Well Dept.

BIENESTAR CORPORATIVO

01

Ciberseguridad.–

Protegiendo tu privacidad en línea: cómo mantener tus datos seguros.

Objetivos del tema

- Compartir recomendaciones para adquirir mejores prácticas de ciberseguridad en la empresa.
- Conocer y crear conciencia sobre los distintos tipos de amenazas a la ciberseguridad de la empresa.
- Dar a conocer estrategias para enfrentar el phishing de manera efectiva.
- Practicar recomendaciones para hacer home office de manera segura.

Beneficios para las audiencias

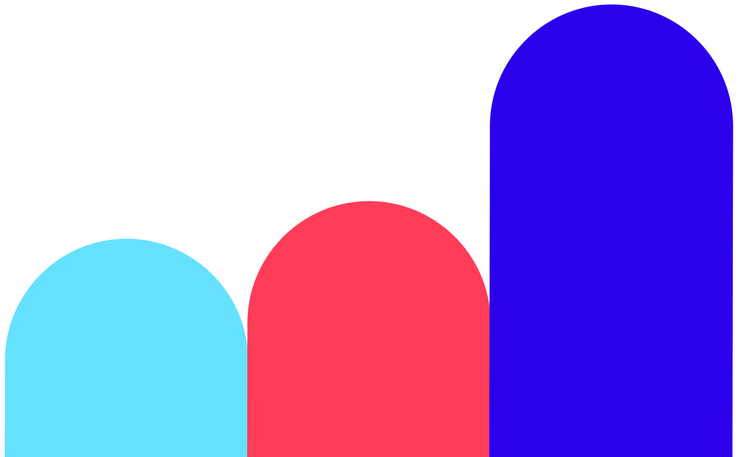
Crear conciencia sobre la importancia de la ciberseguridad de la empresa.

Dar a conocer a los colaboradores que no están solos en este proceso.

Facilitar información básica sobre ciberseguridad.

Ciberseguridad / Relevancia —

La ciberseguridad es **uno de los desafíos más importantes de la era digital.** El crecimiento global de las redes y la información, impulsado por la innovación tecnológica, ha permitido a la sociedad crear prosperidad y elevar la calidad de vida, sin embargo, este rápido cambio ha generado también un desafío: gestionar los riesgos de seguridad a medida que el mundo depende cada vez más de la cibernética y digitalización.



TEMA	**CIBERSEGURIDAD**
OBJETIVOS	Crear cultura entorno a las prácticas de ciberseguridad.
BENEFICIOS	Empresas y colaboradores mejor protegidos.
EXPERTO	Carlos Alanís. (CEO, Banyax)
RELEVANCIA	Existe cada vez más dependencia a la digitalización.
FRECUENCIA	Semanal / Diaria.

Experto

Carlos Alanís

- CEO / Banyax.
- Más de 28 años de experiencia como líder de información.

Semana 1

7 Consejos para mejores prácticas de ciberseguridad.

¿Qué es ciberseguridad? conjunto de medidas y prácticas diseñadas para proteger los sistemas informáticos, redes, dispositivos y datos de posibles amenazas y ataques cibernéticos. Su objetivo principal es salvaguardar la confidencialidad, integridad y disponibilidad de la información.

NÚMERO 1
NO abras correos electrónicos o archivos adjuntos de extraños. Por lo general todos sabemos que no es bueno pero pocos hacemos caso a este consejo.

NÚMERO 2
Protege TODO con contraseñas que solo tú conozcas, como tu celular, computadora, tablets, correo electrónico, IMPORTANTE trata de cambiar con cierta frecuencia la contraseña y utiliza diferentes para cada cuenta.

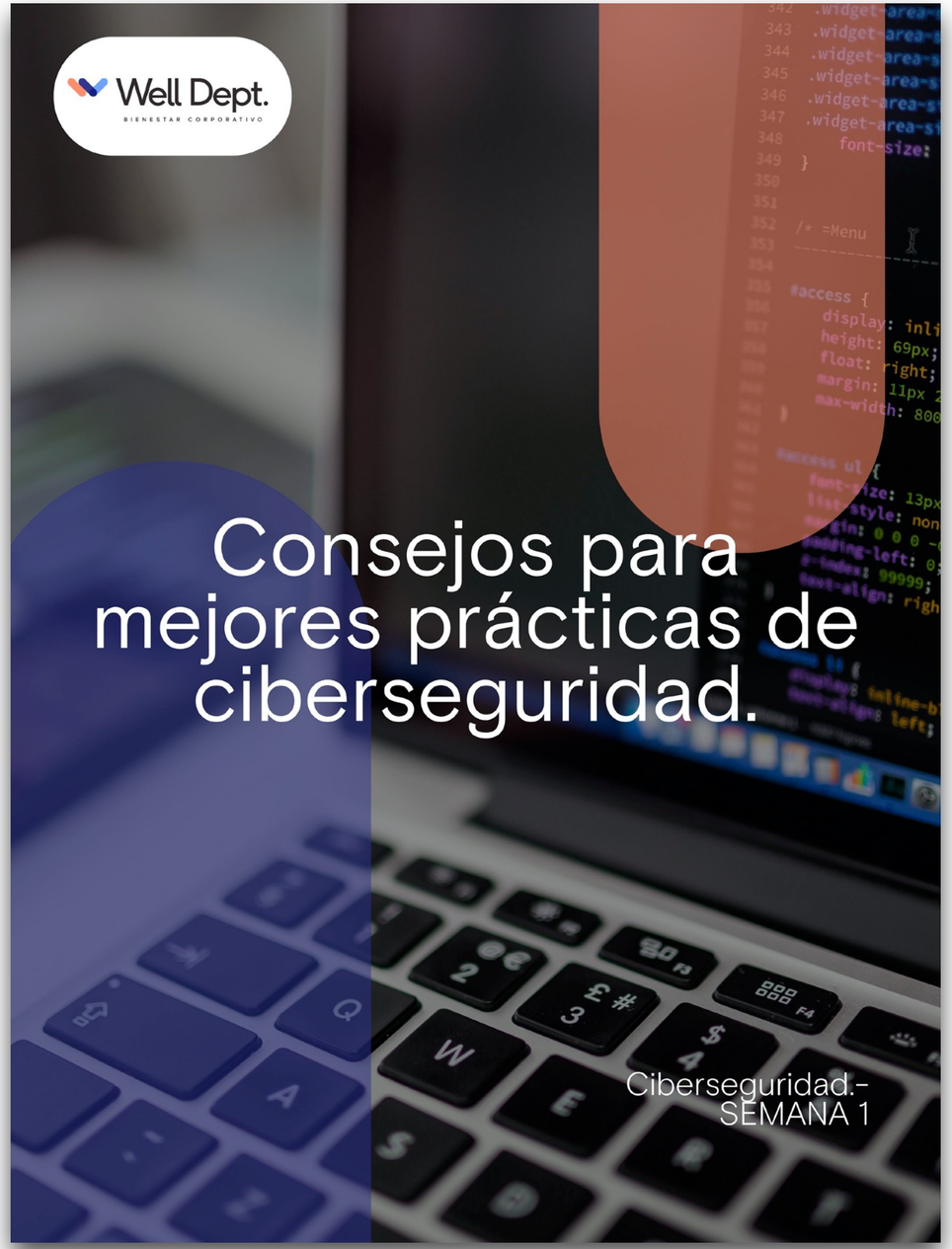
NÚMERO 3
ACTUALIZA, muchos posponemos las actualizaciones de los software por pereza, pero esto nos ayuda a que nuestra información esté cada vez más protegida

NÚMERO 4
Realiza copias de seguridad de forma periódica, la información que contienen tus cuentas son muy importantes

NÚMERO 5
Evita hacer uso de Wi-Fi públicos. Cada vez tenemos estos accesos de forma más rápida pero no es lo ideal, pudieran ser una trampa.

NÚMERO 6
Revela lo menos posible sobre ti en un espacio público. Al limitar la cantidad de información personal que compartimos en espacios públicos, reducimos la posibilidad de que los ciberdelincuentes recopilen datos sobre nosotros y utilicen esa información para cometer robo de identidad o fraudes.

NÚMERO 7
Apaga los dispositivos inteligentes cuando realices llamadas confidenciales. Si los dispositivos inteligentes permanecen encendidos y conectados a la red durante llamadas confidenciales, existe la posibilidad de que puedan ser comprometidos por ciberdelincuentes o interceptores.



*Referencia de diseño de material, imagen y mensaje.

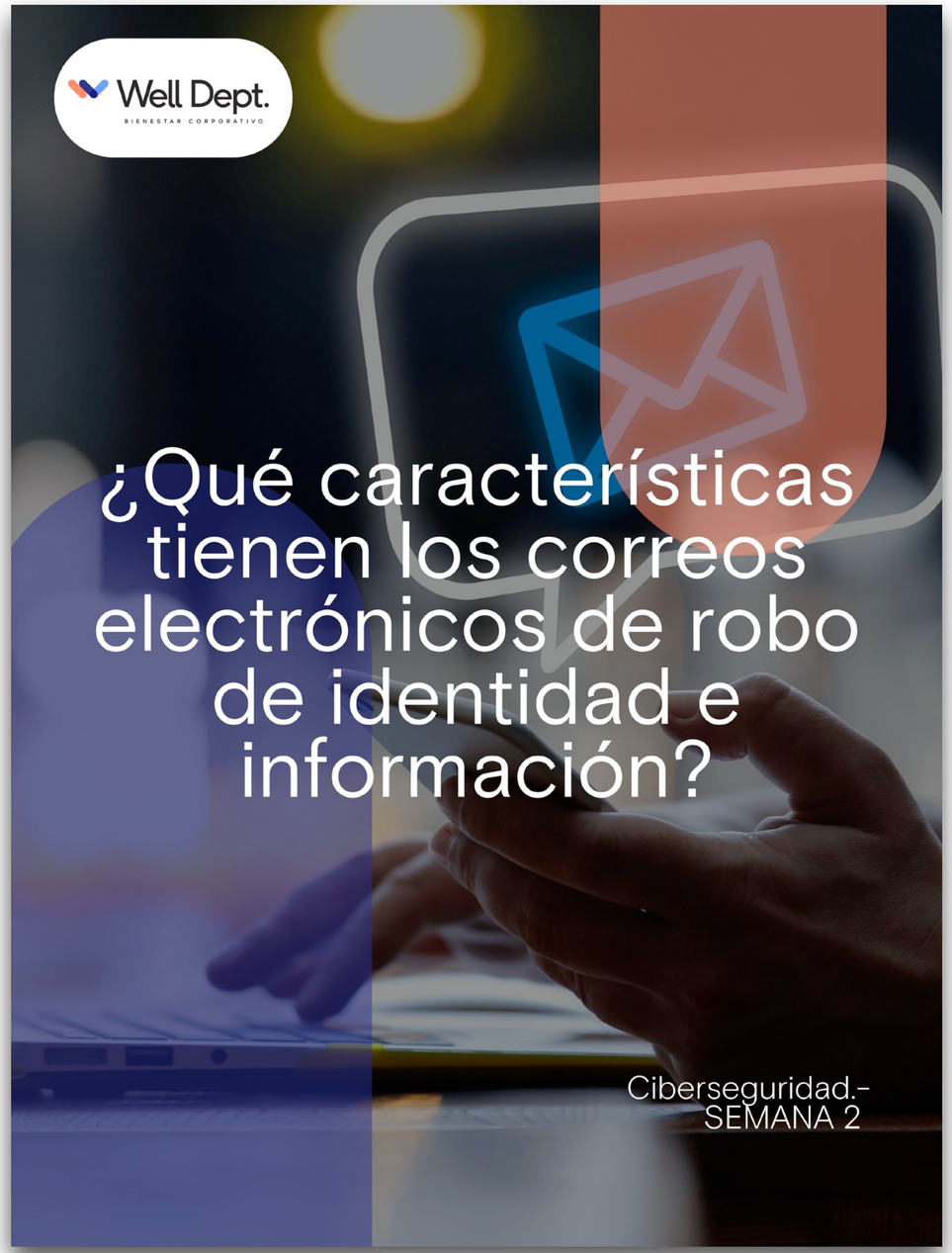
Semana 2

¿Qué características tienen los correos electrónicos de robo de identidad e información?

¿Qué es robo de identidad?
El robo de identidad es un delito en el cual un individuo obtiene, utiliza o manipula información personal de otra persona sin su consentimiento, con el propósito de cometer fraudes financieros, obtener beneficios ilegales o realizar actividades delictivas en nombre de la víctima.

NO ABRAS CORREOS CON LAS SIGUIENTE CARACTERÍSTICAS:
Con archivos adjuntos o vínculos.
Con errores de ortográficos.
Con gramática deficiente.
Con gráficos con aspecto poco profesional.
2 Consejos para evitar este tipo de correos.
Elimina estos correos sin abrirlos.
Bloquea el remitente de forma manual.

Tecnicismos a lenguaje coloquial.
Vínculos: Links o ligas.
Gramática: Con palabras u oraciones mal escritas o estructuradas.
Gráficos: Con imágenes poco profesionales.
Remitente: la dirección de correo electrónico.



*Referencia de diseño de material, imagen y mensaje.

Semana 3

Cómo detectar un sitio de internet falso.

NÚMERO 1
Revisa bien el nombre del dominio, en ocasiones seleccionamos el sitio web desde un buscador sin verificar si es el correcto.

NÚMERO 2
Ten cuidado con el método de pago que usas, si agregas tu información falso puedes perder tu dinero.

NÚMERO 3
Si la información o la oferta es demasiado buena para ser verdad podría ser una práctica fraudulenta.

NÚMERO 4
Si aún no estás seguro de la credibilidad de un sitio web, busca comentarios de otras personas en Internet sobre esa página. Una reputación, sea buena o mala, se esparce por Internet en cuestión de segundos.

Dominio: La manera en la que está estructurada la dirección de la página web.

*Referencia de diseño de material, imagen y mensaje.

Semana 4

Usa tus Redes Sociales de forma segura.

NÚMERO 1
Configura todas las opciones de privacidad de tus redes sociales, procurando dejar poca información visible para personas que no conozcas.

NÚMERO 2
No sigas cuentas de personas desconocidas ni los aceptes en tus redes sociales. Así evitarás al máximo recibir mensajes que vulneren tu seguridad.

NÚMERO 3
Usa los buscadores dentro de las redes sociales para encontrar información sobre archivos o mensajes que consideras sospechosos. En la mayoría de las redes es común que los usuarios compartan su postura frente a este tipo de casos.

NÚMERO 4
Usa contraseñas seguras con combinaciones de letras mayúsculas y minúsculas, caracteres y números. Recuerda que este es el principal medio de protección de tus datos en internet.

*Referencia de diseño de material, imagen y mensaje.

Guía de implementación y manejo de materiales.

Acceso a material:

(A) Identifique la carpeta “**01 Ciberseguridad**”.
(B) Consulte el paquete “**Materiales de implementación**” **incluidos en la carpeta.**

Secuencia de implementación:

Semana 1.- Video 1 (*Consejos para mejores prácticas de ciberseguridad.*), póster 1, archivo digital para difusión 1, actividad grupal 1.

Semana 2.- Video 2 (*Tipos de amenazas a la ciberseguridad.*), póster 2, archivo digital para difusión 2, artículo de apoyo 1.

Semana 3.- Video 3 (*Estrategias para enfrentar el phishing.*), póster 3, archivo digital para difusión 3.

Semana 4.- Video 4 (*Recomendaciones para trabajar home office de manera segura.*), póster 4, archivo digital 4, artículo de apoyo 2, **evaluación**.

Ciberseguridad	Sem. 1	Sem. 2	Sem. 3	Sem. 4
LUNES	Póster	Póster	Póster	Póster
MARTES	Mail		Mail	
MIÉRCOLES	Archivo digital	Archivo digital	Archivo digital	Archivo digital
JUEVES		Mail		Mail
VIERNES	Video	Video	Video	Video

TIPS semanales

1.- Mantén tus contraseñas seguras y cámbialas regularmente.

2.- No compartas información personal o confidencial en correos electrónicos no seguros.

3.- Utiliza una red virtual privada (VPN) para proteger tus datos al navegar en internet.

4.- Actualiza regularmente tu software y antivirus para mantenerlo protegido contra amenazas.

5.- Sé cauteloso con los enlaces y archivos adjuntos desconocidos en correos electrónicos o mensajes.

6.-Crea contraseñas únicas y fuertes para cada cuenta en línea.

TIPS semanales

7.- Utiliza autenticación de dos factores cuando esté disponible.

8.- Evita abrir correos electrónicos o descargar archivos de remitentes desconocidos.

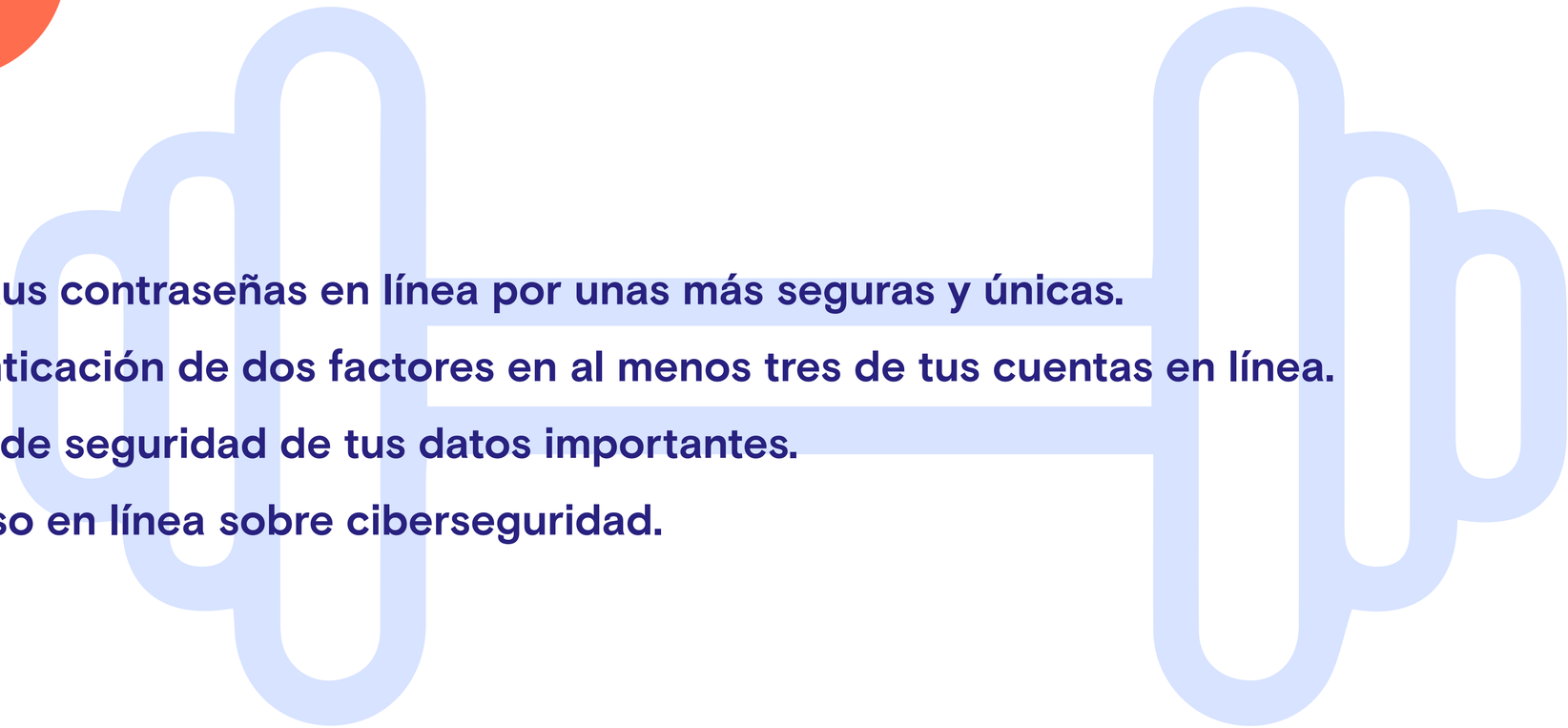
9.- Mantén actualizados todos tus dispositivos y software para garantizar la seguridad más reciente.

10.- No compartas información personal o financiera a través de un enlace de correo electrónico.

11.- Realiza copias de seguridad regulares de tus datos importantes.

12.- Asegúrate de que tu red doméstica esté segura.

RETOS semanales



1.- Cambia todas tus contraseñas en línea por unas más seguras y únicas.

2.- Activa la autenticación de dos factores en al menos tres de tus cuentas en línea.

3.- Haz una copia de seguridad de tus datos importantes.

4.- Realiza un curso en línea sobre ciberseguridad.

RETOS semanales

ACTIVIDADES grupales

1.- Juego de roles de phishing: Uno de los miembros del grupo envía un correo electrónico de phishing (previamente revisado por el instructor para asegurarse de que es seguro) a los demás, y estos tienen que identificar las señales de que es un intento de phishing.

2.- Concurso de contraseñas: Los grupos deben crear la contraseña más segura posible y luego explicar por qué es segura. El instructor determinará cuál es la mejor según los principios de la ciberseguridad.

3.- Taller de navegación segura: En grupos, los participantes pueden investigar y compartir consejos y herramientas para mantener la navegación segura en la web.

ACTIVIDADES grupales

4.- Juego de Escape Room digital: Diseña un juego de escape room que los participantes tengan que resolver utilizando su conocimiento sobre ciberseguridad. Podría implicar descifrar códigos, evitar trampas de phishing y asegurarse de que su "información" esté segura.

5.- Análisis de caso: Proporciona a los grupos un caso de estudio de una violación de ciberseguridad en el mundo real. Los grupos deben analizar qué salió mal y cómo podría haberse evitado.

ACTIVIDADES grupales

*Estas actividades promueven la interacción grupal, ayudando a los participantes a aprender de manera más efectiva sobre este tema.

· **Charla de expertos:** Invita a un experto en ciberseguridad para que dé una charla y luego organiza grupos de discusión para analizar lo que han aprendido.

· **Debate de ética en ciberseguridad:** Proporciona una serie de escenarios que plantean dilemas éticos relacionados con la ciberseguridad (por ejemplo, la tension entre privacidad y seguridad). Los grupos deben debatir y llegar a una conclusión.

· **Crea tu política de ciberseguridad:** Los grupos deben crear una política de ciberseguridad para una empresa ficticia. Deberán considerar todos los aspectos importantes de la ciberseguridad y cómo se aplicarían en un entorno empresarial.

CUESTIONARIO de conocimiento

*Cuestionario ampliado para evaluar el nivel de conocimiento en el módulo de Ciberseguridad.

1.- ¿Qué es la ciberseguridad?

a) Protección de computadoras.

b) Protección de información digital.

c) Protección de redes sociales.

d) Protección de la privacidad en línea.

2.- ¿Qué es un ataque de phishing?

a) Un virus que daña tu computadora.

b) Un intento de obtener información confidencial de manera fraudulenta.

c) Un software que protege tu computadora.

d) Un tipo de malware que ralentiza tu sistema.

3.- ¿Qué debe hacer si recibe un correo electrónico de un remitente desconocido con un enlace adjunto?

a) Abrir el enlace inmediatamente.

b) Responder el correo electrónico.

c) Ignorar el correo electrónico.

d) Enviar el correo electrónico a sus contactos.

4.- ¿Cómo puedes proteger tu información en línea?

a) Usar la misma contraseña en todas las cuentas.

b) Compartir tu contraseña con amigos y familiares.

c) Usar una combinación de letras, números y caracteres especiales en tus contraseñas.

d) No usar contraseña.

CUESTIONARIO de conocimiento

*Cuestionario ampliado para evaluar el nivel de conocimiento en el módulo de Ciberseguridad.

5.- ¿Qué es un firewall y por qué es importante?

a) Es un tipo de virus.

b) Es una barrera de protección para bloquear el acceso no autorizado a tu red.

c) Es un software que mejora la velocidad de tu computadora.

d) Es un hardware que necesitas para conectar tu computadora a Internet.

6.- ¿Qué es un software antivirus?

a) Un programa que protege tu computadora de virus.

b) Un software que crea virus.

c) Un programa que ayuda a tu computadora a funcionar más rápido.

d) Un software que borra todos los archivos de tu computadora.

7.- ¿Qué es el cifrado de datos?

a) Un proceso que hace que los datos sean ilegibles sin una clave de decodificación.

b) Un proceso que duplica los datos.

c) Un proceso que elimina los datos.

d) Un proceso que protege los datos de ser copiados.

8.- ¿Qué es un ataque de fuerza bruta?

a) Un ataque que implica intentar todas las combinaciones posibles de contraseñas hasta que se encuentra la correcta.

b) Un ataque que involucra amenazas físicas para obtener acceso.

c) Un ataque que involucra el uso de un martillo.

d) Un ataque que involucra el uso de mucha electricidad.

CUESTIONARIO de conocimiento

*Cuestionario ampliado para evaluar el nivel de conocimiento en el módulo de Ciberseguridad.

9.- ¿Qué es la autenticación de dos factores (2FA)?

a) Un proceso que requiere dos contraseñas para acceder a una cuenta.

b) Un proceso que requiere una contraseña y un segundo método de verificación para acceder a una cuenta.

c) Un proceso que permite a dos personas acceder a una cuenta simultáneamente.

d) Un proceso que requiere dos computadoras para acceder a una cuenta.

10.- ¿Qué es un ataque DDoS?

a) Un ataque que implica enviar grandes cantidades de tráfico a un sitio web para hacerlo inaccesible.

b) Un ataque que implica enviar spam a un sitio web.

c) Un ataque que implica hackear una base de datos.

d) Un ataque que implica tomar el control de un sitio web.

11.- ¿Qué es la ingeniería social en el contexto de la ciberseguridad?

a) Construcción de redes y sistemas informáticos.

b) Manipulación de personas para que revelen información confidencial.

c) Programación de software.

d) Diseño de sitios web.

12.- ¿Qué se debe hacer si tu información personal ha sido comprometida en una violación de datos?

a) Ignorarlo, probablemente no sea gran cosa.

b) Cambiar todas tus contraseñas y monitorear tus cuentas para detectar actividad inusual.

c) Enviar un correo electrónico a todos tus contactos informándoles sobre la violación.

d) Publicar sobre la violación en las redes sociales.

GUÍA DE INTER-PRETACIÓN

Cada respuesta correcta otorga 1 punto. / Las respuestas correctas son: 1-b, 2-b, 3-c, 4-c, 5-b, 6-a, 7-a, 8-b, 9-a, 10-a, 11-b, 12-b.

0-4 puntos: Nivel de conocimiento básico. Necesita mejorar su conocimiento sobre ciberseguridad. Recomendamos una revisión completa del módulo y/o actividades adicionales de aprendizaje.

5-8 puntos: Nivel de conocimiento intermedio. Posee algunos conocimientos sobre ciberseguridad pero todavía hay áreas para mejorar. Recomendamos una revisión de los temas con los que tuvo dificultades.

9-12 puntos: Nivel de conocimiento avanzado. Posee un buen conocimiento sobre ciberseguridad. Manténgase actualizado y continúe aprendiendo sobre nuevas amenazas y cómo prevenirlas.

LECTURAS RECOMENDADAS

GENERALES:

- Ciberseguridad: "Internet para dummies" de John R. Levine y Margaret Levine Young. Es una lectura introductoria que explica conceptos básicos de internet, incluyendo algunos temas de ciberseguridad.

PARA DIRECTIVOS:

- “Ciberseguridad. La protección de la información en un mundo digital" por Fernando de la Cuadra.
- “El gran libro del Community Manager: Técnicas y herramientas para sacarle partido a las redes sociales y triunfar en social media" por Manuel Moreno.

PARA NO DIRECTIVOS:

- “Internet Segura: Cómo protegerse al usar la red”, por el Instituto Nacional de Ciberseguridad de España.

Muchas gracias.

Well Dept.

BIENESTAR CORPORATIVO