Diseño Instruccional

Ciber Higiene y Buenas Prácticas de Seguridad de la Información para Usuarios

Plan formativo · Formato SENCE

Nombre del curso	Ciber Higiene y Buenas Prácticas de Seguridad de la Información para Usuarios
Modalidad	E-learning asincrónico, sin facilitador, Nivel 2
Duración total	60 horas pedagógicas
N° de módulos	5
Dirigido a	Personas usuarias de sistemas, correo, plataformas y dispositivos digitales en contextos laborales: analistas administrativos, ejecutivos de atención de clientes, asistentes de Recursos Humanos, asistentes contables, técnicos administrativos, funcionarios de apoyo operativo y personal de oficinas que utilizan sistemas informáticos, correo corporativo y dispositivos en el desarrollo habitual de sus funciones.
Requisitos de ingreso	Conocimientos básicos de computador, correo electrónico e Internet. No requiere conocimientos técnicos ni informáticos previos.

Competencia a desarrollar

Aplicar prácticas de ciberhigiene digital en las tareas laborales habituales, de acuerdo con los protocolos organizacionales de seguridad de la información, resguardando la confidencialidad, integridad y disponibilidad de la información.

Aprendizajes esperados, contenidos y horas

N°	Aprendizaje esperado	Contenidos	Horas
1	**Amenazas digitales y seguridad de la información** AE1: Identificar las amenazas digitales y los principios de seguridad de la información (confidencialidad, integridad y disponibilidad) a partir de casos de incidentes informáticos.	• Qué es la ciberseguridad y la ciberhigiene, y por qué importa en el trabajo diario • Amenazas digitales frecuentes: malware, phishing, ransomware y filtración de información, con ejemplos de incidentes reales • Cómo ocurre un incidente informático: vectores de ataque y consecuencias para la persona y la organización • Principios de seguridad de la información: confidencialidad, integridad y disponibilidad (CIA) aplicados a datos y documentos de trabajo • Activos de información y riesgos: qué información se protege, quién la usa y qué puede salir mal	**12**
2	**Credenciales, autenticación e ingeniería social** AE2: Analizar las credenciales de acceso y los ataques de ingeniería social, de acuerdo con las prácticas seguras de autenticación y las señales de alerta en las comunicaciones digitales.	• Credenciales de acceso y autenticación: contraseñas robustas, gestores de contraseñas y errores comunes • Autenticación multifactor (MFA) y por qué añade una capa de protección clave • Gestión de cuentas y principio de privilegio mínimo: cada persona con los accesos justos • Ingeniería social: cómo los atacantes manipulan a las personas (phishing, vishing, smishing, pretexto) • Señales de alerta en correos, enlaces y archivos sospechosos: cómo revisarlos antes de hacer clic	**12**

N°	Aprendizaje esperado	Contenidos	Horas
3	**Uso seguro de dispositivos y teletrabajo** AE3: Analizar el uso seguro de los dispositivos digitales de acuerdo con las prácticas seguras de teletrabajo.	• Dispositivos digitales seguros: actualizaciones, antivirus y bloqueo de pantalla • Almacenamiento y respaldos: dónde guardar la información y cómo protegerla ante pérdida • Redes públicas y teletrabajo: riesgos del wifi abierto y uso de conexiones seguras (VPN) • Uso seguro de dispositivos móviles y del equipo personal para tareas laborales (BYOD) • Qué hacer ante la pérdida o robo de un equipo con información de la organización	**12**
4	**Navegación segura y marco normativo de ciberseguridad** AE4: Distinguir los riesgos de navegación en internet y las obligaciones de ciberseguridad organizacional, conforme a las buenas prácticas de seguridad digital y a la Ley Marco de Ciberseguridad de Chile.	• Navegación segura: identificar sitios fraudulentos, descargas riesgosas y publicidad engañosa • Privacidad y datos personales al usar servicios digitales; buenas prácticas de resguardo • Deberes organizacionales del usuario frente a la información y las políticas internas • Ley Marco de Ciberseguridad de Chile (Ley N°21.663): qué es, la ANCI y el deber de reportar incidentes • Roles y responsabilidades en ciberseguridad dentro de la organización	**12**
5	**Ciberhigiene en la jornada laboral y gestión de incidentes** AE5: Aplicar prácticas de ciberhigiene digital en la jornada laboral, de acuerdo con los protocolos organizacionales de reporte de incidentes.	• Ciberhigiene en la jornada laboral: rutinas y hábitos seguros al empezar, durante y al cerrar el día • Reporte de incidentes: cómo, cuándo y a quién avisar ante una sospecha o un ataque • Contención inicial y escalamiento: primeros pasos correctos sin empeorar la situación • Preservación de evidencia y comunicación responsable durante un incidente • Casos integradores y plan personal de buenas prácticas de ciberhigiene	**12**
	Total horas pedagógicas		**60**

Sistema de evaluación

Instrumento	Descripción
Evaluación diagnóstica	Selección múltiple sin nota; cubre AE1-AE5; 10 preguntas sobre amenazas, autenticación, dispositivos, navegación/normativa y ciberhigiene.
Evaluaciones parciales	Un quiz por módulo (60% de aprobación). 8 preguntas por módulo, cada una etiquetada con el AE del módulo.