OTiC
somos CChC

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El presente documento tiene como propósito declarar la posición de la Corporación de Capacitación de la Construcción (CCC) respecto a la protección de los activos de información corporativos y establecer las directrices generales de Seguridad de la Información, incluida la Ciberseguridad.

CORPORACIÓN DE CAPACITACIÓN
DE LA CONSTRUCCIÓN

ENERO 2024

TABLA DE CONTENIDOS

1. PROPÓSITO 3
2. RESPONSABILIDADES 3
3. DEFINICIONES 3
4. LINEAMIENTOS 4
Generales 4
De la información interna. 5
De la información de clientes 5
De la información de personas o usuarios externos. 5
De las Auditorías. 6
De la gestión de la Seguridad de la Información. 6
Deberes de los colaboradores internos y externos. 6
Organización de seguridad. 6
Revisión de las Políticas. 7
Difusión y capacitación. 7
Documentación de Seguridad de la Información. 7
Documentación de referencia. 7

1. PROPÓSITO

El presente documento entrega las directrices generales de Seguridad de la Información, incluida la Ciberseguridad, y es parte del Modelo de Seguridad de la Información de la Corporación de Capacitación de la Construcción (CCC).

El propósito de la "Política General de Seguridad de la Información", es declarar la posición de la corporación con respecto a la protección 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 la corporación.
- Fijar directrices sobre las cuales se sustenten normativas y procedimientos 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 internos y externos para alineamiento con la Dirección de la corporación.
- Definir plazos y periodicidad para su revisión y evaluación de cumplimiento.

2. RESPONSABILIDADES

El Comité de Seguridad de la Información y el Oficial de Seguridad de la Información y Ciberseguridad son responsables de mantener esta normativa actualizada, debidamente publicada y velar por su cumplimiento.

Todos los colaboradores de la empresa son responsables de conocer esta política, de acatarla y de aplicarla en sus respectivos ámbitos de trabajo.

3. DEFINICIONES

- 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 la norma ISO 27002.
- Activo de Información: Aquello que tenga valor y es importante para la organización, 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.

- 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.
- Colaborador: Toda persona que tenga un vínculo contractual de trabajo con la organización, sea éste indefinido, a plazo fijo o a honorarios.
- Política: Directriz u orientación general expresada formalmente por la Dirección de la organización.
- Norma: Disposición de carácter general que se desprende de las políticas, estableciendo obligaciones, restricciones, prohibiciones u otras conductas esperadas.
- 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.
- Amenaza: Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o proceso.
- 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
- Riesgo: Es la posibilidad que ocurra un evento que afecte adversamente el logro de los objetivos de la organización. Se mide combinando las consecuencias del evento (impacto) y su probabilidad de ocurrencia.

4. LINEAMIENTOS

Generales

4.1 La presente política establece un marco regulatorio aplicable a todos los colaboradores que trabajan en la corporación, ya sea sujeta a Código del Trabajo o externos que presten servicios permanentes o temporales; así como, proveedores, contratistas y colaboradores que estén vinculados y que presten servicios relacionados a la corporación, tanto a nivel central como regional.

4.2 También es aplicable a todo activo de información que la corporación posea en la actualidad o en el futuro, asociados a los procesos de negocio del OTIC CChC, de manera que la no inclusión explícita, no constituye argumento para no proteger estos activos de información.

4.3 La política cubre toda la información, entre otras, la impresa o la escrita en papel, la almacenada electrónicamente, la transmitida por correo o usando otros medios electrónicos, mostrada en video o hablada en una conversación, entre otras formas de información.

De la información interna.

4.4 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 la corporación en cada ámbito en particular.

4.5 La información debe ser protegida, por todos los colaboradores, de una manera consistente con su importancia, valor y criticidad, siguiendo las políticas de seguridad de la información, sus normas y procedimientos asociados y las recomendaciones dadas por el responsable de dicha información.

4.6 Toda información creada o procesada por la corporación, sea propia o de clientes, debe ser considerada como “Restringida” a menos que se determine expresamente lo contrario. Dado lo anterior, no podrá ser transmitida o compartida libremente con terceros externos a la corporación sin que medien justificaciones de negocio y autorizaciones de la Gerencia y/o de clientes en caso de que corresponda.

4.7 La corporación proveerá accesos a la información para los colaboradores, estrictamente de acuerdo con sus funciones, reservándose el derecho de revocar los privilegios si la situación y las condiciones lo ameritan o con ocasión del término de la ejecución de los servicios o de la permanencia como colaborador.

De la información de clientes

4.8 La información de propiedad de clientes será protegida en todos los medios, sustento físico o dispositivos donde se procesa o almacena. En términos generales será considerada como Restringida, sin perjuicio de las clasificaciones que se establezcan a futuro. Lo anterior implica que los colaboradores que tengan acceso a esta información, independientemente de su condición contractual, tendrán la obligación de resguardarla con todos los medios disponibles incluyendo los que la corporación provea o establezca, los que no podrán ser modificados o inhabilitados. Dicha obligación estará contenida en los contratos de trabajo respectivos.

De la información de personas o usuarios externos.

4.9 Si la corporación procesa y mantiene información de usuarios externos que sean datos personales y/o sensibles de acuerdo con la normativa vigente, la corporación se asegurará que esta información no será divulgada sin previa autorización y estará protegida de conformidad a lo establecido en la Ley N°19.628, sobre protección a la vida privada.

4.10 Si se requiere compartir información de usuarios externos de la corporación con otras organizaciones, a éstas se les exigirá un contrato, cláusula y/o convenio de confidencialidad y no divulgación previa a la entrega de la información.

De las Auditorías.

4.11 Con el fin de velar por el correcto uso de los activos de información, la corporación se reserva el derecho de auditar en cualquier momento, o también bajo un plan predefinido, el cumplimiento de las políticas y documentos vigentes. Las auditorías podrán ser realizadas a través de auditores internos, o bien a cargo de organizaciones externas.

De la gestión de la Seguridad de la Información.

4.12 La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por la empresa basado en un Sistema de Gestión de Seguridad de la Información (SGSI) el que deberá ser aplicado a los procesos críticos de negocio conforme lo indicado en el documento “Alcance SGSI OTIC CChC”.

4.13 El cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información de la corporación se basará en la identificación y evaluación de riesgos de seguridad de los activos de información corporativos, que será de responsabilidad de los encargados de los diferentes procesos y subprocesos.

Deberes de los colaboradores internos y externos.

4.14 La información y las tecnologías de información de la corporación o de sus clientes serán usadas solo para los propósitos relacionados con el servicio y los que sean autorizados por la jefatura directa, debiendo aplicar criterios de buen uso y protección.

4.15 Los colaboradores, internos o externos, están en la obligación de alertar de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta y otras políticas de seguridad.

Organización de seguridad.

4.16 Con el objetivo de garantizar el cumplimiento de la presente Política General de Seguridad de la Información, la corporación establecerá una estructura organizacional que contemplará entre otros, la conformación de un Comité de Seguridad de la información y Ciberseguridad, el que se describirá en uno o más documentos dedicados a estos efectos.

Revisión de las Políticas.

4.17 La revisión de la presente Política General de Seguridad de la Información y cualquier política asociada o que forme parte del SGSI, se realizará por lo menos una vez al año. En caso excepcional deberán también ser revisadas ante cualquier cambio significativo de tecnología, colaboradores, estructura de servicios o evento que amerite su actualización para asegurar continuidad, idoneidad, aplicabilidad, eficiencia y efectividad.

Difusión y capacitación.

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

4.19 Se ejecutarán planes de capacitación como actividades permanentes a ser realizadas cuando se elaboren o se produzcan cambios en las políticas. Asimismo, serán incluidas en el proceso de inducción de nuevos colaboradores, sean internos o externos.

Documentación de Seguridad de la Información.

4.20 La documentación de Seguridad de la Información de la corporación es la siguiente:

Modelo de Seguridad de la Información: compuesto por Políticas y Normas, que definen el diseño de los controles de seguridad de la información que se implementarán en la corporación.

Procedimientos: que describen cómo realizar las actividades y tareas relacionadas con los controles de seguridad implementados.

Documentación de referencia.

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

- Ley N°21.459 sobre Delitos Informáticos.

- Ley N°19.628, sobre protección a la vida privada.
- Ley N°19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley N°17.336, sobre Propiedad Intelectual.
- Ley N°20.393, sobre la Responsabilidad Penal de las Personas Jurídicas por los delitos que indica.
- Norma NCh-ISO 27002 Tecnologías de la Información – Técnicas de Seguridad – Código de prácticas para los controles de seguridad de la información.

OTiC

somos CChC

CORPORACIÓN DE CAPACITACIÓN
DE LA CONSTRUCCIÓN

ENERO 2024