por parte del propietario.

A continuación se exponen los principales motivos de amenaza a la imagen y a la reputación online:

- ✓ Impacto de las publicaciones que exceden a la libertad de información
- ✓ Daño reputacional debido a publicaciones falsas, injurias y calumnias
- ✓ Informaciones descontextualizadas
- ✓ Utilización no consentida de derechos de propiedad intelectual

RECOMENDACIONE



Debes aprender a configurar y revisar adecuadamente las opciones de seguridad y privacidad para garantizar al máximo el control de tu información personal

- Valora la información que publicas y antes de hacerlo:
 - Sé especialmente cauto con las fotografías o vídeos que publicas en Internet, ya que te identifican físicamente.
 - Limita el uso de datos de localización a las aplicaciones estrictamente necesarias.
 - Adecua el grado de divulgación de tu información personal al tipo de relación con otras personas.



RECOMENDACIONE

- Configura bien los parámetros de privacidad y seguridad.
- Cierra adecuadamente la sesión en el perfil o servicio al terminar.
- Revisa periódicamente tus perfiles.

- Concede acceso solo a las aplicaciones de terceros que sean dignas de confianza:
 - Verifica al máximo quién es el titular de la aplicación a la que se autoriza el uso de datos de identidad, qué datos precisa y para qué los necesita.
 - Limita el acceso solo a los datos imprescindibles.



PARA SABER MÁS...

Consulta el capítulo 4 de la [Guía para usuarios: identidad digital y reputación online](#)

Consulta el documento de la OCDE [At a Crossroads: Personhood and Digital Identity in the Information Society - OECD.org](#)

Información sobre: [Regulación del derecho de rectificación](#)



**Mondragon
Unibertsitatea**

Biblioteka

Si tienes alguna duda, pregunta en tu [biblioteca](#):



Basque Culinary Center

Biblioteka

Juan Abelino Barriola pasealekua, 101
20009, Donostia, Gipuzkoa.
T. 943574514
biblioteca@bculinary.com

Enpresa Zientzien Fakultatea

Biblioteka

Ibarra Zelaia, 2
20560, Oñati, Gipuzkoa.
T. 943718009
biblioteca.enpresagintza@mondragon.edu

Humanitate eta Hezkuntza Zientzien Fakultatea

Biblioteka

Dorleta, z/g.
20540, Eskoriatza, Gipuzkoa.
T. 943714157
biblioteca.huhezi@mondragon.edu

Goi Eskola Politeknikoa

Biblioteka

Campus Iturripe. Loramendi, 4. 20500 Arrasate – Mondragon, Gipuzkoa.
Campus Orona Ideo. Fundazioa eraikuntza, Jauregi Bailara, z/g. 20120 Hernani, Gipuzkoa.
T. 943794700
biblioteca.mgep@mondragon.edu