I.- Datos Generales

Código	Título
EC1771	Gestión de prácticas seguras y cultura de ciberseguridad en el entorno laboral

Propósito del Estándar de Competencia

Servir como referente para la evaluación y certificación de las personas que gestionan, operan y mantienen la funcionalidad, accesibilidad, seguridad y calidad de las plataformas y sistemas digitales que soportan los trámites y servicios de instituciones públicas y privadas.

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

El presente EC 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

El presente estándar va dirigido a las personas que deban contar con conocimientos, habilidades, destrezas y actitudes necesarias para implementar medidas seguras en el uso de equipos, redes y plataformas digitales, aplicar procedimientos de protección de la información personal y organizacional conforme a lineamientos de ciberseguridad, identificar y reportar incidentes o comportamientos digitales sospechosos mediante los canales institucionales establecidos para que una vez identificadas las amenazas actúe de manera proactiva y las mitigue fomentando la cultura de ciberseguridad y del uso responsable de las tecnologías en el entorno laboral.

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. Depende de las instrucciones de un superior. Se coordina con compañeros de trabajo de su mismo nivel jerárquico.

Comité de Gestión por Competencias que lo desarrolló
Red empresarial de servicios profesionales, educativos y técnicos.

Fecha de aprobación por el Comité Técnico del CONOCER:	Fecha de publicación en el Diario Oficial de la Federación:
23 de febrero de 2026	23 de marzo de 2026
Periodo sugerido de revisión /actualización del EC:	**Tiempo de Vigencia del Certificado de competencia en este EC:**
	2 años

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

Grupo unitario
2271 Desarrolladores y analistas de software y multimedia.
2272 Administradores de bases de datos y redes de computadora.

Ocupaciones asociadas
Sin referencia.

Ocupaciones no contenidas en el Sistema Nacional de Clasificación de Ocupaciones y reconocidas en el Sector para este EC
Sin referencia.

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

Sector:

54 Servicios Profesionales, Científicos y Técnicos.

Subsector:

411 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.

El presente EC, una vez publicado 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

- Agencia de Transformación Digital y Telecomunicaciones del Estado de Morelos.
- Asociación Mexicana de Empresas de Ciberseguridad (AMECS).
- Asociación Nacional de Bienestar y Desarrollo Organizacional (ASCEND).
- Universidad La Salle (Extensión Universitaria / Educación Continua).

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:	• Equipo de cómputo con acceso a las plataformas institucionales o simuladas necesarias para la demostración de los desempeños.

- Conexión a internet y red con configuraciones básicas de seguridad.
- Formatos de lista de verificación de prácticas seguras, registro simple de clasificación o resguardo de información, evidencia documental del cifrado o control de acceso, registro de reporte de incidente, evidencia de incidente permitida por la organización.
- Acceso a un espacio físico adecuado para la demostración práctica de los criterios de evaluación.

Duración estimada de la evaluación

- 1 hora con 30 minutos en gabinete 30 minutos en campo, totalizando 2 horas.

Referencias de Información

- Cámara de Diputados del H. Congreso de la Unión. (2011). Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (DOF 21-12-2011). Cámara de Diputados del H. Congreso de la Unión.
- Cámara de Diputados del H. Congreso de la Unión. (2025). Ley Federal de Protección de Datos Personales en Posesión de los Particulares (texto vigente; última reforma DOF 14-11-2025). Cámara de Diputados del H. Congreso de la Unión.
- Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI). (2025, noviembre). Propuesta de lineamientos para una Estrategia Nacional de Ciberseguridad para México: Contribuciones de la industria para un entorno digital más seguro y confiable para toda la población mexicana. CANIETI.
- Center for Internet Security. (s. f.). CIS Critical Security Controls v8.1. Center for Internet Security.
- International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.
- International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls. ISO.
- International Organization for Standardization & International Electrotechnical Commission. (2023). ISO/IEC 27035-1:2023 — Information security incident management — Part 1: Principles and process. ISO.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2014). Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales (Enero 2014). INAI.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2018). Recomendaciones para el manejo de incidentes de seguridad de datos personales (Junio 2018). INAI.
- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). NIST. https://doi.org/10.6028/NIST.CSWP.29

II.- Perfil del Estándar de Competencia

Estándar de Competencia
Gestión de prácticas seguras y cultura de ciberseguridad en el entorno laboral

Elemento 1 de 3
Implementar medidas seguras en el uso de equipos, redes y plataformas digitales

Elemento 2 de 3
Aplicar procedimientos de protección de la información personal y organizacional conforme a lineamientos de ciberseguridad

Elemento 3 de 3
Identificar y reportar incidentes/comportamientos digitales sospechosos mediante los canales institucionales establecidos

III.- Elementos que conforman el Estándar de Competencia

Referencia	Código	Título
1 de 3	E5604	Implementar medidas seguras en el uso de equipos, redes y plataformas digitales

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra los siguientes:

DESEMPEÑOS

1. Utiliza medidas seguras en el uso de equipos, redes y plataformas digitales:
- Bloqueando su sesión o dispositivo cada vez que se ausenta de su área de trabajo,
- Evitando compartir sus credenciales personales y contraseñas con otros usuarios,
- Evitando conectarse a redes Wi-Fi públicas sin autorización/sin mecanismos de protección, y
- Cerrando sesión correctamente al finalizar sus actividades en plataformas institucionales.

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. La lista de verificación de prácticas seguras aplicada:
- Contiene el registro con las medidas de seguridad implementadas, con fecha y nombre del participante,
- Indica cumplimiento/no cumplimiento de cada medida,
- Registra las acciones preventivas realizadas, y
- Contiene observaciones sobre vulnerabilidades detectadas.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS	NIVEL
1. Lineamientos institucionales para el uso seguro de equipos, redes y plataformas digitales.	Comprensión
2. Características de una contraseña segura conforme a políticas internas.	Conocimiento

ACTITUDES/HÁBITOS/VALORES

1. Responsabilidad:	La manera en que aplica consistentemente las medidas de seguridad al acceder, usar y cerrar equipos y plataformas digitales.

GLOSARIO

1. Bloqueo de sesión:	Acción de restringir temporalmente el acceso a un dispositivo para evitar uso no autorizado.
2. Credenciales personales:	Usuario y contraseña asignados de manera individual para acceder a sistemas autorizados.

3.	Lineamientos institucionales:	Conjunto de reglas definidas por la organización para el uso adecuado de recursos tecnológicos.
4.	Medidas seguras	Acciones específicas aplicadas para proteger equipos, accesos y plataformas contra riesgos digitales.
5.	Vulnerabilidades detectadas	Debilidades o configuraciones incorrectas en equipos, aplicaciones o procesos que pueden permitir accesos no autorizados o riesgos para la información si no se corrigen.

Referencia	Código	Título
2 de 3	E5605	Aplicar procedimientos de protección de la información personal y organizacional conforme a lineamientos de ciberseguridad

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra los siguientes:

DESEMPEÑOS

1. Protege la información personal y organizacional conforme a políticas de confidencialidad y seguridad establecidas:
- Clasificando documentos o archivos según el nivel de sensibilidad establecido por la organización,
- Resguardando la información utilizando los medios/plataformas autorizadas/carpetas institucionales/sistemas oficiales,
- Evitando compartir documentos/contraseñas/datos personales u organizacionales por canales no autorizados,
- Utilizando contraseñas diferentes para cada sistema/servicio,
- Realizando copias de seguridad periódicas conforme a los lineamientos establecidos,
- Cifrando documentos o unidades de almacenamiento con información sensible,
- Verificando la legitimidad de correos, enlaces/solicitudes antes de proporcionar información,
- Eliminando archivos/soportes físicos que contengan datos confidenciales, y
- Evitando el uso de dispositivos personales para almacenar información organizacional sin autorización previa.

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El registro simple de clasificación/resguardo de información elaborado:
- Contiene nombre y fecha de realización,
- Indica el tipo de información tratada interna/confidencial/pública,
- Señala el medio autorizado donde fue resguardada,
- Menciona el nivel de clasificación, e
- Incluye la firma/validación del responsable/área de ciberseguridad.

2. Bitácora de respaldo y resguardo de información diseñada:
- Indica la fecha, método y ubicación del respaldo realizado,
- Contiene la identificación del responsable de la acción, y
- Registra las incidencias/fallos detectados durante el proceso.

3. Evidencia documental del cifrado o control de acceso aplicada:
- Muestra el procedimiento utilizado para proteger los datos,
- Identifica el tipo de información protegida, y
- Señala el *software*/método empleado para el cifrado/resguardo.

CONOCIMIENTOS	NIVEL
1. Niveles de clasificación de la información establecidos por la organización.	Comprensión

CONOCIMIENTOS	NIVEL
2. Procedimientos autorizados de resguardo y manejo de documentos o datos sensibles.	Comprensión
3. Medidas básicas de protección de información personal y organizacional.	Conocimiento

La persona es competente cuando demuestra las siguientes:

ACTITUDES/HÁBITOS/VALORES

1. Orden:	La manera en que organiza, clasifica y resguarda la información conforme a los procedimientos establecidos.

GLOSARIO

1. Canal no autorizado:	Canal no autorizado: Medio no aprobado para compartir información (mensajería personal, apps externas, USB no autorizados).
2. Clasificación de la información:	Asignación de un nivel de sensibilidad para determinar su tratamiento y resguardo.
3. Información sensible:	Datos personales u organizacionales cuya divulgación no autorizada puede causar daño o riesgo.
4. Nivel de clasificación:	Es la etiqueta formal y el conjunto de controles que se asignan a un dato o sistema en función de su sensibilidad
5. Nivel de sensibilidad:	El nivel de sensibilidad en el entorno de la ciberseguridad es una medida cualitativa que indica el grado de daño o impacto negativo que sufriría una organización o un individuo si una pieza de información fuera divulgada, alterada o destruida sin autorización. Es la base para determinar cuánto esfuerzo y qué tipo de controles de seguridad deben aplicarse para proteger un activo de información.

Referencia	Código	Título
3 de 3	E5606	Identificar y reportar incidentes/comportamientos digitales sospechosos mediante los canales institucionales establecidos

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra los siguientes:

DESEMPEÑOS

1. Reporta incidentes digitales sospechosos:
- Identificando un correo/archivo/enlace/actividad inusual que pueda representar un incidente digital sospechoso,
- Verificando la autenticidad de solicitudes que pidan datos personales/institucionales,
- Evitando abrir archivos/enlaces con el contenido sospechoso, y
- Reportando el incidente utilizando el canal institucional establecido.

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El registro de reporte de incidente elaborado:
- Incluye nombre, fecha y área de quien lo elaboró,
- Describe el comportamiento/contenido sospechoso detectado, e
- Indica el canal institucional utilizado para realizar el reporte.

2. Evidencia del incidente permitida por la organización presentada:
- Incluye capturas/descripciones/archivos adjuntos autorizados,
- Muestra únicamente el contenido aprobado sin revelar datos sensibles, y
- Se presenta siguiendo el procedimiento institucional de resguardo de evidencia.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS	NIVEL
1. Indicadores básicos de incidentes digitales sospechosos.	Comprensión
2. Canales institucionales autorizados para el reporte de incidentes de seguridad digital.	Conocimiento

ACTITUDES/HÁBITOS/VALORES

1. Iniciativa:	La manera en que reporta oportunamente un incidente digital sospechoso utilizando los canales institucionales.

GLOSARIO

1. Actividad inusual:	Acciones del sistema o comunicaciones que no corresponden al uso normal esperado.
2. Canal institucional:	Canal institucional: Medio autorizado por la organización para reportar incidentes (correo oficial, ticket, línea interna).

3.	Incidente digital sospechoso:	Actividad, archivo o comunicación que presenta señales de riesgo o comportamiento anómalo.
4.	*Phishing*:	Intento de fraude donde se suplanta identidad para obtener información o acceso.