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, con relator/tutor que acompaña al participante por el foro de consultas de cada módulo y retroalimenta sus avances, Nivel 2
Duración total	60 horas cronológicas
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. Acceso a un computador, notebook o tablet con conexión estable a internet, navegador web actualizado, audio (parlantes o audífonos) y lector de PDF.

Competencia a desarrollar

Analizar situaciones de uso de la información y de los recursos digitales en las tareas laborales habituales en cuanto a las amenazas, los riesgos y las prácticas de ciberhigiene que corresponden, conforme a los protocolos de seguridad de la información de la organización y a la Ley N° 21.663 Marco de Ciberseguridad.

Verbo	Analizar (N4: examinar la situación digital y la práctica de ciberhigiene que corresponde)
Objeto	situaciones de uso de la información y de los recursos digitales (amenazas, riesgos y prácticas de ciberhigiene)
Condición	en las tareas laborales habituales, conforme a los protocolos de seguridad de la información de la organización y a la Ley N° 21.663

Aprendizajes esperados, contenidos y horas

N°	Aprendizaje esperado	Contenidos	Horas
1	**Amenazas digitales y seguridad de la información** AE1: Identificar las amenazas digitales —malware, phishing, ransomware y filtración de información— y el principio de seguridad de la información que afecta cada una, sea la confidencialidad, la integridad o la disponibilidad, en casos simulados de incidentes informáticos. Nivel taxonómico: N1-N2 Recordar/Comprender	• 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	**10**
2	**Credenciales, autenticación e ingeniería social** AE2: Clasificar correos, mensajes, llamadas y prácticas de autenticación presentados en casos simulados como seguros o de riesgo, conforme a las señales de alerta de la ingeniería social y a las prácticas seguras de gestión de credenciales. Nivel taxonómico: N2 Comprender	• 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	**11**
3	**Uso seguro de dispositivos y teletrabajo** AE3: Seleccionar las medidas de uso seguro de dispositivos, de respaldo de la información y de conexión que corresponden a situaciones de trabajo presencial y de teletrabajo presentadas en casos simulados, conforme a las prácticas seguras de la organización. Nivel taxonómico: N3 Aplicar	• 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: Determinar los riesgos de navegación y de privacidad y las obligaciones de la persona usuaria frente a la ciberseguridad organizacional en situaciones simuladas de uso de servicios digitales, conforme a las políticas internas y a la Ley N° 21.663 Marco de Ciberseguridad. Nivel taxonómico: N3 Aplicar	• 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: Analizar incidentes de seguridad de la información presentados en casos simulados de la jornada laboral en cuanto a las acciones de ciberhigiene, reporte, contención inicial y preservación de evidencia que corresponden, conforme a los protocolos organizacionales de gestión de incidentes. Nivel taxonómico: N4 Analizar	• 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	**15**

N°	Aprendizaje esperado	Contenidos	Horas
	Total horas cronológicas		**60**

Carga horaria y su fundamentación

El curso contempla 60 horas cronológicas en modalidad e-learning asincrónica, distribuidas de forma diferenciada (10/11/12/12/15 h) según el nivel taxonómico de cada aprendizaje esperado y la carga real de cada módulo: pantallas de la lección narrada, casos simulados de toma de decisiones, juegos de aplicación, apuntes y evaluaciones. Los módulos de mayor nivel taxonómico concentran más horas de práctica y trabajo autónomo; la última unidad incluye además el tiempo de la evaluación final integradora, que no constituye un AE adicional ni suma horas al total. Cada módulo desglosa su tiempo en lecciones, lectura y estudio de los apuntes, casos simulados y juegos, foro de consultas, trabajo autónomo y evaluación. El trabajo autónomo corresponde al estudio de las referencias del módulo, al reintento de los casos simulados y de los juegos y a la preparación de la evaluación.

Mód.	Lecciones	Lectura / estudio	Casos y actividades	Foro	Trabajo autónomo	Evaluación	Total
1	2	1,5	1,5	1	3,5	0,5	**10**
2	2	1,5	1,5	1	4,5	0,5	**11**
3	2	1,5	1,5	1	5,5	0,5	**12**
4	2	1,5	1,5	1	5,5	0,5	**12**
5	2	2	1,5	1	6,5	2	**15**

Técnicas metodológicas

Curso e-learning asincrónico con lecciones navegables narradas, historias con personajes, bloques interactivos, juegos, casos simulados de toma de decisiones, apuntes y glosario descargables, y evaluaciones con retroalimentación. La metodología avanza de lo conceptual a lo aplicado y al análisis de situaciones laborales, y el participante progresa de forma secuencial: cada módulo se habilita al completar el anterior —lección, evaluación parcial con 60 % de logro y participación en el foro— y la evaluación final integradora se habilita al completar los cinco módulos. En cada módulo, el facilitador abre el foro con una pregunta inicial vinculada al aprendizaje esperado; el participante interviene de forma obligatoria y asincrónica —al menos una intervención fundamentada, aplicando lo aprendido a una situación de su trabajo y apoyándose en el glosario del módulo— y el facilitador orienta, responde las dudas y retroalimenta cada participación. La plataforma registra ingreso, avance, interacción con los recursos, participación en el foro y resultados de evaluación.

Módulo 1 (AE1): El participante revisa la lección navegable narrada y los apuntes del módulo, consulta el glosario del módulo, practica con el juego interactivo y resuelve el caso simulado de toma de decisiones asociado a «Amenazas digitales y seguridad de la información». Rinde la evaluación parcial con retroalimentación por ítem (60 % de logro). Participa de forma obligatoria y asincrónica en el foro del módulo: el facilitador plantea la pregunta inicial vinculada al aprendizaje esperado, el participante publica al menos una respuesta fundamentada —aplicando lo aprendido a una situación de su trabajo— y el facilitador orienta, responde y retroalimenta. Esta participación es condición para avanzar al módulo siguiente.

Módulo 2 (AE2): El participante revisa la lección navegable narrada y los apuntes del módulo, consulta el glosario del módulo, practica con el juego interactivo y resuelve el caso simulado de toma de decisiones asociado a «Credenciales, autenticación e ingeniería social». Rinde la evaluación parcial con retroalimentación por ítem (60 % de logro). Participa de forma obligatoria y asincrónica en el foro del módulo: el facilitador plantea la pregunta inicial vinculada al aprendizaje esperado, el participante publica al menos una respuesta fundamentada —aplicando lo aprendido a una situación de su trabajo— y el facilitador orienta, responde y retroalimenta. Esta participación es condición para avanzar al módulo siguiente.

Módulo 3 (AE3): El participante revisa la lección navegable narrada y los apuntes del módulo, consulta el glosario del módulo, practica con el juego interactivo y resuelve el caso simulado de toma de decisiones asociado a «Uso seguro de dispositivos y teletrabajo». Rinde la evaluación parcial con retroalimentación por ítem (60 % de logro). Participa de forma obligatoria y asincrónica en el foro del módulo: el facilitador plantea la pregunta inicial vinculada al

aprendizaje esperado, el participante publica al menos una respuesta fundamentada —aplicando lo aprendido a una situación de su trabajo— y el facilitador orienta, responde y retroalimenta. Esta participación es condición para avanzar al módulo siguiente.
Módulo 4 (AE4): El participante revisa la lección navegable narrada y los apuntes del módulo, consulta el glosario del módulo, practica con el juego interactivo y resuelve el caso simulado de toma de decisiones asociado a «Navegación segura y marco normativo de ciberseguridad». Rinde la evaluación parcial con retroalimentación por ítem (60 % de logro). Participa de forma obligatoria y asincrónica en el foro del módulo: el facilitador plantea la pregunta inicial vinculada al aprendizaje esperado, el participante publica al menos una respuesta fundamentada —aplicando lo aprendido a una situación de su trabajo— y el facilitador orienta, responde y retroalimenta. Esta participación es condición para avanzar al módulo siguiente.
Módulo 5 (AE5): El participante revisa la lección navegable narrada y los apuntes del módulo, consulta el glosario del módulo, practica con el juego interactivo y resuelve el caso simulado de toma de decisiones asociado a «Ciberhigiene en la jornada laboral y gestión de incidentes». Rinde la evaluación parcial con retroalimentación por ítem (60 % de logro). Participa de forma obligatoria y asincrónica en el foro del módulo: el facilitador plantea la pregunta inicial vinculada al aprendizaje esperado, el participante publica al menos una respuesta fundamentada —aplicando lo aprendido a una situación de su trabajo— y el facilitador orienta, responde y retroalimenta. Al completar todos los módulos se habilita la evaluación final integradora.

Sistema de evaluación

Instrumento	Descripción
Evaluación diagnóstica	Cuestionario de selección múltiple sin calificación que cubre los 5 aprendizajes esperados, para detectar conocimientos previos.
Evaluaciones parciales	Por cada AE: caso simulado de toma de decisiones (lista de cotejo de decisiones críticas) y evaluación parcial del módulo (cuestionario o caso aplicado con retroalimentación), cada uno con exigencia de 60 % de logro.
Cuestionario final integrador	Cuestionario integrador de 12 preguntas que cubre los 5 aprendizajes esperados, con exigencia de 60 % de logro.
Evaluación final aplicada	Evaluación final aplicada sobre el caso «El incidente en la Consultora 'CiberResguardo'» (12 preguntas), evaluada con una rúbrica analítica de 5 criterios y 4 niveles de logro (destacado, adecuado, básico e insuficiente). Integra los aprendizajes esperados sin constituir un AE adicional. Las preguntas se corrigen automáticamente y el relator usa la rúbrica para retroalimentar por el foro.
Escala de calificación	Escala de 1,0 a 7,0. Nota mínima de aprobación 4,0, equivalente al 60 % de logro.
Ponderación	Evaluaciones parciales por aprendizaje esperado 60 % · Evaluación final integradora 40 % (cuestionario integrador y evaluación final aplicada, en partes iguales). La diagnóstica, la introducción y la inducción no inciden en la nota.

Evaluación por aprendizaje esperado

AE	Evidencia	Instrumento	Estándar
AE1	Resolución del caso simulado «Un día en la oficina de Sofía: Alertas inesperadas» (decisiones críticas con retroalimentación inmediata) y evaluación parcial del Módulo 1 (7 ítems).	Lista de cotejo de las decisiones críticas del caso, integrada en la lección del módulo, y cuestionario con clave de corrección y retroalimentación por ítem.	60 % de logro en cada instrumento.
AE2	Resolución del caso simulado «El correo del nuevo proveedor» (decisiones críticas con retroalimentación inmediata) y evaluación parcial del Módulo 2 (7 ítems).	Lista de cotejo de las decisiones críticas del caso, integrada en la lección del módulo, y cuestionario con clave de corrección y retroalimentación por ítem.	60 % de logro en cada instrumento.

AE	Evidencia	Instrumento	Estándar
AE3	Resolución del caso simulado «El desafío del teletrabajo: la seguridad de Sofía» (decisiones críticas con retroalimentación inmediata) y evaluación parcial del Módulo 3 (7 ítems).	Lista de cotejo de las decisiones críticas del caso, integrada en la lección del módulo, y cuestionario con clave de corrección y retroalimentación por ítem.	60 % de logro en cada instrumento.
AE4	Resolución del caso simulado «El extraño correo del lunes» (decisiones críticas con retroalimentación inmediata) y evaluación parcial del Módulo 4 (7 ítems).	Lista de cotejo de las decisiones críticas del caso, integrada en la lección del módulo, y cuestionario con clave de corrección y retroalimentación por ítem.	60 % de logro en cada instrumento.
AE5	Resolución del caso simulado «Un Día Inesperado en la Oficina» (decisiones críticas con retroalimentación inmediata) y evaluación parcial del Módulo 5 (7 ítems).	Lista de cotejo de las decisiones críticas del caso, integrada en la lección del módulo, y cuestionario con clave de corrección y retroalimentación por ítem.	60 % de logro en cada instrumento.

Rúbrica analítica — Evaluación final integradora

Niveles de logro: **Destacado** (4 pts): Resuelve el criterio de forma completa y correcta y fundamenta cada decisión en la norma, el protocolo o el procedimiento que corresponde. · **Adecuado** (3 pts): Resuelve correctamente los aspectos críticos del criterio, con omisiones menores que no afectan el resultado. · **Básico** (2 pts): Resuelve el criterio de forma parcial: reconoce la situación, pero omite o confunde al menos un aspecto crítico. · **Insuficiente** (1 pts): No reconoce la situación o propone acciones incorrectas o contrarias a la norma, al protocolo o al procedimiento.

Criterio	Desempeño esperado (nivel destacado)	Pond.	Destacado	Adecuado	Básico	Insuficiente
Identificación de amenazas y principios de seguridad	El estudiante identifica correctamente las amenazas digitales presentes en el caso (phishing, posible malware, suplantación de identidad) y explica cómo los principios de confidencialidad, integridad y disponibilidad se vieron afectados o podrían verse afectados.	25%	4 pts	3 pts	2 pts	1 pts
Análisis de credenciales y ataques de ingeniería social	El estudiante analiza adecuadamente el correo de phishing, identifica sus señales de alerta y propone acciones preventivas relacionadas con el uso de credenciales seguras y la autenticación multifactor.	25%	4 pts	3 pts	2 pts	1 pts
Uso seguro de dispositivos y prácticas de teletrabajo	El estudiante evalúa los riesgos asociados al uso del dispositivo móvil perdido (BYOD) y al posible malware en el computador portátil, sugiriendo medidas correctivas y preventivas alineadas con las prácticas seguras de teletrabajo.	20%	4 pts	3 pts	2 pts	1 pts
Navegación segura y obligaciones organizacionales	El estudiante reconoce la importancia de la navegación segura ante las descargas riesgosas y relaciona el incidente del cliente con las obligaciones de ciberseguridad organizacional y el deber de reporte según la normativa vigente.	15%	4 pts	3 pts	2 pts	1 pts
Aplicación de ciberhigiene y reporte de incidentes	El estudiante propone un plan de acción coherente para reportar los incidentes, describe los pasos iniciales para contener la situación y ejemplifica rutinas de ciberhigiene para prevenir futuros eventos, demostrando la aplicación de protocolos organizacionales.	15%	4 pts	3 pts	2 pts	1 pts