CAIGG
CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO
Ministerio Secretaría General de la Presidencia

Guía de Auditoría, Seguridad de la Información y Ciberseguridad N°1

AUTOEVALUACIÓN PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

ÍNDICE

Nota

PRESENTACIÓN

En cumplimiento con las instrucciones del Presidente de la República, Gabriel Boric Font, sobre fortalecimiento de la Política de Auditoría Interna de Gobierno; el Consejo de Auditoría Interna General de Gobierno, entidad asesora en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza del Supremo Gobierno, presenta a la Red de Auditoría Gubernamental, la Guía para Auditoría de Seguridad de la Información y Ciberseguridad N° 1: Cuestionario de Autoevaluación para el Sistema de Gestión de Seguridad de la Información.

Esta guía es parte de una iniciativa del Consejo de Auditoría Interna General de Gobierno (CAIGG) que busca fortalecer la posición del sector público en materias de Seguridad de la Información y Ciberseguridad, dotando de instrumentos a los Auditores Internos y Servicios Públicos de instrumentos y herramientas que permitan desarrollar un levantamiento de información en base a las mejores prácticas y la legislación vigente.

Santiago, Marzo 2024.

Daniela Caldana Fulss
Auditora General de Gobierno

Capítulo 1

RESUMEN EJECUTIVO

El surgimiento de nueva normativa legal, (como es la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información), la actualización de los marcos referentes (como la nueva versión de la ISO 27001:2022, NIST CSF 2.0), y la confección de estándares sectoriales relevantes (como la RAN 20-10) generan un desafío importante sobre los auditores internos y equipos de seguridad en actualizar sus herramientas y metodologías para evaluar o incorporar los nuevos requisitos, según corresponda. Esta situación de dinamismo, en conjunto con un nivel profesionalque se encuentra en las primeras etapas de madurez en las competencias asociadas al monitoreo y evaluación del Sistema de Gestión de Seguridad de la Información vuelven más importante la necesidad de contar con instrumentos formales que apoyen al equipo auditor en su labor.

Este documento es parte de un proyecto del Consejo de Auditoría Interna General de Gobierno (CAIGG) que busca fortalecer la posición del sector público en materias de Seguridad de la Información y Ciberseguridad, dotando de instrumentos a los Auditores Internos y Servicios Públicos de instrumentos y herramientas que permitan desarrollar un levantamiento de información en base a las mejores prácticas y la legislación vigente. Este proyecto permitirá:

- ✓ **Aportar en la Capacidad de Alcanzar las Necesidades de Cumplimiento de los Requerimientos**
- ✓ **Apoyar en la Evaluación de los Riesgos Internos de Seguridad de Información**
- ✓ **Fortalecer la Posición de la Organización Frente a los Incidentes de Seguridad**
- ✓ **Proveer Recomendaciones a las Entidades que la Utilicen**
- ✓ **Fomentar la Comunicación con Diferentes Partes Interesadas, en Base a Datos**

Objetivo General

- Desarrollar un instrumento de autoevaluación mediante un cuestionario para determinar el nivel de cumplimiento y brechas de los controles base de seguridad de la información en instituciones públicas.

Objetivos Específicos

- Desarrollar un instrumento (cuestionario) para evaluar el nivel de cumplimiento de los requisitos obligatorios del SGSI (Norma ISO 27001:2022).
- Desarrollar un instrumento (cuestionario) para evaluar el nivel de cumplimiento para estándares de ciberseguridad (CIS Control, ISO 27002).
- Desarrollar un instrumento (cuestionario) para evaluar el nivel de cumplimiento para los nuevos requisitos de cumplimiento en materias de ciberseguridad (Ley Marco, RAN 20-10).

1.1 INTRODUCCIÓN

Este proyecto representa una iniciativa crucial para fortalecer la posición del sector público en temas de Seguridad de la Información y Ciberseguridad. Su objetivo principal es proporcionar a los auditores internos y equipo de Servicios Públicos una herramienta efectiva (cuestionario) para realizar un levantamiento de información basado en las mejores prácticas y la legislación vigente.

En este sentido, el proyecto aporta a varios objetivos clave:

01 **Facilita alcanzar las necesidades de cumplimiento normativo, un aspecto crítico dada la aparición de nueva legislación como la Ley Marco sobre Ciberseguridad e Infraestructura**

02 **Apoya la evaluación de los riesgos internos relacionados con la seguridad de la información, permitiendo a las organizaciones identificar y mitigar posibles vulnerabilidades de manera proactiva.**

03 **Mejora la posición de las organizaciones frente a incidentes de seguridad, proporcionando una base sólida para la respuesta y recuperación eficaz.**

04 **Permite reconocer el nivel cumplimiento para los diferentes requisitos de la norma, y cubrir las brechas en los resultados.**

El contexto actual, marcado por la actualización de marcos de referencia como la ISO 27001:2022 o NIST CSF 2.0, así como la creación de estándares sectoriales como la RAN 20-10, exige una actualización constante de herramientas y metodologías por parte de los equipos de auditoría y seguridad. Las competencias asociadas al monitoreo y evaluación del Sistema de Gestión de Seguridad de la Información están aún desarrollándose, por lo que la necesidad de contar con instrumentos formales y estructurados se vuelve aún más importante.

1.2 COMPOSICIÓN DEL CUESTIONARIO

El cuestionario está compuesto por una serie de grupos de preguntas, estructuradas en tres grupos principales de preguntas, cada uno abordando aspectos fundamentales para garantizar una gestión integral y eficaz de la seguridad de la información. Estos grupos son:

Requisitos del SGSI

a. *Este grupo se enfoca en evaluar el grado de implementación y eficacia de los elementos fundamentales del SGSI.*
b. *Incluye preguntas sobre la política de seguridad de la información, la asignación de responsabilidades, la gestión de activos, la evaluación de riesgos y la gestión de incidentes.*

Controles Generales de Ciberseguridad

a. *Este conjunto de preguntas examina las medidas de seguridad implementadas contra amenazas cibernéticas.*
b. *Incluye temas como la seguridad en redes, la protección contra malware, la seguridad en aplicaciones, el control de acceso y la gestión de vulnerabilidades.*
c. *También evalúa la seguridad física y ambiental, la gestión de operaciones de seguridad y la respuesta a incidentes de ciberseguridad.*

Cumplimiento Normativo

a. *Esta sección se centra en verificar el cumplimiento con la legislación vigente y las normativas específicas del sector público en materia de ciberseguridad.*
b. *Incluye preguntas relacionadas con la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, el DS 83 y RAN 20-10.*

El cuestionario (Anexo N° 1) se estructura en una tabla que contiene los siguientes campos:

1. ***ID**: Identificador del ítem.*
2. ***Control**: Requisito específico sobre el que se realiza la autoevaluación.*
3. ***Fuente**: Norma, buena práctica o fuente de información sobre el que proviene la guía de autoevaluación.*
4. ***Artículo**: Si se trata de un requisito normativo, esta columna corresponde al artículo.*
5. ***ISO 27001**: Vínculo con los requisitos de la norma ISO 27001 / 27002 según corresponda.*
6. ***Guía de Autoevaluación**: Expresión del control en forma de pregunta para autoevaluar.*
7. ***¿Dónde Revisar?**: Recomendación sobre dónde se debería consultar la fuente de información.*
8. ***Autoevaluación**: Permite completar el instrumento con la evaluación correspondiente, admite:*

- ***NL** - No Logrado*
- ***PL** - Parcialmente Logrado*
- ***L** - Logrado*
- ***CL** - Completamente Logrado*

Ejemplo

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
1	Garantizar los atributos esenciales del documento: Confidencialidad; Integridad; Factibilidad de autenticación, y Disponibilidad.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	6	Implementación de Controles Generales	Toda la familia 27002	¿Se han implementado medidas para asegurar la confidencialidad, la integridad, la autenticación y la disponibilidad de los documentos electrónicos?	Garantía de Atributos Esenciales de Documentos	

Tabla 1: Ejemplo de Contenidos.

Se sugiere un esquema de evaluación en la hoja N2 del cuestionario:

	No Logrado NL	Logrado Parcial PL	Logrado L	Completamente Logrado CL
Políticas	No hay evidencia de que la organización tiene implementada la política.	**Implementación:** Implementación inicial con algunos elementos de la política en funcionamiento. **Efectividad:** Evidencia limitada de impacto positivo; Resultados mixtos o inconsistentes. **Cumplimiento:** Cumplimiento parcial con estándares o regulaciones relevantes. Evalúe que la política cumple con el tema específico que es su propósito. Si no se especifica, quedará máximo como parcialmente logrado. **Sostenibilidad y Escalabilidad:** Planes iniciales para sostenibilidad y escalabilidad, pero con limitaciones. **Participación de Interesados:** Participación limitada de grupos de interés, feedback parcialmente integrado.	**Implementación:** Implementación completa de la mayoría de los componentes de la política. **Efectividad:** Evidencia clara de impacto positivo, aunque con margen de mejora. **Cumplimiento:** Cumplimiento general con todos los objetivos específicos, estándares y regulaciones relevantes. **Sostenibilidad y Escalabilidad:** Planes efectivos y en proceso para la sostenibilidad y escalabilidad. **Participación de Interesados:** Buena participación de grupos de interés y uso activo de sus aportes.	**Implementación:** Implementación integral y eficaz de todos los aspectos de la política. **Efectividad:** Impacto positivo significativo y sostenido; Supera las expectativas. **Cumplimiento:** Cumplimiento completo y sobresaliente con todos los estándares y regulaciones. **Sostenibilidad y Escalabilidad:** Excelente sostenibilidad y escalabilidad demostradas, con potencial para expandirse o replicarse. **Participación de Interesados:** Participación excepcional de todos los grupos de interés relevantes; integración completa de sus aportes.
Procesos, Procedimientos y Elementos Documentales	No hay evidencia de que la organización tiene implementado el proceso o procedimiento.	**Definición de Procesos:** Algunos procesos estan definidos y documentados, pero no de manera integral. **Eficiencia y Eficacia:** Mejora en la reducción de errores y retrasos, pero de manera aún inconsistente. **Automatización y Tecnología:** Uso limitado de herramientas tecnológicas para la optimización de procesos. **Medición y Mejora Continua:** Se han establecido métricas básicas, pero la mejora continua es esporádica.	**Definición de Procesos:** La mayoría de los procesos estan bien definidos, documentados y estandarizados. **Eficiencia y Eficacia:** Procesos eficientes y efectivos con menor incidencia de problemas. **Automatización y Tecnología:** Implementación efectiva de tecnologías para apoyar y mejorar los procesos. **Medición y Mejora Continua:** Métricas establecidas y utilizadas regularmente para la mejora continua de procesos.	**Definición de Procesos:** Procesos completamente definidos, documentados, estandarizados y alineados con los objetivos estratégicos. **Eficiencia y Eficacia:** Procesos altamente eficientes, efectivos y consistentemente libres de errores. **Automatización y Tecnología:** Automatización avanzada y uso innovador de tecnología para optimizar procesos. **Medición y Mejora Continua:** Cultura robusta de medición y mejora contínua, con ajustes proactivos y basados en datos.

Tabla 2: Ejemplo de Sugerencias para Autoevaluar.

Este esquema permite guiar al usuario de la herramienta sobre cuando uno de los elementos puede ser considerado logrado, completamente logrado, parcialmente logrado, o no logrado en virtud de las características que aquí se determinan.

1.3 MÉTODO DE APLICACIÓN

Esta herramienta está diseñada para ser un instrumento de uso directo, sin necesidad de configuraciones adicionales. Sin embargo, se sugiere realizar una definición meticulosa del alcance de la evaluación con el fin de que la actividad sea realizable en un periodo de tiempo razonable y utilizando la cantidad de recursos adecuados. De igual forma, la guía para el evaluador puede ser modificada con el fin de incorporar nuevos criterios o remover criterios a discreción dependiendo de cada caso particular. Estas decisiones deberían estar justificadas y aprobadas por quien sea el responsable de los resultados de la aplicación del instrumento.

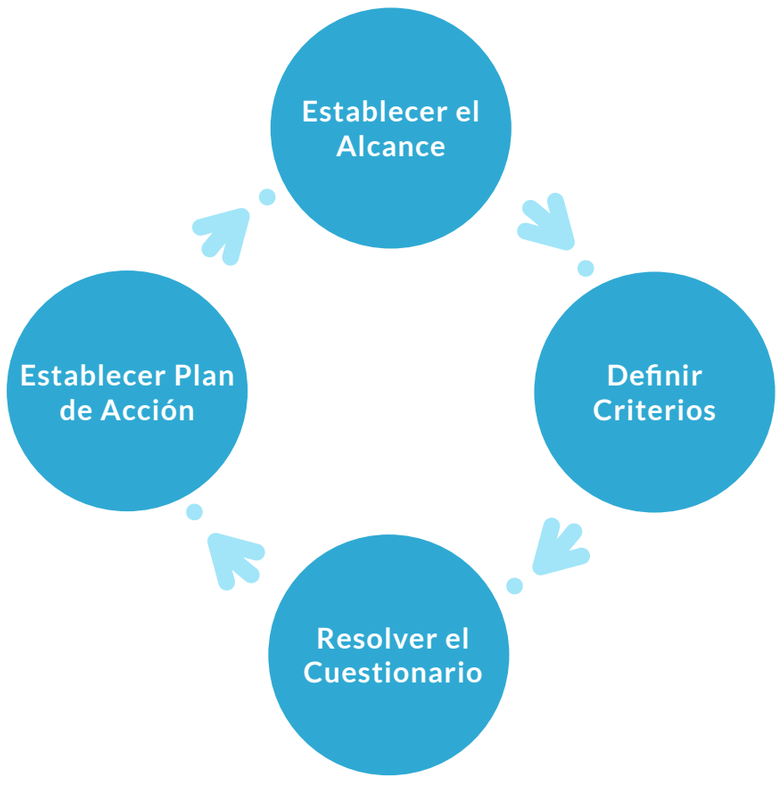

Ilustración 1: Método de evaluación.

Establecer el Alcance:

El instrumento de evaluación contempla actualmente las cláusulas de la norma ISO 27001:2022, la RAN 20-10, Ley Marco de Ciberseguridad y DS 83. La actualización de este instrumento considera la incorporación de nuevos requisitos de cumplimiento y mejores prácticas. Previa aplicación del instrumento se sugiere a cada organización que determine el alcance de aplicación del marco, para ello solo debe utilizar los filtros correspondientes o modificar la consulta SQL según requiera uno o más fuentes.

Definir Criterios de Evaluación:

En segundo lugar, se sugiere consensuar cuál será el criterio de evaluación para establecer la madurez / cumplimiento de cada uno de los criterios. El instrumento provee una guía sugerida (Anexo 2) que puede ser modificada añadiendo nuevos criterios o removiendo criterios, por ejemplo, en la siguiente tabla se ha añadido el criterio de evaluación “Comunicación”:

La modificación de los criterios podrá llevarse a cabo sí y solo sí el ejercicio de evaluación no se encuentra comprendido dentro de un marco de evaluación general, con criterios establecidos por un mandante; ya que la modificación de los criterios afectaría la comparabilidad y efectividad de la evaluación. De igual forma, no es conveniente modificar los criterios de evaluación de dos evaluaciones sobre la misma entidad en diferentes periodos de tiempo.

Criterios de Evaluación Original:

	No Logrado	***Logrado Parcial***	***Logrado***	***Completamente Logrado***
	NL	***PL***	***L***	***CL***
Políticas	*No hay evidencia de que la organización tiene implementada la política.*	***Implementación:*** *Implementación inicial con algunos elementos de la política en funcionamiento.* ***Efectividad:*** *Evidencia limitada de impacto positivo; Resultados mixtos o inconsistentes.* ***Cumplimiento:*** *Cumplimiento parcial con estándares o regulaciones relevantes. Evalúe que la política cumple con el tema específico que es su propósito. Si no se especifica, quedará máximo como parcialmente logrado.* ***Sostenibilidad y Escalabilidad:*** *Planes iniciales para sostenibilidad y escalabilidad, pero con limitaciones.* *Participac**ión de Interesados:** Participación limitada de grupos de interés, feedback parcialmente integrado.*	***Implementación:*** *Implementación completa de la mayoría de los componentes de la política.* ***Efectividad:*** *Evidencia clara de impacto positivo, aunque con margen de mejora.* ***Cumplimiento:*** *Cumplimiento general con todos los objetivos específicos, estándares y regulaciones relevantes.* ***Sostenibilidad y Escalabilidad:*** *Planes efectivos y en proceso para la sostenibilidad y escalabilidad.* ***Participación de Interesados:*** *Buena participación de grupos de interés y uso activo de sus aportes.*	***Implementación:*** *Implementación integral y eficaz de todos los aspectos de la política.* ***Efectividad:*** *Impacto positivo significativo y sostenido; Supera las expectativas.* ***Cumplimiento:*** *Cumplimiento completo y sobresaliente con todos los estándares y regulaciones.* ***Sostenibilidad y Escalabilidad:*** *Excelente sostenibilidad y escalabilidad demostradas, con potencial para expandirse o replicarse.* ***Participación de Interesados:*** *Participación excepcional de todos los grupos de interés relevantes; integración completa de sus aportes.*

Criterios de Evaluación Modificado:

	No Logrado	Logrado Parcial	Logrado	Completamente Logrado
	NL	PL	L	CL
Políticas	*No hay evidencia de que la organización tiene implementada la política.*	***Implementación:*** *Implementación inicial con algunos elementos de la política en funcionamiento.* ***Efectividad:*** *Evidencia limitada de impacto positivo; Resultados mixtos o inconsistentes.* ***Cumplimiento:*** *Cumplimiento parcial con estándares o regulaciones relevantes. Evalúe que la política cumple con el tema específico que es su propósito. Si no se especifica, quedará máximo como parcialmente logrado.* ***Sostenibilidad y Escalabilidad:*** *Planes iniciales para sostenibilidad y escalabilidad, pero con limitaciones.* ***Participación de Interesados:*** *Participación limitada de grupos de interés, feedback parcialmente integrado.* ***Comunicación:*** *La política se encuentra en un repositorio disponible a la organización.*	***Implementación:*** *Implementación completa de la mayoría de los componentes de la política.* ***Efectividad:*** *Evidencia clara de impacto positivo, aunque con margen de mejora.* ***Cumplimiento:*** *Cumplimiento general con todos los objetivos específicos, estándares y regulaciones relevantes.* ***Sostenibilidad y Escalabilidad:*** *Planes efectivos y en proceso para la sostenibilidad y escalabilidad.* ***Participación de Interesados:*** *Buena participación de grupos de interés y uso activo de sus aportes.* ***Comunicación:*** *Existen iniciativas para comunicar activamente la política.*	***Implementación:*** *Implementación integral y eficaz de todos los aspectos de la política.* ***Efectividad:*** *Impacto positivo significativo y sostenido; Supera las expectativas.* ***Cumplimiento:*** *Cumplimiento completo y sobresaliente con todos los estándares y regulaciones.* ***Sostenibilidad y Escalabilidad:*** *Excelente sostenibilidad y escalabilidad demostradas, con potencial para expandirse o replicarse.* ***Participación de Interesados:*** *Participación excepcional de todos los grupos de interés relevantes; integración completa de sus aportes.* ***Comunicación:*** *El conocimiento de la política se refuerza y se evalúa en programas de concientización.*

Tabla 4: Comparativa de Criterios de Evaluación

Resolver Cuestionario:

Durante la tercera etapa, el o los responsables deberán aplicar el cuestionario de autoevaluación sobre la organización a la que pertenecen. Se sugiere consultar con las áreas responsables respectivas a cada tema, con el fin de contar con la información más precisa posible. Este instrumento no obliga ni considera el almacenamiento de evidencia, pero es una buena práctica sugerida.

Establecer un Plan de Acción:

Considerando los resultados obtenidos y el objetivo de la evaluación, se debería establecer un plan de acción que permita elevar el nivel de madurez de aquellos criterios que se consideran críticos. Este plan de acción podría alimentar otras definiciones de nivel estratégico, tales como: Planificación Estratégica de Ciberseguridad, Plan Director de Ciberseguridad, Objetivos del SGSI, etc.

Seguimiento:

Será necesario realizar un monitoreo y seguimiento del estado de avance de las medidas formuladas en el Plan de Acción para elevar el nivel de madurez de aquellos criterios que se consideran críticos

Personalización del Instrumento

Toda modificación a la herramienta en términos de adición y actualización de criterios puede ser realizada directamente en el modelo de datos o las tablas de datos para ser adaptado a las necesidades y alcances particulares de cada organización.

Anexo 1

CUESTIONARIO

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
1	Garantizar los siguientes atributos esenciales del documento: Confidencialidad; Integridad; Factibilidad de autenticación, y Disponibilidad	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	6	Implementación de Controles Generales	Toda la familia 27002	¿Se han implementado medidas para asegurar la confidencialidad, la integridad, la autenticación y la disponibilidad de los documentos electrónicos?	Garantía de Atributos Esenciales de Documentos	
2	Concientizar, capacitar y educar a los usuarios para operar los sistemas informáticos de acuerdo a las exigencias establecidas.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	7	Concientización y Capacitación	7.3	¿Existen y se aplican políticas y procedimientos documentados para la capacitación en operación de sistemas?	Políticas y Procedimientos de Capacitación	
3	Monitorear el cumplimiento de los procedimientos establecidos y revisarlos de manera de evitar incidentes de seguridad.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	7	Evaluación y Monitoreo	9.2 A5.35	¿Se realiza un monitoreo continuo para asegurar el cumplimiento de los procedimientos establecidos y prevenir incidentes de seguridad?	Monitoreo de Cumplimiento de Procedimientos de Seguridad	
4	Desarrollar y documentar políticas de seguridad de uso, almacenamiento, acceso y distribución del documento electrónico y de los sistemas informáticos utilizados en su procesamiento.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	7	Procesos y Procedimientos	A5.1	¿Se han desarrollado y documentado políticas de seguridad para uso, almacenamiento, acceso y distribución de documentos electrónicos y sistemas?	Políticas de Seguridad Documentadas	
5	Diseñar y documentar los procesos y procedimientos para poner en práctica las políticas de seguridad.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	7	Procesos y Procedimientos	A5.37	¿Se han diseñado y documentado los procesos y procedimientos para implementar las políticas de seguridad?	Procesos de Seguridad Documentados	
6	Implementar los procesos y procedimientos señalados precedentemente.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	7	Procesos y Procedimientos	A5.1	¿Se han implementado los procesos y procedimientos de seguridad documentados?	Implementación de Procesos de Seguridad	
7	Definir y documentar los roles y responsabilidad de las entidades e individuos involucrados en cada una de las letras anteriores.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	7	Roles y Responsabilidades	A5.2	¿Se definen y documentan claramente los roles y responsabilidades relacionados con la seguridad?	Roles y Responsabilidades en Seguridad	
8	Garantizar condiciones mínimas de seguridad y confidencialidad en los documentos electrónicos que se generan, envían, reciben, procesan y almacenan entre los órganos de la Administración del Estado.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	10	Implementación de Controles Generales	A5.14 A5.33 A8.13	¿Se garantizan las condiciones mínimas de seguridad y confidencialidad en los documentos electrónicos manejados por la Administración del Estado?	Seguridad de Documentos en la Administración del Estado	
9	Facilitar la adopción de requerimientos de seguridad más estrictos por parte de aquellos organismos y en aquellos tópicos que se estimen necesarios.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	10	Implementación de Controles Generales	N/A	¿Se facilita y verifica la adopción de requerimientos de seguridad más estrictos en organismos y tópicos donde se consideren necesarios?	Adopción de Requerimientos de Seguridad Estrictos	
10	Facilitar el Nivel avanzado de seguridad para el documento electrónico, en aquellos organismos cuyo desarrollo institucional lo requiera.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	10	Otros	A5.14	¿Se facilita el nivel avanzado de seguridad para documentos electrónicos en organismos que lo requieran?	Seguridad Avanzada en Documentos Electrónicos	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
11	Deberá establecerse una política que fije las directrices generales que orienten la materia de seguridad dentro de cada institución, que refleje claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	11	Políticas	5.2 A5.1	¿Incluye la política de seguridad una definición clara, sus objetivos globales, alcance e importancia?	Contenido de la Política de Seguridad	
12	La política de seguridad deberá incluir una definición de seguridad del documento electrónico, sus objetivos globales, alcance e importancia.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	11	Políticas	5.2 A5.1	¿Se difunden los contenidos de la política de seguridad al interior de la organización?	Difusión de la Política de Seguridad	
13	La política de seguridad deberá incluir la difusión de sus contenidos al interior de la organización	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	11	Políticas	5.2 A5.1	¿Se difunde efectivamente la política de seguridad entre todos los miembros de la organización?	Difusión de la Política de Seguridad	
14	La política de seguridad deberá reevaluarse en forma periódica, a lo menos cada 3 años.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	11	Políticas	5.2 A5.1	¿Se reevalúa y actualiza la política de seguridad al menos cada 3 años?	Reevaluación de Política de Seguridad	
15	Deberá existir un encargado de seguridad, que actuará como asesor del Jefe de Servicio correspondiente en las materias relativas a seguridad de los documentos electrónicos.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	12	Roles y Responsabilidades	A5.2	¿Existe un encargado de seguridad designado que asesore en materias de seguridad de documentos electrónicos?	Encargado de Seguridad Designado	
16	El encargado de seguridad deberá tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de su organización y el control de su implementación, y velar por su correcta aplicación.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	12	Roles y Responsabilidades	A5.2	¿El encargado de seguridad desarrolla y controla la implementación de políticas de seguridad al interior de la organización?	Desarrollo e Implementación de Políticas de Seguridad	
17	El encargado de seguridad deberá coordinar la respuesta a incidentes computacionales	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	12	Roles y Responsabilidades	A5.24	¿El encargado de seguridad coordina efectivamente la respuesta a incidentes computacionales?	Coordinación en Respuesta a Incidentes	
18	El encargado de seguridad deberá establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	12	Roles y Responsabilidades	A5.6	¿El encargado de seguridad establece puntos de enlace con otros organismos y especialistas para mantenerse informado sobre tendencias y métodos de seguridad?	Enlaces con Organismos y Especialistas en Seguridad	
19	Los documentos electrónicos y sistemas informáticos deberán clasificarse y etiquetarse para indicar la necesidad, prioridad y grado de protección.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	13	Otros	A5.13	¿Se clasifican y etiquetan los documentos electrónicos y sistemas para indicar la necesidad, prioridad y grado de protección requeridos?	Clasificación y Etiquetado de Documentos y Sistemas	
20	Todo documento electrónico deberá ser asignado, explícita o implícitamente, a un responsable.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	14	Roles y Responsabilidades	A5.9	¿Se asigna la responsabilidad de cada documento electrónico a un responsable específico?	Asignación de Responsabilidad en Documentos Electrónicos	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
21	Los equipos deberán protegerse físicamente de las amenazas de riesgos del ambiente externo, pérdida o daño, incluyendo las instalaciones de apoyo tales como el suministro eléctrico y la infraestructura de cables.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	17	Implementación de Controles Generales	A7.8	¿Están los equipos físicamente protegidos contra riesgos del ambiente externo, pérdida o daño, incluyendo las instalaciones de soporte?	Protección Física de Equipos e Instalaciones	
22	Los documentos electrónicos de la organización clasificados como reservados o secretos deberán almacenarse en áreas seguras, protegidos por un perímetro de seguridad definido, con barreras.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	19	Implementación de Controles Generales	A7.1 A7.2 A7.5	¿Se almacenan los documentos electrónicos clasificados como reservados o secretos en áreas seguras, con barreras y controles de entrada adecuados?	Almacenamiento Seguro de Documentos Sensibles	
23	Los documentos electrónicos de la organización clasificados como reservados o secretos deberán disponerse de manera que se minimicen las posibilidades de percances y descuidos durante su empleo.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	19	Implementación de Controles Generales	Toda la familia 27002	¿Se han implementado medidas para minimizar percances y descuidos durante el uso de documentos electrónicos reservados o secretos?	Manejo Seguro de Documentos Sensibles	
24	Impartir instrucciones para la seguridad de los documentos electrónicos sobre el uso de sistemas informáticos, con énfasis en prohibición de instalación de software no autorizado, documentos y archivos guardados en el computador.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	20	Procesos y Procedimientos	A5.36	¿Se imparten instrucciones claras sobre el uso seguro de sistemas informáticos, incluyendo la prohibición de software no autorizado?	Instrucciones de Uso de Sistemas	
25	Impartir instrucciones para la seguridad de los documentos electrónicos y sistemas informáticos sobre el uso de la red interna, uso de Internet, uso del correo electrónico, acceso a servicios públicos, recursos compartidos, mensajería y comunicación remota, entre otros.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	20	Procesos y Procedimientos	A5.1	¿Se imparten instrucciones detalladas sobre el uso seguro de la red interna, Internet, correo electrónico y otros servicios de comunicación?	Instrucciones de Uso de la Red	
26	Impartir instrucciones para la seguridad de los documentos electrónicos y los sistemas informáticos sobre generación, transmisión, recepción, procesamiento y almacenamiento de documentos electrónicos.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	20	Procesos y Procedimientos	A5.14	¿Se imparten instrucciones sobre el manejo seguro de documentos electrónicos en todos sus procesos?	Manejo Seguro de Documentos Electrónicos	
27	Impartir instrucciones para la seguridad de los documentos electrónicos y los sistemas informáticos sobre procedimientos para reportar incidentes de seguridad.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	20	Procesos y Procedimientos	A5.24	¿Existen instrucciones claras y procedimientos para reportar incidentes de seguridad?	Reporte de Incidentes de Seguridad	
28	Deberán explicitarse y difundirse los contactos de apoyo ante dificultades técnicas u operacionales inesperadas de sistemas informáticos.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	22	Otros	A5.5	¿Se explicitan y difunden los contactos de apoyo ante dificultades técnicas o operacionales inesperadas?	Difusión de Contactos de Apoyo Técnico	
29	Deberán explicitarse y difundirse las exigencias relativas al cumplimiento con las licencias de software y la prohibición del uso de software no autorizado.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	22	Otros	A5.36	¿Se explicitan y difunden las exigencias relativas al cumplimiento de licencias de software y la prohibición del software no autorizado?	Cumplimiento de Licencias de Software	
30	Deberán explicitarse y difundirse las buenas prácticas para protegerse de los riesgos asociados a la obtención de archivos y software a través de las redes de telecomunicaciones, y otros medios, indicando qué medidas de protección se deberán aplicar.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	22	Otros	A5.3	¿Se difunden las buenas prácticas y medidas de protección contra riesgos asociados a la obtención de archivos y software?	Buenas Prácticas en Obtención de Archivos y Software	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
31	Incorpora mecanismos periódicos de auditorías de la integridad de los registros de datos almacenados en documentos electrónicos	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	23	Evaluación y Monitoreo	A5.33	¿Se llevan a cabo auditorías periódicas para verificar la integridad de los registros de datos almacenados en documentos electrónicos?	Auditorías de Integridad de Registros Electrónicos Personales	
32	Deberán aplicarse políticas de segregación de funciones	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	23	Políticas	A5.18 A5.1	¿Se aplican políticas de segregación de funciones para evitar conflictos de interés y riesgos de seguridad?	Segregación de Funciones	
33	Deberán documentarse los procedimientos de operación de sistemas informáticos.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	23	Procesos y Procedimientos	A5.37	¿Se documentan adecuadamente los procedimientos de operación de los sistemas informáticos?	Documentación de Procedimientos de Operación Electrónicos	
34	La periodicidad con que se realizarán los respaldos de los computadores personales de la institución, asignados a usuarios, deberá explicitarse y no podrá ser menor a 1 respaldo anual.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	24	Implementación de Controles Generales	A8.13	¿Se especifica y cumple con la periodicidad de al menos 1 respaldo anual para los computadores personales asignados a usuarios?	Periodicidad de Respaldos de Computadores	
35	La periodicidad con que se realizarán los respaldos de sistemas informáticos y equipos no contemplados en el punto anterior, utilizados en el procesamiento o almacenamiento de documentos electrónicos, deberá explicitarse y no podrá ser menor a 1 respaldo mensual.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	24	Implementación de Controles Generales	A5.13 A5.15 A5.14	¿Se realiza y especifica la periodicidad de al menos 1 respaldo mensual para sistemas informáticos y equipos relacionados?	Periodicidad de Respaldos de Sistemas Informáticos	
36	Deberá garantizarse la disponibilidad de infraestructura adecuada de respaldo, para asegurar que estos estén disponibles incluso después de un desastre o la falla de un dispositivo.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	24	Implementación de Controles Generales	A8.13 A8.14	¿Se garantiza la disponibilidad de una infraestructura adecuada de respaldo para asegurar la disponibilidad de los mismos, incluso tras desastres o fallas?	Infraestructura de Respaldos y Planes de	
37	Las configuraciones de respaldo para sistemas individuales deberán ser probadas con regularidad, al menos cada 2 años, asegurando que satisfacen los requisitos estipulados en los planes de continuidad institucionales.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	24	Implementación de Controles Generales	A8.13 A5.30	¿Se prueban regularmente las configuraciones de respaldo, al menos cada 2 años, para asegurar su eficacia según los planes de continuidad institucionales?	Pruebas de Configuraciones de Respaldos	
38	En ámbitos críticos para la institución, se deberán almacenar al menos tres generaciones o ciclos de información de respaldo.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	24	Implementación de Controles Generales	A8.13 A5.30	¿Se almacenan al menos tres generaciones o ciclos de información de respaldo en áreas críticas de la institución?	Gestión de Información de Respaldos	
39	Los respaldos deberán cumplir con un nivel apropiado de protección física de los medios, consistente con las prácticas aplicadas en el sitio principal.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	24	Implementación de Controles Generales	A8.13 A5.30 A7.1 A7.2	¿Cumplen los respaldos con un nivel apropiado de protección física, consistente con las prácticas en el sitio principal?	Protección Física de Medios de Respaldo.	
40	Los controles asociados a los dispositivos del sitio de producción deberán extenderse para abarcar el sitio de respaldo.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	24	Implementación de Controles Generales	A7.1 A7.2 A7.3 A7.5	¿Se extienden los controles asociados a los dispositivos del sitio de producción para abarcar también el sitio de respaldo?	Controles de Dispositivos en Sitio de Respaldo	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
41	Deberán consignarse plazos de retención de los respaldos de la institución, así como cualquier necesidad de realización de respaldos que estén permanentemente guardados.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	24	Implementación de Controles Generales	A8.13	¿Están claramente definidos y consignados los plazos de retención de los respaldos y las necesidades de respaldos permanentes?	Políticas de Retención de Respaldos	
42	Deberán utilizarse los medios y las condiciones físicas de almacenamiento que garanticen una vida útil concordante con los plazos de retención definidos.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	24	Implementación de Controles Generales	A8.13	¿Se utilizan los medios y las condiciones de almacenamiento adecuados para garantizar una vida útil de respaldos acorde con los plazos de retención?	Condiciones de Almacenamiento	
43	Deberá almacenarse un mínimo de información de respaldo, junto con registros completos y exactos de las copias de respaldo y procedimientos de restablecimiento. Esta instalación remota, deberá estar emplazada a una distancia tal que escape de cualquier daño por un desastre en el sitio principal.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	24	Otros	A8.13	¿Se almacena un nivel mínimo de información de respaldo en ubicaciones remotas con registros y procedimientos adecuados?	Almacenamiento Remoto de Respaldos	
44	Impartir instrucciones respecto al uso seguro del correo electrónico que incluya una advertencia sobre la vulnerabilidad del correo electrónico a modificaciones o accesos no autorizados.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	25	Concientización y Capacitación	7.3	¿Se proporciona material de instrucción adecuado que aborde la seguridad del correo electrónico y sus vulnerabilidades?	Materiales de Instrucción sobre Seguridad del Correo Electrónico Personal	
45	Impartir instrucciones respecto al uso seguro del correo electrónico que incluya una advertencia sobre los peligros asociados a la apertura de archivos adjuntos y/o a la ejecución de programas que se reciban vía correo electrónico.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	25	Concientización y Capacitación	7.3	¿Se han establecido instrucciones claras y accesibles sobre los riesgos asociados con archivos adjuntos y ejecución de programas en el correo electrónico?	Documentación de Instrucciones de Seguridad	
46	Impartir instrucciones respecto al uso seguro del correo electrónico que incluya la responsabilidad de no divulgar contraseñas de acceso al correo electrónico.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	25	Concientización y Capacitación	7.3	¿Existen políticas y procedimientos que prohíban la divulgación de contraseñas de correo electrónico y se comunican eficazmente a los usuarios?	Políticas de No Divulgación de Contraseñas	
47	Impartir instrucciones respecto al uso seguro del correo electrónico que incluya advertencia sobre la inconveniencia de almacenar contraseñas de acceso al correo electrónico en el mismo computador desde el cual se accede a este correo.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	25	Concientización y Capacitación	7.3	¿Hay guías o manuales disponibles que desaconsejen el almacenamiento de contraseñas de correo electrónico en los computadores de acceso?	Guías de Manejo Seguro de Contraseñas	
48	Impartir instrucciones respecto al uso seguro del correo electrónico que incluya indicaciones sobre la elección de contraseñas seguras de acceso al correo electrónico.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	25	Concientización y Capacitación	7.3	¿Se imparten programas de formación efectivos que enseñen cómo elegir contraseñas seguras para el correo electrónico?	Programas de Formación sobre Contraseñas Seguras	
49	Impartir instrucciones respecto al uso seguro del correo electrónico que incluya una recomendación sobre la conveniencia de que los usuarios tengan cuentas de correo electrónico distintas para efectos de su uso personal.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	25	Concientización y Capacitación	7.3	¿Las políticas de la organización incluyen recomendaciones sobre mantener cuentas de correo electrónico separadas para uso personal y profesional?	Políticas de Uso de Cuentas de Correo Electrónico	
50	Impartir instrucciones respecto al uso seguro del correo electrónico que incluya un instructivo de cuándo no usar el correo electrónico.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	25	Concientización y Capacitación	7.3	¿Se han proporcionado directrices claras sobre las situaciones en las que se debe evitar el uso del correo electrónico?	Directrices de Uso Apropiado del Correo Electrónico	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
51	Impartir instrucciones respecto al uso seguro del correo electrónico que incluya una prevención sobre la necesidad de comprobar el origen, despacho, entrega y aceptación mediante firma electrónica.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	25	Concientización y Capacitación	7.3	¿Se ofrecen instrucciones detalladas sobre cómo comprobar el origen, despacho, entrega y uso de firma electrónica en los correos electrónicos?	Instrucciones de Seguridad y Verificación del Correo Electrónico	
52	Impartir instrucciones de uso seguro del correo electrónico, que incluya con precisión las responsabilidades que corresponden a los usuarios en caso de comprometer a la institución, por ejemplo, con el envío de correos electrónicos difamatorios, de acoso, compras no autorizadas, etc.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	25	Concientización y Capacitación	7.3	¿Se han documentado y comunicado claramente las políticas que explican las responsabilidades de los usuarios en caso de uso indebido del correo electrónico, por ejemplo, con el envío de correos electrónicos difamatorios, uso para hostigamiento o acoso, compras no autorizadas, etc?	Políticas de Responsabilidad por Uso Indebido del Correo Electrónico	
53	Evitar el uso de cuentas de correo grupales	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	26	Concientización y Capacitación	A 5.16 A 5.15 A 8.3	¿Se ha implementado una política clara que prohíba el uso de cuentas de correo grupales y se verifica su cumplimiento?	Políticas sobre Uso de Cuentas de Correo Electrónico	
54	Disponer controles adicionales para la verificación de mensajes que no se pueden autenticar.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	26	Implementación de Controles Generales	N/A	¿Se disponen controles adicionales para la verificación de mensajes que no pueden ser autenticados?	Verificación de Mensajes no Autenticables	
55	Verificar que todos los equipos informáticos y medios digitales que sean usados en el almacenamiento y/o procesamiento de documentos electrónicos, de ser posible, sean reformateados previo a ser dados de baja.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	26	Implementación de Controles Generales	A8.10	¿Se verifica que todos los equipos y medios digitales sean reformateados antes de ser dados de baja?	Procedimientos de Baja de Equipos	
56	Instalar un antivirus que proteja frente a la posibilidad de obtener vía correo electrónico software malicioso.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	26	Implementación de Controles Generales	A8.7	¿Se instala y mantiene un antivirus efectivo para proteger frente a software malicioso obtenido vía correo electrónico?	Antivirus para Correo Electrónico	
57	Proveer mecanismos que mediante el uso de técnicas de cifrado, permitan proteger la confidencialidad e integridad de los documentos electrónicos.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	26	Implementación de Controles Generales	A8.5	¿Se utilizan técnicas de cifrado para proteger la confidencialidad e integridad de los documentos electrónicos?	Cifrado de Documentos Electrónicos	
58	La obligación de no registrar los identificadores en papel	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	28	Implementación de Controles Generales	N/A	¿Se cumple la obligación de no registrar los identificadores en papel?	Políticas de Manejo de Identificadores	
59	La prohibición de almacenar identificadores en un computador de manera desprotegida.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	28	Implementación de Controles Generales	A8.2	¿Se prohíbe y verifica el cumplimiento de no almacenar identificadores en un computador de manera desprotegida?	Almacenamiento Seguro de Identificadores	
60	El deber de no compartir los identificadores de usuarios individuales.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	28	Implementación de Controles Generales	A5.15	¿Se cumple y verifica el deber de no compartir los identificadores de usuarios individuales?	Políticas de Uso de Identificadores	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
61	El mandato de no i ncluir el identificador en cualquier proceso de inicio de sesión automatizado, por ejemplo, almacenado	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	28	Implementación de Controles Generales	A8.5	¿Se cumple el mandato de no incluir el identificador en procesos de inicio de sesión automatizados?	Procedimientos de Inicio de Sesión	
62	La indicación de cambiar los identificadores cuando hayan indicios de un	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	28	Implementación de Controles Generales	A5.17	¿Se indica y verifica el cambio de identificadores cuando hay indicios de compromiso del identificador o del sistema?	Gestión de Cambio de Identificadores	
63	Elegir identificadores de longitud mínima de ocho caracteres; sean fáciles de recordar; contengan letras, mayúsculas, dígitos, y puntuación; que no estén basados en cosas de fácil deducción a partir de los datos de la persona: Nombres,cédula de identidad, telefónos; Estén libres de caracteres idénticos consecutivos o grupos completamente numéricos o alfabéticos.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	28	Implementación de Controles Generales	A5.17	¿Se siguen las recomendaciones para elegir identificadores que cumplan con criterios específicos de seguridad y complejidad?	Criterios de]Selección de Identificadores	
64	La indicación de cambiar los identificadores a intervalos regulares. Las contraseñas de accesos privilegiados se deberán cambiar más frecuentemente que los identificadores normales.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	28	Implementación de Controles Generales	A5.17	¿Se cambian los identificadores a intervalos regulares, siendo más frecuentes en los casos de accesos privilegiados?	Políticas de Cambio de Contraseñas	
65	Normas para evitar el reciclaje de identificadores viejos	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	28	Implementación de Controles Generales	A5.17	¿Se cumplen las normas establecidas para evitar el reciclaje de identificadores viejos?	Políticas de Reciclaje de Identificadores	
66	La indicación de cambiar el identificador temporal al iniciar la primera sesión.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	28	Implementación de Controles Generales	A5.16	¿Se cambia el identificador temporal al iniciar la primera sesión como se indica?	Gestión de Identificadores Temporales	
67	Se deberá entregar a los usuarios identificadores temporales de manera segura. Específicamente, se deberá evitar el uso de terceras partes o mensajes de correo electrónico no protegido para comunicar el identificador.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	29	Implementación de Controles Generales	A5.17	¿Se garantiza la entrega segura de identificadores temporales, evitando el uso de correo electrónico no protegido o terceras partes?	Distribución Segura de Identificadores Temporales	
68	Cerrar las sesiones activas en el computador cuando se finaliza la labor, a menos que éstas se puedan asegurar mediante un sistema apropiado de control de acceso, por ejemplo, con un protector de pantalla con una contraseña protegida.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	31	Implementación de Controles Generales	A8.1	¿Se cierran las sesiones activas en el computador al finalizar la labor, a menos que estas estén aseguradas por un sistema de control de acceso?	Cierre de Sesiones Activas	
69	Cerrar las sesiones de los computadores principales cuando la sesión finaliza, lo que no significa, necesariamente, apagar el terminal o los equipos.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	31	Implementación de Controles Generales	A8.1	¿Se asegura el cierre de sesiones en los computadores principales al finalizar, sin necesariamente apagar los equipos?	Gestión de Sesiones en Computadores Principales	
70	Asegurar los terminales o equipos frente al uso no autorizado, mediante una contraseña de traba o de un control equivalente, por ejemplo, una contraseña de acceso cuando no se use.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	31	Implementación de Controles Generales	A8.1	¿Se protegen los terminales o equipos frente al uso no autorizado, mediante contraseñas de traba o controles equivalentes?	Protección de Terminales contra Uso No Autorizado	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
71	Se deberá controlar el acceso a los servicios de red internos y externos mediante el uso de identificadores o certificados digitales.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	32	Implementación de Controles Generales	A5.1	¿Se controla efectivamente el acceso a servicios de red internos y externos usando identificadores o certificados digitales?	Control de Acceso a Servicios de Red	
72	Restringir la instalación de equipamiento personal que dificulte el control de acceso a documentos electrónicos y sistemas informáticos, de manera acorde a las políticas de seguridad de la institución.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	32	Implementación de Controles Generales	A8.1	¿Se restringe la instalación de equipamiento personal según las políticas de seguridad de la institución para controlar el acceso a documentos y sistemas?	Políticas de Instalación de Equipamiento Personal	
73	Mantener un catastro del equipamiento que permita la reproducción, distribución o transmisión masiva de información, y de las personas con privilegios de acceso a ellos.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	32	Implementación de Controles Generales	A5.9	¿Se mantiene un registro actualizado del equipamiento que permite la reproducción y transmisión masiva de información y de las personas con acceso a ellos?	Registro de Equipamiento y Acceso	
74	Impartir instrucciones sobre las redes y servicios de red a las que el acceso está permitido.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	33	Concientización y Capacitación	7.3	¿Existen instrucciones detalladas sobre las redes y servicios de red a los cuales los usuarios están autorizados a acceder?	Instrucciones sobre Acceso a Redes y Servicios de Red.	
75	Impartir instrucciones sobre los procedimientos de autorización para determinar quién tiene permitido acceder a las distintas redes y servicios de red.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	33	Concientización y Capacitación	7.3	¿Se han establecido y documentado procedimientos claros para determinar autorizaciones de acceso a distintas redes y servicios de red?	Procedimientos de Autorización de Acceso	
76	Impartir instrucciones sobre los controles de gestión y procedimientos para proteger el acceso a las conexiones de la red y servicios de red.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	33	Concientización y Capacitación	7.3	¿Se han implementado controles de gestión efectivos y procedimientos para asegurar la protección del acceso a conexiones de red y servicios?	Controles de Gestión y Protección de Acceso	
77	El encargado de seguridad deberá formular un plan de contingencia para asegurar la continuidad de operaciones críticas para la institución.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	35	Procesos y Procedimientos	A5.30	¿El encargado de seguridad ha formulado un plan de contingencia para asegurar la continuidad de operaciones críticas?	Plan de Contingencia de Seguridad	
78	Los controles físicos de entrada en el perímetro de seguridad deberán utilizar el carné de identidad como identificación válida para chilenos y el pasaporte en el caso de los extranjeros.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Implementación de Controles Generales	A7.2	¿Se utilizan controles físicos de entrada en el perímetro de seguridad que requieran carné de identidad o pasaporte como identificación válida?	Controles de Acceso Físico	
79	En Seguridad Organizacional se aplicará la sección 4.1 del capítulo 4 de la norma NCh2777, con excepción de sus puntos 4.1.5 y 4.1.7 que se adoptarán como recomendaciones, y las secciones 4.2 y 4.3 de dicho capítulo.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Otros	A5.1	¿Se aplica la sección 4.1 del capítulo 4 de la norma NCh2777 en seguridad organizacional, con las excepciones indicadas?	-	
80	En Clasificación y control de bienes se aplicará la sección 5.1 del capítulo 5 de la norma NCh2777, en lo referido a bienes relacionados con el Documento Electrónico. Asimismo, se aplicará el punto 5.2.1 de la sección 5.2	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Otros	N/A	¿Se aplica la sección 5.1 del capítulo 5 de la norma NCh2777 para bienes relacionados con el documento electrónico?	-	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
81	El punto 5.1.2 de dicha sección se aplicará con las siguientes adecuaciones: Los procedimientos de etiquetado y manipulación de la información se entienden referidos al Documento Electrónico.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Otros	A5.13	¿Se aplican las adecuaciones indicadas en el punto 5.1.2 de la norma NCh2777 en cuanto al etiquetado y manipulación de información?	-	
82	El punto 5.1.2 de dicha sección se aplicará con las siguientes adecuaciones: Se excluyen las normas contenidas en las letras (c) y (d).	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Otros	N/A	¿Se aplican las secciones 6.1 y 6.3 del capítulo 6 de la norma NCh2777 en seguridad del personal?	-	
83	En Seguridad del Personal se aplicarán las secciones 6.1 y 6.3 del capítulo 6 de la norma NCh2777. La sección 6.2 se adoptará como recomendación.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Otros	N/A	¿Se aplican las secciones 7.1 y 7.2 del capítulo 7 de la norma NCh2777 para repositorios de documentos electrónicos?	-	
84	Se aplicarán las secciones 7.1 y 7.2 del capítulo 7 de la norma NCh2777, para repositorios de documentos electrónicos, con adecuaciones en esta norma.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Otros	N/A	¿Se asegura un suministro eléctrico adecuado para equipos computacionales que almacenan documentos electrónicos y sistemas?	Suministro Eléctrico para Equipos de Almacenamiento	
85	Los equipos de computación en los que se almacenen documentos electrónicos y los sistemas informáticos que los procesen, tengan un adecuado suministro de energía eléctrica, incluyendo no sólo el flujo de energía, sino también la tierra eléctrica de las instalaciones.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Otros	N/A	¿Se mantiene un registro histórico de privilegios asignados con un período de conservación adecuado?	Registro de Privilegios Asignados	
86	Los registros de privilegios asignados, referenciados en la sección 9.2.2 de la norma NCh2777, deberán tener un carácter histórico, es decir, no sólo se deben registrar los privilegios en aplicación. El período de conservación de estos registros será al menos el que las leyes vigentes indiquen.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Otros	N/A	¿Se aplican las normas de la sección 10.3 del capítulo10 de la norma NCh2777 en desarrollo y mantenimiento de sistemas?	-	
87	En mantenimiento y desarrollo de sistemas, se aplicarán únicamente las normas de la sección 10.3 del capítulo 10 de la norma NCh2777, adecuando: En las secciones referidas a firma electrónica, se adoptará lo establecido por la ley 19.799, sobre documentos electrónicos, firma electrónica y sus servicios de certificación.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Otros	N/A	¿Se aplican las estipulaciones del capítulo 11 de la norma NCh2777 en gestión de la continuidad del negocio?	-	
88	En Gestión de la continuidad del negocio se aplicarán las estipulaciones del capítulo 11 de la norma NCh2777, en su integridad.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Otros	N/A	¿Se ha establecido una política que fije las directrices generales de seguridad dentro de cada institución?	Política General de Seguridad	
89	Las políticas deberán contener indicaciones respecto de los sistemas informáticos, con énfasis en el procedimiento de autorización, instalación o modificación de software y archivos de configuración de los sistemas.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Políticas	A8.1 A5.1	¿Contienen las políticas indicaciones específicas sobre autorización de instalación o modificación de software y archivos de configuración?	Políticas de Sistemas Ínformáticos	
90	Las políticas deberán contener indicaciones de uso de la red	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Políticas	A8.22 A5.1	¿Incluyen las políticas indicaciones claras sobre el uso seguro y eficiente de la red?	Políticas de Uso de la Red	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
91	Las políticas deberán contener procedimientos de respuesta a incidentes de seguridad	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Políticas	A5.24 A5.1	¿Contienen las políticas procedimientos específicos de respuesta a incidentes de seguridad?	Procedimientos de Respuesta a Incidentes	
92	Las políticas deberán contener procedimientos de delegación de autoridad para ejecutar acciones de emergencia en los sistemas y los procedimientos correspondientes.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Políticas	A5.1	¿Están definidos los procedimientos de delegación de autoridad para ejecutar acciones de emergencia en sistemas?	Delegación de Autoridad en Emergencias	
93	Las estipulaciones de la sección 9.4 de la norma NCh2777 deberán formalizarse en una política de uso correspondiente, de acuerdo a lo expresado en la sección “Política de Seguridad”.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Políticas	5.2 A5.1	¿Se ha formalizado una política de uso de acuerdo a la sección 9.4 de la norma NCh2777?	Política de Uso según NCh2777	
94	Todo ingreso de visitas al perímetro de seguridad deberá ser autorizado por escrito, quedando constancia del propósito y la duración de ella. Los visitantes serán acompañados en todo momento por alguna persona autorizada de la organización hasta que abandonen el recinto.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Procesos y Procedimientos	A7.2	¿Se controla y registra adecuadamente el ingreso de	Control de Acceso de Visitantes	
95	En Gestión de las operaciones y comunicaciones se aplicarán las normas del capítulo 8 de la norma NCh2777, en su integridad.	DS 83 Aprueba norma técnica para los órganos de la administración del estado sobre seguridad Y confidencialidad de los documentos electrónicos.	37	Procesos y Procedimientos	A5.1	¿Se aplican las normas del capítulo 8 de la norma NCh2777 en la gestión de operaciones y comunicaciones?	Normas de Gestión de Operaciones y Comunicaciones	
96	Principio de responsabilidad: La seguridad de las redes, sistemas y datos es de responsabilidad de aquel que las ofrece u opera, independiente de la naturaleza pública o privada del organismo.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	3	Políticas	N/A	¿Se aplica el principio de que la seguridad es responsabilidad de quien ofrece u opera redes, sistemas y datos?	Principio de Responsabilidad en Seguridad	
97	Principio de protección integral: Se deberán determinar los riesgos potenciales que puedan afectar a las redes o sistemas de información y aplicar las medidas organizativas, de gestión y técnicas apropiadas para la protección de los mismos.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	3	Políticas	N/A	¿Se identifican y se aplican medidas apropiadas para proteger los sistemas contra riesgos potenciales?	Principio de Protección Integral	
98	Principio de confidencialidad de los sistemas de información: Los datos, conectividad y sistemas deberán ser exclusivamente accedidos por personas o entidades autorizadas a tal efecto, las que se encontrarán sujetas a las obligaciones que señalen las leyes.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	3	Políticas	N/A	¿Se asegura que solo personas autorizadas accedan a los sistemas de información y se cumplan las obligaciones legales?	Confidencialidad en Sistemas de Información	
99	Principio de integridad de sistemas informáticos y de la información: Los datos y elementos de configuración de un sistema sólo podrán ser modificados por sistemas o personas autorizadas en el ejercicio de sus funciones respectivas.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	3	Políticas	N/A	¿Se garantiza que los datos y configuraciones solo puedan ser modificados por personas o sistemas autorizados?	Integridad de Sistemas y Datos	
100	Principio de disponibilidad de los sistemas de información: Losdatos, conectividad y sistemas deben estar accesibles para su uso a demanda.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	3	Políticas	N/A	¿Se asegura que los datos y sistemas estén accesibles para su uso a demanda?	Disponibilidad de Sistemas de Información	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
101	Principio de control de daños: Los órganos del Estado e instituciones privadas que posean infraestructura de la información calificada como crítica, en el caso de un incidente de ciberseguridad o de un ciberataque, deben adoptar las medidas necesarias para evitar la escalada del incidente y su posible propagación, notificando de igual forma al CSIRT respectivo.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	3	Políticas	N/A	¿Se actúa diligentemente para controlar y mitigar el daño en incidentes de ciberseguridad, notificando a las autoridades pertinentes?	Control de Daños en Ciberseguridad	
102	Principio de cooperación con la autoridad: Los órganos de la Administración del Estado y los privados deberán cooperar con la autoridad competente para resolver incidentes de ciberseguridad, y, de ser necesario, deberán cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	3	Políticas	N/A	¿Se coopera con las autoridades competentes para resolver incidentes de ciberseguridad?	Cooperación en Ciberseguridad	
103	Principio de especialidad en la sanción: En materia sancionatoria, se preferirá la aplicación de la regulación sectorial por sobre la establecida en esta ley.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	3	Políticas	N/A	¿Se aplica preferentemente la regulación sectorial en materia sancionatoria en lugar de la ley general?	Especialidad en Aplicación de Sanciones	
104	Determinar si el sector o insutución califica como infraestructura crítica, considerando el impacto de una posible interrupción o mal funcionamiento de los componentes, evaluando: i. La cantidad de usuarios potencialmente afectados y su extensión geográfica; ii. El efecto e impacto en la infraestructura y/o servicios de sectores cuya afectación es relevante para la población; iii. La potencial afectación de la vida, integridad física o salud de las personas; iv. La seguridad nacional y el ejercicio de la soberanía.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	4	Evaluación y Monitoreo	A5.30	¿Se ha evaluado si la institución califica como infraestructura crítica considerando la cantidad de usuarios afectados y su extensión geográfica?	Evaluación de Impacto Geográfico y de Usuarios	
105	Determinar si el sector o insutución califica como infraestructura crítica, teniendo en consideración capacidad de la red, el sistema informático, el sistema de información o infraestructura afectada, para ser sustituido o reparado en corto tiempo.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	4	Evaluación y Monitoreo	A5.30	¿Se ha determinado si la infraestructura de la información puede ser reemplazada o reparada rápidamente, para calificar como infraestructura crítica?	Evaluación de Capacidad de Sustitución o Reparación	
106	Determinar si el sector o insutución califica como infraestructura crítica, teniendo en consideración pérdidas financieras potenciales por fallas o ausencia del servicio a nivel nacional o regional asociada al producto interno bruto (PIB).	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	4	Evaluación y Monitoreo	A5.30	¿Se ha evaluado si las pérdidas financieras por fallas o ausencia del servicio impactan significativamente en el PIB, para calificar como infraestructura crítica?	Evaluación de Impacto Financiero y en el PIB	
107	Determinar si el sector o insutución califica como infraestructura crítica, teniendo en consideración afectación relevante del funcionamiento del Estado y sus órganos.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	4	Evaluación y Monitoreo	A5.30	¿Se ha considerado frente a una falla en la institución que afectaría de manera relevante el funcionamiento del Estado para calificar como infraestructura crítica?	Evaluación de Impacto Financiero y en el PIB	
108	Aplicar permanentemente las medidas de seguridad tecnológica, físicas, organizacionales e informativas necesarias para prevenir, reportar y resolver incidentes de ciberseguridad y gestionar los riesgos.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	5	Implementación de Controles Generales	A5.1	¿Se aplican de forma permanente las medidas de seguridad necesarias para prevenir, reportar y resolver incidentes de ciberseguridad?	Medidas de Seguridad en Tecnología y Organización	
109	Contener y mitigar el impacto sobre la continuidad operacional, la confidencialidad e integridad del servicio prestado, de conformidad a lo prescrito en esta ley.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	5	Implementación de Controles Generales	A5.30	¿Se contienen y mitigan efectivamente los impactos sobre la continuidad operacional y la integridad del servicio en caso de incidentes?	Gestión de Impacto en Continuidad Operacional	
110	Implementar un sistema de gestión de riesgo permanente con el fin de determinar aquellos que pueden afectar la seguridad de los sistemas informáticos, las redes y los datos; Cuáles afectarían la continuidad operacional y cuáles propiciarían la ocurrencia de incidentes de ciberseguridad. Dicho sistema debe determinar la gravedad de las consecuencias del incidente.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.	6	Implementación de Controles Generales	A5.27	¿Se ha implementado un sistema de gestión de riesgo para identificar y evaluar riesgos que afecten la seguridad y continuidad operacional?	Sistema de Gestión de Riesgo	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
111	Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de riesgos, de conformidad a lo que señale el reglamento. Lo anterior incluirá el registro del cumplimiento de la normativa sobre ciberseguridad y del conocimiento por los empleados, dependientes y proveedores de los protocolos de ciberseguridad y la aplicación de los mismos, tanto durante el funcionamiento regular como en caso de haber sufrido un incidente de ciberseguridad.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información	6	Implementación de Controles Generales	A5.37	¿Se mantiene un registro detallado de las acciones ejecutadas en el marco del sistema de gestión de riesgos?	Registro del Sistema de Gestión de Riesgos	
112	Elaborar e implementar planes de ciberseguridad y continuidad operacional. Dichos planes deberán ser actualizados periódicamente, a lo menos una vez al año.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información	6	Implementación de Controles Generales	A5.30	¿Se han elaborado e implementado planes de continuidad operacional y ciberseguridad, y se actualizan periódicamente?	Planes de Continuidad y Ciberseguridad	
113	Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos, plataformas y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relativa a dichas acciones o programas al CSIRT Sectorial respectivo o al CSIRT Nacional, según correspondiere, como determine el reglamento.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información	6	Implementación de Controles Generales	A5.24	¿Se realizan operaciones de revisión y simulacros para detectar riesgos de ciberseguridad y se comunica la información relevante a las entidades correspondientes?	Revisión y Simulacros en Sistemas	
114	Adoptar las medidas necesarias para reducir la propagación y el impacto y de un incidente de ciberseguridad, incluida la restricción de uso o el acceso a sistemas informáticos, si fuera necesario.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información	6	Implementación de Controles Generales	A5.26	¿Se adoptan medidas necesarias para reducir el impacto y propagación de incidentes de ciberseguridad?	Medidas de Mitigación de Incidentes de Ciberseguridad	
115	Contar con las certificaciones de los sistemas de gestión y procesos que determine el reglamento.	Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información	6	Implementación de Controles Generales	A5.35	¿Se cuenta con las certificaciones de sistemas de gestión y procesos exigidas por el reglamento?	Certificaciones de Sistemas y Procesos	
116	ISO 27001:2022 - 4 Contexto	ISO 27001:2022	4	-	ISO 27001:2022 - 4 Contexto	¿Ha identificado y documentado la organización los problemas, tanto internos como externos, relevantes para su propósito y dirección estratégica que afectan su capacidad para lograr los resultados previstos de su SGSI?	Documentación SGSI	
117	ISO 27001:2022 - 4 Contexto	ISO 27001:2022	4	-	ISO 27001:2022 - 4 Contexto	¿Ha identificado la organización las necesidades y expectativas de las partes interesadas en la seguridad de la información?	Documentación SGSI	
118	ISO 27001:2022 - 4 Contexto	ISO 27001:2022	4	-	ISO 27001:2022 - 4 Contexto	¿Ha definido y documentado la organización el alcance y los límites del SGSI?	Documentación SGSI	
119	ISO 27001:2022 - 4 Contexto	ISO 27001:2022	4	-	ISO 27001:2022 - 4 Contexto	¿Es el SGSI coherente con la dirección estratégica de la organización?	Documentación SGSI	
120	ISO 27001:2022 - 5 Liderazgo	ISO 27001:2022	5	-	ISO 27001:2022 - 5 Liderazgo	¿Ha demostrado la alta dirección liderazgo y compromiso con el SGSI?	Documentación SGSI	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
121	ISO 27001:2022 - 5 Liderazgo	ISO 27001:2022	5	-	ISO 27001:2022 - 5 Liderazgo	¿Se establece, comunica y mantiene una política de seguridad de la información?	Documentación SGSI	
122	ISO 27001:2022 - 5 Liderazgo	ISO 27001:2022	5	-	ISO 27001:2022 - 5 Liderazgo	¿Están claramente definidas y asignadas las responsabilidades y funciones de seguridad de la información?	Documentación SGSI	
123	ISO 27001:2022 - 5 Liderazgo	ISO 27001:2022	5	-	ISO 27001:2022 - 5 Liderazgo	¿Ha asegurado la alta dirección la integración del SGSI en los procesos de la organización?	Documentación SGSI	
124	ISO 27001:2022 - 6 Planificación	ISO 27001:2022	6	-	ISO 27001:2022 - 6 Planificación	¿Ha identificado la organización los riesgos y oportunidades que deben abordarse para garantizar que el SGSI pueda lograr los resultados esperados?	Documentación SGSI	
125	ISO 27001:2022 - 6 Planificación	ISO 27001:2022	6	-	ISO 27001:2022 - 6 Planificación	¿Ha establecido y aplicado la organización un enfoque sistemático para la evaluación y el tratamiento de riesgos?	Documentación SGSI	
126	ISO 27001:2022 - 6 Planificación	ISO 27001:2022	6	-	ISO 27001:2022 - 6 Planificación	¿La organización ha definido y documentado los objetivos de seguridad de la información?	Documentación SGSI	
127	ISO 27001:2022 - 6 Planificación	ISO 27001:2022	6	-	ISO 27001:2022 - 6 Planificación	¿Se ha documentado una declaración de aplicabilidad del Anexo A (ISO 27002)?	Documentación SGSI	
128	ISO 27001:2022 - 7 Soporte	ISO 27001:2022	7	-	ISO 27001:2022 - 7 Soporte	¿La organización ha determinado y proporcionado los recursos necesarios para el establecimiento, la implementación, el mantenimiento y la mejora continua del SGSI?	Documentación SGSI	
129	ISO 27001:2022 - 7 Soporte	ISO 27001:2022	7	-	ISO 27001:2022 - 7 Soporte	¿Tiene la organización un procedimiento documentado para crear conciencia sobre las políticas y procedimientos de seguridad de la información?	Documentación SGSI	
130	ISO 27001:2022 - 7 Soporte	ISO 27001:2022	7	-	ISO 27001:2022 - 7 Soporte	¿Tienen las personas relevantes las competencias necesarias para cumplir con sus roles dentro del SGSI?	Documentación SGSI	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
131	ISO 27001:2022 - 7 Soporte	ISO 27001:2022	7	-	ISO 27001:2022 - 7 Soporte	¿Se mantiene y controla la información documentada del SGSI?	Documentación SGSI	
132	ISO 27001:2022 - 7 Soporte	ISO 27001:2022	7	-	ISO 27001:2022 - 7 Soporte	¿Se ha determinado la comunicación interna y externa dentro del SGSI?	Documentación SGSI	
133	ISO 27001:2022 - 8 Operación	ISO 27001:2022	8	-	ISO 27001:2022 - 8 Operación	¿La organización ha planeado, implementado y controlado los procesos necesarios para cumplir con los requisitos de seguridad de la información?	Documentación SGSI	
134	ISO 27001:2022 - 8 Operación	ISO 27001:2022	8	-	ISO 27001:2022 - 8 Operación	¿Ha implementado la organización su proceso de evaluación de riesgos e identificado los riesgos que deben abordarse?	Documentación SGSI	
135	ISO 27001:2022 - 8 Operación	ISO 27001:2022	8	-	ISO 27001:2022 - 8 Operación	¿Ha implementado la organización su proceso de tratamiento de riesgos e integrado el tratamiento de riesgos de seguridad de la información en sus procesos operativos?	Documentación SGSI	
136	ISO 27001:2022 - 9 Evaluación	ISO 27001:2022	9	-	ISO 27001:2022 - 9 Evaluación del	¿Ha determinado la organización lo que debe ser monitoreado y medido, incluyendo la efectividad de los controles?	Documentación SGSI	
137	ISO 27001:2022 - 9 Evaluación	ISO 27001:2022	9	-	ISO 27001:2022 - 9 Evaluación del	¿Realiza la organización auditorías internas periódicas para garantizar que el SGSI se ajuste a los acuerdos planificados y se implemente y mantenga de manera efectiva?	Documentación SGSI	
138	ISO 27001:2022 - 9 Evaluación	ISO 27001:2022	9	-	ISO 27001:2022 - 9 Evaluación del	¿La alta dirección revisa periódicamente el SGSI de la organización para garantizar su idoneidad, adecuación y eficacia continuas?	Documentación SGSI	
139	ISO 27001:2022 - 10 Mejora Continua	ISO 27001:2022	10	-	ISO 27001:2022 - 10 Mejora Continua	¿La organización mejora continuamente la idoneidad, adecuación y eficacia del SGSI?	Documentación SGSI	
140	ISO 27001:2022 - 10 Mejora Continua	ISO 27001:2022	10	-	ISO 27001:2022 - 10 Mejora Continua	¿Tiene la organización un proceso documentado para manejar las no conformidades y las acciones correctivas?	Documentación SGSI	

ID	Control	Fuente	Art.	Descripción	ISO 27001:2022	Guía Autoevaluación	¿Dónde Revisar?	Autoevaluación
141	ISO 27001:2022 - 10 Mejora Continua	ISO 27001:2022	10	-	ISO 27001:2022 - 10 Mejora Continua	¿Evalúa la organización la eficacia de las acciones tomadas para abordar los riesgos y oportunidades?	Documentación SGSI	
142	ISO 27001:2022 - 10 Mejora Continua	ISO 27001:2022	10	-	ISO 27001:2022 - 10 Mejora Continua	¿La organización revisa y actualiza el SGSI en respuesta a los cambios en la organización y su contexto, y a los resultados de la evaluación del desempeño?	Documentación SGSI	

Anexo 2

GUÍA PARA EL EVALUADOR

	No Logrado	Logrado Parcial	Logrado	Completamente Logrado
	NL	PL	L	CL
Políticas	*No hay evidencia de que la organización tiene implementada la política.*	***Implementación:*** *Implementación inicial con algunos elementos de la política en funcionamiento.* ***Efectividad:*** *Evidencia limitada de impacto positivo; Resultados mixtos o inconsistentes.* ***Cumplimiento:*** *Cumplimiento parcial con estándares o regulaciones relevantes. Evalúe que la política cumple con el tema específico que es su propósito. Si no se especifica, quedará máximo como parcialmente logrado.* ***Sostenibilidad y Escalabilidad:*** *Planes iniciales para sostenibilidad y escalabilidad, pero con limitaciones.* ***Participación de Interesados:*** *Participación limitada de grupos de interés, feedback parcialmente integrado.*	***Implementación:*** *Implementación completa de la mayoría de los componentes de la política.* ***Efectividad:*** *Evidencia clara de impacto positivo, aunque con margen de mejora.* ***Cumplimiento:*** *Cumplimiento general con todos los objetivos específicos, estándares y regulaciones relevantes.* ***Sostenibilidad y Escalabilidad:*** *Planes efectivos y en proceso para la sostenibilidad y escalabilidad.* ***Participación de Interesados:*** *Buena participación de grupos de interés y uso activo de sus aportes.*	***Implementación:*** *Implementación integral y eficaz de todos los aspectos de la política.* ***Efectividad:*** *Impacto positivo significativo y sostenido; Supera las expectativas.* ***Cumplimiento:*** *Cumplimiento completo y sobresaliente con todos los estándares y regulaciones.* ***Sostenibilidad y Escalabilidad:*** *Excelente sostenibilidad y escalabilidad demostradas, con potencial para expandirse o replicarse.* ***Participación de Interesados:*** *Participación excepcional de todos los grupos de interés relevantes; integración completa de sus aportes.*
Procesos, Procedimientos y Elementos Documentales	*No hay evidencia de que la organización tiene implementado el proceso o procedimiento.*	***Definición de Procesos:*** *Algunos procesos estan definidos y documentados, pero no de manera integral.* ***Eficiencia y Eficacia:*** *Mejora en la reducción de errores y retrasos, pero de manera aún inconsistente.* ***Automatización y Tecnología:*** *Uso limitado de herramientas tecnológicas para la optimización de procesos.* ***Medición y Mejora Continua:*** *Se han establecido métricas básicas, pero la mejora continua es esporádica.*	***Definición de Procesos:*** *La mayoría de los procesos estan bien definidos, documentados y estandarizados.* ***Eficiencia y Eficacia:*** *Procesos eficientes y efectivos con menor incidencia de problemas.* ***Automatización y Tecnología:*** *Implementación efectiva de tecnologías para apoyar y mejorar los procesos.* ***Medición y Mejora Continua:*** *Métricas establecidas y utilizadas regularmente para la mejora continua de procesos.*	***Definición de Procesos:*** *Procesos completamente definidos, documentados, estandarizados y alineados con los objetivos estratégicos.* ***Eficiencia y Eficacia:*** *Procesos altamente eficientes, efectivos y consistentemente libres de errores.* ***Automatización y Tecnología:*** *Automatización avanzada y uso innovador de tecnología para optimizar procesos.* ***Medición y Mejora Continua:*** *Cultura robusta de medición y mejora contínua, con ajustes proactivos y basados en datos.*
Roles y Responsabilidades	*No hay evidencia de que la organización tiene definidas y comunicadas las responsabilidades ni los roles.*	***Claridad y Documentación:*** *Algunos roles y responsabilidades están definidos y documentados, pero no de manera integral.* ***Alineación con Objetivos:*** *Parcial alineación de roles con los objetivos, pero con inconsistencias.* ***Comprensión y Aceptación:*** *Mejora en la comprensión de los roles, aunque todavía existen áreas de confusión.* ***Rendimiento y Responsabilidad:*** *Algo de mejora en rendimiento y responsabilidad, pero aún no óptimo.* ***Flexibilidad y Adaptabilidad:*** *Limitada flexibilidad en los roles, con algunos esfuerzos para adaptarse a cambios.*	***Claridad y Documentación:*** *Roles y responsabilidades bien definidos y documentados para la mayoría del personal.* ***Alineación con Objetivos:*** *Buena alineación de roles con los objetivos estratégicos de la organización.* ***Comprensión y Aceptación:*** *Alta comprensión y aceptación de los roles y responsabilidades entre los empleados.* ***Rendimiento y Responsabilidad:*** *Mejora notable en rendimiento y responsabilidad debido a la claridad de roles.* ***Flexibilidad y Adaptabilidad:*** *Roles y responsabilidades flexibles, permitiendo adaptación eficaz a cambios y necesidades.*	***Claridad y Documentación:*** *Roles y responsabilidades claramente definidos, documentados y comunicados de manera integral.* ***Alineación con Objetivos:*** *Excelente alineación de todos los roles con los objetivos y la estrategia de la organización.* ***Comprensión y Aceptación:*** *Comprensión y aceptación universales de roles yresponsabilidades en toda la organización.* ***Rendimiento y Responsabilidad:*** *Rendimiento óptimo y alta responsabilidad, impulsados por una clara comprensión de roles.* ***Flexibilidad y Adaptabilidad:*** *Gran flexibilidad y adaptabilidad, con roles que evolucionan según las necesidades y el contexto.*
Implementación de Controles Técnicos	*No hay evidencia de que la organización tiene implementado el control técnico*	***Planificación y Estrategia:*** *Planificación básica realizada, pero con carencias en la estrategia general.* ***Implementación y Configuración:*** *Implementación parcial o con configuraciones que no maximizan la eficacia del control.* ***Cumplimiento y Estándares:*** *Cumplimiento parcial con estándares; necesita mejoras paraalcanzar mejores prácticas.* ***Eficiencia y Eficacia:*** *El control muestra cierta eficiencia, pero con margen de mejora significativo.* ***Monitoreo y Respuesta:*** *Monitoreo limitado y respuesta lenta o ineficaz a incidentes.*	***Planificación y Estrategia:*** *Planificación y estrategia bien desarrolladas y alineadas con los objetivos tecnológicos.* ***Implementación y Configuración:*** *Implementación completa con configuraciones que optimizan la funcionalidad del control.* ***Cumplimiento y Estándares:*** *Buen cumplimiento con estándares y prácticas recomendadas.* ***Eficiencia y Eficacia:*** *El control es eficiente y efectivo, contribuyendo a la seguridad y operación tecnológica.* ***Monitoreo y Respuesta:*** *Monitoreo efectivo y capacidad de respuesta rápida y adecuada a incidentes.*	***Planificación y Estrategia:*** *Excelente planificación y estrategia, integralmente alineadas con la visión tecnológica de la organización.* ***Implementación y Configuración:*** *Implementación óptima, con configuraciones que maximizan la eficacia y eficiencia del control.* ***Cumplimiento y Estándares:*** *Cumplimiento total con los más altos estándares y mejores prácticas de la industria.* ***Eficiencia y Eficacia:*** *Control altamente eficiente y efectivo, con impacto positivo demostrado en la seguridad y rendimiento tecnológico.* ***Monitoreo y Respuesta:*** *Monitoreo avanzado y capacidad de respuesta inmediata y efectiva a cualquier incidente o desafío técnico.*
Concientización y Capacitacion	*No hay evidencia que la organización define y realiza la actividad de concientización y capacitación*	***Planificación y Desarrollo:*** *Planificación básica, pero con carencias en cobertura y profundidad.* ***Contenido y Relevancia:*** *El material de capacitación es parcialmente relevante, pero necesita actualización o mejora.* ***Participación y Compromiso:*** *Participación irregular o limitada en actividades de capacitación.* ***Evaluación de la Eficacia:*** *Evaluaciones ocasionales, pero sin un seguimiento sistemático o análisis profundo.* ***Impacto y Aplicación Práctica:*** *Algunos indicios de impacto, pero no consistentes o generalizados en la organización.*	***Planificación y Desarrollo:*** *Planificación y desarrollo bien estructurados de actividades de concientización y capacitación.* ***Contenido y Relevancia:*** *Material de capacitación actualizado, relevante y bien recibido por los participantes.* ***Participación y Compromiso:*** *Buena participación y compromiso activo en las actividades de capacitación.* ***Evaluación de la Eficacia:*** *Evaluaciones regulares que demuestran una mejora en el conocimiento y habilidades.* ***Impacto y Aplicación Práctica:*** *Evidencia clara de impacto positivo en la concientización y prácticas laborales.*	***Planificación y Desarrollo:*** *Excelente planificación y desarrollo de un programa integral de concientización y capacitación.* ***Contenido y Relevancia:*** *Material de capacitación de alta calidad, completamente actualizado y profundamente relevante.* ***Participación y Compromiso:****Participación y compromiso excepcionales en todas las actividades de capacitación.* ***Evaluación de la Eficacia:*** *Evaluaciones exhaustivas y sistemáticas que demuestran un impacto significativo y sostenido.* ***Impacto y Aplicación Práctica:*** *Impacto sobresaliente en la concientización, cultura y prácticas laborales, con mejoras continuas.*