Ministerio Secretaría General de la Presidencia

Gobierno de Chile

GUÍA TÉCNICA

Seguridad de la Información para Órganos del Estado

• BORRADOR •

gob digital CHILE

ÍNDICE

I.
INTRODUCCIÓN

Toda organización que maneja sistemas tecnológicos debe resguardar y proteger la información de la misma o de sus asociados. Por eso, se establecen una serie de medidas preventivas que buscan mantener la integridad y disponibilidad de datos.

Esta guía técnica describe los controles de seguridad de la información que son necesarios para organizaciones gubernamentales.

La implementación de estos controles está dentro de los niveles de seguridad establecidos en la Norma Técnica sobre Seguridad de la Información para los Órganos de la Administración del Estado, en adelante "Norma Técnica".

Además entrega: objetivos, una descripción de su implementación, los mecanismos básicos de verificación o auditoría y una referencia a la norma desde donde se originan.

Para efectos de la selección de controles, se han utilizado las siguientes normas chilenas:

- NCh-ISO 27001:2013, directrices para la gestión de la seguridad de la información.
- NCh-ISO 27002:2013, código de prácticas para los controles de seguridad de la información.
- NCh-ISO 22301:2013, en relación a los aspectos de la continuidad del negocio.

II.
CONSIDERACIONES INICIALES

Todos los controles establecidos como de nivel básico en esta guía de implementación, deben ser desarrollados.

Aquellos que son calificados como controles de nivel avanzado, deben ser desarrollados en las instituciones donde se requiera un mayor de nivel de seguridad.

Si una institución estima que determinados controles del nivel avanzado:

1. no son aplicables,
2. no se configuran dentro de situaciones de riesgo que justifiquen su implementación o bien,
3. no pueden ser implementados por razones técnicas, económicas o estratégicas,

La institución deberá documentar las exclusiones a través de la sentencia de aplicabilidad del sistema de gestión, según lo establecido en el Artículo 8° letra f) de la Norma Técnica.

III.
DEFINICIONES

Para efectos de la presente guía técnica se utilizarán las definiciones del Artículo 3° de la Norma Técnica. De forma adicional, se dispondrán las siguientes definiciones:

- **Continuidad del Negocio**

  Persistencia de las operaciones de la institución.

- **Factor de Autenticación**

  Proceso por el cual se verifica/confirma que un usuario es quien dice ser.

  Existen tres tipos de factores de autenticación:

  1. lo que el usuario sabe (por ejemplo una contraseña),
  2. lo que el usuario tiene (por ejemplo un dispositivo o una tarjeta de coordenadas) y,
  3. algo que el usuario es (por ejemplo la biometría).

- **Información de Autenticación**

  Información que permite acreditar la identidad del usuario con variados grados de certeza. Puede tomar la forma de contraseñas, tarjetas de coordenadas, One Time Password, certificados digitales, biometría u otros. No se debe confundir la información con el factor de autenticación.

- **One Time Password (OTP)**

  Contraseña válida sólo para una autenticación, generada por un aplicativo o un dispositivo físico, la cual es utilizada de forma adicional a la contraseña primaria del usuario.

- **Passphrase**

  Tipo de contraseña, que en lugar de contar con una secuencia de caracteres aleatoria, cuenta con una secuencia de palabras aleatoria.

- **Principio de compartimentalización**

  Establece que exista un acceso limitado a la información, concedido a ciertas personas o grupos, y sólo para realizar tareas específicas.

- **Principio de menor privilegio**

  Extensión del principio de necesidad de saber a sistemas y procesos, establece únicamente se tenga permitido acceder a la información necesaria para el desempeño de cierta actividad.

- **Principio de necesidad de saber**

  Implementación del principio de compartimentalización.

  Establece que sólo se entregue acceso a la información que el usuario deba conocer para realizar sus funciones, aún cuando posea la jerarquía o autorizaciones apropiadas para acceder a ella.

Si la institución ha definido o requiere definir algún concepto o término específico, asociado a sus funciones u operaciones, será necesario que agrupe tales definiciones en un glosario.

Éste debe formar parte de la documentación del sistema de gestión, debiendo quedar disponible para todos los interesados en las materias de seguridad de la información y ser sometido al ejercicio establecido de revisiones periódicas, de manera de verificar su validez y relevancia.

Si las definiciones o términos utilizados provienen de normas o estándares internacionales, en el glosario de términos debe indicarse la fuente de tal definición.

IV.
NIVEL BÁSICO DE SEGURIDAD

Para la obtención del nivel básico de seguridad, los Órganos de la Administración del Estado deberán implementar los siguientes controles:

a) POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Control PS.01	Adoptar políticas de seguridad de la información
Objetivo	Proporcionar lineamientos de gestión compatibles con la misión y los objetivos estratégicos de la institución, orientadas a mitigar sus riesgos de seguridad de la información. Disponer de lineamientos para conservar la confidencialidad, integridad y disponibilidad de la información manejada por la institución. Demostrar el compromiso, apoyo e interés de la institución en el fomento y desarrollo de una cultura de seguridad.
Descripción de Implementación	Deberá establecerse un conjunto de políticas de seguridad que se encuentren respaldadas por una planificación estratégica institucional. Los documentos de políticas de seguridad deberán ser: o Aprobados por la dirección de la institución o por el Comité de Seguridad de la misma, y ser comunicada y difundida al personal y stakeholders. o Revisados regularmente, al menos cada 2 años, o cuando se produzcan cambios significativos, debiendo realizar las modificaciones necesarias.
Guía de referencia para auditoría	o Resolución Exenta o similar, con la aprobación de la Política General de Seguridad. o Políticas relevantes por dominio, si las hubiera, debidamente formalizadas. o Evidencia de difusión y revisión de las políticas.
Referencia	ISO 27001: A.5.1.1, A.5.1.2

b) SEGURIDAD ORGANIZACIONAL

Control OR.01	Designar un encargado de seguridad de la información
Objetivo	Lograr liderazgo y guía en la implementación, operación y mejora del Sistema de Gestión de Seguridad de la Información.
Descripción de Implementación	Se debe designar formalmente a un encargado de seguridad de la información, que lidere los esfuerzos de la institución en materia de seguridad de la información, y que reporte directamente al Jefe de Servicio o similar. El encargado de seguridad de la información debe tener un perfil adecuado a sus funciones, además de las cualidades de liderazgo, conocimiento técnico en materias de seguridad de la información y capacidad de gestión. Las funciones del encargado de seguridad de la información deberán estar claramente definidas en la resolución que lo designe.
Guía de referencia para auditoría	○ Resolución Exenta o similar con el nombramiento del Encargado de Seguridad. ○ Difusión de la designación del Encargado. ○ Antecedentes que permitan validar que la persona designada cumple con los requisitos mínimos para este rol, tales como certificados de estudios, certificaciones técnicas u otros.
Referencia	ISO 27001: A.6.1.1

Control OR.02	Establecer un comité de seguridad
Objetivo	Contar con un equipo de personas con capacidad de decisión sobre los objetivos organizacionales, y que apoyen al encargado de seguridad en su función.
Descripción de Implementación	Se debe designar a los integrantes del comité de seguridad de la información de la institución formalmente. El comité de seguridad debe contar con representantes de todas las áreas de la institución donde se identifiquen riesgos de seguridad de la información, incluyendo, al menos, a un representante del área de tecnología. El comité deberá sesionar al menos de forma anual.
Guía de referencia para auditoría	○ Resolución Exenta o similar con la conformación, responsabilidades y funcionamiento del comité de seguridad. ○ Difusión de la conformación del comité de seguridad. ○ Evidencia de sesiones del comité realizadas durante el período.

Referencia	ISO 27001: A.6.1.1, A.6.1.2

Control OR.03	**Segregación de funciones**
Objetivo	Reducir el riesgo de negligencia, mal uso o compromiso de la información de la institución.
Descripción de Implementación	Se debe establecer una política de segregación de funciones que establezca que no se pueda acceder, modificar, utilizar o destruir activos sin autorización o detección, considerando la posibilidad de sabotaje o colusión en las operaciones de la institución. En caso necesario, esta política podrá ser aplicable sólo a algunos procesos o sistemas específicos, limitando su alcance acorde a las necesidades de la institución.
Guía de referencia para auditoría	○ Política de segregación de funciones con alcance bien definido. ○ Evidencia de implementación de las políticas de segregación de funciones.
Referencia	ISO 27001: A.6.1.2

Control OR.04	**Contacto con autoridades y grupos de interés**
Objetivo	Mantener contacto con autoridades y grupos de interés para efectos de gestión de incidentes, información, buenas prácticas, entre otros.
Descripción de Implementación	Se debe establecer: ○ Un procedimiento con autoridades internas y externas, para el manejo de incidentes de seguridad, incluyendo: medios a través de los que se realizará el contacto, mecanismos de constancia de las comunicaciones y pasos a seguir para realizar el contacto pertinente. ○ Una lista de grupos de interés especial, la que debe ser contactada con regularidad, que permitirán a la institución mantenerse al tanto de las tendencias, normas y métodos de seguridad relevantes. También, se debe mantener contacto con regularidad con el CSIRT[1] del Ministerio del Interior y Seguridad Pública. Todos los contactos deben revisarse y hacerse regularmente y, al menos, de forma anual.
Guía de referencia para auditoría	○ Plan de gestión de incidentes de seguridad que establezca situaciones donde se requiera el contacto con autoridades o grupos de interés. ○ Evidencia de revisión de las listas de contactos en el intervalo establecido en el documento. ○ Evidencia de contacto con CSIRT del Ministerio del Interior y Seguridad Pública.

[1] CSIRT: Equipo de Respuesta ante Incidentes de Seguridad Informática

Referencia	ISO 27001: A.6.1.3, A.6.1.4

c) SEGURIDAD EN RELACIÓN CON LAS PERSONAS

Control SP.01	**Formalización de los términos de la relación laboral**
Objetivo	Los contratos que describen la relación laboral del funcionario y la institución deben indicar las responsabilidades de ambos en cuanto a la seguridad de la información.
Descripción de Implementación	Cada colaborador contratado bajo la modalidad de honorarios a suma alzada debe firmar un contrato que especifique sus responsabilidades en materia de seguridad de la información. La resolución de ingreso de funcionarios de planta o a contrata debe especificar las responsabilidades del funcionario en materia de seguridad de la información. Como parte del contrato anterior, o en un documento complementario, el funcionario debe firmar un acuerdo de confidencialidad de la información con la institución, en los casos que amerite.
Guía de referencia para auditoría	○ Listado del personal contratado en el período. ○ Contratos firmados que pertenezcan al período, con las cláusulas de confidencialidad y seguridad de la información correspondientes. ○ Acuerdos de confidencialidad firmados que pertenezcan al período, si corresponde.
Referencia	ISO 27001: A.7.1.2

Control SP.02	**Responsabilidades de la dirección**
Objetivo	Concientizar a los trabajadores respecto de sus responsabilidades, en materias de seguridad de la información. Concretar el compromiso de la dirección en con medidas claras respecto de la seguridad de la información.
Descripción de Implementación	La dirección de la institución debe impartir instrucciones y orientación sobre seguridad de la información al personal, en intervalos regulares, al menos, sobre las siguientes materias: 1. Uso seguro de sistemas informáticos, incluyendo estaciones de trabajo. 2. Uso seguro de la de red interna e internet, incluyendo acceso a recursos compartidos u otros. 3. Generación, transmisión, recepción, procesamiento y almacenamiento de información.

	4. Procedimientos para el reporte de incidentes. Estas instrucciones podrán ser impartidas mediante actividades personales y/o grupales, o por medio de mecanismos acorde a las necesidades de la institución.
Guía de referencia para auditoría	○ Programa anual de capacitación y sensibilización en materias de seguridad de la información. ○ Evidencia de material de capacitación y sensibilización utilizado en el período. ○ Evidencia de las actividades de capacitación y sensibilización realizadas en el período.
Referencia	ISO 27001: A.7.2.1, A.7.2.2

d) ADMINISTRACIÓN DE ACTIVOS

Control AA.01	**Identificación de activos de la institución y asignación de sus responsables**
Objetivo	Identificar los activos de información de la institución y sus responsables, para garantizar la correcta gestión de seguridad de la información los mismos.
Descripción de Implementación	Se debe identificar e inventariar los activos de información de la institución mediante un procedimiento documentado, asignando un responsable para cada uno de los activos mencionados. El inventario de activos debe ser actualizado con una frecuencia, al menos anual.
Guía de referencia para auditoría	○ Procedimiento o metodología para la generación y actualización del inventario de activos. ○ Inventario de activos actualizado de la institución. ○ Responsable de cada activo identificado en el inventario de activos.
Referencia	ISO 27001: A.8.1.1, A.8.1.2

Control AA.02	**Clasificación y etiquetado de activos de la institución**
Objetivo	Clasificar y etiquetar los activos de información de la institución para garantizar la correcta gestión de seguridad de la información de los mismos durante su ciclo de vida.
Descripción de Implementación	Se debe analizar y valorar cada activo de información con el fin de determinar la necesidad, prioridad y grado de protección que sea apropiado a cada uno. Cada activo debe tener una categoría de clasificación acorde a la necesidad de protección, la que debe estar en conformidad con la Ley Orgánica

	Constitucional de Bases Generales de la Administración del Estado. Es necesario definir un procedimiento para el etiquetado de los activos acorde a la clasificación realizada, incluyendo el etiquetado en la salida de los sistemas.
Guía de referencia para auditoría	○ Procedimiento o metodología para la generación y actualización del inventario de activos. ○ Inventario de activos actualizado de la institución. ○ Clasificación de cada activo identificada en el inventario de activos. ○ Procedimientos para el etiquetado de activos.
Referencia	ISO 27001: A.8.2.1, A.8.2.2

Control AA.03	**Uso aceptable de los activos de la institución**
Objetivo	Garantizar que el personal y stakeholders, conozcan y apliquen los lineamientos de la institución para proteger los activos de información.
Descripción de Implementación	Se debe definir una política de uso aceptable de activos, donde se establezca, al menos, lo siguiente: 1. Las responsabilidades del personal en el cuidado de los activos de la institución. 2. Lineamientos respecto del uso de: correo electrónico, internet y medios de almacenamiento extraíbles, como mínimo. 3. La prohibición del uso de software no autorizado en la institución (ver control SO.04). Esta política debe estar alineada a lo establecido en el control SP.02.
Guía de referencia para auditoría	○ Política de uso aceptable de activos. ○ Evidencia de difusión de la política.
Referencia	ISO 27001: A.8.1.3, A.8.2.3

Control AA.04	**Gestión de los medios de almacenamiento**
Objetivo	Garantizar la seguridad de la información contenida en medios de almacenamiento.
Descripción de Implementación	Se deben definir los procedimientos de manejo seguro de medios de almacenamiento, alineada al control AA.03, incluyendo como mínimo: la solicitud, entrega, uso, transporte, devolución y eliminación de los medios de almacenamiento de la institución. Se debe establecer claramente las restricciones de acceso a los medios de almacenamiento extraíbles en los sistemas.

Guía de referencia para auditoría	○ Procedimientos para la gestión de los medios de almacenamiento. ○ Evidencia de medidas de seguridad aplicadas a los medios de almacenamiento (encriptación, restricciones de conexión, entre otros). ○ Evidencia de solicitud, entrega, devolución y eliminación de medios en el período.
Referencia	ISO 27001: A.8.1.4, A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3

e) CONTROL DE ACCESO

Control CA.01	**Definición de políticas para el control de acceso lógico**
Objetivo	Gestionar el acceso lógico a los sistemas y activos de información de la institución.
Descripción de Implementación	Se debe contar con controles de acceso lógico basados, al menos, en un identificador único y su contraseña correspondiente. En el caso de requerimientos más estrictos, se debe privilegiar el uso de sistemas con múltiples factores de autenticación, tales como: firma electrónica, segundas claves (OTP o similar), biometría u otros, como mecanismos de validación más fuertes de la identidad del usuario. Se debe definir una política de gestión de acceso lógico que establezca, al menos, lo siguiente: 1. Métodos de autenticación autorizados por la institución. 2. Métodos de gestión de los identificadores y contraseñas, incluyendo: autorización de acceso, requerimientos mínimos de largo y complejidad, vida útil e historial de uso de contraseñas y clasificación de usuarios privilegiados. En cualquier caso, las contraseñas no podrán ser de largo inferior a 10 caracteres y no podrán estar relacionadas con datos de la persona que hagan fácil su deducción. Si los sistemas de la institución lo soportan, se recomienda el uso de una passphrase en lugar de una contraseña. 3. Métodos de revisión periódica de los accesos lógicos otorgados. 4. Redes y servicios de red de la institución a los que estará permitido el acceso. 5. Lineamientos para establecer quién tiene permitido el acceso a las distintas redes y servicios de la institución. Esta política debe estar basada en los principios de compartimentalización, necesidad de saber y de menor privilegio. De forma adicional, se deben establecer políticas de acceso lógico alineadas con este control para todos los sistemas de información, ya sea en esta misma política o en documentos independientes.
Guía de referencia para	○ Procedimientos para la gestión de los medios de almacenamiento. ○ Evidencia de medidas de seguridad aplicadas a los medios de

auditoría	almacenamiento (encriptación, restricciones de conexión, etc). ○ Evidencia de solicitud, entrega, devolución y eliminación de medios en el período. ○ Política de gestión de acceso lógico, usuarios y contraseñas. ○ Políticas complementarias. ○ Evidencia de difusión de las políticas.
Referencia	ISO 27001: A.9.1.1, A.9.1.2, A.9.4.3

Control CA.02	**Definición de procedimientos de acceso lógico**
Objetivo	Gestionar el acceso lógico a los sistemas y activos de información de la institución.
Descripción de Implementación	Se debe definir procedimientos de gestión de acceso lógico que establezcan, al menos, los siguientes mecanismos: 1. De asignación de información de autenticación a los usuarios, donde el jefe directo de quien lo pide, sea el responsable de la solicitud. 2. De alta, baja y modificaciones de usuarios y derechos de acceso, incluyendo los derechos de acceso privilegiado. 3. De entrega segura de la información de autenticación temporal de los usuarios, incluyendo la prohibición de entrega mediante texto no protegido y la obligación al usuario de acusar el recibo de la misma. 4. Que establezcan la obligación de cambiar la información de autenticación temporal o inicial con el primer uso y por consiguiente, a intervalos regulares. 5. Que establezcan el uso de información de autenticación diferente en los distintos sistemas o servicios de la institución, así como de la información de autenticación de uso personal del usuario. 6. Para minimizar el uso de cuentas grupales. Además de controles y procedimientos para proteger el acceso a los servicios de red.
Guía de referencia para auditoría	○ Procedimientos para la gestión del acceso lógico. ○ Evidencia de aplicación del procedimiento en los distintos sistemas y servicios de la institución. ○ Evidencia del proceso de alta, baja y modificación de usuarios y derechos de acceso. ○ Evidencia de la entrega segura de contraseñas temporales.
Referencia	ISO 27001: A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.4.3

Control CA.03	**Responsabilidades del usuario en el control de acceso lógico**

Objetivo	Responsabilizar a los usuarios del buen uso de los mecanismos de acceso lógico de la institución.
Descripción de Implementación	Se debe impartir instrucciones a los usuarios respecto a los mecanismos de control de acceso lógico en, al menos, las siguientes materias: 1. La obligación de mantener, en forma confidencial la información de autenticación que se asigne. 2. La obligación de no registrar la información de autenticación en papel. 3. La obligación de no almacenar la información de autenticación de forma desprotegida. 4. El deber de no compartir la información de autenticación del usuario con otros usuarios. 5. El deber de mantener la información de autenticación grupal sólo dentro de los miembros del grupo. 6. El deber de no incluir la información de autenticación del usuario en procesos automatizados o de inicio de sesión automáticos, por ejemplo, una macro o script. 7. La obligación de cambiar la información de autenticación cuando hayan indicios de un posible compromiso de un sistema. Es importante evaluar adecuadamente los factores de autenticación inmutables en estos casos, tales como los factores biométricos.
Guía de referencia para auditoría	○ Procedimientos para la gestión del acceso lógico. ○ Evidencia de aplicación del procedimiento en los distintos sistemas y servicios de la institución. ○ Evidencia del proceso de alta, baja y modificación de usuarios y derechos de acceso. ○ Evidencia de la entrega segura de contraseñas temporales.
Referencia	ISO 27001: A.9.3.1, A.9.2.4

Control CA.04	**Procesos de inicio de sesión seguros**
Objetivo	Aplicar mecanismos de inicio de sesión seguro a los sistemas, acorde a la política de control de acceso.
Descripción de Implementación	Para proteger la información contenida en los sistemas de la institución, éstos se deberán configurar de manera que exijan procesos de inicio de sesión seguros y que cumplan, al menos, con lo siguiente: 1. Terminar las sesiones después de un periodo de inactividad. 2. No mostrar la contraseña que se ingresa. 3. Proteger contra los inicios de sesión forzados. 4. No transmitir la información de autenticación sin cifrar.
Guía de referencia para auditoría	○ Procedimientos para la gestión del acceso lógico. ○ Evidencia de aplicación del procedimiento en los distintos sistemas y servicios de la institución.

	○ Evidencia del proceso de inicio de sesión seguro en los distintos sistemas y servicios de la institución.
Referencia	ISO 27001: A.9.4.2

f) CRIPTOGRAFÍA

Control CR.01	**Definiciones sobre el uso de controles criptográficos**
Objetivo	Proteger la confidencialidad, integridad y autenticidad de la información de la institución mediante el correcto uso de la criptografía.
Descripción de Implementación	Se debe establecer una política de uso de controles criptográficos para la institución que aborde, al menos, los siguientes temas: 1. Mecanismos de cifrado para proteger la información de la institución (por ejemplo, cifrado de discos duros, respaldos u otros). 2. Uso y gestión de certificados digitales en la institución, ya sea para firma electrónica, firma electrónica avanzada u otros usos. 3. Uso de mecanismos criptográficos para el establecimiento de canales seguros para comunicaciones, tales como correo electrónico, VPN, SSL/TLS (HTTPS), IPSec, SSH u otros, incluyendo el uso y gestión de llaves y certificados digitales para estos fines. 4. Listado de algoritmos o protocolos criptográficos inseguros, y de uso prohibido en las instituciones, salvo en caso de excepciones debidamente justificadas por la autoridad competente. Este listado debe contener, al menos, los siguientes: a. MD4, MD5, SHA-1. b. DES, 3DES. c. RC4. d. RSA o DSA con largo de llaves igual o inferior a 1024-bits. e. Criptografía basada en curvas elípticas con largo de llaves igual o inferior a 160-bits. f. Cualquier tipo de algoritmo criptográfico "casero" o implementaciones "caseras" de algoritmos criptográficos existentes.
Guía de referencia para auditoría	○ Política de uso de controles criptográficos. ○ Política de gestión de llaves criptográficas, si corresponde. ○ Listado de sistemas que utilizan firma electrónica avanzada u otros mecanismos criptográficos.
Referencia	ISO 27001: A.10.1.1, A.10.1.2

g) SEGURIDAD FÍSICA Y DEL AMBIENTE

Control SF.01	Implementación de políticas de acceso físico
Objetivo	Proteger las instalaciones de procesamiento de accesos no autorizados, robos, mal uso o daños producto de peligros ambientales.
Descripción de Implementación	Se debe establecer una política de seguridad física alineada a lo establecido en el control CA.01 y al análisis de riesgos realizado por la institución. Adicionalmente, se deben establecer todos los procedimientos necesarios para su implementación. Se debe definir los perímetros de seguridad física donde se alojen los activos que den soporte a los servicios de la institución (áreas seguras). Dichos perímetros deben tener barreras de resguardo, controles de acceso apropiados y estar físicamente protegidos del acceso no autorizado, daños e interferencias, así como proveer instalaciones de apoyo tales como cableado y suministro eléctrico apropiados. Se debe establecer un procedimiento de acceso a las áreas seguras y designar al personal autorizado para acceder a éstas.
Guía de referencia para auditoría	○ Política de seguridad física. ○ Procedimientos necesarios para la implementación de las políticas de seguridad física. ○ Listado de áreas seguras de la institución y personal autorizado para acceder a ellas. ○ Registros de acceso a las áreas seguras.
Referencia	ISO 27001: A.11.1.1, A.11.1.2

Control SF.02	Implementación de controles ambientales en áreas seguras
Objetivo	Proteger el equipamiento de daño producto de accesos no autorizados, robos o peligros ambientales, permitiendo la continuidad operacional y reducir el daño ante la materialización de algún desastre.
Descripción de Implementación	Se debe establecer una política de seguridad del equipamiento alineada a lo establecido en el control SF.01 que aborde, al menos, los siguientes temas: 1. Ubicación del equipamiento, de forma de minimizar el acceso innecesario y percances producto de mala manipulación o descuidos. 2. Implementación de controles de seguridad física, de forma de minimizar el riesgo de, al menos, las siguientes amenazas ambientales: robos, incendios, humo, agua, vibraciones o terremotos, interferencia del suministro eléctrico. 3. Mecanismos para el monitoreo y control de las condiciones ambientales tales como humedad, temperatura, etc. 4. Mecanismos para la detección temprana y extinción de incendios. 5. Mecanismos para garantizar la mantención periódica del

	equipamiento.
Guía de referencia para auditoría	○ Política de seguridad del equipamiento. ○ Evidencia de controles de seguridad física implementados. ○ Contratos con proveedores relacionados (alarmas, extintores, refrigeración, etc). ○ Evidencia de los mecanismos de monitoreo ambiental y sus últimas alertas y/o pruebas de funcionamiento. ○ Evidencias del mantenimiento realizado al equipamiento.
Referencia	ISO 27001: A.11.1.4, A.11.2.1, A.11.2.4

Control SF.03	**Seguridad en la reutilización o descarte de equipos**
Objetivo	Prevenir pérdida de confidencialidad de la información de la institución durante o después de descartar o desechar equipamiento.
Descripción de Implementación	Se debe establecer una política de reutilización o descarte de activos, incluyendo al menos: requisitos para los mecanismos de borrado, sobreescritura o destrucción de activos y tipo de información correspondiente a mecanismos, alineado a la clasificación establecida en el control AA.02. Se debe establecer un procedimiento de borrado seguro de equipamiento tecnológico que establezca, al menos, lo siguiente: 1. Los datos de la institución deben ser eliminados o sobrescritos de manera segura, y con un mecanismo que entregue un alto grado de confianza en que la información no se pueda recuperar, antes de reutilizar o descartar el equipamiento. 2. La prohibición de un formateo normal, en el caso de descarte de equipos, debiendo de forma obligatoria requerir un borrado seguro de los medios. 3. Para el caso de datos sensibles, que así lo ameriten, el medio de almacenamiento deberá ser destruido de forma segura. Una alternativa al borrado seguro es utilizar encriptación de la información, de forma tal que, al destruir la llave de encriptación, la información no se pueda recuperar (ver control CR.01).
Guía de referencia para auditoría	○ Política de reutilización o descarte de activos. ○ Procedimientos para el borrado seguro o destrucción de medios de almacenamiento.
Referencia	ISO 27001: A.11.2.7

Control SF.04	**Implementación de políticas de escritorio y pantalla limpias**
Objetivo	Proteger el equipamiento de daño producto de descuidos o accidentes. Proteger la información de la institución de accesos no autorizados a ella.
Descripción de	Se debe establecer una política de escritorio y pantalla limpios que aborde,

Implementación	al menos, lo siguiente: 1. La prohibición de consumo de alimentos, bebidas o tabaco en las cercanías del equipamiento, en particular en áreas seguras. 2. La obligación del cierre o bloqueo de sesión una vez terminadas las funciones y antes de levantarse del puesto de trabajo, forzando el uso de algún mecanismo de autenticación para su posterior uso. 3. La obligación de la mantención de un escritorio limpio de papeles o medios de almacenamiento con información de la institución.
Guía de referencia para auditoría	○ Política de escritorio y pantalla limpia. ○ Evidencia de difusión de la política.
Referencia	ISO 27001: A.11.2.1, A.11.2.8, A.11.2.9

h) SEGURIDAD EN LAS OPERACIONES

Control SO.01	Implementación de controles contra código malicioso
Objetivo	Proteger la información de la institución contra el código malicioso.
Descripción de Implementación	Se debe establecer una política contra código malicioso, así como todos los procedimientos necesarios para su implementación, que establezcan al menos, lo siguiente: 1. Características de la solución contra código malicioso de la institución (si es centralizada o no, si posee funcionalidad de lista blanca, gris o negra, frecuencia de actualización de las firmas, entre otros). 2. Capacitaciones necesarias al personal respecto al uso de las herramientas contra código malicioso y conductas de riesgo asociadas a código malicioso, como por ejemplo, abrir archivos adjuntos de un correo electrónico, uso de medios de almacenamiento extraíbles en computadores no seguros, etc. Estas capacitaciones deben estar alineadas a los controles SP.02 y AA.03
Guía de referencia para auditoría	○ Política y procedimiento contra código malicioso. ○ Evidencia de capacitaciones al personal respecto a conductas de riesgo asociadas a código malicioso.
Referencia	ISO 27001: A.12.2.1

Control SO.02	Respaldo de la información
Objetivo	Proteger la información de la institución en casos como pérdida de datos y restauración de éstos.

Descripción de Implementación	Se debe establecer una política de respaldos, así como todos los procedimientos necesarios para su implementación, estableciendo claramente los requerimientos, los que deben incluir, al menos, lo siguiente: 1. Sistemas o equipamiento que debe ser respaldado. 2. Periodicidad de los respaldos de las estaciones de trabajo, que no podrá ser menor a un respaldo anual. 3. Periodicidad de los respaldos de los sistemas de información, que no podrá ser inferior a un respaldo mensual. 4. Retención de los respaldos, que no podrá ser inferior a tres ciclos de respaldo para los sistemas de información. 5. Infraestructura necesaria para el almacenamiento de los respaldos. 6. Ubicación de la infraestructura de almacenamiento de los respaldos, que deberá estar ubicada, de forma tal, que minimice el riesgo de ser afectada por los mismos incidentes que la ubicación de los sistemas de información. 7. Requerimientos de seguridad para la infraestructura de almacenamiento de los respaldos, incluyendo controles de acceso y condiciones físicas y ambientales. 8. Realización de pruebas de restauración de los respaldos de los sistemas de información, que no podrá ser inferior a una prueba anual por sistema, debiendo quedar documentadas. 9. Los procedimientos de restauración de los respaldos deben estar disponibles en caso de querer utilizarlos, ya sea almacenando dichos procedimientos de forma conjunta con los respaldos o en alguna ubicación que asegure su disponibilidad.
Guía de referencia para auditoría	○ Política de respaldos. ○ Procedimientos de respaldos para los sistemas y estaciones de trabajo definidas en la política. ○ Procedimientos de restauración de los respaldos. ○ Evidencia de realización de respaldos acorde a las políticas. ○ Evidencia de pruebas de restauración de los respaldos. ○ Evidencia de controles de seguridad implementados en la infraestructura de almacenamiento de respaldos.
Referencia	ISO 27001: A.12.3.1

Control SO.03	**Sincronización de Relojes**
Objetivo	Facilitar el seguimiento de los eventos y la consistencia de los registros de los sistemas de la institución.
Descripción de Implementación	Se debe establecer una política de sincronización de relojes, así como todos los procedimientos necesarios para su implementación, los que deben incluir, al menos, lo siguiente: 1. Establecimiento de la fuente de tiempo para los sistemas de la institución a la hora oficial de Chile. 2. Mecanismos para mantener la sincronización de los relojes en los sistemas de la institución.
Guía de	○ Política de sincronización de relojes.

referencia para auditoría	○ Procedimientos operacionales de los sistemas de la institución que incluyan la sincronización de relojes. ○ Evidencia de la correcta sincronización de los relojes de los sistemas de la institución.
Referencia	ISO 27001: A.12.4.4

Control SO.04	**Instalación de software**
Objetivo	Asegurar la integridad de los sistemas de la institución.
Descripción de Implementación	Se debe establecer, en alguna de las políticas de seguridad de la institución (por ejemplo, en la política de uso aceptable de activos, control AA.03), la prohibición del uso de software no autorizado. Se debe establecer un procedimiento de instalación de software que abarque, al menos, lo siguiente: 1. Instalación de software en sistemas. 2. Instalación de software en estaciones de trabajo. 3. Listado de software permitido, incluyendo software base, los tipos de software que puedan instalar los usuarios o software que requiera algún tipo de autorización especial. 4. Listado de software o categorías de software prohibido. 5. Mecanismos de revisión de software instalado en la institución.
Guía de referencia para auditoría	○ Establecimiento de la prohibición del uso de software no autorizado en alguna política de la institución. ○ Procedimiento de instalación de software. ○ Evidencia de los resultados de las revisiones de software instalado en la institución.
Referencia	ISO 27001: A.12.5.1, A.12.6.2

i) SEGURIDAD DE LAS COMUNICACIONES

Control SC.01	**Implementación de controles de seguridad en las redes**
Objetivo	Proteger la información en sistemas y aplicaciones de la institución mediante la administración y control de las redes.
Descripción de Implementación	Se debe establecer una política de seguridad de red, así como todos los procedimientos necesarios para su implementación, los que deben incluir, al menos, lo siguiente: 1. Mecanismos y responsabilidades para la administración de equipos de redes. 2. Mecanismos de autorización del acceso a las distintas redes y sistemas de red.

	3. Mecanismos para controlar y/o restringir la conexión a las distintas redes y sistemas de red internos y externos.
Guía de referencia para auditoría	○ Política de seguridad de red. ○ Listado de controles de red implementados y procedimientos para su correcto uso. ○ Evidencia de los controles de red implementados.
Referencia	ISO 27001: A.13.1.1

Control SC.02	**Políticas y procedimientos para la transferencia de información**
Objetivo	Mantener la seguridad de la información transferida al interior o exterior de la institución.
Descripción de Implementación	Se debe establecer una política de comunicaciones seguras, así como todos los procedimientos necesarios para su implementación, los que deben incluir, al menos, lo siguiente: 1. Medidas de protección para la transferencia de información a través de cualquier medio de comunicación, incluyendo los de transporte físico. 2. Medidas para la protección de la información transferida contra la intercepción, copia, modificación y/o destrucción. 3. Medidas para la detección y protección contra el código malicioso que se pueda transmitir por medios electrónicos, alineadas al control SO.01. 4. Los lineamientos para el uso aceptable de los mecanismos de transferencia de información, en relación al control AA.03. 5. Uso de controles criptográficos para proteger la información transferida, alineado al control CR.01. 6. Disponer de controles adicionales para los mensajes que no se puedan autenticar.
Guía de referencia para auditoría	○ Política y procedimientos para comunicaciones seguras. ○ Evidencia de configuración de sistemas de transferencia de información acorde a la política, tales como correo electrónico, mensajería electrónica y otros.
Referencia	ISO 27001: A.8.3.3, A.13.2.1, A.13.2.3

j) ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Control AD.01	**Incluir requisitos de seguridad de la información en los procesos de adquisición o desarrollo de sistemas**
Objetivo	Incorporar la seguridad de la información al ciclo de vida de los sistemas de

	la institución.
Descripción de Implementación	Los requisitos de seguridad de la información deben ser definidos e incluidos en los procesos, proyectos de adquisición, desarrollo de nuevos sistemas o mejora de sistemas existentes. Se deben establecer criterios de aceptación de los sistemas que incluyan el cumplimiento de los requisitos de seguridad de la información establecidos.
Guía de referencia para auditoría	○ Evidencia de incorporación de requisitos de seguridad de la información en los proyectos de adquisición, desarrollo o mejora de sistemas. ○ Evidencia de pruebas de aceptación de sistemas que incorporen los requisitos de seguridad de la información.
Referencia	ISO 27001: A.14.1.1, A.14.2.9

k) SEGURIDAD EN LA RELACIÓN CON PROVEEDORES

Control RP.01	Políticas de seguridad para las relaciones con proveedores
Objetivo	Mantener la seguridad de la información de los activos de la institución a los que tengan acceso proveedores.
Descripción de Implementación	Se debe establecer una política de seguridad para las relaciones con proveedores, que establezca los requisitos de seguridad que deben cumplir, alineada a los objetivos estratégicos de la institución y a sus políticas de seguridad establecidas en el control PS.01.
Guía de referencia para auditoría	○ Política de seguridad para las relaciones con proveedores.
Referencia	ISO 27001: A.15.1.1

l) GESTIÓN DE INCIDENTES

Control GI.01	Políticas y procedimientos para la gestión de incidentes
Objetivo	Asegurar un enfoque consistente y eficaz en la gestión de los incidentes de seguridad de la información de la institución.
Descripción de Implementación	Se debe establecer una política de gestión de incidentes de seguridad de la información que establezca, al menos, lo siguiente: 1. Los roles y responsabilidades asociados a la gestión de incidentes, alineado a lo establecido en el control SP.02. 2. Deber de informar los incidentes a la autoridad correspondiente o

	grupos de interés, alineado a lo establecido en el control OR.04. Se debe establecer un procedimiento de respuesta ante incidentes de seguridad que establezca, al menos, lo siguiente: 1. Mecanismos de detección de incidentes de seguridad. 2. Mecanismos para el registro, reporte y clasificación de los incidentes de seguridad. 3. Evaluación de los incidentes de seguridad y respuesta a ellos. 4. Seguimiento de los incidentes y mejora continua.
Guía de referencia para auditoría	○ Política de gestión de incidentes de seguridad de la información. ○ Responsables de la gestión de incidentes formalmente definidos. ○ Listado de incidentes del período.
Referencia	ISO 27001: A.16.1.1, A.16.1.2, A.16.1.4, A.16.1.5, A.16.1.6

m) SEGURIDAD EN LA CONTINUIDAD DE LAS OPERACIONES

Control CO.01	Establecimiento de un plan de continuidad del negocio
Objetivo	Mantener la continuidad de las operaciones y de la seguridad de la información de la institución durante situaciones de contingencia o emergencia. Mitigar el daño que un evento de continuidad podría causar a la institución. Volver a la operación normal de forma segura y ordenada después de un evento que afecte la continuidad de las operaciones.
Descripción de Implementación	Se debe establecer un plan de continuidad del negocio que aborde, al menos, lo siguiente: 1. Definición de roles y responsabilidades durante y después de contingencia. 2. Proceso para declarar la contingencia y convocar a los equipos de respuesta. 3. Detalles para gestionar las consecuencias de un evento de contingencia en, al menos, los siguientes aspectos: a. Seguridad de las personas. b. Opciones y mecanismos de respuesta a la contingencia, incluyendo las definiciones de seguridad de la información durante los eventos de contingencia. c. Mitigación y prevención de futuros daños producto del incidente en curso. 4. Detalles respecto a la comunicación con colaboradores, funcionarios y sus familiares, stakeholders y autoridades (policía, bomberos, autoridades directivas, etc.) 5. Detalles respecto a la continuidad de las operaciones críticas durante la contingencia. 6. Detalles respecto a la efectiva gestión de las relaciones públicas durante la contingencia. 7. Proceso para la vuelta a la normalidad, una vez terminada la contingencia.

	Adicionalmente, se debe establecer un plan de pruebas de continuidad del negocio, que establezca una frecuencia de pruebas al menos anual, así como también que los resultados de dichas pruebas deben resultar en la mejora continua del plan de continuidad del negocio.
Guía de referencia para auditoría	○ Plan de continuidad del negocio, que incorpore un plan de contingencia y recuperación. ○ Plan de pruebas del plan de continuidad del negocio. ○ Resultados de las pruebas al plan de continuidad de negocio.
Referencia	ISO 27001: A.17.1.1, A.17.1.2, A.17.1.3, ISO 22301: 8.4.4

n) CUMPLIMIENTO

Control CU.01	**Identificar y documentar los requerimientos legales y contractuales**
Objetivo	Evitar incumplimientos de cualquier tipo de obligación legal o contractual relacionadas con la seguridad de la información.
Descripción de Implementación	Se debe identificar y documentar todos los requerimientos legales y contractuales relacionados con la seguridad de la información que apliquen a la institución. Se debe establecer un procedimiento para asegurar el cumplimiento de dichos requisitos.
Guía de referencia para auditoría	○ Resolución Exenta o similar con la aprobación de la Política General de Seguridad, con un apartado referido a la obligación del cumplimiento legal y normativo. ○ Planilla o documento similar, donde se identifique: los requerimientos legales y contractuales de la institución, estado de su cumplimiento y plan de acción para requerimientos no cumplidos.
Referencia	ISO 27001: A.18.1.1

Control CU.02	**Establecer mecanismos de protección de los registros.**
Objetivo	Proteger los registros de operación de la institución contra cualquier modificación no autorizada o accidental que comprometa la confidencialidad, integridad o disponibilidad de ellos.
Descripción de Implementación	Se debe establecer un procedimiento para auditar, de forma periódica, la integridad de los registros de operación de la institución, de conformidad con los requisitos identificados en el control CU.01.
Guía de referencia para auditoría	○ Resolución Exenta o similar con la aprobación de la Política General de Seguridad, con un apartado referido a la obligación del cumplimiento legal y normativo. ○ Planilla o documento similar, donde se identifique: los requerimientos legales y contractuales de la institución, estado de su cumplimiento y

	plan de acción para requerimientos no cumplidos.
Referencia	ISO 27001: A.18.1.3

Control CU.03	**Establecer mecanismos de protección de la información personal**
Objetivo	Asegurar y proteger la información de carácter personal que maneje la institución contra cualquier brecha de confidencialidad o privacidad.
Descripción de Implementación	Se debe establecer una política de privacidad, que establezca claramente la protección de la información personal que maneje la institución y los mecanismos que utiliza para garantizar su confidencialidad y privacidad.
Guía de referencia para auditoría	○ Política de privacidad y protección de datos personales.
Referencia	ISO 27001: A.18.1.4

V.
NIVEL AVANZADO SEGURIDAD

Los controles del nivel avanzado de seguridad corresponderá a todos los controles establecidos en el Anexo A de la NCh-ISO 27001 vigente, que no estén referenciados por los controles del nivel básico de seguridad.

Para mayor información, diríjase a la referencia mencionada en el párrafo anterior.