1. MARCO

La Asociación Chilena de Seguridad, en adelante ACHS, en su calidad de organismo administrador del seguro social contra riesgos de accidentes del trabajo y enfermedades profesionales establecido en la Ley N°16.744, se ve expuesta a riesgos que de materializarse podrían ocasionar consecuencias operacionales y financieras negativas, impactando directamente en la capacidad para cumplir con el otorgamiento de las prestaciones preventivas, de salud, y económicas comprometidas, y en el patrimonio. Desde esta perspectiva, la ACHS considera que las decisiones operacionales y financieras, que adopten los miembros del Directorio, así como también la alta administración, deben incorporar las mejores prácticas respecto a la gestión de los riesgos.

El presente documento tiene por finalidad establecer los conceptos, principios y directrices generales de la gestión de la seguridad de la información aplicable a la ACHS.

A partir de los conceptos, principios y directrices establecidos en esta política, la ACHS fortalece su gobierno y estructura de gestión de riesgo, ofrece mayor seguridad a sus empresas afiliadas y trabajadores respecto al tratamiento de los datos e información considerada confidencial y que se encuentra protegida por ley, buscando garantizar un adecuado nivel de seguridad durante el ciclo de vida de la información.

Para asegurar el cabal cumplimiento de esta política, se establecen roles y responsabilidades específicas, los cuales requieren del compromiso de todo el personal y de quienes se relacionan con la ACHS, a objeto de crear y mantener un ambiente propicio para el efectivo resguardo y/o protección de la información.

La seguridad de la información consiste en un conjunto de medidas preventivas y correctivas que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Cualquier forma que tome la información, ya sea impresa o escrita en papel, almacenada electrónicamente, transmitida por correo, por otros medios electrónicos, mostrada en material audiovisual o en una conversación, y/o cualquier medio, independientemente de

los dispositivos a través de los cuales es compartida y almacenada, siempre debe estar protegida.

2. OBJETIVOS

- Estructurar un marco formal de trabajo con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información generada por cada uno de los procesos y el cumplimiento de las regulaciones que norman las prestaciones otorgadas por la ACHS.
- Entregar lineamientos de la gestión de seguridad de la información en la ACHS, sus principales roles y responsabilidades.
- Establecer, lineamientos para la aplicación de los principios y directrices de protección de las informaciones que posee la organización, garantizando que el personal de las distintas áreas de la ACHS esté concientizado respecto a las responsabilidades que les corresponden en el marco de esta política.

3. ALCANCE

Esta política aplica para todas las unidades operacionales y procesos que forman parte de la ACHS, y todos aquellos responsables de participar en las actividades de establecer, implementar, operar, monitorear, mantener y mejorar la gestión de la seguridad de la información, que incluye:

- La administración de activos de información ya sea en custodia de terceros o propia.
- La infraestructura tecnológica que permite la generación, procesamiento, transferencia y almacenamiento de información.
- Las instalaciones físicas donde residen los activos de información.
- Las personas que hacen uso de estos activos (internos y externos).

4. DEFINICIONES

La definición de términos relacionados con la presente política, se encuentran detallados en el Anexo N° 1 – Glosario de Términos.

5. POLÍTICA

Se ha desarrollado por parte de la ACHS una metodología para gestionar la seguridad de la información, que contiene la identificación y evaluación de riesgos, controles preventivos, establecimiento de indicadores claves de riesgo y su actualización.

Para que esta política se mantenga en el tiempo, debe estar soportada, a su vez, por una sólida estructura de administración de la seguridad, la cual, esté alineada con la presente política.

Todos los recursos y activos de información son de propiedad de la ACHS, razón por la cual esta política aplica íntegramente sobre ellos.

5.1. Directrices de la Seguridad de la Información

La seguridad de la información en la ACHS, ha establecido los principales controles, denominados directrices que a continuación se desarrollan:

a) La información de la Asociación, de las empresas adheridas, de los afiliados y de los colaboradores de la ACHS se deben tratar de forma ética y prudente y de acuerdo con las leyes vigentes y normas internas, evitándose el mal uso y la exposición indebida.

b) La información se debe utilizar de forma transparente y sólo con la finalidad para la cual se obtuvo.

c) Todos los procesos de la ACHS, durante su ciclo de vida (de la información), deben garantizar la segregación de funciones, por medio de la participación de más de un colaborador o equipo de colaboradores.

d) El acceso a las informaciones y recursos sólo se debe hacer si está autorizado por el dueño del proceso.

e) La identificación de cualquier colaborador debe ser única, personal e intransferible, siendo responsable por todas las acciones realizadas.

f) El otorgamiento de accesos debe obedecer al criterio de menor privilegio, en el cual los usuarios tienen acceso solamente a los recursos de información imprescindibles para el pleno desempeño de sus actividades diarias.

g) Las claves entregadas a los usuarios deben ser secretas, estando prohibido compartirlas.

h) Los riesgos que se identifiquen a la información de la ACHS, deben ser informados a la Subgerencia de Riesgos y Cumplimiento y en particular al Jefe de Riesgo Operacional.

i) Las responsabilidades en lo que se refiere a la seguridad de la información se deben dar a conocer a todos los colaboradores de la ACHS, quienes deben aplicar estas directrices.

5.2. Clasificación de Activos de Información

La clasificación de activos de información considera la forma de almacenamiento, la clasificación según el nivel de confidencialidad y uso, y los tipos de información existente y su clasificación respectiva.

Para efectos de esta política, las formas de almacenamiento de la información se definen en tres tipos:

- **Información en documentación escrita:** Cualquier dato o información contenido en documentos físicos como impresiones, contratos, informes u otros antecedentes.
- **Información en documentación digital o electrónica:** Cualquier registro de datos o información en sistemas, softwares, notebooks, correo electrónico u otros.
- **Información transmitida oralmente:** Cualquier dato o información en conocimiento de las personas, transmitida en conversaciones.

Se clasificarán los activos de información, **según su nivel de confidencialidad**, en cuatro tipos:

- **Confidencial:** Alto nivel de confidencialidad. No puede ser divulgada a excepción de instancias particulares y autorizadas.
- **Restringida:** Medio nivel de confidencialidad. Información sensible de uso exclusivamente interno, áreas específicas.
- **Uso interno:** Bajo nivel de confidencialidad. Información que puede estar disponible para todos los colaboradores.

- **Pública:** No requiere confidencialidad.

Dependiendo del tipo de información, ésta se clasificará según el siguiente recuadro:

TIPO DE INFORMACIÓN	CLASIFICACIÓN
Estratégica	Restringida
Normativa	Restringida
Comunicación interna	Uso interno
Comunicación externa	Pública
Financiera contable	Restringida
Soporte Interno	Uso Interno
Antecedentes pacientes	Confidencial
Antecedentes de empresas adheridas	Restringida
Antecedentes de colaboradores	Restringida

Los tipos de información son una lista no exhaustiva que podrá ser modificada por la Subgerencia de Riesgos y Cumplimiento en conjunto con las áreas usuarias cada vez que sea requerido.

Es responsabilidad de cada área identificar, definir y clasificar los tipos de información que generan, gestionan y/o almacenan asegurando su adecuado resguardo y tratamiento, con el apoyo metodológico de la Subgerencia de Riesgos y Cumplimiento.

Gestión de Seguridad de la Información

La política de seguridad de la información y los procedimientos que se derivan de ésta, se desarrollan para reforzar nuestro compromiso como organización, respecto al tratamiento adecuado de la información.

Lo anterior, se encuentra fundado en los principios básicos de la seguridad de la información:

Confidencialidad

Garantizar que el acceso a la información se otorga solamente a personas autorizadas.

Integridad

Garantizar la exactitud y la completitud de la información y de los métodos de su procesamiento, así como de la transparencia en el trato con los distintos públicos de interés.

Disponibilidad

Garantizar que las personas autorizadas tengan acceso a la información, siempre que sea necesario.

5.3. Difusión de Seguridad de la Información

Será responsabilidad de todos los dueños de procesos promover y reforzar en sus equipos de trabajo las temáticas relacionadas con la seguridad de la información. Adicionalmente, el Jefe de Riesgo Operacional deberá proponer un conjunto de temáticas a desarrollar anualmente, además de buscar diferentes medios de difusión, con el fin de fortalecer la cultura de resguardo de los activos de información.

Propiedad Intelectual

Tecnologías, marcas, metodologías y cualquier otra información que pertenezca a la ACHS no se debe utilizar para fines particulares, ni transferir a otro, aunque hayan sido obtenidas o desarrolladas por el propio colaborador en su ambiente de trabajo.

5.4. Estándar de Referencia (ISO 27002: 2013)

Dentro de los estándares relacionados a la seguridad de la información, el estándar ISO 27002:2013 es uno de los más reconocidos y con el cual se pueden abarcar todas las áreas de diferentes organizaciones. Dicho estándar, posee en forma general dominios, controles y objetivos para cada uno de estos, los cuales se pueden adaptar a la realidad de la ACHS.

El estándar será considerado un marco de referencia en temáticas de seguridad de la información, sin embargo no constituye una obligación en la implementación de todos los objetivos de control allí descritos.

5.5. Ciberseguridad

El avance hacia la digitalización de las organizaciones y la masificación del uso de las tecnologías supone plantearse importantes desafíos en materias de seguridad para prevenir la fuga de información, ciberataques o fraudes informáticos entre otros riesgos, que pueden vulnerar no solo nuestros servicios críticos, sino también afectar a aquellos grupos de interés con quién la ACHS tiene relación.

Atendiendo a esto último, la Asociación ha ampliado su compromiso con la gestión de la seguridad de la información, promoviendo instancias que garanticen un ciberespacio robusto, seguro y resiliente que tiene por objetivos específicos:

- Reducir brechas de accesos y gestionar los riesgos del ciberespacio, a través de la identificación y gestión de vulnerabilidades o potenciales amenazas.
- Desarrollar e implementar mecanismos estandarizados de reporte y gestión para la prevención y recuperación ante incidentes de ciberseguridad.
- Resguardar la seguridad de las personas en el ciberespacio.
- Generar conciencia sobre el uso seguro y responsable de las tecnologías digitales.
- Promover instancias colaborativas, en materias de ciberseguridad, con otras instituciones.
- Fortalecer el gobierno corporativo en materias de ciberseguridad.

Gestión del ciber–riesgo

La gestión del ciber–riesgo se realizará en base a los lineamientos de la Política de Gestión Integral de Riesgos en lo que respecta a la identificación, evaluación y respuesta al riesgo, así como en lo relativo al ambiente de control interno, establecimiento de objetivos e información y comunicación detallados en el punto 5.2 Proceso de Gestión de dicha Política.

6. ROLES Y RESPONSABILIDADES

Comité de Riesgos de Directores:

- Aprobación de la estrategia de seguridad de la información y su política.
- Promover que los criterios establecidos en la Política General de Seguridad de la Información se consideren en la definición de nuevos proyectos y servicios.

Continuidad y Servicios TI, Transformación Digital, Analytics y Canales Remotos:

- Proponer los procedimientos específicos para el resguardo de los activos de información en formato digital y los controles operativos de los mismos.
- Informar e involucrar a la Subgerencia de Riesgos y Cumplimiento, en su rol de asesor, respecto a todos los nuevos proyectos o servicios que se encuentren en evaluación y/o definición, de tal forma de fortalecer el cumplimiento de los criterios de seguridad de la información.
- Mantener informados a la Subgerencia de Riesgos y Cumplimiento y al Jefe de Riesgo Operacional ante todo evento que impacte en la confidencialidad, integridad y disponibilidad de la información.
- Adoptar las medidas necesarias para resguardar los activos de información, contenidas en cualquier medio de almacenamiento.

Gerencia de Personas:

- Mantener actualizada y custodiada toda la información de los colaboradores que sea propiedad de la ACHS.
- Mantener informadas a las áreas de Mantención y Administración de Contratos Centrales y Área de Seguridad TI y SQA cada vez que exista una baja de algún colaborador o cambio de funciones o ubicación.

Administración y Servicios Generales:

- Proponer los procedimientos específicos para el acceso a las instalaciones y los controles operativos de los mismos, para todo colaborador ACHS o personal externo que ingrese a la ACHS.

- Adoptar las medidas necesarias para resguardar los activos físicos en conformidad a la clasificación de los activos de información.

Dueños de Proceso:

- Velar por el cumplimiento de la Política General de Seguridad de la Información y los procedimientos derivados de ésta.
- Realizar la identificación, definición y clasificación de los activos de información que generan, gestionan y/o almacenan en sus procesos, asegurando su adecuado resguardo y tratamiento, con el apoyo metodológico de la Subgerencia de Riesgos y Cumplimiento.
- Implementar los controles necesarios para resguardar y tratar adecuadamente los activos de información.
- Entregar a las áreas que correspondan los activos de información de los colaboradores bajo su dependencia que hayan dejado de prestar sus servicios a la ACHS.
- Informar e involucrar a la Subgerencia de Riesgos y Cumplimiento, en su rol de asesor, respecto a todos los nuevos proyectos o servicios que se encuentren en evaluación y/o definición, de tal forma de asegurar el cumplimiento de los criterios de seguridad de la información.

Subgerencia de Riesgos y Cumplimiento:

- Apoyar y reportar al Comité de Riesgos en lo relacionado al cumplimiento de la Política General de Seguridad de la Información.
- Custodiar la Política General de Seguridad de la Información, velando por su actualización.
- Brindar apoyo metodológico a los dueños de procesos para evaluar los riesgos asociados a la seguridad de la información.

Jefe de Gestión Integral de Riesgos:

- Tener a su cargo la actualización de la Política General de Seguridad de la Información, el control de su implementación y velar por su correcta aplicación.
- Ser asesor en materias de seguridad de la información para todas las áreas de la ACHS, donde sea necesaria su participación, tanto en nuevos proyectos como en servicios que serán entregados por la ACHS.
- Definir el o los marcos de trabajo respecto del cual se alineará y evaluará la implementación de prácticas relacionadas a Seguridad de la Información y Ciberseguridad.
- Establecer instancias de control o seguimiento permanente, de la identificación de brechas y la mejora continua implementada para el fortalecimiento de la seguridad de la información.

7. INFORMACIÓN Y COMUNICACIÓN

La periodicidad y forma de entrega de la información están contenidas en el capítulo 5.2 de la Política de Gestión Integral de Riesgos.

8. MONITOREO Y ADMINISTRACIÓN

Reporte y Escalamiento de Eventos

La Subgerencia de Riesgos y Cumplimiento, realizará un monitoreo permanente a los eventos reportados en la organización realizando el escalamiento, cada vez que se requiera, con los responsables y las áreas correspondientes según la materia y alcance de los mismos.

Gestión de incidentes

La gestión de incidentes operacionales corresponde a un proceso continuo de captura y revisión de los incidentes asociados a riesgo operacional, continuidad operacional y seguridad de la información ocurridos en la ACHS. Cada incidente detectado requerirá de acciones para el restablecimiento de las operaciones.

La Subgerencia de Riesgos y Cumplimiento administrará la Base de Incidentes y determinará aquellos que correspondan a Eventos de Riesgo Operacional (ERO), cuyos antecedentes serán informados al Comité de Directores de Riesgos y remitidos periódicamente a la SUSESO, dando cumplimiento a lo definido en el Compendio – Libro VII Aspectos Operacionales y Administrativos, en su Título VI, Letra B, Capítulo V Riesgo Operacional, y Título V, Letra D, Capítulo II Reporte de ciberincidentes.

Actualización

Esta política será actualizada cada tres años o cuando sea necesario producto de cambios normativos o en las prácticas de la organización.

Para llevar a cabo la actualización, el área especializada en gestión de riesgos debe realizar las siguientes actividades:

- Revisar y definir los potenciales cambios y actualizaciones a la política.
- Presentar la propuesta al Comité de Riesgos para su revisión y aprobación.

En la eventualidad de no presentar cambios, se considerará la última versión vigente.

No obstante lo anterior, el área especializada en gestión de riesgos informará anualmente sobre el estado de las políticas al Comité de Riesgos.

9. INFORMACIÓN DE CONTROL

Vigencia: 01.10.2022 hasta 30.09.2025

Versión: 8

Primera versión: 01.06.2014

Atención a necesidades específicas: (x) Si ( ) No

Registro de modificaciones:

Versión	Ítem modificado	Descripción resumida de modificación	Motivo	Fecha
8	5.5 Ciberseguridad	Incorporación de sección sobre Gestión del ciber-riesgo en referencia al punto 5.2 Proceso de Gestión de la Política de Gestión Integral de Riesgos.	Actualización	Septiembre 2022
8	6. Roles y Responsabilidades	Precisión sobre la aprobación de la presente Política la cual corresponde al Comité de Riesgos de Directores.	Actualización	Septiembre 2022
8	8. Monitoreo y Administración	Se actualiza sección incorporando actualización cada 3 años, con revisión anual a nivel del Comité de Riesgos de Directores.	Actualización	Septiembre 2022
7	4. Definiciones	Se complementan las definiciones según la Circular N° 3579 Gestión de la Seguridad de la Información.	Actualización	Junio 2021
7	6. Roles y Responsabilidades	Se amplía el alcance a las Gerencias de Transformación Digital, Analytics y Canales Remotos.	Actualización	Junio 2021
7	8. Monitoreo y Administración	Se incorpora sección Gestión de incidentes.	Actualización	Junio 2021
7	General	Correcciones en la redacción, precisiones conceptuales de acuerdo con lineamientos vigentes de la ACHS y ajustes de formato.	Actualización	Junio 2021

Responsables por el documento:

	Nombre del área
Elaboración	Subgerencia de Riesgo y Cumplimiento
Revisión	Gerencia División Planificación Estratégica y Control de Gestión
Aprobación	Comité de Riesgos de Directores

ANEXO N°1 – Glosario de Términos

Amenaza: Posible causa de un incidente no deseado, el cual puede ocasionar un daño a un sistema o una organización.

Análisis de riesgos: Utilización sistémica de la información disponible para identificar peligros y estimar los riesgos.

Ciberseguridad: Conjunto de acciones posibles para la prevención, mitigación, investigación y manejo de las amenazas e incidentes sobre los activos de información, datos y servicios, así como para la reducción de los efectos de los mismos y del daño causado antes, durante y después de su ocurrencia.

Ciberincidente: Todo evento que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y su infraestructura, que puedan afectar al normal funcionamiento de los mismos.

Confidencialidad: Adoptar las medidas necesarias que impidan la divulgación de información a individuos, entidades o procesos no autorizados. A su vez, asegurar que, en el ambiente interno del organismo administrador, sólo las personas autorizadas dentro de ésta tengan acceso a la información.

Continuidad de servicios: Adoptar las medidas que permitan proveer un nivel mínimo de servicio, entendiendo por esto las prestaciones propias del seguro, reduciendo el riesgo de eventos que puedan crear una interrupción o inestabilidad en las operaciones de la entidad hasta niveles aceptables y planificando la recuperación de los servicios de las tecnologías de la información (TI).

Control: Medio de gestión del riesgo, que incluye políticas, procedimientos, directrices, prácticas, o estructuras de la organización, y que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Directriz: Una descripción que clarifica lo que se debería hacer y cómo debería hacerse, para conseguir los objetivos establecidos en las políticas.

Disponibilidad: Adoptar las medidas necesarias que permitan que la información esté a disposición de quienes la necesitan, entendiendo por esto a trabajadores protegidos, pensionados, trabajadores de los organismos administradores, procesos o aplicaciones, Superintendencia de Seguridad Social y otras entidades con competencia en materias del Seguro de la Ley N° 16.744.

Evaluación del riesgo: El proceso general del análisis y estimación de los riesgos.

Gestión de incidentes: Procedimiento para la detección, análisis, manejo, contención y resolución de un incidente de ciberseguridad.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Integridad: Adoptar las medidas necesarias que aseguren que los datos están protegidos de modificaciones no autorizadas y que dichos datos mantienen exactitud respecto del origen de los mismos.

Normativa: Declaración expresa de reglas u orden, emitidas para el cumplimiento de quien le aplica.

Política de Seguridad de la Información: Documento que tiene por finalidad establecer los conceptos, principios y directrices generales de la gestión de la seguridad de la información aplicable a la ACHS.

Procedimiento: Conjunto de actividades coordinadas que se llevan a cabo sobre un proceso para lograr su objetivo, es decir, planear, controlar y mejorar aquellos procesos de una organización que influyen en logro del objetivo y en los resultados deseados por la organización.

Proceso: Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un determinado fin.

Protección de los activos de información: Adoptar las medidas que resguarden la seguridad física de los dispositivos, así como los accesos a éstos. Se entenderá por infraestructura crítica las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción

pueden tener una repercusión importante en los trabajadores protegidos, pensionados, empresas adherentes o afiliadas y en las prestaciones preventivas, médicas y económicas que debe brindar el seguro.

Recursos de tratamiento de la información: Cualquier sistema, servicio o infraestructura de tratamiento de la información, o bien las localizaciones físicas que alojan dicho sistema, servicio o infraestructura.

Riesgo: Combinación de la probabilidad de un suceso y de su ocurrencia.

Seguridad de la información: La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como autenticidad, la responsabilidad, la fiabilidad y el no repudio.

Sistema de Gestión de Seguridad de la Información: La parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Conjunto de medidas preventivas y reactivas de los organismos administradores y sus respectivos sistemas tecnológicos, que tienen por objeto resguardar y proteger la información, asegurando la confidencialidad, integridad, autenticidad y disponibilidad de los datos, continuidad de servicios y protección de activos de información.

Terceros: Aquellas personas o entidades que está reconocida como independiente de las partes implicadas para el asunto en cuestión.

Tratamiento de riesgos: El proceso de selección e implementación de las medidas encaminadas a modificar los riesgos.

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

ANEXO N°2

Norma ISO 27002:2013.

La ISO 27002 es una guía de recomendaciones de buenas prácticas para la gestión de seguridad de la información.

Para lo anterior, se definen para su selección un total de 114 controles generales de seguridad a partir de 35 objetivos de control estructurados en 14 dominios, 4 de ellos técnicos, 9 de gestión y 1 de seguridad física. A continuación, se presenta un resumen de éstos.

a) Política de seguridad de la información: Toda organización, debe definir un conjunto de políticas que traten las materias de seguridad de la información. Dichas políticas, deberían ser aprobadas por el Directorio, antes de ser publicadas y comunicadas a los colaboradores y a todas las partes externas interesadas.

b) Organización de la seguridad de la información: Se deben definir y asignar todas las responsabilidades de seguridad de la información dentro de la organización. Dicha asignación de responsabilidades deberá estar de acuerdo con la política establecida y aprobada por el Directorio.

c) Seguridad de recursos humanos: Se deben establecer controles que permitan garantizar que, en todo momento, tanto los colaboradores, como contratistas, estén enterados de sus responsabilidades y acuerdos contractuales, que deben cumplir hasta, en algunos casos, luego de dejar de prestar sus servicios en la organización.

d) Administración de activos de información: Se deben identificar los activos asociados a la información y las instalaciones donde es procesada la información, debiendo elaborar y mantener inventarios de estos activos con su ubicación.

e) Control de acceso lógico: Se deberán implementar controles de acceso lógicos en base a los requisitos de la organización y de la seguridad de la información.

f) Criptografía: Se deben desarrollar e implementar controles tendientes a encriptar la información considerada crítica o sensible para la organización, con el fin de proteger la confidencialidad, autenticidad y/o integridad de la información.

g) Seguridad física y ambiental: Se deben establecer perímetros de seguridad físicos, para proteger las áreas y las instalaciones que procesan información consideradas sensibles para la organización.

h) Seguridad de las operaciones: Se deben mantener documentados todos los procesos considerados críticos o que generen información sensible para la organización de tal forma de garantizar las operaciones que se ejecuten de forma correcta y segura, obteniendo información integra y confiable.

i) Seguridad en las comunicaciones: Se deben establecer controles que permitan administrar de forma segura, las redes de comunicación de la organización, protegiendo la información que transita por estos canales.

j) Adquisición, desarrollo y mantenimiento de sistemas: Se debe garantizar que la seguridad de la información sea parte integral de los sistemas de información en todo su ciclo de vida.

k) Relación con los proveedores: Se deben establecer controles tendientes a proteger todos los activos de información a que tengan acceso los proveedores y que sean de propiedad de la organización.

l) Administración de incidentes de seguridad de la información: Se deben establecer controles que permitan garantizar un enfoque coherente y eficaz en la administración de incidentes de seguridad de la información.

m) Aspectos de la seguridad de la información en la administración de la continuidad operacional: Se deben determinar los requisitos necesarios para mantener la seguridad de la información ante situaciones adversas (o de contingencias).

n) Cumplimiento de leyes, políticas, y procedimientos en materias de seguridad de la información: Se deben establecer controles que garanticen el cumplimiento de las obligaciones legales, normativas o contractuales relacionadas con la seguridad de la información.