

I.- Datos Generales

Código	Título
EC1865	Implementación del sistema de gestión de cumplimiento normativo y regulatorio en Ciberseguridad y Protección de Datos

Propósito del Estándar de Competencia

Servir como referente para la evaluación y certificación de las personas que desempeñan funciones de Oficial de Cumplimiento en Ciberseguridad y Protección de Datos está orientado a profesionales responsables de diseñar, implementar, supervisar, evaluar y fortalecer los mecanismos institucionales destinados a garantizar la seguridad de la información, la protección de datos personales y el cumplimiento de las disposiciones normativas, regulatorias y organizacionales aplicables en estas materias.

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 de Competencia describe los conocimientos, habilidades, actitudes, hábitos y valores que debe contar una persona que labora en organizaciones públicas, privadas y sociales, independientemente de su tamaño o sector económico, que tienen bajo su responsabilidad la gestión del cumplimiento relacionado con la privacidad de los datos, la seguridad de los activos de información, la administración de riesgos tecnológicos, la continuidad operativa, la gobernanza digital y la protección de la información sensible.

Esta función denominada internacionalmente como Cybersecurity (CCO) Compliance Officer, Son responsables de la implementación de marcos de referencia, controles, políticas y procedimientos destinados a prevenir incidentes de seguridad, reducir vulnerabilidades, proteger la información de clientes, usuarios, colaboradores y terceros, así como asegurar el cumplimiento de obligaciones legales y regulatorias derivadas del tratamiento de datos personales y del uso de tecnologías de la información

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: Cinco

Desempeña una amplia gama de actividades tanto programadas poco rutinarias como impredecibles, que implican la aplicación de un rango variado de principios fundamentales y técnicas complejas. Emite lineamientos generales a sus subordinados. Es el último responsable de la planeación y la programación de las actividades de la organización o grupo de trabajo. Es el

último responsable de los resultados finales del trabajo de todos los equipos y personas que de él dependen.

Comité de Gestión por Competencias que lo desarrolló

Servicios Sociales y Cumplimiento Normativo en Organizaciones Públicas y Privadas

**Fecha de aprobación por el Comité
Técnico del CONOCER:**

24 de septiembre de 2026

**Fecha de publicación en el Diario Oficial
de la Federación:**

**Periodo sugerido de
/actualización del EC:**

3 años

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

Grupo unitario

2111 Administradores y profesionistas en recursos humanos y sistemas de gestión.

Ocupaciones asociadas

Especialista en calidad administrativa.

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

Administradores y asesores en implementación de sistemas de calidad.

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

Sector:

54 Servicios profesionales, científicos y técnicos.

Subsector:

541 Servicios profesionales, científicos y técnicos.

Rama:

5416 Servicios de consultoría administrativa, científica y técnica.

Subrama:

54161 Servicios de consultoría en administración.

Clase:

541610 Servicios de consultoría en administración.

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

- Asociación Mexicana de Contadores Públicos, (AMCP).
- Asociación Mexicana de Contadores Públicos de Hidalgo.
- Asociación Mexicana de Mujeres jefas de Empresas en Morelos
- Federación Iberoamericana de Compliance y Sostenibilidad.
- Fundación Baraona Burguett.
- International Compliance & Compliance Officers.
- Procuraduría Federal de la Defensa del Trabajo (PROFEDET).

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 software de oficina para la elaboración de documentos.
- Acceso a internet para consulta de disposiciones normativas y regulatorias, cuando corresponda.
- Información documental del sujeto obligado (real o simulada), suficiente para desarrollar los productos solicitados.
- Marco normativo aplicable en materia de Prevención de Lavado de Dinero y Financiamiento al Terrorismo, incluyendo leyes, reglamentos, disposiciones de carácter general y guías vigentes.
- Formatos establecidos para la integración de evidencias, cuando sean requeridos durante la evaluación.
- Espacio físico o virtual que permita desarrollar las actividades de evaluación en condiciones adecuadas.
- Material de consulta autorizado durante la evaluación, de conformidad con las reglas establecidas por el Organismo Certificador.
- Medios para la presentación y entrega de los productos desarrollados durante la evaluación, en formato físico y/o electrónico.
- Acceso a información ficticia o anonimizada cuando el caso de evaluación involucre datos sujetos a confidencialidad o protección de datos personales.

Duración estimada de la evaluación

- 4 horas en gabinete y 0 horas en campo, totalizando 4 horas.

Referencias de Información

- ISO 37301:2021 – Sistemas de gestión del compliance — Requisitos con orientación para su uso.
- ISO 37000:2021 – Gobernanza de las organizaciones — Orientación.
- ISO/IEC 27001:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de seguridad de la información — Requisitos.
- ISO/IEC 27002:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información.
- ISO/IEC 27005:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad — Orientación sobre la gestión de riesgos de seguridad de la información.
- ISO/IEC 27035-1:2023 – Seguridad de la información, ciberseguridad y protección de la privacidad — Gestión de incidentes de seguridad de la información — Parte 1: Principios y proceso.
- ISO/IEC 27701:2019 – Técnicas de seguridad — Extensión de ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información de privacidad — Requisitos y directrices.
- ISO/IEC 29100:2024 – Seguridad de la información, ciberseguridad y protección de la privacidad — Marco de privacidad.
- ISO/IEC 29134:2023 – Seguridad de la información, ciberseguridad y protección de la privacidad — Directrices para la evaluación de impacto de la privacidad.
- ISO 31000:2018 – Gestión del riesgo — Directrices.
- ISO 19011:2018 – Directrices para la auditoría de los sistemas de gestión.
- ISO 9000:2015 – Sistemas de gestión de la calidad — Fundamentos y vocabulario. (Como referencia complementaria para conceptos de mejora continua y acciones correctivas.)
- NIST Cybersecurity Framework (CSF) 2.0 – Framework for Improving Critical Infrastructure Cybersecurity.
- NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide.
- NIST Privacy Framework 1.0 – A Tool for Improving Privacy through Enterprise Risk Management.
- NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations.
- Reglamento (UE) 2016/679 (RGPD) – Reglamento General de Protección de Datos.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares – México.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares – México.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados – México.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público – México.
- Ley General de Transparencia y Acceso a la Información Pública – México.
- Reglamento General de Protección de Datos (GDPR) - Unión Europea. Principal regulación europea que establece derechos, obligaciones y medidas para proteger datos personales. Es reconocido mundialmente como un estándar en protección de datos. Referencia: European Commission. Regulation (EU) 2016/679 (GDPR). Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Disponible en: <https://www.inai.org.mx/>
- NIST Cybersecurity Framework (NIST CSF). Marco referencia en ciberseguridad desarrollado por el Instituto Nacional de Estándares y Tecnología de EE.UU., que ofrece directrices para gestionar riesgos cibernéticos. Referencia: NIST. “Framework for Improving Critical Infrastructure Cybersecurity”. Disponible en: <https://www.nist.gov/cyberframework>
- ISO/IEC 27001 - Sistemas de Gestión de Seguridad de la Información

- Norma internacional para establecer, implementar, mantener y mejorar sistemas de gestión de seguridad de la información (SGSI). Referencia: ISO/IEC 27001:2013. Disponible en: <https://www.iso.org/isoiec-27001-information-security.html>
- Directiva NIS (Network and Information Security Directive) - Unión Europea Directiva que establece medidas para lograr un alto nivel común de seguridad en redes y sistemas de información dentro de la UE. Referencia: European Union Agency for Cybersecurity (ENISA). Disponible en: <https://www.enisa.europa.eu/topics/nis-directive>
- HIPAA (Health Insurance Portability and Accountability Act) - EE.UU. Proporciona regulaciones específicas sobre protección de datos en el sector salud, incluyendo aspectos de seguridad y privacidad. Referencia: U.S. Department of Health & Human Services (HHS). Disponible en: <https://www.hhs.gov/hipaa/index.html>.
- COBIT (Control Objectives for Information and Related Technologies) Marco de gobernanza y gestión de TI, con un fuerte componente en controles para seguridad y cumplimiento. Referencia: ISACA. Disponible en: <https://www.isaca.org/resources/cobit>.

II.- Perfil del Estándar de Competencia

Estándar de Competencia

Implementación del sistema de gestión de cumplimiento normativo y regulatorio en Ciberseguridad y Protección de Datos

Elemento 1 de 7

Diagnosticar el contexto de cumplimiento especializado en Ciberseguridad y Protección de Datos

Elemento 2 de 7

Identificar y analizar las obligaciones y riesgos de cumplimiento asociados a la Ciberseguridad y Protección de Datos

Elemento 3 de 7

Diseñar el marco especializado de cumplimiento en Ciberseguridad y Protección de Datos

Elemento 4 de 7

Implementar los controles y mecanismos de cumplimiento en Ciberseguridad y Protección de Datos

Elemento 5 de 7

Gestionar incidentes y eventos con impacto en el cumplimiento normativo y la Protección de Datos

Elemento 6 de 7

Evaluar el cumplimiento y la efectividad del sistema especializado de Ciberseguridad y Protección de Datos

Elemento 7 de 7

Implementar acciones de mejora y fortalecimiento del sistema de cumplimiento especializado

III.- Elementos que conforman el Estándar de Competencia

Referencia	Código	Título
1 de 7	E5930	Diagnosticar el contexto de cumplimiento especializado en Ciberseguridad y Protección de Datos

CRITERIOS DE EVALUACIÓN

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El diagnóstico del contexto organizacional, elaborado:

- Contiene el nombre de la organización,
- Indica la fecha de elaboración,
- Describe el objetivo del diagnóstico,
- Identifica los factores internos que pueden afectar el cumplimiento en materia de ciberseguridad y protección de datos,
- Contiene los factores externos que pueden afectar el cumplimiento en materia de ciberseguridad y protección de datos,
- Describe las características relevantes de la organización relacionadas con ciberseguridad y protección de datos,
- Indica los procesos organizacionales relacionados con el tratamiento de información y datos personales,
- Determina las partes interesadas internas y externas relacionadas con el cumplimiento en materia de ciberseguridad y protección de datos,
- Determina las funciones y áreas de la organización que intervienen en el cumplimiento especializado,
- Describe las interacciones existentes entre las áreas de cumplimiento, ciberseguridad, seguridad de la información, privacidad y protección de datos, cuando existan,
- Identifica las condiciones que pueden favorecer o dificultar el cumplimiento de las obligaciones aplicables, y
- Contiene las conclusiones derivadas del análisis del contexto organizacional.

2. El inventario de activos de información y datos sujetos a protección, elaborado:

- Contiene el nombre de la organización,
- Indica la fecha de elaboración,
- Describe los procesos organizacionales asociados con los activos de información,
- Indica los activos de información utilizados en los procesos analizados,
- Clasifica los activos de información de acuerdo con los criterios establecidos por la organización,
- Describe los activos que contienen o procesan datos personales,
- Describe los tipos o categorías de datos personales tratados, cuando corresponda,
- Indica los responsables de los activos de información,
- Indica la ubicación o medio en el que se encuentran los activos de información,
- Describe las etapas del ciclo de vida de la información y los datos personales,
- Indica los terceros que intervienen en el tratamiento, almacenamiento, transmisión o procesamiento de la información y datos personales, cuando existan,
- Indica los criterios utilizados para determinar los activos de información sujetos a protección, y
- Contiene la fecha de actualización del inventario.

3. El mapa de procesos y flujo de información y datos personales, elaborado:

- Contiene el nombre de la organización,
- Indica la fecha de elaboración
- Describe los procesos organizacionales incluidos en el alcance del análisis,
- Indica el origen de la información y los datos personales,
- Describe los procesos en los que se recopila información y datos personales,
- Describe los procesos en los que se utilizan o procesan los datos personales,
- Indica los medios utilizados para almacenar la información y los datos personales,
- Indica los medios utilizados para transmitir o transferir la información y los datos personales,
- Identifica los terceros que intervienen en el flujo de información y datos personales, cuando existan,
- Indica el destino de la información y los datos personales al concluir su tratamiento,
- Indica las transferencias de información y datos personales entre áreas, sistemas o terceros, cuando existan,
- Representa gráficamente el flujo de información y datos personales, y
- Identifica los puntos del flujo en los que existen obligaciones de cumplimiento relacionadas con ciberseguridad y protección de datos.

4. El documento de determinación del alcance del sistema especializado de cumplimiento, elaborado:

- Contiene el nombre de la organización,
- Indica la fecha de elaboración,
- Define el objetivo del alcance determinado,
- Describe las unidades organizacionales incluidas,
- Indica los procesos incluidos,
- Indica los activos de información incluidos,
- Indica los tipos de información y datos personales incluidos,
- Describe las actividades de tratamiento de datos personales incluidas,
- Indica las ubicaciones físicas y digitales incluidas, cuando corresponda,
- Define los terceros que forman parte del alcance, cuando corresponda,
- Describe las interfaces y relaciones con otros sistemas de gestión de la organización, cuando existan,
- Indica las exclusiones del alcance, cuando existan,
- Justifica las exclusiones determinadas, cuando existan, y
- Contiene la aprobación o validación del alcance por la instancia responsable de la organización.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS

NIVEL

1. Contexto organizacional en materia de ciberseguridad y protección de datos
 - Factores internos y externos.
 - Partes interesadas.
 - Procesos organizacionales.
 - Áreas y funciones involucradas.
 - Alcance organizacional.

Aplicación

CONOCIMIENTOS

NIVEL

2. Gestión de activos de información y ciclo de vida de los datos

Aplicación

- Identificación y clasificación de activos de información.
- Tipos y categorías de datos personales.
- Ciclo de vida de la información y los datos personales.
- Flujo, almacenamiento, tratamiento y transferencia de información y datos.

3. Alcance del sistema especializado de cumplimiento

Aplicación

- Determinación del alcance.
- Unidades, procesos y actividades incluidas.
- Límites e interfaces del sistema.
- Exclusiones y su justificación.

La persona es competente cuando demuestra la siguiente:

ACTITUD/HÁBITO/VALOR

1. Orden:

La manera en que organiza y relaciona la información del contexto, los procesos, los activos de información, los flujos de datos y el alcance del sistema especializado, manteniendo una secuencia lógica y coherente.

GLOSARIO

1. Activo de información:

Información o recurso relacionado con su tratamiento que tiene valor para la organización y que requiere protección de acuerdo con su importancia y características.

2. Alcance:

Límites y extensión de aplicación del sistema especializado de cumplimiento, incluyendo los procesos, áreas, actividades, información, datos y demás elementos comprendidos.

3. Ciclo de vida de los datos:

Conjunto de etapas por las que pasan los datos desde su obtención o recopilación hasta su uso, almacenamiento, transferencia, conservación y eliminación.

4. Contexto organizacional:

Conjunto de factores internos y externos que pueden influir en la capacidad de una organización para alcanzar sus objetivos y cumplir con sus obligaciones.

Referencia

Código

Título

2 de 7

E5931

Identificar y analizar las obligaciones y riesgos de cumplimiento asociados a la Ciberseguridad y Protección de Datos

CRITERIOS DE EVALUACIÓN

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. La matriz de obligaciones normativas y regulatorias aplicables, elaborada:

- Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Indica el objetivo y alcance de la matriz,
 - Contiene la relación de las disposiciones legales, reglamentarias y normativas aplicables,
 - Señala la denominación de cada disposición aplicable,
 - Indica la referencia específica de los artículos, fracciones, apartados o disposiciones aplicables,
 - Describe la obligación de cumplimiento establecida en cada disposición,
 - Relaciona cada obligación con los procesos, actividades o servicios de la organización a los que resulta aplicable,
 - Indica las áreas o funciones responsables de atender cada obligación,
 - Señala la periodicidad/momento en que debe cumplirse cada obligación, cuando corresponda,
 - Indica las consecuencias asociadas al incumplimiento, cuando se encuentren previstas,
 - Contiene la fuente de consulta de cada disposición normativa,
 - Indica la fecha de vigencia o actualización de las disposiciones consideradas, y
 - Contiene la fecha prevista para su revisión y actualización.
2. La matriz de análisis de obligaciones y riesgos de cumplimiento, elaborada:
- Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Relaciona cada obligación normativa con el proceso o actividad organizacional correspondiente,
 - Describe el riesgo de incumplimiento asociado a cada obligación,
 - Señala las causas que pueden originar el incumplimiento,
 - Describe las posibles consecuencias legales, regulatorias, operativas o reputacionales derivadas del incumplimiento,
 - Establece los criterios utilizados para valorar los riesgos de cumplimiento,
 - Contiene la valoración asignada a cada riesgo,
 - Indica el nivel de prioridad de atención de cada riesgo,
 - Relaciona los riesgos de cumplimiento con las obligaciones normativas que les dan origen,
 - Señala las áreas o funciones responsables de gestionar cada riesgo, y
 - Contiene la fecha de revisión de los riesgos analizados.
3. El informe de determinación de brechas de cumplimiento, elaborado:
- Contiene la identificación de los riesgos,
 - Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Describe la metodología utilizada para determinar las brechas de cumplimiento,
 - Contiene las obligaciones normativas consideradas en el análisis,
 - Describe la situación actual de cumplimiento de cada obligación evaluada,
 - Indica los requisitos de cumplimiento que se encuentran atendidos,
 - Señala los requisitos de cumplimiento que se encuentran parcialmente atendidos,
 - Describe los requisitos de cumplimiento que no se encuentran atendidos,
 - Contiene las evidencias utilizadas para sustentar la determinación de las brechas,
 - Describe las desviaciones identificadas respecto de las obligaciones aplicables,
 - Establece el nivel o grado de cumplimiento determinado para cada obligación evaluada,
 - Indica la prioridad de atención de las brechas identificadas, y
 - Contiene las conclusiones derivadas del análisis realizado.

4. El registro de actualización de obligaciones y riesgos de cumplimiento, elaborado:

- Contiene el nombre de la organización,
- Indica la fecha de elaboración,
- Contiene la relación de cambios normativos y regulatorios detectados,
- Describe las modificaciones realizadas a las obligaciones previamente registradas,
- Señala las nuevas obligaciones incorporadas,
- Indica las obligaciones que dejaron de ser aplicables, cuando corresponda,
- Describe los cambios en los riesgos de cumplimiento derivados de las modificaciones normativas,
- Indica los procesos, actividades o áreas afectados por los cambios identificados,
- Señala la fecha en que se detectó cada cambio,
- Contiene la fuente normativa utilizada para validar cada modificación,
- Indica las acciones requeridas para mantener actualizado el universo de obligaciones y riesgos de cumplimiento, y
- Contiene el registro de la fecha de actualización de la matriz de obligaciones y riesgos.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS

1. Riesgo y brechas de cumplimiento:
 - Riesgo de cumplimiento.
 - Causas y consecuencias del incumplimiento.
 - Criterios de valoración y priorización.
 - Brechas y desviaciones de cumplimiento.
 - Análisis del nivel de cumplimiento.
2. Identificación y análisis de obligaciones de cumplimiento aplicable a la ciberseguridad y protección de datos:
 - Universo de obligaciones aplicables.
 - Relación entre obligaciones, procesos y actividades organizacionales.
 - Responsables del cumplimiento.
 - Consecuencias del incumplimiento.
 - Actualización y seguimiento de obligaciones normativas.

NIVEL

Aplicación

Aplicación

La persona es competente cuando demuestra la siguiente:

ACTITUD/HÁBITO/VALOR

1. Responsabilidad: La manera en que sustenta las obligaciones y riesgos de cumplimiento registrados mediante fuentes normativas vigentes y verificables, manteniendo actualizada la información utilizada para el análisis.

GLOSARIO

1. Brecha de cumplimiento: Diferencia existente entre el nivel de cumplimiento requerido por una obligación aplicable y la situación real de cumplimiento de la organización.

2. Universo de obligaciones: Conjunto de obligaciones legales, reglamentarias, normativas y otros requisitos de cumplimiento que resultan aplicables a una organización de acuerdo con su contexto, actividades y operaciones.

Referencia	Código	Título
3 de 7	E5932	Diseñar el marco especializado de cumplimiento en Ciberseguridad y Protección de Datos

CRITERIOS DE EVALUACIÓN

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

- El modelo especializado de cumplimiento en ciberseguridad y protección de datos, elaborado:
 - Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Establece el objetivo del modelo especializado de cumplimiento,
 - Define el alcance de aplicación del modelo,
 - Describe los componentes que integran el modelo especializado de cumplimiento,
 - Establece los principios que orientan su funcionamiento,
 - Define las funciones y responsabilidades de las áreas involucradas,
 - Describe la interacción entre las funciones de cumplimiento, ciberseguridad, seguridad de la información, privacidad y protección de datos,
 - Establece los mecanismos de coordinación entre las funciones involucradas,
 - Define los mecanismos para gestionar las obligaciones de cumplimiento aplicables,
 - Establece los mecanismos para gestionar los riesgos y brechas de cumplimiento,
 - Define los mecanismos para monitorear y evaluar el cumplimiento,
 - Establece los mecanismos para gestionar incumplimientos y desviaciones,
 - Define los mecanismos para revisar y actualizar el modelo, y
 - Contiene la aprobación o validación del modelo por la instancia correspondiente.
- La matriz de roles y responsabilidades del modelo especializado de cumplimiento, elaborada:
 - Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Contiene la relación de las áreas y funciones que participan en el modelo especializado,
 - Describe las responsabilidades de la función de cumplimiento,
 - Describe las responsabilidades de la función de ciberseguridad,
 - Describe las responsabilidades de la función de seguridad de la información,
 - Describe las responsabilidades de la función de privacidad y protección de datos, cuando exista,
 - Señala las responsabilidades de las áreas operativas involucradas,
 - Define las responsabilidades relacionadas con la identificación y actualización de obligaciones de cumplimiento,
 - Define las responsabilidades relacionadas con la gestión de riesgos de cumplimiento,
 - Define las responsabilidades relacionadas con la implementación y seguimiento de controles,
 - Establece los mecanismos de coordinación y comunicación entre las funciones involucradas,
 - Define los niveles de autoridad para la toma de decisiones relacionadas con el cumplimiento,

- Contiene la aprobación/validación de los roles y responsabilidades por la instancia correspondiente.
3. El esquema de controles y mecanismos de cumplimiento especializado, elaborado:
- Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Relaciona los controles con las obligaciones normativas aplicables,
 - Relaciona los controles con los riesgos de incumplimiento correspondientes,
 - Describe el objetivo de cada control,
 - Establece el tipo de control aplicable, cuando corresponda,
 - Describe las actividades necesarias para la ejecución de cada control,
 - Indica el responsable de ejecutar cada control,
 - Establece la periodicidad de ejecución de cada control,
 - Define las evidencias requeridas para demostrar la ejecución de cada control,
 - Establece los mecanismos para conservar y consultar las evidencias,
 - Define los mecanismos para verificar la efectividad de los controles,
 - Contiene los criterios para determinar el tratamiento de desviaciones en la ejecución de los controles, y
 - Establece los mecanismos para revisar y actualizar los controles.
4. El plan de implementación del modelo especializado de cumplimiento, elaborado:
- Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Establece las etapas para la implementación del modelo especializado,
 - Describe las actividades requeridas para cada etapa,
 - Relaciona las actividades con los componentes del modelo especializado,
 - Define los responsables de ejecutar cada actividad,
 - Establece los recursos requeridos para la implementación,
 - Define las fechas programadas para la ejecución de las actividades,
 - Establece los mecanismos para documentar los avances de implementación,
 - Define los indicadores para medir el avance de implementación,
 - Establece los mecanismos para reportar retrasos, desviaciones o incumplimientos,
 - Define los criterios para determinar la conclusión de cada etapa de implementación, y
 - Contiene la aprobación o validación del plan por la instancia correspondiente.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS

NIVEL

Aplicación

1. Diseño y gestión de controles de cumplimiento:
- Tipos de controles: preventivos, detectivos y correctivos.
 - Diseño de controles.
 - Relación entre obligaciones, riesgos y controles.
 - Evidencias de cumplimiento.
 - Monitoreo y evaluación de controles.
 - Efectividad de los controles.

CONOCIMIENTOS

NIVEL

2. Gobernanza de ciberseguridad, seguridad de la información y protección de datos:

Aplicación

- Principios de gobernanza.
- Funciones y responsabilidades.
- Segregación de funciones.
- Coordinación entre cumplimiento, ciberseguridad, seguridad de la información, privacidad y protección de datos.
- Modelos de gobernanza y líneas de responsabilidad.

La persona es competente cuando demuestra la siguiente:

ACTITUD/HÁBITO/VALOR

1. Orden:

La manera en que propone mecanismos de coordinación y soluciones para integrar las funciones de cumplimiento, ciberseguridad, seguridad de la información, privacidad y protección de datos, considerando las características y necesidades de la organización.

GLOSARIO

1. Modelo especializado de cumplimiento: Estructura organizada de principios, componentes, responsabilidades, procesos y mecanismos establecidos para gestionar y supervisar el cumplimiento de las obligaciones relacionadas con ciberseguridad y protección de datos.

Referencia

Código

Título

4 de 7

E5933

Implementar los controles y mecanismos de cumplimiento en Ciberseguridad y Protección de Datos

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El plan de implementación y operación de controles de cumplimiento, elaborado:

- Contiene el nombre de la organización,
- Indica la fecha de elaboración,
- Contiene la relación de los controles que serán implementados y operados,
- Relaciona cada control con la obligación de cumplimiento correspondiente,
- Relaciona cada control con el riesgo de incumplimiento que atiende,
- Describe las actividades requeridas para la implementación y operación de cada control,
- Indica el responsable de la ejecución de cada control,
- Establece la periodicidad de ejecución de cada control,
- Define los recursos requeridos para la implementación y operación de los controles,

- Establece las fechas programadas para la ejecución de las actividades,
 - Define los mecanismos para documentar la ejecución de los controles,
 - Establece los mecanismos para reportar desviaciones en la implementación u operación de los controles, y
 - Contiene los criterios para determinar la implementación y operación de cada control.
2. El registro de evidencias de cumplimiento, elaborado:
- Contiene el nombre de la organización,
 - Indica la fecha de elaboración o actualización,
 - Contiene la relación de las obligaciones de cumplimiento atendidas,
 - Relaciona cada obligación con el control o mecanismo de cumplimiento correspondiente,
 - Describe las actividades realizadas para atender cada obligación,
 - Contiene las evidencias documentales, electrónicas o de otro tipo que sustentan el cumplimiento,
 - Indica la fecha de generación o recopilación de cada evidencia,
 - Señala el responsable de generar o proporcionar cada evidencia,
 - Indica el periodo de vigencia de la evidencia, cuando corresponda,
 - Contiene la ubicación o referencia para consultar cada evidencia,
 - Establece los mecanismos de control de acceso y conservación de las evidencias,
 - Indica el estado de disponibilidad y actualización de las evidencias, y
 - Contiene el registro de las evidencias faltantes o pendientes de integración, cuando existan.
3. El informe de seguimiento a la implementación y operación de controles, elaborado:
- Contiene el nombre de la organización,
 - Indica el periodo que comprende el seguimiento,
 - Indica la fecha de elaboración,
 - Contiene la relación de los controles sujetos a seguimiento,
 - Describe el avance de implementación de cada control,
 - Describe el estado de operación de cada control,
 - Contiene los resultados obtenidos durante el periodo de seguimiento,
 - Relaciona los resultados con las obligaciones de cumplimiento correspondientes,
 - Describe las desviaciones detectadas en la implementación u operación de los controles,
 - Indica las causas de las desviaciones, cuando hayan sido determinadas,
 - Señala los controles que no fueron ejecutados o que presentaron fallas, cuando corresponda,
 - Contiene las acciones requeridas para atender las desviaciones detectadas,
 - Indica los responsables y fechas compromiso para las acciones de atención, y
 - Contiene las evidencias que sustentan los resultados del seguimiento.
4. El informe de comunicación y reporte del cumplimiento especializado, elaborado:
- Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Indica el periodo que comprende el reporte,
 - Contiene los resultados relevantes del cumplimiento de las obligaciones aplicables,
 - Describe el estado de implementación y operación de los controles de cumplimiento,
 - Señala las obligaciones que presentan incumplimientos o desviaciones, cuando existan,
 - Describe los riesgos de cumplimiento que requieren atención prioritaria,
 - Contiene el estado de las acciones implementadas para atender incumplimientos y desviaciones,

- Indica los asuntos que requieren decisión o intervención de los niveles directivos correspondientes,
- Contiene los indicadores de cumplimiento establecidos para el periodo reportado,
- Presenta las conclusiones sobre el estado general del cumplimiento especializado,
- Contiene las recomendaciones de atención, cuando correspondan,
- Señala los destinatarios del reporte de acuerdo con sus responsabilidades y nivel de autoridad, y
- Contiene la evidencia de la comunicación o presentación del reporte a los destinatarios correspondientes.

La persona es competente cuando posee el siguiente:

CONOCIMIENTO

NIVEL

1. Implementación y operación de controles de cumplimiento:

Aplicación

- Implementación y operación de controles.
- Controles preventivos, detectivos y correctivos.
- Responsabilidades en la ejecución de controles.
- Periodicidad de controles.
- Seguimiento de controles.
- Desviaciones en la ejecución de controles.

La persona es competente cuando demuestra la siguiente:

ACTITUD/HÁBITO/VALOR

1. Responsabilidad:

La manera en que organiza y relaciona las obligaciones, controles, actividades, responsables y evidencias, manteniendo la trazabilidad de la información generada durante la implementación y operación del modelo especializado.

GLOSARIO

1. Monitoreo de cumplimiento:

Proceso sistemático de seguimiento mediante el cual se recopila y analiza información para conocer el estado de cumplimiento de las obligaciones y la operación de los controles establecidos.

2. Trazabilidad:

Capacidad para seguir y verificar el historial, origen, procesamiento, ubicación y relación de una información, actividad, evidencia o registro durante un periodo determinado.

Referencia

Código

Título

5 de 7

E5934

Gestionar incidentes y eventos con impacto en el cumplimiento normativo y la Protección de Datos

CRITERIOS DE EVALUACIÓN

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El análisis de impacto de cumplimiento derivado de un incidente o evento de ciberseguridad, elaborado:

- Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Contiene la fecha y hora de detección del incidente o evento, cuando se encuentren disponibles,
 - Describe las circunstancias conocidas relacionadas con el incidente o evento,
 - Describe los sistemas, procesos o activos de información involucrados,
 - Señala la información y los datos personales potencialmente afectados, cuando corresponda,
 - Describe el alcance conocido o estimado de la afectación,
 - Contiene las obligaciones legales y regulatorias relacionadas con el incidente o evento,
 - Determina la existencia de posibles incumplimientos normativos,
 - Describe las posibles consecuencias legales, regulatorias, operativas o reputacionales,
 - Establece el nivel de impacto del incidente desde la perspectiva del cumplimiento normativo,
 - Contiene los criterios utilizados para determinar el impacto de cumplimiento,
 - Indica las acciones de atención que requieren seguimiento desde la perspectiva de cumplimiento, y
 - Contiene las conclusiones del análisis realizado.
2. El informe de gestión y coordinación de la respuesta de cumplimiento ante el incidente o evento, elaborado:
- Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Describe el incidente o evento que originó la gestión de respuesta,
 - Contiene la cronología de las acciones realizadas desde su detección,
 - Describe las acciones ejecutadas por las áreas responsables de la atención técnica del incidente,
 - Indica la participación de las funciones de cumplimiento, ciberseguridad, seguridad de la información, privacidad y protección de datos, cuando corresponda,
 - Describe los mecanismos de coordinación utilizados entre las áreas involucradas,
 - Contiene las obligaciones de comunicación o notificación aplicables,
 - Indica las comunicaciones o notificaciones realizadas y su fecha, cuando corresponda,
 - Contiene las decisiones adoptadas respecto de las obligaciones de cumplimiento derivadas del incidente,
 - Describe las medidas implementadas para atender o mitigar las consecuencias de cumplimiento,
 - Contiene las evidencias documentales que sustentan las acciones realizadas,
 - Indica los asuntos pendientes de atención y los responsables correspondientes, y
 - Contiene las conclusiones sobre la gestión de la respuesta desde la perspectiva de cumplimiento.
3. El informe de cierre y acciones de mejora derivadas del incidente o evento, elaborado:
- Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Contiene la referencia del incidente/evento atendido,
 - Describe las causas determinadas del incidente o evento, cuando hayan sido establecidas,
 - Describe las consecuencias generadas desde la perspectiva del cumplimiento normativo,
 - Contiene los incumplimientos normativos confirmados, cuando existan,
 - Describe las acciones realizadas para atender los incumplimientos identificados,
 - Contiene las acciones correctivas y de mejora derivadas del incidente,
 - Relaciona cada acción con el incumplimiento, desviación o causa que le dio origen,

- Define los responsables de ejecutar las acciones establecidas,
- Establece las fechas compromiso para la ejecución de las acciones,
- Define los mecanismos para verificar la eficacia de las acciones implementadas,
- Contiene las evidencias que sustentan el cierre del incidente desde la perspectiva de cumplimiento,
- Describe las lecciones aprendidas relacionadas con el sistema especializado de cumplimiento, y
- Contiene las conclusiones sobre las mejoras requeridas para fortalecer el sistema.

La persona es competente cuando posee el siguiente:

CONOCIMIENTO

NIVEL

1. Gestión de incidentes de ciberseguridad y brechas de datos personales

Aplicación

- Conceptos de incidente de ciberseguridad.
- Brechas o violaciones de seguridad de datos personales.
- Ciclo de gestión de incidentes.
- Detección, análisis, contención y recuperación.
- Roles y responsabilidades durante la gestión de incidentes.

2. Obligaciones de cumplimiento derivadas de incidentes y brechas

Aplicación

- Obligaciones legales y regulatorias relacionadas con incidentes.
- Notificación y comunicación de incidentes.
- Plazos y requisitos de notificación, cuando sean aplicables.
- Consecuencias del incumplimiento de las obligaciones de comunicación.
- Protección y manejo de información durante la gestión del incidente.

La persona es competente cuando demuestra la siguiente:

ACTITUD/HÁBITO/VALOR

1. Responsabilidad: La manera en que protege y maneja la información relacionada con los incidentes, brechas y datos personales afectados, respetando los niveles de acceso y las restricciones establecidas por la organización.

GLOSARIO

1. Brecha de datos personales: Evento de seguridad que ocasiona, o puede ocasionar, la destrucción, pérdida, alteración, divulgación o acceso no autorizado a datos personales.

2. Incidente de ciberseguridad: de Evento que afecta o puede afectar la confidencialidad, integridad o disponibilidad de la información, los sistemas o los servicios tecnológicos de una organización.

Referencia	Código	Título
6 de 7	E5935	Evaluar el cumplimiento y la efectividad del sistema especializado de Ciberseguridad y Protección de Datos

CRITERIOS DE EVALUACIÓN

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

- El programa de evaluación del cumplimiento especializado, elaborado:
 - Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Establece el objetivo de la evaluación,
 - Define el alcance de la evaluación,
 - Contiene la relación de las obligaciones de cumplimiento que serán evaluadas,
 - Indica los procesos, áreas o funciones que serán evaluados,
 - Establece los criterios de evaluación aplicables,
 - Describe la metodología que será utilizada para realizar la evaluación,
 - Define las fuentes de información y evidencias que serán consideradas,
 - Establece las fechas programadas para realizar la evaluación,
 - Define los responsables de ejecutar las actividades de evaluación,
 - Establece los mecanismos para documentar los resultados obtenidos,
 - Contiene los criterios para determinar el nivel de cumplimiento, e
 - Indica los mecanismos para comunicar los resultados de la evaluación.
- El informe de evaluación del cumplimiento normativo y regulatorio, elaborado:
 - Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Indica el periodo que comprende la evaluación,
 - Contiene las obligaciones de cumplimiento evaluadas,
 - Describe los criterios utilizados para realizar la evaluación,
 - Describe la metodología aplicada,
 - Indica los procesos, áreas o funciones evaluados,
 - Contiene las evidencias analizadas durante la evaluación,
 - Describe el resultado obtenido para cada obligación evaluada,
 - Indica el nivel de cumplimiento determinado para cada obligación,
 - Describe las desviaciones o incumplimientos identificados,
 - Describe las causas de los incumplimientos, cuando hayan sido determinadas,
 - Describe las consecuencias o riesgos asociados a las desviaciones identificadas,
 - Establece la prioridad de atención de los incumplimientos y desviaciones, y
 - Contiene las conclusiones derivadas de la evaluación.
- El informe de evaluación de la efectividad de los controles de cumplimiento, elaborado:
 - Contiene el nombre de la organización,
 - Indica la fecha de elaboración,

- Indica el periodo que comprende la evaluación,
 - Contiene la relación de los controles evaluados,
 - Relaciona cada control evaluado con la obligación de cumplimiento correspondiente,
 - Relaciona cada control con el riesgo de incumplimiento que atiende,
 - Describe los criterios utilizados para evaluar la efectividad de los controles,
 - Contiene las evidencias revisadas para determinar la operación de los controles,
 - Describe los resultados obtenidos para cada control evaluado,
 - Indica los controles que operan conforme a los criterios establecidos,
 - Señala los controles que presentan desviaciones o deficiencias,
 - Describe las causas de las deficiencias identificadas, cuando hayan sido determinadas,
 - Determina el nivel de efectividad de los controles evaluados,
 - Describe las consecuencias de las deficiencias identificadas, y
 - Contiene las conclusiones sobre la efectividad general de los controles evaluados.
4. El informe de indicadores y desempeño del sistema especializado de cumplimiento, elaborado:
- Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Indica el periodo que comprende el análisis,
 - Contiene la relación de los indicadores de cumplimiento y desempeño utilizados,
 - Describe el objetivo de cada indicador,
 - Indica la fórmula o método utilizado para determinar cada indicador, cuando corresponda,
 - Señala la fuente de información utilizada para obtener los datos,
 - Contiene los resultados obtenidos para cada indicador,
 - Compara los resultados obtenidos con las metas/valores de referencia establecidos,
 - Describe el comportamiento de los indicadores durante el periodo evaluado,
 - Señala las tendencias relevantes observadas,
 - Describe las desviaciones respecto de las metas establecidas, cuando existan,
 - Contiene el análisis de las causas asociadas a las desviaciones, cuando hayan sido determinadas,
 - Describe las acciones requeridas para mejorar los resultados de los indicadores, y
 - Contiene las conclusiones sobre el desempeño del sistema especializado de cumplimiento.

La persona es competente cuando posee el siguiente:

CONOCIMIENTO

1. Evaluación de la efectividad de controles
 - Diseño y operación de controles.
 - Eficacia y efectividad.
 - Criterios de evaluación de controles.
 - Evidencias de operación.
 - Deficiencias y desviaciones de controles.
 - Relación entre controles, obligaciones y riesgos.

NIVEL

Aplicación

La persona es competente cuando demuestra la siguiente:

ACTITUD/HÁBITO/VALOR

1. Responsabilidad: La manera en que sustenta los resultados de la evaluación del cumplimiento y la efectividad de los controles en criterios

previamente establecidos y en evidencias verificables, evitando conclusiones basadas en opiniones o apreciaciones personales.

Referencia	Código	Título
7 de 7	E5936	Implementar acciones de mejora y fortalecimiento del sistema de cumplimiento especializado

CRITERIOS DE EVALUACIÓN

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El análisis de causas de los incumplimientos, desviaciones y oportunidades de mejora, elaborado:
 - Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Contiene la relación de los incumplimientos, desviaciones y oportunidades de mejora analizados,
 - Describe el origen de cada incumplimiento, desviación u oportunidad de mejora,
 - Contiene las evidencias que sustentan los problemas identificados,
 - Describe las causas inmediatas asociadas a cada incumplimiento/desviación,
 - Describe las causas raíz determinadas, cuando corresponda,
 - Señala los factores que contribuyeron a la ocurrencia de los incumplimientos o desviaciones,
 - Relaciona las causas determinadas con los procesos, controles o mecanismos de cumplimiento involucrados,
 - Describe las consecuencias reales o potenciales derivadas de las causas identificadas,
 - Establece la prioridad de atención de las causas determinadas, y
 - Contiene las conclusiones derivadas del análisis de causas.
2. El plan de acciones correctivas y de mejora del sistema especializado de cumplimiento, elaborado:
 - Contiene el nombre de la organización,
 - Indica la fecha de elaboración,
 - Contiene la relación de los incumplimientos, desviaciones y oportunidades de mejora que serán atendidos,
 - Relaciona cada acción con el incumplimiento, desviación u oportunidad de mejora correspondiente,
 - Describe las acciones correctivas y de mejora requeridas,
 - Relaciona las acciones establecidas con las causas determinadas,
 - Establece el resultado esperado para cada acción,
 - Define los responsables de ejecutar las acciones,
 - Establece las fechas compromiso para su ejecución,
 - Define los recursos requeridos para implementar las acciones,
 - Establece los indicadores o criterios para medir el avance de las acciones,
 - Define los mecanismos para documentar la ejecución de las acciones,
 - Establece los criterios para determinar la conclusión de cada acción, y
 - Contiene la aprobación o validación del plan por la instancia correspondiente.
3. El informe de seguimiento y verificación de la eficacia de las acciones correctivas y de mejora, elaborado:

- Contiene el nombre de la organización,
- Indica la fecha de elaboración,
- Contiene la relación de las acciones correctivas y de mejora sujetas a seguimiento,
- Describe el avance de cada acción respecto de las fechas compromiso establecidas,
- Indica las acciones concluidas y las acciones pendientes de ejecución,
- Contiene las evidencias que sustentan la ejecución de las acciones concluidas,
- Describe los resultados obtenidos después de implementar cada acción,
- Compara los resultados obtenidos con los resultados esperados,
- Determina la eficacia de las acciones implementadas,
- Describe las acciones que no resultaron eficaces, cuando corresponda,
- Señala las acciones adicionales requeridas para atender las causas que permanezcan sin resolver,
- Contiene las acciones cerradas y la fecha de cierre correspondiente,
- Contiene las conclusiones sobre la contribución de las acciones implementadas al fortalecimiento del sistema especializado de cumplimiento, y
- Contiene las recomendaciones de mejora derivadas del seguimiento, cuando correspondan.

La persona es competente cuando posee el siguiente:

CONOCIMIENTO

NIVEL

1. Gestión de acciones correctivas:

Aplicación

- No conformidad.
- Corrección.
- Acción correctiva.
- Análisis de causa raíz.
- Evaluación de la eficacia.
- Cierre de acciones correctivas.

La persona es competente cuando demuestra la siguiente:

ACTITUD/HÁBITO/VALOR

1. Orden:

La manera en que relaciona las causas de los incumplimientos y desviaciones con las acciones correctivas y de mejora establecidas, valorando los resultados obtenidos para determinar su eficacia.

GLOSARIO

1. Acción correctiva:

Acción implementada para eliminar la causa de una no conformidad o desviación identificada, con el propósito de prevenir su recurrencia y fortalecer el desempeño del Sistema de Gestión de Cumplimiento.

2. Mejora continua:

Actividad permanente orientada a incrementar la eficacia, eficiencia y capacidad del Sistema de Gestión de Cumplimiento para alcanzar sus objetivos, adaptarse a cambios en el contexto organizacional y responder a nuevas obligaciones normativas y riesgos.