POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

60 AÑOS 1961 2021 ENAC caritas
Centro de Formación Técnica

1 • INTRODUCCIÓN

El presente documento entrega las directrices de organización, roles y responsabilidades para gestionar la Seguridad de la Información, incluida la Ciberseguridad, y es parte del Modelo de Seguridad de la Información y Ciberseguridad de ENAC, todo de acuerdo a los principios institucionales de integridad, transparencia y responsabilidad.

2 • OBJETIVOS

El propósito de la "Política General de Seguridad de la Información y Ciberseguridad", es declarar la posición de ENAC con respecto al buen uso de los activos de información corporativos. Esto se traduce en:

2.1 Definir lineamientos o principios generales que sirven de medio para alcanzar los objetivos de un Sistema de Seguridad de la Información y Ciberseguridad.

2.2 Establecer responsabilidades aplicables a los distintos niveles jerárquicos y a todo el personal vinculado al CFT ENAC.

2.3 Fijar directrices sobre las cuales se sustenten normativas e instructivos de seguridad que desarrollen con mayor grado de detalle aspectos relativos a la seguridad de un tema particular o sistema en específico.

2.5 Definir plazos y periodicidad para su revisión y evaluación de cumplimiento.

2.6 Entregar las directrices para conformar estructuras organizacionales, roles y responsabilidades que permitan gestionar la Seguridad de la Información y Ciberseguridad dentro de ENAC, en forma oportuna y adecuada.

2.7 Definir lineamientos para la clasificación de los Activos de Información de acuerdo con su criticidad, sensibilidad, importancia y propiedad, entre otros factores, que permitan definir e implementar controles para su resguardo y tratamiento.

2.8 Definir lineamientos en relación a las responsabilidades sobre el riesgo y el buen uso, o uso aceptable, de los Activos de Información.

3 • ALCANCE O CAMPO DE APLICACIÓN

La presente Política establece un marco regulatorio aplicable a todas las personas que trabajen en ENAC, ya sea bajo el Código del Trabajo, servicios a honorarios, estudiantes en práctica o personas externas que presten servicios permanentes o temporales, así como también a proveedores, contratistas y personal que esté vinculado y que preste servicios en ENAC o que esté relacionado con él.

También es aplicable a todo activo de información que la organización posea en la actualidad o en el futuro, asociado a los procesos de negocio de ENAC, de manera que la no inclusión explicita en el documento, no constituye argumento para no proteger estos activos de información. La política cubre toda la información impresa o la escrita en papel, la almacenada electrónicamente, la transmitida por correo o usando medios electrónicos, mostrada en video o hablada en una conversación, entre otras formas de información.

4 • DIRECTRICES

El objetivo general de la Seguridad de la Información y Ciberseguridad corresponde a lograr niveles adecuados de integridad de la información, confidencialidad y disponibilidad para los activos de información que sean relevantes para la institución.

Integridad de la información: la información no puede ser alterada ni eliminada por cambios no autorizados o accidentales. Este principio fundamental de seguridad busca garantizar la precisión, suficiencia y validez de la información, métodos de procesamiento y todas las transacciones, de acuerdo con los valores y expectativas de la institución, así como, evitar fraudes o irregularidades de cualquier índole que haga que la información sea alterada.

Confidencialidad de la información: la información sólo debe ser conocida por el personal que la requiera para el desarrollo de sus funciones. Este principio fundamental de seguridad busca garantizar que toda la información de los ciudadanos, funcionarios y proveedores; y sus medios de procesamiento o conservación esténprotegidos del uso no autorizado o divulgación accidental, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran poner en riesgo dicha información.

Disponibilidad de la información: la información debe estar disponible para el personal, usuarios y entidades reguladoras de manera oportuna y acorde a sus niveles de autorización. Este principio fundamental de seguridad busca garantizar que los usuarios autorizados tengan acceso a la información cuando esta es requerida por el proceso de la institución. Para ello se debe procurar que la información y la capacidad de procesamiento sean resguardados y puedan ser recuperados en forma rápida y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento o equipamiento de procesamiento.

Todo Activo de Información está expuesto a riesgos y amenazas dinámicos, que pueden provenir desde dentro o como fuera de la organización, y pueden ser intencionales o accidentales. Por ello, es importante gestionar adecuadamente los Activos de Información de la organización, alineados con los objetivos estratégicos de la actividad de ENAC.

5 • CUMPLIMIENTO

El cumplimiento de esta Política, políticas específicas y procedimientos, u otros documentos que se deriven, deberá ser una tarea cotidiana y de estricta aplicación por parte de todo el personal de ENAC.

Ante cualquier incumplimiento o violación del contenido del presente documento y sus normas complementarias, ya sea parcial o total, el coordinador de Seguridad de la Información deberá comunicarlo a la Comisión de Seguridad de la Información y Ciberseguridad.

Es importante señalar, que ENAC ejercerá las acciones disciplinarias y legales cuando corresponda, en contra de quienes no cumplan con lo estipulado en esta Política, normativas, procedimientos y/o documentos que se desprendan de ella. Por lo tanto, ENAC aplicará las sanciones establecidas en su Reglamento Interno de Orden, Higiene y Seguridad, para el caso de sus docentes y colaboradores, y las sanciones establecidas en cada uno de los contratos, cuando corresponda a un tercero.

Es responsabilidad de la Comisión de Seguridad de la Información y Ciberseguridad (Comisión SIC) y del Coordinador de Seguridad de la Información (CSI), como estructura organizacional definida al efecto, cumplir y hacer cumplir lo señalado en esta Política específica, en cuanto a gestionar la Seguridad de la Información en forma adecuada de acuerdo a sus respectivos roles y responsabilidades y en concordancia con lo señalado en la Política General de Seguridad de la Información y Ciberseguridad definida por ENAC y con los intereses institucionales.

6 • DEFINICIONES

6.1 Modelo de Seguridad de la Información (MSI): es el conjunto de políticas y normas de Seguridad de la Información que definen y describen el diseño de los controles de seguridad de la información, basados en las normas ISO 27001, ISO 27002 e ISO 27032, que se aplican, o se aplicarán, en ENAC.

6.2 Política: directriz u orientación general expresada formalmente por la Administración ENAC.

6.3 Norma: disposición de carácter general que se desprende de las políticas, estableciendo obligaciones, restricciones, prohibiciones u otras conductas esperadas.

6.4 Activo de Información: aquello que tiene valor y es importante para ENAC, sean documentos, sistemas o personas. Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. Se distinguen tres niveles:

a) La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.).

b) Los equipos, sistemas e infraestructura que soportan o contienen esta información.

c) Las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

6.5 Colaborador: toda persona que tenga un vínculo contractual con ENAC, sea éste indefinido, a plazo fijo o a honorarios.

6.6 Procedimiento: sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles, en este caso, de Seguridad de la Información.

6.7 Riesgo: es la posibilidad que ocurra un evento que afecte adversamente el logro de los objetivos de ENAC. Se mide combinando las consecuencias del evento (impacto) y su probabilidad de ocurrencia.

6.8 Amenaza: causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o proceso.

6.9 Vulnerabilidad: debilidad de un activo o grupo de activos que puede ser materializada por una o más amenazas.

6 • DEFINICIONES

6.10 Evento de Seguridad de la Información: actividad o serie de actividades sospechosas que amerita ser analizada desde la perspectiva de la Seguridad de la Información.

6.11 Incidente de Seguridad de la Información: evento o serie de eventos de Seguridad de la Información, no deseados o inesperados, que compromete la Seguridad de la Información y amenaza la operación del negocio.

6.12 Confidencialidad de la información: propiedad de la información que determina que sólo podrá ser accedida por personas, entidades o procesos debidamente autorizados. Es un principio fundamental de esta Política.

6.13 Integridad de la información: propiedad de la información según la cual sólo puede ser modificada, agregada o eliminada por las personas o sistemas autorizados para cada proceso, de tal forma de salvaguardar la exactitud y completitud de los activos de información. Es un principio fundamental de esta Política.

6.14 Disponibilidad de la información: propiedad de la información según la cual es accesible y utilizable oportunamente por las personas o sistemas o procesos autorizados, en el formato requerido para su procesamiento. Es un principio fundamental de esta Política.

6.15 Comisión de Seguridad de la Información y Ciberseguridad: conjunto de personas de nivel directivo que tiene la responsabilidad de que la Seguridad de la Información se gestione de acuerdo con las políticas aprobadas por ENAC.

6.16 Coordinador de Seguridad de la Información (CSI): persona calificada que tiene la responsabilidad sobre la gestión de la Seguridad de la Información en las operaciones de ENAC, que depende y que opera estrechamente coordinado con la Comisión de Seguridad de la Información y Ciberseguridad.

6.17 Uso aceptable del Activo: Se refiere a las reglas de uso que debe respetar todo colaborador o personal externo con acceso a Activos de Información de ENAC, con el fin de no poner en riesgo la confidencialidad, integridad y disponibilidad de dichos activos, y con ello, proteger a los colaboradores y a la Institución de perjuicios derivados por el uso inapropiado de estos.

7 • CLÁUSLA DE LA POLÍTICA

7.1 Enunciado de la política.

ENAC reconoce la información como un activo clave, por lo que asume la responsabilidad de implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información y Ciberseguridad (SGSIC) que preserve niveles adecuados de integridad de la información, confidencialidad y disponibilidad para todos los activos de información institucionales.

7.2 De la información interna.

La información es un activo vital, por lo que su utilización, es decir, accesos, procesamiento y mantenimiento deberán ser consistentes con lo instruido en las políticas, normas, y procedimientos emitidos por ENAC en cada ámbito en particular.

La información debe ser protegida, por sus custodios, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de Seguridad de la Información y Ciberseguridad, sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información. A este conjunto de políticas y normas se le llamará también "Modelo de Seguridad de la Información y Ciberseguridad".

Toda información creada o procesada por la institución debe ser considerada como "interna", a menos que se determine expresamente lo contrario. ENAC proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo con sus funciones así lo requiera. Sin embargo, se reserva el derecho de revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameritan.

7.3 De la información de los usuarios externos.

Si la institución procesa y mantiene información de usuarios externos que sean datos personales y/o sensibles de acuerdo con la normativa vigente, la institución se compromete a asegurar que esta información no será divulgada sin previa autorización y estará protegida de igual manera que la información interna, de conformidad a lo establecido en la Ley N°19.628, Sobre Protección A La Vida Privada, sin perjuicio de lo señalado en la Ley N°20.285.

En el caso de información de usuarios externos que se procese, mantenga y que no tenga las características anteriormente mencionadas, está podrá ser divulgada sin previa autorización.

Si se requiere compartir información de los usuarios externos de ENAC con instituciones externas, con motivo de externalizar servicios, a estas se les exigirá un contrato, clausula y/o convenio de confidencialidad y no divulgación previa a la entrega de la información.

7.4 De las auditorías.

Con el fin de velar por el correcto uso de los activos de información, ENAC se reserva el derecho de auditar en cualquier momento el cumplimiento de las políticas y documentos vigentes que digan relación con el acceso y uso que los usuarios hacen de los activos de información.

Las auditorías podrán ser realizadas internamente o por auditorías a cargo de organizaciones externas, cuando sea pertinente y requerido por el Coordinador de Seguridad de la Información, en coordinación con la Comisión de Seguridad de la Información y Ciberseguridad.

7.5 De la gestión de la seguridad de la información y ciberseguridad.

La gestión de la seguridad de la información y ciberseguridad se realizará mediante un proceso sistemático, documentado y conocido por la institución. Este proceso de gestión deberá ser aplicado a los procesos de negocio críticos de la institución.

7 • CLÁUSULA DE LA POLÍTICA

El cumplimiento de los objetivos del sistema de gestión de ENAC se basará en la identificación de los activos de información involucrados en los procesos de negocio críticos, lo que implica al Coordinador de Seguridad de la Información, junto a los responsables de los diferentes procesos y subprocesos de las actividades de ENAC, realizar las siguientes acciones fundamentales:

a) Identificar y clasificar los activos de información involucrados.

b) Para cada activo de información, identificar un responsable.

c) Analizar el riesgo al cual están expuestos.

d) Difundir en forma planificada entre todo el personal de la institución el objetivo corporativo de la preservación de la información, sus características y las responsabilidades individuales para lograrlo, inserto esto, en planes de capacitación anual de la institución como actividades permanentes y en el proceso de inducción del nuevo personal.

7.6 Deberes del personal y de terceros.

a) La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados con el servicio y autorizados por la jefatura directa, debiéndose aplicar criterios de buen uso en su utilización.

b) Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.

c) El personal está en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política según procedimientos que se establezcan en el manejo de incidentes.

d) Se prohíbe la divulgación de información que esté considerada o clasificada como "reservada".

7.7 De la Estructura Organizacional.

La estructura organizacional que define ENAC para gestionar la Seguridad de la Información y Ciberseguridad es por medio de una Comisión de Seguridad de la Información y Ciberseguridad y de una persona encargada de la Seguridad de la Información en las operaciones cotidianas de la organización denominada Coordinador de Seguridad de la Información ("CSI"), que reporta y apoya a la referida Comisión, Comisión que dependerá de Rectoría y estará compuesta por las siguientes personas: el Rector, el Vicerrector de Administración y Finanzas, el Vicerrector Académico, El Secretario General, el Director de Tecnologías de la Información y el Coordinador de Seguridad de la Información.

7.8 De la Comisión de Seguridad de la Información y Ciberseguridad.

La Comisión de Seguridad de la I mación y Ciberseguridad de ENAC, en su calidad de tal, es responsable de difundir, impulsar y apoyar el desarrollo del "Modelo de Seguridad de la Información y Ciberseguridad", como asimismo de la revisión de la "Política General de Seguridad de la Información y Ciberseguridad" y sus modificaciones, y demás Políticas y Procedimientos asociados.

7.9 Del Coordinador de Seguridad de la Información.

El Coordinador de Seguridad de la Información de ENAC, es el responsable directo de ejecución oportuna y correcta de los criterios de Seguridad de la Información y Ciberseguridad de la institución.

7.10 De los colaboradores.

Los colaboradores de ENAC tienen la responsabilidad de cumplir con cada una de las políticas, normativas, procedimientos, instructivos, etc., que se definan en el Modelo de Seguridad de la Información y Ciberseguridad, y aplicarlo en su entorno laboral.

Además, tienen la obligación de alertar de manera oportuna y adecuada cualquier incidente que atente contra la seguridad de los activos de información, de acuerdo con el procedimiento establecido para estos fines.

7.11 De terceras partes.

Las terceras partes, en lo relativo a la información que obtengan a través de ENAC, deberán asumir la responsabilidad de cumplir con las políticas, normativas y procedimientos que se definan en el Modelo de Seguridad de la Información y Ciberseguridad de ENAC y aplicarlo en la relación de que se trate, debiendo establecerse formalmente esta responsabilidad en los contratos escritos con terceros.

7.12 Identificación de Activos de Información

ENAC deberá identificar sus Activos de Información y deberá mantener por medio de un inventario debidamente documentado, la información de la existencia, vigencia y clasificación de los mismos.

7.13 Propiedad de los Activos

Todos los Activos de Información de ENAC deberán ser asociados a un dueño designado por la organización, ya sea por un proceso operativo determinado, por un conjunto definido de actividades, por un aplicativo o por un conjunto específico de datos. El dueño del Activo de Información será también dueño del riesgo de éste.

7.14 Clasificación de Información

ENAC reconoce que su información tiene distintos grados de criticidad y sensibilidad, de modo que la clasifica en términos de su valor, riesgos y requisitos legales específicos.

La clasificación adoptada por ENAC debe permitir conocer la necesidad, las prioridades y el grado de protección esperado en el manejo de la información.

En tal sentido, se distinguirán las siguientes categorías:

- Información Pública: Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea colaborador de ENAC o no.

- Información Interna: Información que puede ser conocida y utilizada por todos los colaboradores de ENAC , y algunas entidades externas debidamente autorizadas.

- Información Restringida: Información que sólo puede ser conocida y utilizada por un grupo de colaboradores de ENAC que la necesiten para realizar su trabajo.

- Información Confidencial: Información que sólo puede ser conocida y utilizada por un grupo muy reducido de colaboradores de ENAC, generalmente de la Alta Dirección.

7.14.1 Criterios de Clasificación de la Información

Clasificación	Criterio de Clasificación	Restricción de acceso
Información Pública	Hacer pública la información no puede dañar a la reputación de la organización de ninguna forma.	Puede ser entregada al público en general.
Información Interna	El acceso, divulgación o uso no autorizado podría ocasionar daños o pérdidas leves para la organización o a terceros.	La información está disponible para todos los colaboradores y terceros seleccionados. Esta información puede ser entregada a otros terceros, sólo con autorización del Dueño del Activo.
Información Restringida	La divulgación o uso no autorizados de la información podría ocasionar pérdidas significativas a la organización o a terceros.	La información está disponible solamente para un grupo específico de colaboradores y de terceros autorizados.
Información Confidencial	Información altamente sensible, de uso exclusivamente interno. Su divulgación podría implicar un impacto no deseado para la organización.	La información está disponible solamente para un grupo específico de colaboradores, que ejercen funciones definidas en la organización.

7.15 Clasificación

ENAC deberá clasificar los activos físicos y digitales, según corresponda, de acuerdo con lo señalado en el punto 7.14.

7.16 Manejo e Intercambio

Para cada nivel de clasificación, se deben definir procedimientos para el manejo e intercambio de la información. Tales procedimientos deben considerar, entre otros aspectos, los posibles cambios de estado excepcionales por los que pasa un activo al ser utilizado, en especial cuando deba autorizarse su entrega a terceros a pesar de su clasificación interna, restringida o confidencial.

Asimismo, debe generarse un inventario de aquella información confidencial sobre la que existe algún acuerdo de intercambio de información con terceros.

En caso de una interrupción de la continuidad operacional, los procedimientos de recuperación deben considerar, entre otros aspectos, los mismos controles aplicados cotidianamente según la clasificación (interna, restringida o confidencial) de los Activos de Información involucrados en el incidente.

7.17 Uso debido o aceptable de los Activos de Información

ENAC establecerá de forma clara y documentada a través de la Rectoría y Direcciones de áreas las reglas de uso debido o aceptable de los Activos. Sin perjuicio de ello, a continuación, se señalan las directrices que ENAC considera relevantes en este sentido:

7.17.1 Uso General y Propiedad

- La información propiedad de ENAC almacenada en dispositivos electrónicos e informáticos ya sea propietarios o arrendados por la organización, de un colaborador o de un tercero, sigue siendo propiedad exclusiva de ENAC. Todo colaborador debe asegurarse a través de medios legales y/o técnicos de que la información propietaria está protegida en conformidad con los estándares de protección de datos chilenos.

- El colaborador tiene la responsabilidad de realizar en todo momento sus respaldos de información con las herramientas establecidas y habilitadas por la Dirección de Tecnologías de la Información.

- Todo colaborador tiene la responsabilidad de reportar de inmediato sobre un robo, pérdida o divulgación no autorizada de información propietaria de ENAC.

- Todo colaborador puede acceder, usar o compartir información propiedad de ENAC, en la medida en que esté autorizado y sea necesario para cumplir con sus funciones asignadas de trabajo.

- Los colaboradores son responsables de ejercer un buen juicio sobre el uso de aplicaciones de interés personal. La Rectoría y Direcciones de áreas de forma individual son responsables de la creación de guías referentes al uso de sistemas de interés personal en Internet / Intranet / Extranet. En ausencia de tales guías, los colaboradores deben siempre consultar a su Jefatura Directa.

- Por razones de seguridad y mantención de la red, existirán colaboradores autorizados dentro de la institución que podrá monitorear equipos, sistemas y el tráfico de red en cualquier momento. Sin perjuicio de ello, ENAC se reserva el derecho de auditar las redes y sistemas de manera periódica para asegurar el cumplimiento de esta cláusula.

7.17.2 Seguridad de Información Propietaria

- Todos los dispositivos móviles y estaciones de trabajo que se conectan a la red interna deben cumplir con las disposiciones pertinentes de las políticas y procedimientos internos que fueren aplicables, en particular, las Políticas de Tecnologías de la Información y Comunicaciones.

- Las contraseñas a nivel de sistema y a nivel de usuario deben cumplir con las disposiciones pertinentes de las políticas y procedimientos internos que fueren aplicables, en particular, las Políticas de Tecnologías de la Información y Comunicaciones. Está prohibido facilitar el acceso a otros individuos, ya sea deliberadamente o por error.

- Todos los dispositivos informáticos deben asegurarse y protegerse por contraseña de acuerdo con las disposiciones pertinentes de las políticas y procedimientos internos que fueren aplicables, en particular, las Políticas de Tecnologías de la Información y Comunicaciones.

- Cualquier publicación de información realizada por colaboradores utilizando o asociada a una dirección de correo electrónico de ENAC a medios periodísticos, foros, redes sociales, etc., debe contener una advertencia que indique que las opiniones expresadas son estrictamente personales y que no representan necesariamente las de ENAC, a menos que las publicaciones formen parte de sus labores en la organización.

- Los colaboradores deben extremar precauciones al abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos, que pueden contener software malicioso.

7.17.3 Uso Inaceptable

Bajo ninguna circunstancia un colaborador de ENAC está autorizado a participar en actividades que sean ilegales bajo las leyes locales o internacionales, utilizando recursos de la organización.

La lista a continuación, no siendo exhaustiva, intenta proporcionar un marco para las actividades que entran en la categoría de uso inaceptable y que, en consecuencia, está prohibido:

- Violaciones a los derechos de cualquier persona o institución protegida por derechos de autor, secretos de marca, patentes u otra propiedad intelectual o a leyes o reglamentos similares, incluyendo, pero no limitado a la instalación o distribución de software "pirata" (sin licencia autorizada) u otros productos de software que no tengan licencia apropiada para su uso en la organización.

- La copia no autorizada de materiales con derechos de autor, incluyendo, pero no limitado a la digitalización y distribución de fotografías de revistas, libros u otras fuentes con derechos de autor, la música con derechos de autor y la instalación de software con derechos de autor para el cual la institución o el usuario final no cuenta con una licencia activa.

- El acceso a datos, servidores o cuentas para cualquier propósito que no sea para la realización de actividades propias de ENAC, incluso si cuenta con acceso autorizado.

- Introducción de programas maliciosos en la red o en servidores (por ejemplo, virus, gusanos, caballos de Troya, spam de correo electrónico, etc.).

- Dar contraseñas de sus cuena a otras personas o permitir el uso de sus cuentas por otros. Esto incluye a amigos y familiares cuando el trabajo se está haciendo en casa.

- El uso de un computador de la institución para participar, reclutar o transmitir materiales que están en violación de las leyes de acoso sexual y laborales.

- Hacer ofertas de productos, artículos o servicios de propiedad de la institución, sin la autorización expresa para ello por parte de ENAC.

7 • CLÁUSULA DE LA POLÍTICA

- Efectuar brechas de seguridad o interrupciones de la comunicación en red. Las violaciones de seguridad incluyen, pero no se limitan a acceder a datos para los que no se es destinatario o conectarse a un servidor o cuenta a la cual el colaborador no está expresamente autorizado a acceder, a menos que estas funciones estén dentro del alcance de sus funciones regulares. Para los propósitos de esta sección, "interrupción" incluye, pero no se limita al espionaje en la red, mapeo de red, suplantación de paquetes de información, denegación de servicios, etc., con fines maliciosos.

- El barrido de puertos y escaneos de seguridad están expresamente prohibidos a menos que se realice una notificación y autorización previa ante la Comisión de Seguridad de la Información y Ciberseguridad.

- La ejecución de cualquier forma de análisis de red que intercepte datos no destinados al equipo del colaborador, a menos que esta actividad sea parte del trabajo normal de este.

- Eludir la autenticación de usuarios y la seguridad de cualquier computadora, de red o cuenta.

- Interferir o negar servicios a cualquier usuario diferente a el mismo (por ejemplo, ataque de denegación de servicio).

- El uso de cualquier programa / script / comando o el envío de mensajes de cualquier tipo, con la intención de interferir o deshabilitar las sesiones de terminal de algún usuario, a través de cualquier medio, de forma local o a través de Internet / Intranet / Extranet.

- Proporcionar información sobre colaboradores, estudiantes, profesores, proveedores o listas de los mismos a externos.

- La utilización de cualquier dispositivo de almacenamiento masivo tales como memorias USB, discos duros, etc., no autorizado expresamente por la Dirección de Tecnologías de la Información.

- La extracción de información propiedad de ENAC utilizando cualquier medio, que no esté relacionada con las labores normales de trabajo del colaborador.

- El acceso a sitios Web de dudosa reputación o potencialmente peligrosos, tales como de sitios de pornografía, malware, piratería, proxy, etc.

7.17.4 En Correo Electrónico y otras comunicaciones

Al utilizar recursos de la institución para acceder y utilizar el Internet, los colaboradores y usuarios en general, deben tener siempre presente que involucran a ENAC. En consecuencia, se prohíbe lo siguiente:

- Envío de mensajes de correo electrónico no solicitados, incluyendo el envío de "correo basura" u otro material publicitario a personas que no hayan solicitado específicamente dicho material (correo electrónico no deseado).
- Cualquier forma de acoso a través de correo electrónico, teléfono u otro medio, ya sea a través del lenguaje, frecuencia o tamaño de los mensajes.
- El uso no autorizado o la alteración del contenido de encabezados de correo electrónico.
- Solicitar por correo direcciones de correo electrónico a cualquier persona, con la intención de acosar o para recolectar información.
- Crear o reenviar "cadenas de correo" o esquemas similares de cualquier tipo.
- El uso de correo electrónico no solicitado procedente desde dentro de las redes de la institución o por sus proveedores de servicios de Internet / Intranet / Extranet a nombre de la misma, para hacer publicidad o por cualquier servicio hospedado por la Institución o conectado vía red de la institución.
- La publicación repetida de los mismos mensajes o similares, no relacionados con las actividades de ENAC a un gran número de grupos de noticias de foros, blogs, redes sociales, etc.

7.17.5 En Blogs y otros medios sociales

- Hacer publicaciones en blogs o redes sociales por los colaboradores, ya sea utilizando computadoras, sistemas u otras personas de la institución, también está sujeto a los términos y restricciones establecidas en la presente Política.

- Los colaboradores tienen prohibido revelar cualquier información confidencial o propietaria, secretos comerciales o cualquier otro material confidencial esto incluye cuando se participa en los blogs y redes sociales.

- Los colaboradores no podrán participar en ningún blog o red social que pueda dañar o ensuciar la imagen, reputación y/o buena voluntad de la institución y/o cualquiera de sus colaboradores. Los colaboradores también tienen prohibido hacer cualquier comentario de discriminación.

- Los colaboradores tampoco pueden atribuir las declaraciones personales, opiniones o creencias a la institución cuando participan en los blogs y redes sociales.

Además de respetar todas las leyes referentes al manejo y la divulgación de materiales con derechos de autor o de exportación controlada, las marcas registradas, logotipos y cualquier otro material que sea propiedad intelectual de La institución tampoco podrá ser utilizada en ninguna actividad de los blogs y redes sociales.

7.18 Revisión de la Política.

Una de las tareas a realizar por la Comisión de Seguridad de la Información y Ciberseguridad de ENAC, es la reevaluación de la Política General de la Seguridad de la Información y Ciberseguridad. Esto deberá realizarse por lo menos una vez al año o ante cualquier cambio significativo de tecnología, personal o evento que amerite su reevaluación para asegurar continuidad, idoneidad, eficiencia y efectividad.

7.19 Difusión de la Política.

Las Autoridades de ENAC consideran fundamental integrar en la cultura organizacional, la existencia de un plan formal de difusión, capacitación y sensibilización en torno a la Seguridad de la Información y Ciberseguridad.

7.20 Documentación de Seguridad de la Información y Ciberseguridad.

La documentación de Seguridad de la Información de ENAC es la siguiente:

- Modelo de Seguridad de la Información, compuesto por la Política que define el diseño de los controles de seguridad de la información que se implementarán en la organización.
- Procedimientos, que describen las actividades y tareas relacionadas con los controles de seguridad implementados.

7.21 Procedimientos de Seguridad de la Información y Ciberseguridad.

Los procedimientos que describen las actividades y tareas operativas relacionadas con los controles de seguridad son los siguientes:

- SEG-PRC-001 Procedimiento de Teletrabajo y Uso Dispositivos Móviles
- SEG-PRC-002 Procedimiento de Gestión de Equipos y Medios Móviles y BYOD
- SEG-PRC-003 Procedimiento de Control de Acceso
- SEG-PRC-004 Procedimiento de Gestión de Cuentas y Accesos
- SEG-PRC-005 Procedimiento Seguridad de Identificación y Autenticación de Usuarios
- SEG-PRC-006 Procedimiento de Pantallas y Escritorios Limpios
- SEG-PRC-007 Procedimiento de Gestión de Respaldo de la Información
- SEG-PRC-008 Procedimiento de Gestión de Vulnerabilidades Técnicas
- SEG-PRC-009 Procedimiento Correo Electrónico y Mensajería Instantánea
- SEG-PRC-010 Procedimiento de Recuperación de Incidentes (DRP)

7.22 Documentación de referencia.

Se considerará como documentación de referencia para la presente Política, toda la normativa vigente en Chile a esta fecha, a saber:

- Ley N°17.336, sobre Propiedad Intelectual.
- Ley N°19.223 que tipifica figuras penales relativas a la informática.
- Ley N°19.628, sobre Protección a la Vida Privada.
- Ley N°20.285, sobre Acceso a la Información Pública.
- Ley N°19.799 sobre Documentos electrónicos, Firma electrónica y Servicios de Certificación de dicha firma.
- Decreto Supremo N°83 de 2004, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Norma NCh- ISO 27001:2013.
- Norma NCh- ISO 27002:2013.
- Norma NCh- ISO 27032:2012.

8 • GOBERNABILIDAD

La aprobación de la presente política está a cargo del Comité de Rectoría del Centro de Formación Técnica de ENAC. Cualquier modificación deberá ser aprobada por este mismo órgano.

La vigilancia y actualización de esta política será responsabilidad de la Dirección de Tecnología de la institución.

9 • DIVULGACIÓN Y ACTUALIZACIÓN

La presente política se divulgará a los Miembros del Comité de Rectoría, Directivos, Colaboradores, Docentes y proveedores que gestionen información de la institución.

Se actualizará de acuerdo con los cambios organizacionales, disposiciones legales u otros aspectos que puedan afectar los lineamientos aquí establecidos.

A su vez, se establecerán reuniones anuales de los responsables mencionados en esta política con el objetivo de establecer cambios en los niveles de protección y evaluar opciones de gestión de riesgo de seguridad de la información y ciberseguridad.

10 • REVISION DE POLITICAS (Historial de ajustes)

Preparado por:	Revisado por:	Aprobado por:
Gustavo Igor Pablo Sanhueza	Comité de Rectoría	Comité de Rectoría
13/04/2022		

60 AÑOS 1961 2021

ENAC caritas

Centro de Formación Técnica

enac.cl