I.- Datos Generales

Código	Título
EC1802	Gestión estratégica de ciber riesgos en entornos institucionales

Propósito del Estándar de Competencia

Servir como referente para la evaluación y certificación de las personas líderes de tecnologías de información (TI), directores de seguridad de la información y gestores de riesgo que buscan evolucionar de una ciberseguridad reactiva a una actuación estratégica. Para alinear la seguridad de la información con los objetivos institucionales, asegurando que la toma de decisiones sobre protección de datos se base en el impacto estratégico.

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

Este EC contempla las funciones que una persona realiza para evaluar la competencia de gestionar los ciber riesgos estratégicos en entornos institucionales ya sean privado o públicos. Determinando los ciber riesgos estratégicos analizando la información para contextualizar las amenazas. Tomando decisiones para maximizar la resiliencia operativa y atender los ciber riesgos. Mantener la vigilancia sobre la eficacia de los controles y asegurar que la alta dirección esté informada para la toma de decisiones.

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: Cuatro

Desempeña diversas actividades tanto programas, poco rutinarias como impredecibles que suponen la aplicación de técnicas y principios básicos. Recibe lineamientos generales de un superior. Requiere emitir orientaciones generales e instrucciones específicas a personas y equipos de trabajo subordinados. Es responsable de los resultados de las actividades de sus subordinados y del suyo.

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:
22 de mayo 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. • Documentos, archivos o materiales simulados para la clasificación, resguardo y análisis de información. • Formatos solicitados en el estándar: El documento de identificación de ciber riesgos, el documento de priorización de ciber riesgos, el acta, acuerdo o documento de autorización del tratamiento de ciber riesgos, y el informe ejecutivo de seguimiento de ciber riesgos. • Acceso a un espacio físico adecuado para la demostración práctica de los criterios de evaluación.

Duración estimada de la evaluación

- 1 hora 20 minutos en gabinete y 1 hora en campo, totalizando 2 horas con 20 minutos.

Referencias de Información

- International Organization for Standardization. (2018). *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management*. https://www.iso.org/standard/75281.html
- International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001
- National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- National Institute of Standards and Technology. (2012). *Guide for Conducting Risk Assessments (SP 800-30 Rev. 1)*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)*. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
- ISACA. (2019). *COBIT 2019 Framework: Governance and Management Objectives*. https://www.isaca.org/resources/cobit
- The Open Group. (2018). *TOGAF® Standard, Version 9.2*. https://www.opengroup.org/togaf
- World Economic Forum. (2023). *Global Cybersecurity Outlook 2023*. https://www.weforum.org/reports/global-cybersecurity-outlook-2023
- European Union Agency for Cybersecurity (ENISA). (2022). *ENISA Threat Landscape 2022*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

- Microsoft. (2023). *Microsoft Digital Defense Report 2023*. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

II.- Perfil del Estándar de Competencia

Estándar de Competencia
Gestión estratégica de ciber riesgos en entornos institucionales

Elemento 1 de 3
Determinar los ciber riesgos estratégicos relevantes para la organización

Elemento 2 de 3
Priorizar el tratamiento de los ciber riesgos conforme a la estrategia organizacional

Elemento 3 de 3
Dirigir el seguimiento organizacional de la gestión de ciber riesgos

III.- Elementos que conforman el Estándar de Competencia

Referencia	Código	Título
1 de 3	E5712	Determinar los ciber riesgos estratégicos relevantes para la organización

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra los siguientes:

DESEMPEÑOS

1. Revisa información organizacional relevante para identificar ciber riesgos estratégicos:
- Comprobando objetivos institucionales/contexto organizacional,
- Analizando procesos críticos,
- Considerando información interna y externa relacionada con amenazas digitales,
- Tomando en consideración el entorno regulatorio vigente,
- Vinculando cada ciber riesgo con objetivos del plan estratégico institucional, y
- Clasificando los riesgos para enfocar los recursos en aquellos que representan una amenaza crítica para la organización.

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El documento de identificación de ciber riesgos estratégicos elaborado:
- Incluye nombre del responsable/fecha/firma,
- Enlista los ciber riesgos relevantes para la organización,
- Hace referencia a los objetivos/procesos/áreas afectadas, y
- Describe el impacto organizacional asociado a cada ciber riesgo.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS	NIVEL
1. Concepto de ciber riesgo estratégico.	Conocimiento
2. Relación entre ciber riesgos, objetivos organizacionales y continuidad operativa.	Conocimiento

La persona es competente cuando demuestra las siguientes:

ACTITUDES/HÁBITOS/VALORES

1. Iniciativa:	La manera en que identifica riesgos relevantes aun cuando no estén explícitamente documentados.
2. Responsabilidad:	La manera en que analiza y documenta los ciber riesgos estratégicos considerando el impacto institucional.

GLOSARIO

1. Amenaza crítica:	Se trata de un riesgo de tal magnitud que tiene el potencial de destruir permanentemente, colapsar o invalidar la viabilidad operativa de una organización, un sector crítico o, en casos extremos, la seguridad nacional de un país.

2.	Ciber riesgo estratégico:	Riesgo derivado del uso de tecnologías de la información que puede afectar los objetivos, la continuidad o la reputación de la organización.
3.	Objetivos organizacionales:	Metas estratégicas definidas por la organización para su operación y desarrollo.

Referencia	Código	Título
2 de 3	E5713	Priorizar el tratamiento de los ciber riesgos conforme a la estrategia organizacional

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra los siguientes:

DESEMPEÑOS

1. Organiza los ciber riesgos estratégicos conforme a criterios institucionales definidos:
- Aplicando criterios de impacto/urgencia/ alineación con los objetivos institucionales,
- Estipulando un orden de atención de los ciber riesgos,
- Estableciendo las acciones correspondientes para cada ciber riesgo priorizado,
- Definiendo acciones de tratamiento para los ciber riesgos estratégicos,
- Determinando el tipo de tratamiento a aplicar/mitigar/transferir/aceptar/evitar y,
- Estableciendo un orden de atención justificable de los ciber riesgos.

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El documento de priorización de ciber riesgos estratégicos elaborado:
- Incluye nombre de la organización/nombre del responsable/fecha/firma,
- Enlista los ciber riesgos estratégicos identificados,
- Menciona los criterios utilizados para su priorización,
- Establece la priorización de los ciber riesgos conforme a criterios institucionales de impacto/ urgencia/alineación con los objetivos institucionales, e
- Integra la justificación de la prioridad asignada a cada ciber riesgo.

2. El acta acuerdo/documento de autorización del tratamiento de ciber riesgos requisitada:
- Incluye nombre de la organización/nombre del responsable/fecha/firma,
- Señala las áreas involucradas,
- Establece el tipo de tratamiento definido para cada ciber riesgo, y
- Menciona las decisiones de tratamiento autorizadas por su superior.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS	NIVEL
1. Enfoques de tratamiento de ciber riesgos (mitigar, transferir, aceptar, evitar).	Conocimiento
2. Relación entre ciber riesgos, estrategia organizacional y toma de decisiones directivas.	Conocimiento

La persona es competente cuando demuestra las siguientes:

ACTITUDES/HÁBITOS/VALORES

1. Orden: La manera en que establece y documenta la priorización de los ciber riesgos estratégicos.

2.	Responsabilidad:	La manera en que solicita la autorización del tratamiento de los ciber riesgos considerando las implicaciones institucionales.

GLOSARIO

1.	Priorización:	Proceso de ordenamiento de ciber riesgos conforme a criterios definidos por la organización.
2.	Tratamiento de ciber riesgos:	Decisión organizacional para mitigar, transferir, aceptar o evitar un ciber riesgo.

Referencia	Código	Título
3 de 3	E5714	Dirigir el seguimiento organizacional de la gestión de ciber riesgos

CRITERIOS DE EVALUACIÓN

La persona es competente cuando demuestra los siguientes:

DESEMPEÑOS

1. Presenta a instancias directivas el seguimiento organizacional de la gestión de ciber riesgos estratégicos:
- Comunicando los antecedentes de la gestión de ciber riesgos,
- Describiendo el estado actual de los ciber riesgos priorizados,
- Exponiendo los avances/desviaciones en la ejecución de las acciones de tratamiento autorizadas,
- Identificando los riesgos emergentes/situaciones relevantes para la organización,
- Señalando requerimientos de decisión o ajuste estratégico por parte de las instancias directivas, y
- Presentando el cumplimiento de los acuerdos/decisiones autorizadas.

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El informe ejecutivo de seguimiento de ciber riesgo elaborado:
- Incluye nombre de la organización/nombre del responsable/fecha/firma,
- Muestra cómo los controles actuales han disminuido el riesgo hacia zonas de menor peligro,
- Identifica riesgos emergentes desde el último seguimiento,
- Explica la razón de ocurrencia de los incidentes graves,
- Menciona las acciones tomadas para evitar la recurrencia,
- Analiza el estado general de los ciber riesgos estratégicos, y
- Establece el progreso/desviaciones en las acciones autorizadas.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS	NIVEL
1. Principios de gobernanza de la ciberseguridad.	Conocimiento
2. Mecanismos de seguimiento y reporte ejecutivo de riesgos.	Conocimiento

La persona es competente cuando demuestra las siguientes:

ACTITUDES/HÁBITOS/VALORES

1.	Cooperación:	La manera en que coordina la comunicación con las áreas responsables del tratamiento de ciber riesgos.
2.	Perseverancia:	La manera en que mantiene el seguimiento continuo de los ciber riesgos estratégicos.

GLOSARIO

1.	Informe ejecutivo:	Documento sintético dirigido a instancias directivas para la toma de decisiones.
2.	Principios de gobernanza:	Conjunto de lineamientos que orientan la dirección, supervisión y control de la gestión organizacional para asegurar la toma de decisiones, la rendición de cuentas y el cumplimiento de los objetivos organizacionales.
3.	Seguimiento institucional:	Revisión periódica del estado de los ciber riesgos estratégicos y de las acciones autorizadas por la organización.