ICDL
The Digital Skills Standard

ICDL Laboral

SEGURIDAD INFORMÁTICA

Programa de Estudio 2.0

Documento del Programa de estudio

Objetivo

Este documento presenta el programa de estudio para el módulo Seguridad Informática. El programa de estudio describe, a través de los aprendizajes, el conocimiento y las competencias necesarias que debería poseer un candidato para el módulo Seguridad Informática. El programa de estudio también ofrece una base para el examen teórico y práctico que comprende este módulo.

Descargo de responsabilidades

A pesar del cuidado aportado por ICDL Foundation a la preparación de esta publicación, ICDL Foundation, en su calidad de editor, no garantiza que la información contenida aquí esté completa, y tampoco ICDL Foundation será responsable de cualquier error, omisión, inexactitud, pérdida o daño en virtud de dicha información o cualquier instrucción o recomendación de esta publicación. ICDL Foundation se reserva el derecho, a su entera discreción, de aportar cambios en cualquier momento y sin previo aviso.

Seguridad Informática

Este módulo expone conceptos y habilidades esenciales en relación con el uso seguro de las TIC en la vida diaria y habilidades usadas para mantener una conexión de red segura, utilizar Internet de manera segura y gestionar datos e información de manera adecuada.

Objetivos del módulo

Los candidatos exitosos serán capaces de:

- Comprender la importancia de mantener la seguridad de información y datos, e identificar principios comunes de protección de datos / privacidad, retención y control.
- Reconocer amenazas a la seguridad personal por robo de identidad y las posibles amenazas a datos debido al utilizar computación en la nube.
- Poder usar contraseñas y encriptación para asegurar archivos y datos.
- Comprender la amenaza del software malicioso (malware) y poder proteger una computadora, dispositivo o red del malware y abordar ataques de malware.
- Reconocer los tipos comunes de seguridad inalámbrica y de red y poder usar firewalls personales y puntos de acceso personales.
- Proteger una computadora o dispositivo de accesos no autorizados y poder administrar y actualizar contraseñas de manera segura.
- Utilizar una configuración adecuada del navegador web y comprender cómo autenticar sitios web y navegar por la web de forma segura.
- Comprender los problemas de seguridad en la comunicación que pueden surgir del uso de correo electrónico, redes sociales, voz sobre protocolo de Internet (VoIP), mensajería instantánea (IM) y dispositivos móviles.
- Realizar una copia de seguridad y restaurar los datos en ubicaciones de almacenamiento local y en la nube y eliminar y desechar los datos y dispositivos de forma segura.

CATEGORÍA	ÁREA DE CONOCIMIENTO	REF.	UNIDAD DE TRABAJO
1. Conceptos de seguridad	*1.1 Amenazas para los datos*	1.1.1	Distinguir entre datos e información.
		1.1.2	Comprender el término delito informático, piratería (hacking)
		1.1.3	Reconocer amenazas maliciosas y accidentales a los datos de individuos, proveedores de servicios, organizaciones externas.
		1.1.4	Reconocer amenazas para los datos por circunstancias extraordinarias, como: incendio, inundaciones, guerra, terremoto.
		1.1.5	Reconocer las amenazas a los datos por el uso de la computación en la nube como: control de datos, pérdida

CATEGORÍA	ÁREA DE CONOCIMIENTO	REF.	UNIDAD DE TRABAJO
			potencial de privacidad.
	1.2 Valor de la información	1.2.1	Comprender las características básicas de seguridad de la información, como: confidencialidad, integridad, disponibilidad.
		1.2.2	Comprender los motivos para proteger la información personal, como: evitar el robo de identidad, fraude, mantener la privacidad.
		1.2.3	Comprender los motivos para proteger la información del lugar de trabajo en computadoras y dispositivos como: prevención de robo, uso fraudulento, pérdida accidental de datos, sabotaje.
		1.2.4	Identificar principios comunes de protección de datos / privacidad, retención y principios de control como: transparencia, propósitos legítimos, proporcionalidad.
		1.2.5	Comprender los términos titulares de datos y controladores de datos y cómo se aplican a ellos los principios de protección, retención y control de datos / privacidad.
		1.2.6	Comprender la importancia de cumplir con las normas y políticas para el uso de las TIC y cómo acceder a ellas.
	1.3 Seguridad personal	1.3.1	Comprender el término ingeniería social y sus consecuencias como: acceso no autorizado a computadoras y dispositivos, recopilación de información no autorizada, fraude.
		1.3.2	Identificar métodos de ingeniería social, como: llamadas telefónicas, fraude (phishing), espionaje.
		1.3.3	Comprender el término robo de identidad y sus consecuencias: personales, financieras, comerciales, legales.
		1.3.4	Identificar métodos de robo de identidad como: buceo de información, copiado (skimming), pretextos (pretexting)
	1.4 Seguridad de archivos	1.4.1	Comprender el efecto de la activación/desactivación de las configuraciones de los macros de

CATEGORÍA	ÁREA DE CONOCIMIENTO	REF.	UNIDAD DE TRABAJO
			seguridad.
		1.4.2	Comprender las ventajas, limitaciones del cifrado. Tener en cuenta la importancia de no divulgar o perder la contraseña de cifrado, clave, certificado.
		1.4.3	Cifrar un archivo, carpeta, disco.
		1.4.4	Establecer una contraseña para archivos como: documentos, hojas de cálculo, archivos comprimidos
2. Malware	*2.1 Tipos y métodos*	2.1.1	Comprender el término malware. Reconocer las diferentes formas en que el malware puede ocultarse en computadoras y dispositivos como: troyanos (trojans), encubridrores (rootkits), puertas traseras (backdoors).
		2.1.2	Reconocer los tipos de malware infeccioso y comprender cómo trabajan: virus, gusanos.
		2.1.3	Reconocer los tipos de robo de datos, malware de extorsión/con ánimo de lucro y comprender cómo trabajan: adware, spyware, botnets, registro de pulsaciones de teclas (keystrokes logging) y marcadores (diallers).
	2.2 Protección	2.2.1	Comprender cómo funciona un software de antivirus y sus limitaciones.
		2.2.2	Comprender que el software de antivirus debe instalarse en computadoras y dispositivos
		2.2.3	Comprender la importancia de actualizar regularmente software como: antivirus, navegador web, plug-in, aplicación, sistema operativo.
		2.2.4	Analizar unidades, carpetas y archivos específicos usando un software de antivirus. Programar análisis usando un software de antivirus.
		2.2.5	Comprender los riesgos de usar software obsoleto y no compatible como: aumento de amenazas de software malicioso (malware), incompatibilidad.

CATEGORÍA	ÁREA DE CONOCIMIENTO	REF.	UNIDAD DE TRABAJO
	2.3 Resolución y eliminación	2.3.1	Comprender el término cuarentena y el efecto de poner en cuarentena los archivos infectados / sospechosos.
		2.3.2	Cuarentena, eliminar archivos infectados / sospechosos
		2.3.3	Comprender que un ataque de software malicioso (malware) puede diagnosticarse y resolverse utilizando recursos en línea como: sitios web del sistema operativo, antivirus, proveedores de software de navegador web, sitios web de las autoridades pertinentes.
3. Seguridad de la red	*3.1 Redes y conexiones*	3.1.1	Comprender el término red y reconocer los tipos de red comunes como: red de área local (LAN), red de área local inalámbrica (WLAN), red de área amplia (WAN), red privada virtual (VPN).
		3.1.2	Comprender de qué manera conectarse a una red tiene implicancias para la seguridad, como: malware, acceso no autorizado a datos, mantener la privacidad.
		3.1.3	Comprender la función del administrador de la red en la gestión de la autenticación, la autorización y las cuentas, el monitoreo y la instalación de parches y actualizaciones de seguridad relevantes, el monitoreo del tráfico de la red y el manejo del software malicioso (malware) encontrado dentro de una red.
		3.1.4	Comprender las funciones y limitaciones de un cortafuegos (firewall) en un ambiente personal, laboral.
		3.1.5	Prender, apagar un cortafuegos (firewall) personal. Permitir, bloquear una aplicación, servicio / acceso a funciones a través de un cortafuegos (firewall) personal.
	3.2 Seguridad inalámbrica	3.2.1	Reconocer las diferentes opciones de seguridad inalámbrica y sus limitaciones como: Privacidad equivalente a cableado (WEP), Acceso protegido por Wi-Fi (WPA) / Acceso protegido por Wi-Fi 2 (WPA2), filtrado de control de acceso de medios (MAC), Identificador de

CATEGORÍA	ÁREA DE CONOCIMIENTO	REF.	UNIDAD DE TRABAJO
			conjunto de servicios oculto (SSID).
		3.2.2	Comprender que el uso de una red inalámbrica desprotegida puede provocar ataques como: escuchas, secuestro de redes, hombre en el medio.
		3.2.3	Comprender el término punto de acceso personal (hotspot).
		3.2.4	Habilitar, deshabilitar un punto de acceso personal (hotspot) seguro y conectar, desconectar dispositivos de forma segura.
4. Control del acceso	*4.1 Métodos*	4.1.1	Identificar medidas para prevenir el acceso no autorizado a datos como: nombre de usuario, contraseña, PIN, cifrado, autenticación de múltiples factores.
		4.1.2	Comprender el término contraseña de un solo uso y su uso típico.
		4.1.3	Comprender el propósito de una cuenta de red.
		4.1.4	Entender que se debe acceder a una cuenta de red a través de un nombre de usuario y contraseña y bloquearla, cerrar sesión cuando no está en uso.
		4.1.5	Identificar técnicas comunes de seguridad biométrica utilizadas en el control de acceso, como: huella digital, escaneo ocular, reconocimiento facial, geometría de la mano.
	4.2 Gestión de contraseñas	4.2.1	Reconocer buenas políticas de contraseña, como: longitud de contraseña adecuada, combinación adecuada de letras, números y caracteres especiales, no compartir contraseñas, cambiarlas regularmente, diferentes contraseñas para diferentes servicios.
		4.2.2	Comprender la función, limitaciones del software administrador de contraseñas.
5. Uso seguro de la Web	*5.1 Configuración del navegador*	5.1.1	Seleccionar las configuraciones adecuadas para activar, desactivar autocompletado, guardar automáticamente cuando llene un formulario.
		5.1.2	Eliminar los datos privados de

CATEGORÍA	ÁREA DE CONOCIMIENTO	REF.	UNIDAD DE TRABAJO
			un navegador, como: historial de navegación, archivos caché de Internet, contraseñas, cookies, datos de la función autocompletar.
	5.2 Navegación segura	5.2.1	Reconocer que determinadas actividades en línea (compras, transacciones financieras) solo deben realizarse en páginas Web seguras utilizando una conexión segura.
		5.2.2	Identificar formas de confirmar la autenticidad de un sitio web como: calidad del contenido, moneda, URL válida, información de la empresa o del propietario, información de contacto, certificado de seguridad, validación del propietario del dominio.
		5.2.3	Reconocer el término redirección a una página web falsa (pharming).
		5.2.4	Comprender el objetivo, la función y los tipos de software para controlar contenidos, como: software de filtro de Internet, software de control parental
6. Comunicaciones	*6.1 Correo electrónico*	6.1.1	Comprender el objetivo del cifrado, descifrado de un correo electrónico.
		6.1.2	Comprender el término firma digital.
		6.1.3	Identificar posibles correos electrónicos fraudulentos, no solicitados.
		6.1.4	Identificar características comunes del fraude (phishing) como: usar nombres de organizaciones legítimas, personas, enlaces web falsos, logotipos y marcas, promover la divulgación de información personal.
		6.1.5	Tener en cuenta que puede informar los intentos de fraude (phishing) a la organización legítima, las autoridades pertinentes.
		6.1.6	Tener conciencia del peligro de infectar el equipo con software malicioso (malware) al abrir un archivo adjunto en un correo electrónico que contiene una macro o un archivo ejecutable.
	6.2 Redes sociales	6.2.1	Comprender la importancia de no divulgar información confidencial o información personal identificable en

CATEGORÍA	ÁREA DE CONOCIMIENTO	REF.	UNIDAD DE TRABAJO
			sitios de redes sociales.
		6.2.2	Tener en cuenta la necesidad de aplicar y revisar periódicamente la configuración adecuada de las cuentas de redes sociales como: privacidad de la cuenta, ubicación.
		6.2.3	Aplicar la configuración de la cuenta de redes sociales: privacidad de la cuenta, ubicación.
		6.2.4	Comprender los potenciales peligros al usar sitios de redes sociales, como: ciber acoso (cyber bulling), acoso a menores (grooming), divulgación maliciosa de contenido personal, identidades falsas, enlaces, contenido, mensajes fraudulentos o maliciosos.
		6.2.5	Tener en cuenta que puede informar el uso o comportamiento inapropiado en las redes sociales al proveedor de servicios, las autoridades pertinentes.
	6.3 Voz sobre protocolo de Internet (VoIP) y mensajería instantánea (IM)	6.3.1	Comprender las vulnerabilidades de seguridad de la mensajería instantánea (IM) y la voz sobre protocolo de Internet (VoIP) como: software malicioso (malware), acceso a la puerta trasera, acceso a archivos, escucha.
		6.3.2	Reconocer métodos para asegurar la confidencialidad al usar IM y VoIP como: cifrado, no divulgación de información importante, restricción de archivos compartidos.
	6.4 Móvil	6.4.1	Comprender las posibles consecuencias del uso de aplicaciones de tiendas de aplicaciones no oficiales como: software móvil malicioso (malware), utilización innecesaria de recursos, acceso a datos personales, mala calidad, costos ocultos.
		6.4.2	Comprender el término permisos de aplicación.
		6.4.3	Tener en cuenta que las aplicaciones móviles pueden extraer información privada del dispositivo móvil como: detalles de contacto, historial de ubicación, imágenes.
		6.4.4	Tener en cuenta las medidas de

CATEGORÍA	ÁREA DE CONOCIMIENTO	REF.	UNIDAD DE TRABAJO
			emergencia y precaución si se pierde un dispositivo, como: deshabilitación remota, borrado remoto, localizar dispositivo.
7. Gestión de datos seguros	*7.1 Asegurar y realizar copias de seguridad de los datos*	7.1.1	Reconocer formas de garantizar la seguridad física de las computadoras y dispositivos como: no dejarlos desatendidos, registrar la ubicación y los detalles del equipo, usar bloqueos por cable, control de acceso.
		7.1.2	Reconocer la importancia de contar con un procedimiento de copia de seguridad en caso de pérdida de datos de computadoras y dispositivos.
		7.1.3	Identificar las características de un procedimiento de copia de datos, como: regularidad/frecuencia, programación, ubicación de almacenamiento, compresión de datos.
		7.1.4	Realizar una copia de seguridad de los datos en una ubicación como: unidad local, unidad / medios externos, servicio en la nube.
		7.1.5	Restaurar datos de una copia de seguridad en una ubicación como: unidad local, unidad / medios externos, servicio en la nube.
	7.2 Destrucción segura	7.2.1	Distinguir entre eliminar y destruir datos de manera permanente.
		7.2.2	Comprender el motivo para eliminar datos de unidades o dispositivos de manera permanente.
		7.2.3	Tener en cuenta que la eliminación de contenido puede no ser permanente en servicios como: sitio de redes sociales, blog, foro de Internet, servicios en la nube.
		7.2.4	Identificar métodos comunes para destruir de manera permanente datos como: borrado, destrucción de unidades/medios, desmagnetización, utilizar herramientas para la destrucción de datos.