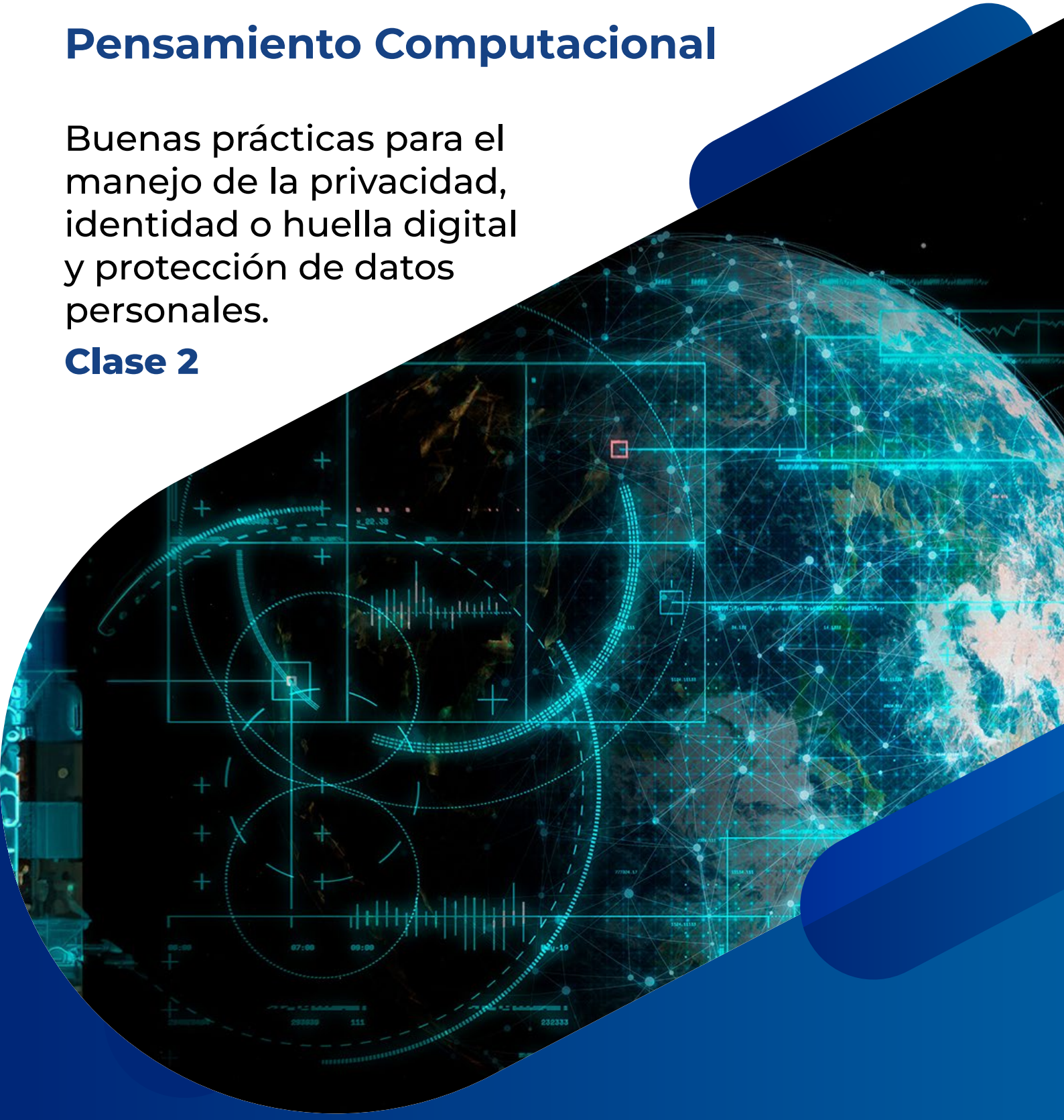
Pensamiento Computacional

Buenas prácticas para el manejo de la privacidad, identidad o huella digital y protección de datos personales.

Clase 2



Ingeniería en ciberseguridad

La excelencia no se improvisa

CLASE 2

1.1. Buenas prácticas para el manejo de la privacidad, identidad o huella digital y protección de datos personales.

Hemos visto los conceptos básicos sobre imagen y huella digital, y conoces la importancia de la protección de datos personales. A continuación, se presentan ocho buenas prácticas para gestionar y proteger tu información. ¡Ponlas en práctica para crear hábitos de seguridad!

Figura 1

Seguridad Datos personales

Nota. Licencia Creative Commons

1.1.1. Crea contraseñas seguras

Una contraseña segura te ayuda a proteger tu información personal y evita que otras personas puedan acceder a tus correos electrónicos, cuentas bancarias, redes sociales o archivos. Las mejores contraseñas son aquellas que son difíciles de adivinar y que tardan tiempo en ser descifradas.

Figura 2

Contraseñas seguras

Nota. Licencia Creative Commons.

Sigue estos consejos para tus contraseñas:

a) Utiliza un mínimo de 12 caracteres, combinando números, símbolos (caracteres ASCII estándar), letras mayúsculas y minúsculas.
b) Toma como base una frase, la letra de una canción, un poema o algo que te guste para crear tu contraseña. Ejemplo: L4v!d4E$Un4Av3ntur4 (La vida es una aventura).
c) Evita usar tu fecha de nacimiento, tu cédula o tu nombre de pila, ya que sería fácil para otra persona adivinar tu contraseña.
d) Crea una contraseña distinta para cada aplicación: una para el correo electrónico, otra para el acceso al banco y otra para redes sociales, etc.
e) Si te resulta difícil recordar todas tus contraseñas, utiliza un administrador de contraseñas.
f) Por ejemplo, el que provee Google: https://support.google.com/accounts/answer/620865.
g) Protege tus contraseñas al momento de escribirlas o activa la opción de ocultar cuando estén escritas.

APRENDIENDO MÁS:

¿Cuál es una medida importante para proteger tus datos al utilizar sitios web?

a) Utilizar la misma contraseña en todos los sitios.
b) Compartir tu información personal en los formularios en línea.
c) Evitar el uso de autenticación de dos factores.
d) Utilizar contraseñas únicas y fuertes para cada sitio.

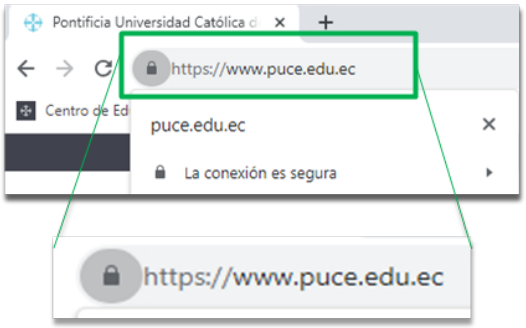
Respuesta correcta: D

1.1.2. Comprueba si un sitio web es seguro antes de acceder a él

a) Mira la URL del sitio web; asegúrate de que tenga el protocolo seguro https. b) Busca que el candado esté cerrado al lado de la dirección URL. c) Observa que la dirección del sitio sea correcta y esté bien escrita. Las páginas fraudulentas pueden tener otra dirección y, además, pueden presentar faltas ortográficas o enlaces vacíos que no llevan a ningún sitio. d) Ten cuidado con las páginas que muestren publicidad agresiva o ventanas emergentes que soliciten claves o datos personales. e) Si desconfías de un sitio web, utiliza un comprobador de seguridad como Google Safe Browsing: https://transparencyreport.google.com/safe-browsing/search.

Figura 3

Como detectar un sitio web seguro.



Nota. Captura: Sitio web www.puce.edu.ec.

APRENDIENDO MÁS:

¿Cómo puedes verificar si un sitio web es seguro para realizar transacciones en línea?

a) Verificar que el sitio tenga un diseño atractivo.
b) b) Buscar el ícono de un candado en la barra de direcciones y que la URL comience con https://.
c) Ignorar cualquier advertencia de seguridad que aparezca.
d) Basarse únicamente en la apariencia visual del sitio.

Respuesta correcta: B

1.1.3. **Ajusta tu configuración de privacidad en las redes sociales**

Sigue estas recomendaciones para cuidar tu privacidad:

a) Lee la política de privacidad para conocer cómo utilizará la empresa la información que recopile sobre ti. Si no te sientes seguro con los términos, no uses la aplicación.
b) Utiliza contraseñas seguras.
c) Activa la autenticación de dos pasos. Algunas redes sociales, además de solicitar el ingreso de tu contraseña, también piden un código de uso único que se envía a tu correo electrónico o a tu celular.
d) Cierra las cuentas que ya no uses y borra tus datos. No basta con solo desactivar tu cuenta; tus datos podrían permanecer en los servidores de la empresa, así que solicita que la red social los elimine.
e) Revisa las opciones de privacidad que ofrece cada red social que utilizas.

Figura 4

Redes sociales

Nota. Licencia Creative Commons.

APRENDIENDO MÁS:

¿Cómo puedes protegerte del robo de identidad en redes sociales?

a) Compartiendo toda tu información personal.
b) Aceptando todas las solicitudes de amistad.
c) Revisando y ajustando la configuración de privacidad regularmente.
d) Desactivando tu cuenta temporalmente.

Respuesta correcta: C

1.1.4. **Limita la cantidad de datos personales que compartes en Internet**

Figura 5

Compartir datos

Nota. Licencia Creative Commons.

Publicar lo que hacemos en redes sociales se ha vuelto una práctica cotidiana, especialmente entre los jóvenes, quienes a menudo no son conscientes del riesgo que conlleva. Exponer nuestras vidas en las redes sociales abre la puerta a desconocidos, hackers o delincuentes para acceder a nuestra información personal y utilizarla para delitos informáticos, extorsiones o secuestros.

- Cuida lo que publicas en tus muros; evita **compartir información sensible** como ubicaciones, tiquetes de viaje, información bancaria, fotos de menores, y la dirección de tu casa o de tu trabajo.
- Piensa dos veces antes de publicar algo; no lo hagas cuando estés con sentimientos encontrados y evita **escribir o decir algo de lo que puedas arrepentirte más tarde**.
- Comparte tu información solo con tu grupo íntimo de contactos, así aseguras que no llegue a manos indeseadas.

APRENDIENDO MÁS:

¿Cuál de los siguientes NO es un ejemplo de información personal sensible?

a) Marca de tu computadora
b) Nombre y apellido
c) Número de teléfono
d) Número de seguro social

Respuesta correcta: A

1.1.5. Ten cuidado si utilizas la función Iniciar sesión con Facebook o Google

Figura 6

Inicios de sesión redes

Nota. Captura de pantalla

Varios sitios web o aplicaciones han optado por utilizar el inicio de sesión con cuentas de Google, Microsoft, LinkedIn, Facebook u otra red social. Este método de autenticación se conoce como **inicio de sesión único (SSO)** o **inicio de sesión social**, y se usa para las cuentas personales en línea.

Cuando se vinculan cuentas, se permite que la información personal se transmita al sitio web. Debido a lo fácil que es configurarlo, se podría estar consintiendo la transferencia de más información de la que se espera.

Si bien Facebook, Google, Microsoft y Apple permiten comprobar todas las conexiones con terceros, revocar el acceso no significa que también se esté revocando el consentimiento de un sitio web para utilizar los datos.

Según Camilo Gutiérrez Amaya, jefe del Laboratorio de Investigación de ESET Latinoamérica, iniciar sesión con tus cuentas sociales puede ahorrar tiempo. Sin embargo, si los sitios web guardan tu información personal, como nombre completo, direcciones, datos bancarios o tarjetas de crédito, lo mejor es optar por crear una cuenta independiente.

Otras recomendaciones para usar el inicio de sesión social son:

- La contraseña nunca se comparte con el sitio web o la aplicación, sino que la identidad se verifica mediante un token de autenticación.
- Protege la **contraseña de inicio social**, asegurándote de que sea **robusta** y difícil de hackear.
- Procura que las **contraseñas** sean **distintas** entre las **diferentes redes sociales**.

APRENDIENDO MÁS:

¿Qué es el Inicio de Sesión Único (SSO)?

a) Un método para tener múltiples contraseñas para diferentes cuentas.
b) Un enfoque que permite a los usuarios acceder a varias aplicaciones con una única identificación.
c) Un sistema que requiere autenticación en cada aplicación por separado.
d) Un programa de edición de imágenes.

Respuesta correcta: B

1.1.6. **Configura alertas de Google con tu nombre para supervisar el contenido que has creado.**

Figura 7

Seguridad datos

Nota. Licencia Creative Commons.

Google tiene una herramienta que te permite crear alertas sobre un tema que aparezca en los resultados de su buscador. Te envían correos electrónicos sobre las alertas que hayas creado; estas pueden ser sobre noticias, productos o menciones de tu nombre.

Al crear una alerta para tu nombre, podrás dar seguimiento al contenido que has publicado en Internet y te ayudará a detectar si alguien usa tu nombre de forma inapropiada.

Para crear una alerta, necesitas una cuenta en Google. El siguiente enlace te mostrará los pasos para crear, cambiar o eliminar una alerta: Crear una alerta.

APRENDIENDO MÁS:

¿Cómo puedes personalizar una alerta en Google Alerts?

a) No es posible personalizar las alertas.

b) Seleccionar la opción “Alerta General”.
c) Especificar palabras clave, frecuencia de entrega y tipo de contenido.
d) Enviar un correo electrónico a Google con tus preferencias.

Respuesta correcta: C

1.1.7. Actualiza siempre el software de tus dispositivos.

Figura 8

Actualización software

Nota. Licencia Creative Commons.

Las actualizaciones de software son mejoras que crean los desarrolladores de los diferentes programas instalados en tu computador o dispositivo móvil. Estas mejoras se implementan con el objetivo de corregir errores y optimizar las funciones que ya están en funcionamiento. Son gratuitas, fáciles y rápidas de instalar, y normalmente se realizan de forma automática.

La principal razón para actualizar el software es la seguridad, ya que así mantenemos protegidos nuestros datos y los sistemas que usamos a diario.

Un dato curioso: según el blog Idearius, “más del 90% de las actualizaciones de programas y sistemas operativos (como Windows y Android) son para corregir vulnerabilidades de seguridad. Los agujeros en la seguridad son los puntos de entrada más comunes para el malware (acrónimo formado a partir de ‘software malicioso’ en inglés) y los intrusos en los sistemas.

APRENDIENDO MÁS:

¿Qué es el malware?

a) Un tipo de pez.
b) Un software malicioso diseñado para dañar o infiltrar un sistema.

c) Un servicio de almacenamiento en la nube.
d) Un programa de seguridad en línea.

Respuesta correcta: B

1.1.8. **Protección de datos personales en las organizaciones.**

La Ley de Protección de Datos en Ecuador entra en vigor dos años a partir de la fecha de su publicación, el 26 de mayo de 2021.

Todas las organizaciones están obligadas a identificar los datos personales que manejan, los soportes donde se encuentran esos datos y a revisar el tratamiento que se les da. Todo esto con el fin de verificar si el tratamiento cumple con lo determinado en la ley.

Cada organización debe adaptar su infraestructura y su giro de negocio al tratamiento de datos, lo que permitirá aplicar la ley de manera adecuada. Además, será necesario evaluar sus procedimientos para implementar los cambios y adaptaciones que sean necesarios.

REFERENCIAS

Agencia Española de Protección de Datos (AEPD). (2021). Guía sobre el uso de contraseñas. Recuperado de https://www.aepd.es/sites/default/files/2021-01/guia-uso-contrasenas.pdf

Cybersecurity and Infrastructure Security Agency (CISA). (2019). Security Tip (ST04-002): Choosing and protecting passwords. Recuperado de https://us-cert.cisa.gov/ncas/tips/ST04-002

European Union Agency for Cybersecurity (ENISA). (2019). Password guidance: Simplifying your approach. Recuperado de https://www.enisa.europa.eu/publications/password-guidance

Google Support. (s.f.). Usar el administrador de contraseñas. Recuperado de https://support.google.com/accounts/answer/620865

Instituto Nacional de Ciberseguridad (INCIBE). (2020). Guía para la creación de contraseñas seguras. Recuperado de https://www.incibe.es/protege-tu-empresa/guia-para-la-creacion-de-contrasenas-seguras

International Association of Privacy Professionals (IAPP). (2021). Data protection in practice. Recuperado de https://iapp.org/resources/article/data-protection-in-practice

PricewaterhouseCoopers. (s.f.). Todo lo que debes conocer sobre la protección de datos personales. PwC. Recuperado de https://www.pwc.ec/es/entrevistas-de-temas-de-interes/todo-lo-que-debes-conocer-sobre-la-proteccion-de-datos-personales.html

The National Institute of Standards and Technology (NIST). (2020). Digital identity guidelines. Recuperado de https://pages.nist.gov/800-63-3/sp800-63b.html

GLOSARIO

Contraseñas seguras: Son claves utilizadas para proteger información personal en diversas plataformas digitales. Una contraseña segura incluye una combinación de caracteres alfanuméricos y símbolos, y tiene una longitud mínima de 12 caracteres, lo que la hace difícil de adivinar o descifrar. Se recomienda usar una contraseña distinta para cada aplicación y emplear un administrador de contraseñas para gestionarlas.

Protección de datos personales: Se refiere a las medidas y prácticas implementadas para asegurar que la información personal de los individuos sea tratada de acuerdo con las leyes y regulaciones pertinentes. En Ecuador, la Ley de Protección de Datos Personales obliga a las organizaciones a identificar, gestionar y proteger los datos personales que manejan, garantizando que su tratamiento cumpla con las normativas establecidas.

PUCE Virtual

La excelencia no se improvisa

síguenos

ICYS - 12 - 241