Expertos en educación online

SISTEMA DE ASEGURAMIENTO INTERNO DE LA CALIDAD

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Información Pública

Comisión Nacional de Acreditación CNA-Chile

INSTITUTO PROFESIONAL
IACC ACREDITADO
- NIVEL AVANZADO
- GESTIÓN INSTITUCIONAL
- DOCENCIA DE PREGRADO

4 Años (junio 2026)

INTRODUCCIÓN

Toda acción que de manera preventiva o reactiva busque resguardar y proteger la información es parte de lo que se entiende por seguridad de la información. La cantidad de datos e información que son compartidos por medio de tecnología de la información son sumamente altos en una institución que dicta sus programas académicos en modalidad cien por ciento online y que realiza toda su operatividad de manera remota con sus colaboradores en jornadas home office, es por esto que IACC requiere del desarrollo de una estructura fuerte y especifica que genere el poder realizar la operatividad sin necesidad de sentir que se es vulnerable o que se están asumiendo demasiados riesgos.

IACC desarrolla la seguridad de la información no solo pensando en la información institucional, sino también en la de estudiantes, docentes, colaboradores, y de todos aquellos que interactúan con datos en sus sistemas, plataformas, entre otros. La conciencia y conocimiento respecto a lo sensible que es la información que está disponible en la red, es una preocupación transversal y por la que se trabaja para poder entregar el máximo de resguardo a la privacidad.

IACC por medio del desarrollo de acciones que generan seguridad de la información, orienta su aplicación a la disponibilidad de la información, es decir asegurar acceso a la información institucional cuando es requerida, confidencialidad el acceso a información solo estará permitido para personas previamente validadas y autorizadas, información de calidad, se protege la información de alteraciones que pudieran intervenirla desde el exterior de la institución, mermando la veracidad de ella.

El desarrollo de la Seguridad de la Información de IACC, incluyendo la Ciberseguridad, se ha basado en las normas internacionales ISO 27001/2:2013 e ISO 27032.

PROPÓSITO

El propósito de la política general de seguridad de la información es declarar la posición de IACC con respecto al buen uso de los activos de información corporativos. Esto se traduce en:

- Definir lineamientos o principios generales que sirven de medio para alcanzar los objetivos de un Sistema de Seguridad de la Información.
- Establecer responsabilidades aplicables a los distintos niveles jerárquicos y a todo el personal vinculado a IACC.
- 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.

- Definir medios de difusión al interior y exterior del servicio para alineamiento con la Dirección.
- Definir plazos y periodicidad para su revisión y evaluación de cumplimiento.

La presente política establece un marco regulatorio aplicable a todos los colaboradores de IACC, ya sea por medio del Código del Trabajo, dotación a honorarios, alumnos en práctica o externos que presten servicios permanentes o temporales; así como, proveedores, contratistas y personal que estén vinculados y que presten servicios en IACC o que estén relacionados, tanto a nivel central como regional.

Es aplicable también, a todo activo de información que la organización posea en la actualidad o en el futuro, asociados a los procesos de negocio de IACC, de manera que la no inclusión explícita en el documento, no constituye argumento para no proteger estos activos de información.

Esta política además cubre toda la información, entre otras, la 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.

LINEAMIENTOS

Los principios que guiaran la presente política se desarrollan de la siguiente manera:

1. 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, normas, y procedimientos emitidos por IACC 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 directrices de seguridad de la información, sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información. A este conjunto de directrices se le llamará “Modelo de Seguridad de la Información”.

Toda información creada o procesada por la institución debe ser considerada como “interna”, a menos que se determine expresamente lo contrario. IACC 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.

2. 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, esta podrá ser divulgada sin previa autorización.

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

3. De las auditorias

Con el fin de velar por el correcto uso de los activos de información, IACC se reserva el derecho de auditar en cualquier momento el cumplimiento de los documentos vigentes que digan relación con el acceso y uso que los usuarios hacen de los activos de información. Las auditorias podrán ser realizadas internamente, a través del auditor interno, o por auditorías a cargo de organizaciones externas, cuando sea pertinente y requerido por el Oficial de Seguridad de la Información, en coordinación con el Comité de Seguridad de la Información.

4. De la gestión de la seguridad de la información

La gestión de la seguridad de la información 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.

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

- Identificar y clasificar los activos de información involucrados.
- Para cada activo de información, identificar un responsable.
- Analizar el riesgo al cual están expuestos.
- 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.

5. De los colaboradores

Los colaboradores de IACC, tienen la responsabilidad de cumplir con cada una de las políticas, normativas, procedimientos, instructivos, etc., que se definan en este Sistema de Gestión de Seguridad de la Información, y aplicarlo en su entorno laboral.

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

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

El personal tiene 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 de registro de incidentes establecido para estos fines. (Ver documento Reglamento Interno de Orden, Higiene y Seguridad, en las cláusulas relativas a la Seguridad de la Información).

Se prohíbe la divulgación de información que esté considerada o clasificada como “reservada”.

6. De terceras partes

Las terceras partes, en lo relativo a la información que obtengan a través de IACC, deberán asumir la responsabilidad de cumplir con las políticas, normativas, y procedimientos, que se definan en el Sistema de Gestión de Seguridad de la Información de IACC y aplicarlo en la relación laboral contratada. Se deberá establecer formalmente esta responsabilidad en los contratos escritos con terceros.

Se prohíbe la divulgación de información que esté considerada o clasificada como “reservada”.

7. Organización de la seguridad

Con el objetivo de garantizar el cumplimiento de la presente Política General de Seguridad de la Información y las directrices que sean definidas en el Modelo de Seguridad de la Información, IACC ha establecido una estructura organizacional de seguridad que contempla la definición de funciones específicas en el ámbito de seguridad, las cuales se encuentran señaladas en el documento Constitución de Comité de Calidad y Cumplimiento.

8. Del Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información de IACC, es el responsable directo de la definición de los criterios de seguridad de la información, de organizar y de coordinar su ejecución oportuna y correcta. Las funciones y responsabilidades del Oficial de Seguridad de la Información se señalan en el documento Manual de descriptores de cargos.

9. Revisión de la Política

Una de las tareas a realizar por el Comité de Seguridad de la Información de IACC, es la reevaluación de la Política General de la Seguridad de la Información. 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.

10. Difusión de la Política

La Dirección de IACC considera fundamental integrar en la cultura organizacional, la existencia de un plan formal de difusión, comunicación, capacitación y sensibilización en torno a la seguridad de la información.

11. Otras directrices específicas de Seguridad de la Información

Se establecen y se consideran como parte de este marco normativo de Seguridad de la Información, directrices relevantes y pertinentes de Seguridad de la Información, de acuerdo con los catorce dominios definidos en la norma ISO 27001:2013

12. Documentación de Seguridad de la Información

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

- Modelo de Seguridad de la Información, compuesto por directrices, que definen 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.

DEFINICIONES

- **Activo de Información**: aquello que tenga valor y es importante para IACC, 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.

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

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

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

- **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.

- **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.

- **Confidencialidad:** propiedad de la información que determina que sólo podrá ser accedida por personas, entidades o procesos debidamente autorizados.

- **Integridad:** 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.

- **Disponibilidad:** 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.

- **Modelo de Seguridad de la Información (MSI)** Es el conjunto de directrices de la Información que definen y describen el diseño de los controles de seguridad de la información, basados en la normas ISO 27001, ISO 27002 e ISO 27032, y que se aplican en IACC.

- **Comité de Seguridad de la Información:** 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 IACC.

- **Oficial de Seguridad de la Información (OSI):** persona calificada que tiene la responsabilidad sobre la gestión de la seguridad de la Información en las operaciones de IACC, que depende y que opera estrechamente coordinado con el Comité de Seguridad de la Información.

IMPLEMENTACIÓN

El Oficial de Seguridad de la Información (OSI), es responsable de velar por el cumplimiento de esta política en lo que se refiere a la gestión y planes de desarrollo anual, las cuales serán coordinadas institucionalmente a través del Comité de Calidad y Cumplimiento, órgano que ejercerá el rol de Comité de Seguridad de la Información.

Los planes y proyectos en materia de seguridad de la información serán financiados exclusivamente con fondos provenientes del Instituto.

MEDICIÓN DE IMPACTO

Esta política será revisada según se señala en lineamiento nueve de este documento. El cumplimiento de la presente política se mide en función del estado de madurez del proceso de gestión de seguridad de la información que IACC.