I.- Datos Generales

Código	Título
EC1544	Gestión integral de riesgos a la ciberseguridad

Propósito del Estándar de Competencia

Servir como referente para la evaluación y certificación de las personas que se desempeñan en la gestión integral de riesgos a la ciberseguridad y cuyas competencias incluyen plantificar el riesgo de la información digital, priorizar riesgos de la información digital y mitigar el riesgo de la información digital.

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 EC describe el desempeño del analista al identificar los activos de la información de la organización e informar los resultados de riesgos de los activos elaborados, realizar el análisis de riesgos de activos e implementar la evaluación de las amenazas priorizadas, de acuerdo con la lista elaborada de los activos, desarrollar el impacto de pérdida del riesgo; elaborar el impacto de riesgo y diseñar la matriz de riesgo elaborada. También establece los conocimientos teóricos, básicos y prácticos con los que debe de contar la persona para realizar su trabajo, así como las actitudes relevantes en su desempeño.

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 del mismo nivel jerárquico.

Comité de Gestión por Competencias que lo desarrolló

Del Sector de Seguridad Privada.

Fecha de aprobación por el Comité Técnico del CONOCER:	Fecha de publicación en el Diario Oficial de la Federación:
19 de junio del 2023	04 de agosto del 2023

Periodo sugerido de revisión /actualización del EC:	Tiempo de Vigencia del Certificado de competencia en este EC:
5 años	5 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:
5411 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.

Organizaciones participantes en el desarrollo del Estándar de Competencia
- Asociación Mexicana de Empresas de Seguridad Privada, S.A. de C.V.
- Cyber Black, S.A. de C.V.
- Training Black, S.A. de C.V.
- Cyberhuntersmx, S.A. de C.V.
- TGK CSS, SAPI DE C.V.

Relación con otros estándares de competencia
Estándares equivalentes:
- EC0329 Analizar información para el desarrollo de productos de inteligencia.

Estándares relacionados:
- EC0060 Vigilancia presencial de bienes y personas.
- EC0061 Coordinación de servicios de vigilancia de bienes y personas.
- EC1262 Aplicación de la entrevista para la investigación de la información.

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 paquetería *office*, conexión a internet, impresora y hojas blancas. • 1 persona que realice el papel de "usuario" y al menos 2 personas que realicen el papel de personas de su entorno.

Duración estimada de la evaluación

- 2 horas en gabinete y 1 hora en campo, totalizando 3 horas.

Referencias de Información

- Constitución Política de los Estados Unidos Mexicanos. Artículo 6 y 76.
- La “Ley Olimpia: Conjunto de reformas legislativas encaminadas a reconocer y sancionar la violencia digital, también conocida como “ciberviolencia”; Artículo 199 Octies y Artículo 199 Decies del Código Penal Federal.
- Se adiciona un Capítulo IV Ter denominado "De la Violencia Digital y Mediática" al Título II, compuesto por los artículos 20 Quáter, 20 Quinquies y 20 Sexies a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia. Publicada en el DOF: 01/06/2021, Vigente.
- Estrategia Nacional Digital y de Ciberseguridad con perspectiva de derechos humanos y enfoque basado en prevención y gestión de riesgos, así como de eficiencia en los procesos digitales. Publicada en el DOF, 06 de septiembre de 2021, Vigente.
- Ley General del Sistema Nacional de Seguridad Pública. Artículo 40 Fracción II. Publicada en el DOF, 2 de enero de 2009, Vigente.
- Norma ISO 27001/2013. Medidas fase 3 del modelo de sistemas de gestión de la seguridad de la información.
- Norma ISO 310001/2018. Gestión de Riesgos. Procedimiento, gestión y evaluación de riesgos.

II.- Perfil del Estándar de Competencia

Estándar de Competencia
Gestión integral de riesgos a la ciberseguridad

Elemento 1 de 3
Planificar el riesgo de la información digital

Elemento 2 de 3
Priorizar los riesgos de la información digital

Elemento 3 de 3
Mitigar el riesgo de la información digital

III.- Elementos que conforman el Estándar de Competencia

Referencia	Código	Título
1 de 3	E4748	Planificar el riesgo de la información digital

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra el siguiente:

DESEMPEÑO

1. Identifica los activos de la información de la organización:
   - Realizando el cuestionamiento al usuario sobre ¿qué? ¿cómo? ¿cuándo? ¿dónde? ¿por qué?, para la obtención de los activos de la información digital,
   - Realizando entrevistas a personas allegadas al usuario, del primer círculo de afectación del activo observado,
   - Clasificando el activo digital, de acuerdo con las características aportadas por el usuario,
   - Registrando las amenazas y vulnerabilidades internas y externas en el inventario de activos, y
   - Requisitando la tabla de activos y amenazas de riesgos.

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. La tabla de activos y amenazas de riesgos, requisitada:
   - Contiene un número/folio consecutivo,
   - Contiene el nombre de la persona que lo elaboró,
   - Indica la fecha en la que se complementó el mismo,
   - Contiene el ID del código del activo y su significado, y
   - Describe el tipo de activos y amenazas de riesgos observados.

2. El inventario de activos, corroborado:
   - Contiene un número/folio consecutivo,
   - Contiene el nombre de la persona que lo elaboró,
   - Indica la fecha en la que se complementó el mismo,
   - Contiene el ID del código del activo y su significado,
   - Describe los tipos de activos,
   - Describe la clasificación de la información, y
   - Contiene la descripción del cuestionamiento al usuario sobre ¿qué?, ¿quién?, ¿cómo?, ¿cuándo?, ¿dónde?, ¿por qué?

La persona es competente cuando demuestra los siguientes:

CONOCIMIENTOS	NIVEL
1. Conceptos básicos sobre ciberseguridad.	Conocimiento
2. Gestión de riesgos en dispositivos móviles.	Conocimiento

GLOSARIO

1.	Activos de la información:	Todo lo que genere valor para la organización, como procesos, personas, infraestructuras y tecnologías.
2.	Características de los activos de información:	Hace referencia a personas, procesos, infraestructura y equipo e información; confidencialidad; disponibilidad e integridad.
3.	Riesgos cualitativos:	El análisis de riesgo cualitativo es el proceso de calificación o puntuación del riesgo basado en la percepción de una persona sobre la gravedad y la probabilidad de sus consecuencias. El objetivo del análisis cualitativo de riesgos es elaborar una lista corta de riesgos que deben ser priorizados por encima de otros.
4.	Riesgos cuantitativos:	El análisis de riesgo cuantitativo es el proceso de calcular el riesgo a partir de los datos recogidos. El objetivo del análisis cuantitativo de riesgos es especificar con más detalle cuánto le costará a la empresa el impacto del riesgo.
5.	Usuario:	Persona que utiliza un producto o servicio de forma habitual, beneficiándose de algún modo de dicha utilización, sin entrar a valorar la marca, el precio o las características técnicas de lo que utiliza.

Referencia	Código	Título
2 de 3	E4749	Priorizar los riesgos de la información digital

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra los siguientes:

DESEMPEÑOS

1. Realiza el análisis de riesgos de los activos:
   - Especificando en la tabla de activos las amenazas elaboradas, de acuerdo a la clasificación de los activos observados,
   - Priorizando, a través de una lista las amenazas observadas en las tablas de los activos, y
   - Aplicando los criterios de función (F), sustitución (S), profundidad (P), extensión (E), agresión (A) y vulnerabilidad (V).

2. Desarrolla el impacto de pérdida del riesgo:
   - Estableciendo los indicadores del impacto de pérdida del riesgo,
   - Calculando los indicadores del impacto de pérdida del riesgo,
   - Registrando los datos en la matriz de riesgo, y
   - Presentando los resultados obtenidos al usuario.

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. La matriz de riesgos, elaborada:
   - Contiene el nombre de la persona que lo elaboró,

- Indica la fecha en la que se complementó el mismo,
- Contiene los indicadores del impacto de pérdida del riesgo,
- Contiene los indicadores de probabilidad de pérdida del riesgo, y
- Describe los resultados obtenidos.

2. El reporte de probabilidad de pérdida del riesgo, elaborado:
   - Contiene los indicadores de la probabilidad de pérdida del riesgo,
   - Contiene el cálculo obtenido de los indicadores de probabilidad de pérdida del riesgo,
   - Contiene los datos en la matriz de riesgo, y
   - Presenta los resultados obtenidos.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS	NIVEL
1. Estrategia Nacional Digital y de Ciberseguridad con perspectiva de derechos humanos y enfoque basado en prevención y gestión de riesgos, así como de eficiencia en los procesos digitales.	Conocimiento
2. La “Ley Olimpia” y el combate a la violencia digital.	Conocimiento

GLOSARIO

1. Cálculo del carácter del riesgo:	Se refiere al resultado obtenido de sumar la importancia del suceso más los daños ocasionados.
2. Cálculo de la probabilidad del riesgo:	Se refiere al resultado obtenido de multiplicar el criterio de agresión (A) por el criterio de vulnerabilidad (V) “Pb” Cálculo de la probabilidad.
3. Criterio de Agresión “A”:	Se refiere a la posibilidad o probabilidad de que el riesgo se manifieste.
4. Criterio de Extensión “E”:	Se refiere al alcance que los daños o pérdidas pueden conseguir.
5. Criterio de Función “F”:	Se refiere a las consecuencias negativas o daños que pueden alterar o afectar a la propia actividad de la empresa.
6. Criterio de Profundidad “P”:	Se refiere a la perturbación y efectos psicológicos que se podrían producir como consecuencia en la propia imagen de la empresa.
7. Criterio de Sustitución “S”:	Se refiere a las dificultades que pueden tenerse para sustituir los productos o los bienes.
8. Criterio de Vulnerabilidad “V”:	Se refiere a la posibilidad o probabilidad de que realmente se produzcan daños o pérdidas.
9. Impacto de pérdida:	Es una medición de la peor consecuencia creíble que puede ocurrir como resultado de un incidente. El impacto es definido por un grado de daño potencial, enfermedad, daño a la propiedad, pérdida de recursos (tiempo, dinero y personal) o potencial para afectar una misión. La

	combinación de dos o más incidentes puede incrementar el nivel global de riesgo.
10. Matriz de Riesgos:	Es una herramienta de análisis de riesgos que sirve para evaluar la probabilidad y la gravedad del riesgo durante el proceso de planificación del proyecto.
11. Probabilidad de Pérdida.	Es un grado de lo probable de que un evento ocurra. A la probabilidad se le asigna una letra de acuerdo con los criterios establecidos.

Referencia	Código	Título
3 de 3	E4750	Mitigar el riesgo de la información digital

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra los siguientes:

DESEMPEÑOS

1. Implementa un programa de Manejo Operativo de Riesgos (MOR):
   - Estableciendo el nivel operativo básico, basado en la identificación, comunicación e implementación,
   - Implementando el nivel táctico, tomando en cuenta la identificación, apreciación, decisión, comunicación, implementación y supervisión, y
   - Desarrollando el nivel estratégico mediante la identificación, apreciación, decisión, comunicación, implementación y supervisión.

2. Elabora la matriz de evaluación de riesgos:
   - Estableciendo las categorías de impacto,
   - Identificando la probabilidad de pérdidas, y
   - Destacando el uso de códigos de evaluación de riesgos.

3. Informa resultados de riesgos de los activos elaborados:
   - Comunicando al usuario el nivel del riesgo cuantitativo y cualitativo, y
   - Exponiendo al usuario el resultado de la tabla de activos y amenazas de riesgos.

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. La matriz de evaluación de riesgos, elaborada:
   - Contiene el nombre de la persona que lo elaboró,
   - Indica la fecha en la que se complementó el mismo,
   - Contiene las categorías de impacto,
   - Contiene la probabilidad de pérdidas, y
   - Contiene el uso de códigos de evaluación de riesgos.

2. El plan de mitigación de riesgo, elaborado:
   - Contiene el nombre de la persona que lo elaboró,

- Indica la fecha en la que se complementó el mismo,
- Describe la ruta del riesgo que se utilizará: aceptación, transferencia, reducción y rechazo,
- Contiene la programación sistematizada: planear; hacer; verificar y actuar, y
- Contiene los resultados obtenidos.

La persona es competente cuando demuestra el siguiente:

CONOCIMIENTO	NIVEL
1. Tipos de riesgos para su tratamiento: evitar, reducir y asumir.	Conocimiento

GLOSARIO

1. Manejo Operativo de Riesgos (MOR):	El MOR es un proceso de toma de decisiones en cinco etapas que es diseñado para habilitar a los individuos a identificar peligros, evaluar riesgos e implementar controles para reducir el riesgo asociado con cualquier acción u operación. El programa MOR original fue desarrollado por la Armada de los EE UU en 1989 y fue adoptado por la *US Navy* y otras ramas de servicios del Departamento de Defensa poco después.
2. Mitigación de riesgo:	Acciones tomadas con anticipación que aumentan la resiliencia para reducir o eliminar a largo plazo el impacto (pérdida de vida y propiedad) proveniente de peligros naturales y antropogénicos.