I.- Datos Generales

Código	Título
EC1566	Aplicación de principios básicos de ciberseguridad para usuario final en organizaciones

Propósito del Estándar de Competencia

Servir como referente para la evaluación y certificación de las personas que utilizan de manera segura los equipos de cómputo, dispositivos móviles, de almacenamiento y del uso de internet para el desempeño de sus labores.

Asimismo, puede ser referente para el desarrollo de programas de capacitación y de formación basados en Estándares de Competencia (EC).

Este estándar se refiere únicamente a funciones para cuya realización no se requiere por disposición legal, la posesión de un título profesional. Por lo que para certificarse en este EC no deberá ser requisito el poseer dicho documento académico.

Descripción general del Estándar de Competencia

Describe la función de las personas cuando demuestran que pueden utilizar de manera segura las contraseñas, respaldos de información, navegación en sitios web, uso de correo electrónico y uso de redes sociales.

El presente EC se fundamenta en criterios rectores de legalidad, competitividad, libre acceso, respeto, trabajo digno y responsabilidad social.

Nivel en el Sistema Nacional de Competencias: Dos

Desempeña actividades programadas que, en su mayoría son rutinarias y predecibles. Dependen de las instrucciones de un superior. Se coordina con compañeros de trabajo del mismo nivel jerárquico.

Comité de Gestión por Competencias que lo desarrolló
ANUIES-FESE

Fecha de aprobación por el Comité Técnico del CONOCER:
25 de agosto de 2023

Fecha de publicación en el Diario Oficial de la Federación:
3 de octubre de 2023

Periodo sugerido de revisión /actualización del EC:
2 años

Ocupaciones relacionadas con este EC de acuerdo con el Sistema Nacional de Clasificación de Ocupaciones (SINCO)

Grupo unitario

2992 Otros técnicos no clasificados anteriormente.

Ocupaciones asociadas
Otros.

Ocupaciones no contenidas en el Sistema Nacional de Clasificación de Ocupaciones y reconocidas en el Sector para este EC
Usuarios en general de equipos de cómputo dentro de organizaciones

Clasificación según el sistema de Clasificación Industrial de América del Norte (SCIAN)

Sector:
54 Servicios profesionales, científicos y técnicos.
Subsector:
541 Servicios profesionales, científicos y técnicos.
Rama:
5419 Otros servicios profesionales, científicos y técnicos.
Subrama:
54199 Otros servicios profesionales, científicos y técnicos.
Clase:
541990 Otros servicios profesionales, científicos y técnicos.

Una vez publicado el presente EC en el Diario Oficial de la Federación, se integrará en el Registro Nacional de Estándares de Competencia que opera el CONOCER a fin de facilitar su uso y consulta gratuita.

Organizaciones participantes en el desarrollo del Estándar de Competencia

- Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES)
- Instituto Politécnico Nacional (IPN)
- Instituto Tecnológico de Sonora (ITSON)
- Universidad Autónoma de Campeche (UACAM)
- Universidad Autónoma de Yucatán (UADY)
- Universidad Autónoma del Estado de México (UAEMex)

Relación con otros estándares de competencia

Estándares relacionados

EC0156 Manejo básico del equipo de cómputo
EC0157 Manejo de Internet y correo electrónico
EC0190 Manejo de aplicaciones e información en equipo de cómputo, nivel básico

Aspectos relevantes de la evaluación

Detalles de la práctica:	• Para demostrar la competencia en este EC, se recomienda que se lleve a cabo en el lugar de trabajo y durante su jornada laboral; sin embargo, pudiera realizarse de forma simulada si el área de evaluación cuenta con los materiales, insumos, e infraestructura, para llevar a cabo el desarrollo de todos los criterios de evaluación referidos en el EC.
Apoyos/Requerimientos:	• Escritorio/mesa y silla. • Equipo de cómputo con acceso a internet, procesador de textos digitales, navegador web, software de antivirus,

software de transferencia archivos (fast copy), dispositivo de almacenamiento USB.
- Pluma, papelería, documentación con las instrucciones para el desarrollo de las actividades.

Duración estimada de la evaluación

- 3 horas en gabinete y 20 minutos en campo, totalizando 3 horas con 20 minutos

Referencias de Información

- Alegre Ramos, M. D., & García-Cervigón Hurtado, A. (2011). *Seguridad informática.* España: Ediciones Paraninfo, S.A.
- Argentina.gob.ar. (junio de 2023). Ministerio de Justicia y Derechos Humano. Obtenido de ¿Cómo reconozco una página falsa de internet?: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-puedo-detectar-una-pagina-falsa
- Avast. (2023). Avast. Obtenido de Cómo liberar espacio en disco: https://www.avast.com/es-es/c-how-to-free-up-disk space#:~:text=El%20espacio%20en%20disco%20es,disco%20o%20capacidad%20de%20almacenamiento.
- AVG.COM. (24 de septiembre de 2021). AVG. Obtenido de Comprobación de seguridad de sitios web: ¿Este sitio web es seguro?: https://www.avg.com/es/signal/website-safety
- BBVA. (2019). BBVA. Obtenido de ¿Qué son los enlaces maliciosos y cómo protegerse ante esta amenaza?: https://www.bbva.com/es/innovacion/que-son-los-enlaces-maliciosos-y-como-protegerse-ante-esta-amenaza/
- Caballero Escudero, P., Carbajosa Domínguez, J. M., & Gallego Cano, J. C. (2022). CFGB Montaje y mantenimiento de sistemas y componentes informáticos 2022. España: Editex.
- CEPAL. (2023). Comisión Económica para América Latina y el Caribe CEPAL Biblioteca CEPAL Repositorio Digital Pregúntanos. Obtenido de Qué son los Códigos QR: https://biblioguias.cepal.org/QR
- Colobran Huguet, M., Arqués Soldevila, J. M., & Marco Galindo, A. (2008). Administración de sistemas operativos en red. España: Editorial UOC, S.L.
- David Ngo, R. E. (2017). Virtual Private Network (VPN): Uses, Benefits, and Security Considerations. International Conference on Network and System Security (NSS).
- DGTID. (2021). Gobierno de Oaxaca. Obtenido de DGTID: https://www.oaxaca.gob.mx/dgtid/wp-content/uploads/sites/2/2021/07/Reconocer-spam.pdf
- Fernández, J. A. (2017). Sistemas seguros de acceso y transmisión de datos (MF0489_3). España: RA-MA S.A.
- Guevara Soriano, A. (2023). UNAM. Obtenido de Dispositivos Móviles: https://revista.seguridad.unam.mx/numero-07/dispositivos-moviles
- ICANN.ORG. (2023). Acerca de los nombres de dominio. Obtenido de: https://www.icann.org/resources/pages/about-domain-names-2018-09-12-es
- incibe. (2018). INCIBE. Obtenido de Copias de seguridad una guía de aproximación para el empresario: https://www.incibe.es/empresas/blog/copias-seguridad-guia-aproximacion-el-empresario
- incibe. (26 de junio de 2023). Obtenido de Cómo crear una copia de seguridad: https://www.incibe.es/sites/default/files/docs/guia_como_crear_una_copia_de_seguridad.pdf
- incibe. (2023). INCIBE. Obtenido de Phishing: https://www.incibe.es/aprendeciberseguridad/phishing

- Incibe.es. (27 de 01 de 2021). Gestores de contraseñas: ¿cómo funcionan? Obtenido de: https://www.incibe.es/ciudadania/blog/gestores-de-contrasenas-como-funcionan
- Incibe.es. (18 de 05 de 2021). Glosario de términos de ciberseguridad: una guía de aproximación para el empresario. Obtenido de: https://www.incibe.es/empresas/guias/glosario-de-terminos-de-ciberseguridad-una-guia-de-aproximacion-para-el
- incibe.es. (1 de septiembre de 2021). INCIBE. Obtenido de Cómo identificar una notificación maliciosa: https://www.incibe.es/ciudadania/blog/que-significan-los-mensajes-y-notificaciones-que-aparecen-al-navegar-por-internet
- Lederkremer, M. (2020). REDES INFORMATICAS Avanzado. Ciudad Autónoma de Buenos Aires: RedUsers.
- Microsoft Outlook. (2021). Microsoft. Obtenido de Ver encabezados de mensajes de Internet en Outlook: https://support.microsoft.com/es-es/office/ver-encabezados-de-mensajes-de-internet-en-outlook-cd039382-dc6e-4264-ac74-c048563d212c#:~:text=Un%20encabezado%20de%20internet%20de,transmitido%20hasta%20llegar%20al%20destinatario.
- Moreno González, L. R., & Nájera Domínguez, N. M. (2022). Los últimos avances de la criminalística en la administración de justicia. México: INACIPE.
- Mozilla.org. (26 de abril de 2023). ¿Qué es una URL? Obtenido de: https://developer.mozilla.org/es/docs/Learn/Common_questions/Web_mechanics/What_is_a_URL
- Mozilla.org. (28 de febrero de 2023). HTTPS. Obtenido de: https://developer.mozilla.org/es/docs/Glossary/HTTPS
- RAE. (2022). Diccionario de la lengua española. Real Academia Española. Obtenido de: https://www.rae.es/
- Regino, E. O. (2015). Lógica de programación orientada a objetos. Colombia: Ecoe Ediciones.
- Sandoval-Almazan, R., MontesdeOcaLópez, J. C., & OrtegaPonce, C. (2021). ETIQUETADODIGITALSOCIALCOMOACTIVISMOENREDESSOCIALES:#LADIESY#LORDSENMÉXICO. Obtenido de: https://gmjmexico.uanl.mx/index.php/GMJ_EI/article/view/421
- Social Media. (2023). Redes sociales y el contenido, mejores amigos. Obtenido de: https://www.wearecontent.com/blog/social-media/contenido-y-redes-sociales#:~:text=Lo%20que%20llamamos%20contenido%20en%20redes%20sociales,-Principalmente%20los%20contenidos&text=En%20otras%20palabras%2C%20es%20aquello,y%20aportar%20valor%20al%20p%C3%BAbli
- SSL.COM. (2023). ¿Qué es un certificado SSL? Obtenido de: SSL.COM: https://www.ssl.com/es/faqs/faq-what-is-ssl/
- UNAM. (2014). Instructivo de uso para Redes Sociales Institucionales de la UNAM. Universidad Nacional Autónoma de México. Obtenido de: http://arquitectura.unam.mx/uploads/8/1/1/0/8110907/instructivo_de_uso_para_redes_sociales_institucionales_de_la_unam.pdf
- Universidad Veracruzana. (16 de mayo de 2016). Universidad Veracruzana. Obtenido de ¿Cómo puedes identificar que estás navegando en una página legítima?: https://www.uv.mx/infosegura/general/conocimientos_navegacion-3/
- Urbina, G. B. (2017). *Introducción a la seguridad informática.* México: Grupo Editorial Patria.

II.- Perfil del Estándar de Competencia

Estándar de Competencia
Aplicación de principios básicos de ciberseguridad para usuario final en organizaciones

Elemento 1 de 5
Aplicar principios de seguridad en la creación y uso de contraseñas y otros mecanismos de autenticación, así como en la gestión de sesiones

Elemento 2 de 5
Aplicar principios de seguridad para el respaldo de información de equipo de cómputo/dispositivos móviles

Elemento 3 de 5
Aplicar los principios de seguridad para la navegación en sitios web, acceso a aplicativos y aplicaciones mediante el uso de equipo de cómputo/dispositivos móviles

Elemento 4 de 5
Aplicar los principios de seguridad en el uso del correo electrónico en equipo de cómputo/dispositivos móviles

Elemento 5 de 5
Aplicar los principios de seguridad en el uso de redes sociales

III.- Elementos que conforman el Estándar de Competencia

Referencia	Código	Título
1 de 5	E4830	Aplicar principios de seguridad en la creación y uso de contraseñas y otros mecanismos de autenticación, así como en la gestión de sesiones

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra los siguientes:

DESEMPEÑOS

1. Gestiona la autenticación de sesiones aplicando principios de seguridad:
- Iniciando sesión libre de mensajes de error en sistema operativo con una cuenta de usuario válida y una contraseña fuerte/robusta/algún dispositivo biométrico,
- Manteniendo la sesión activa cuando esté haciendo uso del servicio digital,
- Bloqueando con contraseña la sesión del sistema operativo al ausentarse del lugar de trabajo y finalice sus actividades, y
- Cerrando sesión de los servicios digitales/sistema operativo cuando se tengan periodos prolongados de inactividad y al término de su uso.

2. Crea contraseñas fuertes/robustas aplicando principios de seguridad:
- Combinando al menos un carácter en mayúscula, minúscula, símbolo especial y número,
- Estableciendo una longitud de al menos 8 caracteres para la contraseña, y
- Descartando palabras que sean comunes, fáciles de intuir y adivinar por terceras personas como la palabra contraseña, password, admin, administrador, números consecutivos, fechas importantes/relevantes, nombres propios.

3. Emplea y resguarda contraseñas aplicando principios de seguridad:
- Utilizando una contraseña distinta para cada sitio/aplicativo/app/archivos/carpetas/equipo de cómputo,
- Cambiando la/las contraseñas cuando haya sospecha/incidente de seguridad,
- Resguardando las contraseñas en herramientas de acceso controlado como un gestor de contraseñas y evitar anotarlas en lugares de fácil acceso como notas adhesivas/hojas sueltas, y
- Habilitando el factor de doble autenticación.

4. Ejecuta prácticas de seguridad de la información para evitar ser víctima de ingeniería social en el uso de contraseñas y otros mecanismos de autenticación:
- Evitando compartir cuentas de usuario y contraseñas solicitadas por terceros de manera personal/a través de llamadas telefónicas/correos electrónicos/SMS/mensajería instantánea/redes sociales, y
- Reportando al CAU/equipo técnico los incidentes.

La persona es competente cuando obtiene el siguiente:

PRODUCTO

1. El respaldo de uso de contraseñas elaborado:
- Contiene la lista de las contraseñas generadas para un sitio web/aplicativo,

- Contiene la evidencia de la realización del cambio de contraseñas predeterminadas y por defecto,
- Muestra que las contraseñas generadas son diferentes para cada sitio web/aplicativo, y
- Presenta en las contraseñas generadas al menos un carácter en mayúscula, minúscula, símbolo especial y número.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS	NIVEL
1. Contraseñas: • Características. • Fuerte/robusta. • Débil/no segura.	Conocimiento
2. Cuentas informáticas: • De usuario. • De administrador/privilegiada. • Roles/perfiles. • Niveles de acceso/privilegios.	Conocimiento
3. Firma electrónica para usuario final: • Firma electrónica. • Componentes de la firma electrónica para el usuario final; llave privada “archivo .key”, llave pública “archivo .cer”, contraseña de la llave privada.	Conocimiento
4. Sesiones informáticas: • De sistema operativo. • De servicios digitales. • Inicio de sesión. • Sesión activa. • Sesión inactiva/desatendida. • Cierre de sesión.	Conocimiento

GLOSARIO

1. App:	Abreviatura de la palabra inglesa *application* para referirse a un programa que se instala en dispositivos móviles o tabletas para ayudar al usuario en una labor concreta, ya sea de carácter profesional o de ocio y entretenimiento.
2. Archivo .cer:	Archivo que contiene un certificado digital utilizado para verificar la autenticidad e integridad de documentos electrónicos.
3. Archivo .key:	Archivo que contiene la clave privada utilizada para autenticar y firmar documentos digitalmente.
4. Caracteres alfanuméricos:	Es un conjunto de elementos que incluye los diez dígitos decimales, las 26 letras mayúsculas del alfabeto, las 26 letras minúsculas y caracteres especiales tales como $, +, =, *, etcétera. En total: 256 caracteres.
5. CAU:	Centro de Apoyo a Usuarios. Servicio que se encarga de resolver problemas y atender solicitudes relacionadas con las tecnologías de la información (TI). Esto incluye equipos

	informáticos, periféricos, software y plataformas utilizadas por la mayoría de las organizaciones. El CAU sirve como un punto centralizado de acceso para los empleados o usuarios que requieren asistencia y desempeña un papel importante en la prestación de servicios de TI.
6. Contraseña segura/fuerte/robusta:	Tipo de contraseña que se destaca por ser lo suficientemente larga, generada de forma aleatoria o mediante la combinación de caracteres alfanuméricos, mayúscula, minúscula, números y Símbolos y caracteres especiales. Estas características dificultan considerablemente su descubrimiento, ya que se necesita un tiempo considerable para calcularla.
7. Dispositivo biométrico:	Equipo tecnológico que puede medir, codificar, comparar, almacenar, transmitir y reconocer características únicas de una persona, como huellas dactilares, rasgos faciales o patrones de voz, con un alto grado de precisión y confiabilidad.
8. Doble autenticación:	Método de seguridad que añade una capa adicional a la autenticación básica. Además de la contraseña, se utiliza otro factor, como un código enviado a un dispositivo móvil, huella dactilar, sistema OTP (contraseña de único uso), entre otros. Esto mejora significativamente la seguridad en comparación con la autenticación simple.
9. Ingeniería social:	Práctica utilizada para obtener información confidencial de una persona, mediante la manipulación o el engaño sutil. Consiste en aprovechar la buena voluntad de las personas para obtener la información deseada. Este enfoque se utiliza con el propósito de cometer fraudes.
10. Password:	Forma de autentificación de un usuario, a través de una clave secreta, para controlar el acceso a algún recurso o herramienta. En caso de que no se proporcione la clave correcta no se permitirá el acceso a dichos elementos.
11. Símbolos/caracteres especiales:	Son aquellos símbolos que se pueden escribir utilizando el teclado de tu computadora y que no se consideran ni números ni letras. Estos símbolos adicionales incluyen signos de puntuación, símbolos matemáticos, caracteres de moneda y otros elementos que no son comúnmente utilizados en palabras o números.
12. Sitios web:	Colección de páginas en internet que están relacionadas entre sí y que comparten una dirección web única. Es un espacio virtual donde la información, el contenido y los servicios se presentan y se hacen accesibles para los usuarios a través de un navegador web.
13. SMS:	Servicio de mensajería de texto que te permite enviar y recibir mensajes cortos a través de tu teléfono móvil. Es una forma rápida y conveniente de comunicarse utilizando texto escrito, similar a enviar un mensaje de texto.

Referencia	Código	Título
2 de 5	E4831	Aplicar principios de seguridad para el respaldo de información de equipo de cómputo/dispositivos móviles

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra el siguiente:

DESEMPEÑO

1. Realiza respaldos de información:
- Verificando la integridad del dispositivo de almacenamiento extraíble por medio del software antivirus,
- Generando la copia de la información en un dispositivo de almacenamiento extraíble,
- Guardando con una nomenclatura clara que permita identificar el contenido y fecha del respaldo,
- Protegiendo el respaldo de información confidencial y sensible con contraseña de acuerdo a lo establecido en el lugar de trabajo, y
- Corroborando que el proceso de respaldo en dispositivo de almacenamiento extraíble se haya realizado libre de mensajes/ventanas emergentes que indiquen errores de copiado y de haber excedido el espacio de destino.

La persona es competente cuando obtiene el siguiente:

PRODUCTO

1. El respaldo de información elaborado:
- Contiene la información sensible protegida,
- Contiene en el nombre la nomenclatura de identificación del archivo y la fecha del archivo generado, y
- Coincide con el contenido y tamaño de información respaldada en relación con la original.

La persona es competente cuando posee el siguiente:

CONOCIMIENTO	NIVEL
1. Respaldo: • Total. • Parcial. • Incremental.	Conocimiento

La persona es competente cuando demuestra la siguiente:

RESPUESTAS ANTE SITUACIÓN EMERGENTE

Situación emergente

1. Durante el análisis de la USB surge ventana emergente indicando la presencia de virus/daño.

Respuestas esperadas

1. Informar al CAU/área de soporte.

GLOSARIO

1. Errores de copiado: Datos que no fueron duplicados o copiados de manera integral a un disco duro o una unidad.
2. Espacio de destino: Cantidad total de datos que puede almacenar un disco duro o una unidad.
3. Nomenclatura clara: Se hace referencia a la práctica de utilizar nombres y términos que sean fáciles de entender y comunicar. Se trata de elegir palabras o etiquetas que sean simples y descriptivas, de manera que cualquier persona pueda comprender rápidamente a qué se refieren.
4. Software: Definimos software del inglés como un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en un dispositivo. El software conforma todas aquellas acciones que se pueden realizar gracias a las instrucciones previamente contempladas y programadas e incluidas dentro de un programa que permite al usuario interactuar con el sistema de forma fácil e intuitiva.

Referencia	Código	Título
3 de 5	E4832	Aplicar los principios de seguridad para la navegación en sitios web, acceso a aplicativos y aplicaciones mediante el uso de equipo de cómputo/dispositivos móviles

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra el siguiente:

DESEMPEÑO

1. Navega en sitios web al aplicar principios de seguridad:
   - Accediendo únicamente a sitios web de entidades, organizaciones e instituciones conocidas y libres de mensajes/ventanas emergentes/alertas que indiquen lo contrario,
   - Escribiendo la dirección URL en el navegador libre de errores tipográficos,
   - Reportando al CAU/equipo técnico la evidencia, capturas de pantalla de los mensajes de alerta del navegador/del software antivirus/antimalware al detectar un sitio web sospechoso,
   - Corroborando los indicadores de conexión segura del navegador al verificar el certificado de seguridad, ícono de candado, etiqueta https en la URL y nombres de dominio verificados,
   - Reportando al CAU/equipo técnico vínculos y enlaces sospechosos proporcionados para el ingreso a sitios web,
   - Transfiriendo información personal/datos confidenciales/financieros/institucionales/organizacionales en el sitio web de entidades/organizaciones/instituciones conocidas y con conexión segura,
   - Utilizando el factor de doble autenticación, como mensaje de texto, mensaje de correo electrónico, app de autenticación, token físico, token móvil, en los sitios web institucionales/organizacionales, de servicios financieros y servicios públicos, y
   - Configurando el factor de doble autenticación en los sitios web que lo permitan.

La persona es competente cuando obtiene el siguiente:

PRODUCTO

1. El reporte de los riesgos de seguridad de la información en la navegación de sitios web, aplicativos/aplicaciones elaborado:

- Contiene nombre completo de quien reporta,
- Contiene área a la que pertenece la persona que realiza el reporte,
- Contiene fecha de reporte,
- Menciona el tipo de riesgo detectado,
- Contiene la descripción del riesgo,
- Enlista los activos de información afectados, e
- Incluye evidencia documentada/captada como capturas de pantalla, fotografías, sobre el riesgo detectado.

La persona es competente cuando posee el siguiente:

CONOCIMIENTO	NIVEL
1. Generalidades de la navegación segura en sitios web: • Acceso a sitios web. • Sitio web autentico/legítimo. • Sitio web falso o apócrifo. • Controles de seguridad en sitios web. • Hábitos de navegación segura en sitios web. • Riesgos de la navegación en sitios web. • Riesgos de la navegación en sitios web de servicios públicos y financieros.	Conocimiento

La persona es competente cuando demuestra la siguiente:

ACTITUD/HÁBITO/VALOR

1. Responsabilidad:	La manera en que realiza el reporte al CAU/equipo técnico, sobre situaciones de posible fraude, engaño, virus durante la navegación en sitios web, al enviar y redactar la evidencia sin omitir detalles que impidan resarcir la posible afectación.

GLOSARIO

1. Antimalware:	Software de protección para evitar que ejecutemos algún tipo de software malicioso en nuestro equipo que infecte al equipo.
2. Certificado de seguridad (SSL):	Archivo digital que se utiliza para garantizar la seguridad de las comunicaciones en línea, dicho archivo vincula la identidad de un sitio web a un par de claves criptográficas que consta de una clave pública y una clave privada.
3. Enlaces sospechosos:	Es un vínculo aparentemente fiable pero que, al dar clic en él, redirige a una web falsa que imita ser una web oficial legítima. Una vez que el usuario cree estar navegando por una web de confianza, podría introducir datos personales como su correo electrónico, contraseñas e incluso datos bancarios.

4. Etiqueta HTTP:	HTTPS (Protocolo seguro de transferencia de hipertexto, por sus siglas en inglés) es un conjunto de reglas que permite que los navegadores web y los servidores se comuniquen entre sí. Es el protocolo que utilizamos cuando navegamos por internet para ver páginas web.
5. Indicadores de conexión segura del navegador:	Si al lado de la URL, el navegador muestra un símbolo de un candado (habitualmente de color verde) es buena señal. Significa que la web es segura. Si hacemos clic en este candado, el navegador nos indicará qué tipo de certificado SSL tiene instalada la web en la que nos encontramos.
6. Mensajes de alerta del navegador:	Son ventanas que salen al navegar en internet, con una gran cantidad de anuncios y ventanas nuevas con notificaciones de todo tipo, algunos no son maliciosos, sin embargo, otras notificaciones están diseñadas para llamar nuestra atención y conseguir que hagamos clic en ellas con fines menos positivos para nosotros ya que tratarán de llevarnos a una web falsa, hacer que nos descarguemos algún virus o malware o que rellenemos algún formulario con nuestros datos personales para usarlos en su beneficio.
7. Nombre de dominio:	Cadena alfanumérica utilizada para identificar y localizar una entidad en Internet, como un sitio web, una dirección de correo electrónico o un servidor. Está compuesto por dos partes principales: el nombre y la extensión.
8. Token:	Dispositivo físico (hardware) o digital (software) que permite el acceso a un recurso restringido en lugar de usar una contraseña, firma digital o dato biométrico; es decir, actúa como una llave con la que acceder a un recurso.
9. URL:	Del inglés *Uniform Resource Locator (Localizador de Recursos Uniforme)*. Es el mecanismo usado por los navegadores para obtener cualquier recurso publicado en la web.

Referencia	**Código**	**Título**
4 de 5	E4833	Aplicar los principios de seguridad en el uso del correo electrónico en equipo de cómputo/dispositivos móviles

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra el siguiente:

DESEMPEÑO

1. Utiliza el correo electrónico aplicando principios de seguridad:
   - Iniciando sesión en su cuenta de correo electrónico al utilizar contraseña fuerte y robusta,
   - Evitando abrir/dar respuesta/descargar archivos adjuntos de algún correo electrónico cuando existan mensajes de advertencia del antivirus/antimalware/el cliente/aplicativo del correo electrónico,

- Verificando que el nombre y dirección de correo electrónico del remitente esté libre de errores tipográficos al abrir el mensaje,
- Descartando correos electrónicos que presenten posibles situaciones de fraude/engaño/desinformación en el texto del mensaje/soliciten información confidencial/envíen enlaces/vínculos/ligas/códigos QR/archivos adjuntos sospechosos como SPAM/phishing, y
- Reportando al CAU/equipo técnico contenido sospechoso/enlaces/vínculos/archivos/imágenes dentro del correo electrónico.

La persona es competente cuando obtiene el siguiente:

PRODUCTO

1. El reporte de un correo electrónico sospechoso generado:
   - Contiene nombre completo de quien reporta,
   - Contiene área a la que pertenece la persona que realiza el reporte,
   - Contiene fecha de reporte,
   - Describe las características irregulares del correo electrónico, e
   - Incluye evidencia documentada y captada, como capturas de pantalla de archivos, imágenes, vínculos, enlaces, remitentes y contenido sospechoso dentro del mensaje del correo electrónico, mensajes de advertencia del cliente/aplicativo de correo electrónico, así como los encabezados del mismo.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS	NIVEL
1. Elementos que componen un mensaje de correo electrónico.	Conocimiento
2. Respaldos de correo electrónico.	Conocimiento
3. Uso del correo electrónico.	Conocimiento

La persona es competente cuando demuestra las siguientes:

ACTITUDES/HÁBITOS/VALORES

1. Responsabilidad:	La manera en que realiza el reporte al CAU/equipo técnico, sobre situaciones de posible fraude, engaño, virus en correo electrónico, al envía y redactar la evidencia sin omitir detalles que impidan resarcir la posible afectación.

GLOSARIO

1. Cliente/aplicativo del correo electrónico:	Es un programa que se usa para enviar, recibir y gestionar el correo electrónico desde un dispositivo móvil.
2. Código QR:	Quick Response son códigos de barras, capaces de almacenar determinado tipo de información, como una URL, SMS, Email, Texto, etc.
3. Encabezados de correo electrónico:	Un encabezado de internet de mensaje de correo electrónico proporciona una lista de detalles técnicos sobre el mensaje, como quién lo envió, el software usado para redactarlo y los servidores de correo electrónico por los que se ha transmitido hasta llegar al destinatario.

4. Phishing:	Técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico.
5. Remitentes conocidos/de confianza:	Las direcciones de correo electrónico emitidos que son identificados plenamente por el usuario destinatario.
6. Remitentes desconocidos/sospechosos:	Son todos aquellos correos electrónicos recibidos que presentan algunas características anormales, por ejemplo: el dominio de la dirección de email no coincide con el de la empresa/entidad, el origen del correo no corresponde al asunto de cuerpo del correo, contar con errores ortográficos.
7. SPAM:	Es un término genérico para cualquier mensaje no solicitado, recibido y entregado a través de mensajes de correo electrónico.

Referencia	Código	Título
5 de 5	E4834	Aplicar los principios de seguridad en el uso de redes sociales

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra los siguientes:

DESEMPEÑOS

1. Establece configuraciones de seguridad y privacidad en las cuentas de redes sociales:
- Asegurando la confidencialidad de las distintas cuentas en redes sociales del usuario al utilizar contraseñas fuertes/robustas diferentes en cada una, así como el factor de doble autenticación cuando éste se encuentre disponible,
- Verificando el aviso/política de privacidad de las distintas redes sociales,
- Verificando los términos y condiciones de uso de las distintas redes sociales como permisos, usos, accesos a ubicación, contactos, cámara, micrófono, imágenes,
- Configurando reglas básicas de seguridad que resguarden la información sensible del perfil al evitar que sea pública,
- Configurando la incorporación de nuevos contactos mediante previa autorización, y
- Configurando/verificando que la visualización, etiquetado de publicaciones y contenido como fotografías, videos, información personal, laboral, ubicación, contactos, comentarios, sea exclusiva para usuarios conocidos y de confianza.

2. Utiliza las redes sociales aplicando principios de seguridad:
- Consultando y verificando que las fuentes de información sean conocidas y de confianza, válidas para descartar, compartir y reenviar desinformación y noticias falsas, y
- Utilizando la funcionalidad de "denunciar" en cualquier situación de contactos y contenidos sospechosos que presenten posibles escenarios de fraude, engaño y desinformación, así como consultarlo y reportarlo al CAU/equipo técnico.

La persona es competente cuando obtiene el siguiente:

PRODUCTO

1. La evidencia de apertura y uso de las redes sociales elaborada:
   - Contiene el listado de contraseñas fuertes y robustas diferentes para las distintas redes sociales del usuario,
   - Contiene la evidencia de la realización del cambio de contraseñas de las distintas redes sociales del usuario,
   - Contiene captura de pantalla del inicio de la sección de los términos y condiciones de uso de alguna red social,
   - Contiene captura de pantalla del inicio de la sección del aviso/política de privacidad de alguna red social,
   - Contiene captura de pantalla del inicio de la sección de la solicitud de permisos de uso de recursos por parte de alguna red social, y
   - Contiene una lista de características/propiedades que deben verificarse sobre la identidad de nuevos contactos.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS	NIVEL
1. Configuraciones de seguridad y privacidad.	Conocimiento
2. Fuente de información válida y de confianza.	Conocimiento
3. Uso seguro de redes sociales.	Conocimiento

GLOSARIO

1. Desinformación:	Es la difusión de contenidos de información falsa, para engañar, manipular y generar influencias que modifican y distorsionan la realidad en las redes sociales y otros medios de comunicación digitales.
2. Etiquetado en redes sociales:	Es una función, mediante la cual, las plataformas de redes sociales pueden ordenar y clasificar contenidos para visibilizarlos y hacer más fácil el acceso a la información.
3. Funcionalidad de denuncia en redes sociales:	Es una función que las plataformas de redes sociales deben contener, permitiendo informar o exponer situaciones de conducta o información, ilegales, inapropiadas o perjudiciales como: el abuso, el acoso, la discriminación de género, o racial, así como, la violación de derechos humanos y los fraudes o engaños hacia los usuarios.
4. Identidad de contactos:	Es la información de las personas, que, a manera de listado de contactos de confianza, muestra los datos y características de los Perfil de redes sociales, con quien se mantiene una relación de interacción en redes sociales.
5. Información sensible:	Se refiere a cualquier tipo de datos o detalles que, si se divulgan o se acceden de manera no autorizada, podrían causar daño, violar la privacidad o comprometer la seguridad de una persona o entidad.

6. Noticias falsas:	Del inglés: fake news, son noticias que, mediante la Desinformación, son expuestas en las redes sociales, o en otros medios de comunicación digitales, tal cual, como si fueran verdaderas.
7. Perfil de redes sociales:	Es una representación (Cuenta de usuario) de una persona u organización en una plataforma de redes sociales, la cual, está personalizada para compartir la información para interactuar con otros usuarios y publicar contenidos. Un perfil de redes sociales suele contener datos de nombre del usuario, fotografía de perfil e información general, acorde a cada plataforma.
8. Publicaciones/contenido en redes sociales:	Es la información que se publica a través de mensajes que se crean y comparten a través del Perfil de redes sociales, y que pueden ser consultados y retroalimentados por otros usuarios a través de una plataforma. Lo anterior, generalmente, para orientar e informar a las personas que son consideradas como un público objetivo. Los mensajes de las publicaciones o contenidos más comunes son: texto, imagen, video, entre otros.
9. Redes sociales:	Plataformas en línea que permiten a las personas conectarse, interactuar y compartir contenido con otros usuarios a través de internet.