POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CORPORACIÓN CULTURAL DE VITACURA

DICIEMBRE, 2024

ÍNDICE

1. Introducción

En la **Corporación Cultural de Vitacura** (en adelante "**Corporación**" o la "**CCV**") establece en la presente Política de Riesgos Informáticos (en adelante la "Política") los principios y directrices que se deben seguir para identificar, clasificar, asignar propietarios y proteger adecuadamente los activos de información en nuestra organización, con el objetivo de salvaguardar la integridad de los datos, garantizar la confidencialidad y asegurar la disponibilidad de la información necesaria para cumplir con nuestros objetivos de negocio y compromisos ambientales.

La Política establece los lineamientos para identificar y evaluar los activos de información críticos, así como para clasificarlos en función de su importancia, sensibilidad y valor. Considera, además, asignar a cada activo de información un propietario responsable de su protección y gestión adecuada, quien velará por su integridad y confidencialidad.

La CCV se compromete a implementar y mantener controles de seguridad adecuados para proteger sus activos de información contra amenazas internas y externas, como el acceso no autorizado, la divulgación indebida o la pérdida de datos. A través de esta Política, se establecerán lineamientos técnicos y administrativos para salvaguardar la información y promover prácticas seguras en toda la organización.

En resumen, esta Política refuerza nuestra dedicación a la seguridad, integridad y disponibilidad de los activos de información que respaldan las operaciones que reafirma el compromiso con el cumplimiento normativo.

2. Destinatarios.

Esta Política tiene un alcance amplio y se aplica a todas las personas que ocupan un cargo, función o posición en la Corporación, incluyendo directores, ejecutivos principales y trabajadores - desde ahora e indistintamente “colaboradores” o “trabajadores”. Además, todos aquellos que presten servicios a la CCV como contratistas, proveedores o asesores, así como a los terceros que acceden, utilizan o manejan activos de información de la Corporación.

Por otra parte, esta Política se extiende a todos los activos de información, tales como computadores, servidores, equipos de red, servicios en la nube, portales y sistemas de propiedad de la Corporación, dispositivos de almacenamiento extraíbles, discos duros físicos y virtuales, independientemente de su formato o ubicación, que son fundamentales.

3. Definiciones.

a) Datos informáticos: Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

b) Sistema informático: Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

c) Seguridad de la información: Conjunto de procesos, metodologías, políticas, normativas, estándares, procedimientos, controles, software, hardware, y otros elementos necesarios para mantener la confidencialidad, integridad y disponibilidad de la información.

d) Activo de información: Recurso del sistema de información como personas, instalaciones, procesos, archivos digitales, documentos físicos, base de datos, intangibles e información en general, entre otros, necesario para que la Corporación funcione correctamente y alcance los objetivos propuestos.

e) Tratamiento de información: Actividad de creación, digitación, transmisión, procesamiento, almacenamiento, modificación, eliminación, consulta, o cualquier otra acción que diga relación con manipulación de información.

f) Proceso: Conjunto de actividades o eventos que se realizan de manera estructurada o alternativa con el fin de cumplir un objetivo determinado.

g) Confidencialidad: Propiedad de la información que apunta a que el acceso a la información, sólo pueda ser realizado por personas, sistemas o entidades autorizadas para hacerlo.

h) Integridad: Propiedad de la información que apunta a mantener la exactitud y totalidad de la información, como también los métodos y mecanismos de tratamiento en general.

i) Disponibilidad: Propiedad de la información que apunta a que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

j) Sistema de información: Uno o más computadores, software asociado, hardware y periféricos, terminales, procesos físicos, medios de transferencia, bases de datos, entre otros, que forman un todo autónomo capaz de realizar tratamiento de información.

k) Riesgo de información: Cualquier acción o situación que podría afectar las propiedades de la información y a su vez ocasionar resultados no esperados para la institución.

4. Principios de Seguridad de la Información

a. **Confidencialidad:** La CCV se compromete a tratar toda la información que tengamos de manera confidencial, protegiéndola contra accesos no autorizados o divulgaciones indebidas. Toda la información confidencial será utilizada exclusivamente para cumplir el objeto y finalidad para la cual es generada, recopilada o tratada por la Corporación, debiendo ser guardada como información confidencial y no será revelada ni divulgada a terceros sin autorización previa, escrita y expresa de la Corporación.

b. **Integridad:** Se mantendrá la precisión y la integridad de la información a través de controles adecuados para evitar alteraciones no autorizadas o no intencionadas.

c. **Disponibilidad:** Se debe garantizar la disponibilidad de la información y los sistemas necesarios para el funcionamiento continuo y eficiente de nuestras operaciones.

d. **Cumplimiento legal:** La CCV cumplirá todas las leyes, regulaciones y requisitos contractuales aplicables en relación con la seguridad de la información.

e. **Responsabilidad:** Toda persona que ocupa un cargo, función o posición en la Corporación, incluyendo directores, ejecutivos principales, trabajadores y todos aquellos que presten servicios a la corporación como contratistas, proveedores o asesores, así como los terceros que acceden, utilizan o manejan activos de información de la Corporación son responsable de cumplir con las políticas y procedimientos de seguridad de la información establecidos por la Corporación.

5. Obligaciones

Todo colaborador tiene el deber de velar por la seguridad de la información y deben cumplir con esta Política y los procedimientos que de ella deriven.

Lo anterior incluye, sin ser taxativo, lo siguiente:

a. Conocer y cumplir la Política y procedimientos de seguridad de la información de la Corporación, incluida la clasificación de los activos de la información y el manejo adecuado de la información confidencial.
b. Participar en programas de capacitación y concientización sobre seguridad de la información para comprender los riesgos y las mejores prácticas de seguridad.
c. Informar cualquier incidente de seguridad o vulnerabilidad detectada al Encargado de Prevención del Delito y cooperar en la resolución de dichos incidentes.
d. Utilizar los activos de información de manera responsable y asegurarse de protegerlos contra pérdidas, robos o daños físicos.
e. Prestadores de servicios (contratistas, proveedores o asesores). Es importante establecer medidas de seguridad de la información para los prestadores de servicios que interactúan con la Corporación, como contratistas, proveedores o asesores, las que considerarán a lo menos:
f. Acuerdos de Confidencialidad y Cláusulas de Seguridad. Establecemos acuerdos de confidencialidad que definan claramente la responsabilidad de los prestadores de servicios para proteger la información confidencial y cumplir con las políticas de seguridad de la información de la Corporación.

6. Prevención de delitos informáticos

La gestión adecuada de la seguridad de la información y ciberseguridad mejora los procesos corporativos, evita el acceso no autorizado a información sensible de la CCV, y crea un entorno de control que previene conductas delictivas de los colaboradores en el ámbito informático.

En este sentido, todo el que ocupa un cargo, función o posición en la Corporación, incluyendo directores, ejecutivos principales y trabajadores, y todos aquellos que presten servicios a la Corporación como contratistas, proveedores o asesores, así como los terceros que acceden, utilizan o manejan activos de información de la Corporación, tienen prohibido cometer conductas ilícitas a través de medios informáticos o en contra de sistemas informáticos.

Dichas conductas se encuentran sancionadas en la Ley N°21.459, que establece normas sobre delitos informáticos, los cuales se describen a continuación.

a. Ataque a la integridad de un sistema informático (sabotaje informático):

Consiste en obstaculizar o impedir el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos (art. 1° ley 21.459).

b. Acceso ilícito:

Acceder a un sistema informático sin autorización o excediendo la autorización que se posea y superando barreras técnicas o medidas tecnológicas de seguridad. La pena se agrava si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático. También se castiga la divulgación de la información a la cual se accedió de manera ilícita (art. 2° ley 21.459).

Interceptación ilícita:

Interceptar, interrumpir o interferir indebidamente, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos. También captar, sin contar con la debida autorización, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos (art. 3° ley 21.459).

c. Interceptación ilícita.

Interceptar, interrumpir o interferir indebidamente, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos. También captar, sin contar con la debida autorización, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos (art. 3° ley 21.459).

d. Ataque a la integridad de los datos informáticos (sabotaje de datos):

Alterar, dañar o suprimir indebidamente datos informáticos, siempre que con ello se cause un daño grave al titular de estos mismos (art. 4° ley 21.459).

e. Falsificación informática:

Introducir, alterar, dañar o suprimir indebidamente datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos (art. 5° ley 21.459).

f. Receptación de datos informáticos:

Se sanciona al que, conociendo su origen o no pudiendo menos que conocerlo, comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas de acceso ilícito, interceptación ilícita y falsificación informática (art. 6° ley 21.459).

g. Fraude Informático

Manipular un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero. Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito (art. 7° ley 21.459).

h. Abuso de los dispositivos:

Sanciona al que para la perpetración de los delitos de ataque a la integridad de un sistema informático, acceso ilícito, interceptación ilícita, ataque a la integridad de los datos informáticos y delito de uso fraudulento de tarjetas de pago y transacciones electrónicas, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos (art. 8° ley 21.459).

7. Sanciones

Los trabajadores y directivos que no den fiel cumplimiento a las obligaciones y prohibiciones establecidas en la presente política serán objeto de medidas disciplinarias de acuerdo con lo establecido en la normativa interna de la Corporación y en el Modelo de Prevención de Delitos. La sanción, según la gravedad de la infracción, irá desde una amonestación verbal hasta la desvinculación de la Corporación.