Seguridad Informática

Programa de estudio versión 1.0

The European Computer Driving Licence Foundation Ltd (ECDL Foundation)

Third Floor Portview House Thorncastle Street

Dublin 4, Ireland

Tel: +353 1 6306000

Fax: +353 1 6306001

E-mail: info@ecdl.com

URL: www.ecdl.com

La versión oficial del programa de estudios ECDL / ICDL versión 1.0 es la versión publicada en el sitio web de ECDL Foundation, que se puede encontrar en: www.ecdl.com

Objetivo

Este documento presenta el programa de estudio ECDL / ICDL para el modulo Seguridad informática. El programa describe, a través de los aprendizajes, el conocimiento y las competencias necesarias para que un candidato apruebe el modulo Seguridad informática. El programa también ofrece una base para el examen teórico y práctico que comprende este módulo.

Limitaciones de responsabilidad

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

Módulo– Seguridad Informática

A continuación se describe el programa de estudio correspondiente al modulo *Seguridad informática*, el cual constituye la base para el examen teórico y práctico de este módulo.

Objetivos del módulo

Se exige al candidato que muestre su competencia en los conceptos y habilidades esenciales que subyacen al uso seguro de las TIC en la vida diaria y para utilizar técnicas y aplicaciones relevantes que mantengan una conexión de red segura, utilicen Internet de manera segura y gestionen datos e información de manera adecuada.

El candidato debe ser capaz de:

- Comprender los conceptos clave relacionados con la importancia de datos e información seguros, seguridad física, privacidad y robo de identidad.
- Proteger un equipo, dispositivo o red de malware y acceso no autorizado.
- Comprender los tipos de redes, tipos de conexión y problemas específicos de la red, incluidos los firewalls.
- Navegar en la World Wide Web y comunicarse por Internet de manera segura.
- Comprender los problemas de seguridad relacionados con las comunicaciones, incluidos el correo electrónico y la mensajería instantánea.
- Utilizar copias de seguridad y restaurar los datos de manera apropiada y segura, y eliminar datos y dispositivos de manera 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”.
		1.1.3	Comprender la diferencia entre hackear, crackear y hackeo ético.
		1.1.4	Reconocer amenazas para los datos por motivos de fuerza mayor, como: incendio, inundaciones, guerra, terremoto.
		1.1.5	Reconocer amenazas para los datos provenientes de: empleados, proveedores de servicios y personas externas.
	1.2 Valor de la información	1.2.1	Comprender los motivos para proteger la información personal, como: evitar el robo de identidad, fraude.

		1.2.2	Comprender los motivos para proteger la información comercialmente delicada, como: evitar el robo o el mal uso de los datos de clientes, información financiera.
		1.2.3	Identificar las medidas para evitar el acceso no autorizado a datos como: cifrado, contraseñas.
		1.2.4	Comprender las características básicas de seguridad de la información, como: confidencialidad, integridad, disponibilidad.
		1.2.5	Identificar los requisitos de protección, almacenamiento y control de datos/privacidad en su país.
		1.2.6	Comprender la importancia de crear y ceñirse a pautas y políticas para el uso de TIC.
	1.3 Seguridad personal	1.3.1	Comprender el término ingeniería social y sus implicaciones como: recolección de información, fraude, acceso al sistema informático.
		1.3.2	Identificar métodos de ingeniería social, como: llamadas telefónicas, phishing, shoulder surfing.
		1.3.3	Comprender el término robo de identidad y sus implicancias: personales, financieras, comerciales, legales.
		1.3.4	Identificar métodos de robo de identidad, como: búsqueda de información, fraude / clonación de tarjetas de crédito, pretextos.
	1.4 Seguridad de un archivo	1.4.1	Comprender el efecto de la activación/desactivación de las configuraciones de los macros de seguridad.
		1.4.2	Establecer una contraseña para archivos como: documentos, archivos comprimidos, hojas de cálculo.
		1.4.3	Comprender las ventajas y limitaciones del cifrado.
2. Malware	*2.1 Definición y función*	2.1.1	Comprender el término “malware”.
		2.1.2	Reconocer diferentes formas en que puede concebirse el malware, como: troyanos, rootkits y backdoors.

	2.2 Tipos	2.2.1	Reconocer los tipos de malware infeccioso y comprender cómo trabajan: virus, gusanos.
		2.2.2	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 Web (diallers).
	2.3 Protección	2.3.1	Comprender cómo funciona un software de antivirus y sus limitaciones.
		2.3.2	Analizar unidades, carpetas y archivos específicos usando un software de antivirus. Programar análisis usando un software de antivirus.
		2.3.3	Comprender el término “cuarentena” y el efecto de poner en cuarentena archivos infectados/sospechosos.
		2.3.4	Comprender la importancia de descargar y actualizar las actualizaciones de software, archivos de definición de antivirus.
3. Seguridad de la red	*3.1 Redes*	3.1.1	Comprender el término red y reconocer los tipos de redes comunes, como: red de área local (LAN), red de área extensa (WAN), red privada virtual (VPN).
		3.1.2	Comprender el rol del administrador de la red en la gestión de la autenticación, la autorización y las cuentas dentro de una red.
		3.1.3	Comprender las funciones y limitaciones de un firewall (servidor de seguridad).
	3.2 Conexiones de red	3.2.1	Reconocer las opciones para conectarse a una red como: cable, inalámbrico.
		3.2.2	Comprender de qué manera conectarse a una red tiene implicancias para la seguridad, como: malware, acceso no autorizado a datos, privacidad de mantenimiento.
	3.3 Seguridad inalámbrica	3.3.1	Reconocer la importancia de exigir una contraseña para proteger el acceso a redes inalámbricas.

		3.3.2	Reconocer diferentes tipos de seguridad inalámbrica, como: privacidad equivalente por cable (WEP), acceso protegido Wi-Fi (WPA), control de acceso a medios (MAC).
		3.3.3	Reconocer que el uso de una red inalámbrica sin protección puede permitir a entrometidos de la red inalámbrica acceder a sus datos.
		3.3.4	Conectarse a una red inalámbrica protegida/sin protección.
	3.4 Control del acceso	3.4.1	Comprender el objetivo de una cuenta de red y cómo se debe ingresar a ella a través de un nombre de usuario y una contraseña.
		3.4.2	Reconocer las políticas de buenas contraseñas, como: no compartir contraseñas, cambiarlas habitualmente, longitud adecuada de la contraseña, mezcla adecuada de letras, números y caracteres especiales.
		3.4.3	Identificar técnicas comunes de seguridad biométrica utilizadas en el control de acceso, como: escaneo de huellas digitales, reconocimiento ocular.
4. Uso seguro de la Web	*4.1 Navegación Web*	4.1.1	Reconocer que determinadas actividades en línea (compras, transacciones financieras) solo deben realizarse en páginas Web seguras.
		4.1.2	Identificar un sitio Web seguro, como: https, símbolo del candado.
		4.1.3	Reconocer el pharming.
		4.1.4	Comprender el término certificado digital. Validar un certificado digital.
		4.1.5	Comprender el término contraseña de un solo uso.
		4.1.6	Seleccionar las configuraciones adecuadas para activar, desactivar autocompletado, guardar automáticamente cuando llene un formulario.
		4.1.7	Comprender el término cookie.
		4.1.8	Seleccionar las configuraciones apropiadas para autorizar, bloquear cookies.

		14.1.9	Eliminar los datos privados de un navegador, como: historial de navegación, archivos caché de Internet, contraseñas, cookies, datos de la función autocompletar.
		4.1.10	Comprender el objetivo, la función y los tipos de software para controlar contenidos, como: software de filtro de Internet, software de control parental.
	4.2 Redes sociales	4.2.1	Comprender la importancia de no divulgar información confidencial en sitios de redes sociales.
		4.2.2	Reconocer la necesidad de aplicar configuraciones de privacidad apropiadas para las cuentas de redes sociales.
		4.2.3	Comprender los potenciales peligros al usar sitios de redes sociales, como: ciber acoso (cyber bulling), acoso a menores (grooming), desinformación / información peligrosa, identidades falsas, enlaces fraudulentos o mensajes.
5. Comunicaciones	*5.1 Correo electrónico*	5.1.1	Comprender el objetivo del cifrado, descifrado de un correo electrónico.
		5.1.2	Comprender el término firma digital.
		5.1.3	Crear y agregar una firma digital.
		5.1.4	Reconocer la posibilidad de recibir correos electrónicos fraudulentos y no solicitados.
		5.1.5	Comprender el término phishing. Identificar las características comunes del phishing, como: usar el nombre de empresas legítimas, personas, enlaces a páginas falsas.
		5.1.6	Tener conciencia del peligro de infectar el equipo con malware al abrir un archivo adjunto en un correo electrónico que contiene una macro o un archivo ejecutable.
	15.2 Mensajería instantánea	5.2.1	Comprender el término mensajería instantánea (IM) y sus usos.
		5.2.2	Comprender las vulnerabilidades de seguridad del IM, como: malware, acceso a backdoors, acceso a archivos.

		5.2.3	Reconocer métodos para asegurar la confidencialidad al usar IM como: cifrado, no divulgación de información importante, restricción de archivos compartidos.
6. Gestión de datos seguros	*6.1 Asegurar y utilizar copias de seguridad de los datos*	6.1.1	Reconocer formas de propiciar la seguridad física de los dispositivos, como: registrar la ubicación y los detalles del equipo, utilizar cable de seguridad con candado, control de acceso.
		6.1.2	Reconocer la importancia de tener un procedimiento de respaldo y copia de seguridad en caso de pérdida de datos, registros financieros, marcadores Web/historial.
		6.1.3	Identificar las características de un procedimiento de copia de datos, como: regularidad/frecuencia, programación, ubicación de almacenamiento.
		6.1.4	Datos de una copia de seguridad
		6.1.5	Restaurar y validar los datos respaldados.
	6.2 Destrucción segura	6.2.1	Comprender el motivo para eliminar datos de unidades o dispositivos de manera permanente.
		6.2.2	Distinguir entre eliminar y destruir datos de manera permanente.
		6.2.3	Identificar métodos comunes para destruir de manera permanente datos como: borrado, destrucción de unidades/medios, desimantación, uso de programas utilitarios de destrucción de datos.