

PROTECCIÓN DE DATOS PERSONALES E IDENTIDAD DIGITAL

Documento para el alumnado

Duración del reto

Entre 4 y 6 horas

Tu equipo

Nombre del equipo:

Miembros del equipo:

Descripción de la situación

Te han regalado un nuevo dispositivo digital (el profesor o profesora te dirá qué tipo, si un móvil, una Tablet... o si tu equipo puede escogerlo libremente). Como usuario/a responsable, quieres asegurarte de que el dispositivo y la información que introduzcas en él están lo más protegidos posible.

Tu intención es usar el dispositivo para uso general: e-mail, explorador web, redes sociales, banca on-line...

Tu reto es demostrar que eres consciente y entiendes los riesgos que presenta el uso de dispositivos digitales y que sabes cómo protegerte a nivel de usuario.

En particular, céntrate en cómo proteger tus datos personales y tu identidad digital de posibles brechas de seguridad. Ten en cuenta, de forma muy importante, también tu presencia on-line.

Resultados de aprendizaje

U2L01. El alumno/a es capaz de adecuar su comportamiento en el mundo digital y gestionar su huella digital adecuadamente.

U2L02. El alumno/a es capaz de identificar los peligros de que su identidad sea robada o utilizada indebidamente por otros.

U2L03. El alumno/a es capaz de proteger información relevante para otra persona de su entorno (como un compañero de trabajo, una amiga...)

U2L04. El alumno/a es capaz de encontrar, borrar y/o modificar información on-line sobre sí mismo/a.

U2L05. El alumno/a es capaz de gestionar su propio rastro digital.

U2L06. El alumno/a es capaz de actuar de forma crítica cuando comparte información on-line sobre sí mismo/a.

U2L07. El alumno/a es capaz de hacer uso de múltiples identidades digitales, dirigidas a diferentes objetivos.

Recursos que puedes usar para empezar

- <http://www.identitytheft.org.uk/>
- <https://www.internetsociety.org/es/tutorials/your-digital-footprint-matters/> (ES)
- <https://www.tomsguide.com/us/personally-identifiable-information-definition,news-18036.html>
- <https://www.bing.com/videos/search?q=How+to+Be+Safe+Online&&view=detail&mid=D895C76F4EB8001A78B0D895C76F4EB8001A78B0&&FORM=VRDGAR>
- <https://www.bing.com/videos/search?q=How+to+Be+Safe+Online&&view=detail&mid=5824FB060F03A2765DDD5824FB060F03A2765DDD&&FORM=VDRVRV>
- <https://www.osi.es/es/actualidad/blog/2019/03/20/consideraciones-tener-en-cuenta-al-publicar-en-redes-sociales> (ES)
- <https://www.bing.com/videos/search?q=how+to+keep+information+secure+on+a+computer&&view=detail&mid=62715D037BCDF795775C62715D037BCDF795775C&&FORM=VRDGAR>
- <https://www.bing.com/videos/search?q=how+to+protect+your+passwords+logins&&view=detail&mid=3FEF7F7615BF3B1226653FEF7F7615BF3B122665&&FORM=VDRVRV>

Esta es sólo una pequeña lista de recursos, pero encontrarás muchos más en internet.

Estos recursos también se comparten con el alumnado en el documento del reto correspondiente.

Recommended process

Para resolver el reto, tendréis que trabajar de forma organizada. Os recomendamos seguir estos pasos:

1. Estableced los parámetros que necesitaréis para resolver el reto. Por ejemplo, en este caso podrían ser: riesgos asociados a la tecnología, medidas protectoras, identificación de información vulnerable...
2. Buscad información relacionada con esos parámetros (ved los recursos propuestos, pero buscad también otros que consideréis necesarios).
3. Seleccionad qué información es importante para resolver el reto.
4. Identificad distintas propuestas para resolver el reto.
5. Seleccionad la propuesta o propuestas que son más efectivas desde el punto de vista del grupo.
6. Planificad qué acciones necesitáis para resolver el reto (una vez que sabéis qué necesitáis, describid cómo lo haréis).
7. Implementad las acciones.
8. Presentad vuestros resultados y conclusiones (siguiendo las indicaciones del profesor o profesora).
9. Evaluad cómo habéis realizado el reto.

Criterios de evaluación

1. Tu equipo es capaz de describir y entender el concepto de huella digital y su rastro digital así como la normativa al respecto.
2. Tu equipo describe las desventajas de que su PII (Información personal identificable) sea usada por otros.
3. Tu equipo es capaz de identificar y explicar técnicas que puedan usarse para proteger la PII de personas y organizaciones.
4. Tu equipo, y de forma individual cada miembro, es capaz de encontrar y editar información de sus propios perfiles en la red
5. Tu equipo es capaz de gestionar su huella digital
6. Tu equipo es capaz de identificar métodos para asegurar que su PII se comparte de forma segura.
7. Tu equipo es capaz de usar la identidad digital más adecuada para propósitos específicos, tanto como individuos como a nivel de organización.