PROTOCOLO

DELITOS INFORMÁTICOS

Y

PROTECCIÓN DE DATOS PERSONALES

IC CORP SpA

PROTOCOLO DELITOS INFORMÁTICOS

IC CORP SpA

1. OBJETIVOS

IC Corp SpA, en adelante "*Iconstruye*", reconocen la importancia de la protección de los activos de información para el funcionamiento seguro de las operaciones de su empresa, tanto internamente, como en relación con los clientes, teniendo en especial consideración el componente tecnológico que caracteriza el negocio de Iconstruye.

Por lo anterior, el presente protocolo tiene como objetivo materializar el compromiso de Iconstruye en la prevención de delitos informáticos, y en la implementación de controles de seguridad adecuados para la protección de activos de información contra amenazas externas e internas.

En el mismo sentido, este protocolo tiene como propósito servir de guía a los accionistas, directores, ejecutivos, trabajadores, proveedores, y terceros que tengan algún tipo de relación con Iconstruye, con la finalidad de que tomen conocimiento de los conceptos básicos que regula la Ley N°21.459, sobre Delitos Informáticos, entregando herramientas para identificar y denunciar eventuales hechos que puedan ser considerados como constitutivos de delito.

Por otro lado, se establecen los lineamientos y principios que rigen el debido resguardo y protección de Datos Personales que la empresa recolecte, almacene, procese o transfiera en el ejercicio de sus actividades, dando cumplimiento a la Ley N°19.628, sobre Protección de la Vida Privada.

En resumen, este documento refuerza la dedicación de Iconstruye a la seguridad, integridad y disponibilidad de los activos de información, y reafirma el compromiso de la empresa con el cumplimiento normativo en esta materia.

2. ÁMBITO DE APLICACIÓN

El presente Protocolo es aplicable a todos los accionistas, directores, ejecutivos, trabajadores, colaboradores, así como a cualquier tercero que acceda, utilice o maneje Activos de Información de Iconstruye.

3. ACTIVOS DE INFORMACIÓN

Para efectos de la aplicación del presente protocolo, se entiende por "**Activos de Información**", todos aquellos dispositivos y/o mecanismos que contengan información relevante de Iconstruye, sus clientes, o de cualquier otra naturaleza, tales como computadores, servidores, equipos de red, servicios en la nube, portales y sistemas de propiedad de Iconstruye, dispositivos de almacenamiento extraíbles, discos duros físicos

y virtuales, independientemente de su formato o ubicación. Los Activos de Información incluyen, pero no se limitan a:

- **Datos y registros**: Aquella información contenida en bases de datos que incluya registros o información propia, de clientes o terceros, registros financieros, informes de cumplimiento normativo, datos personales y cualquier otra información utilizada para respaldar las operaciones y/o servicios prestados por Iconstruye.

- **Sistemas y aplicaciones**: Sistemas informáticos, software, plataformas, sitios web, aplicaciones, y/o cualquier otro sistema que maneje, almacene o procese información utilizada por Iconstruye para el desarrollo de su negocio.

- **Redes y comunicaciones**: Infraestructura de red utilizada por Iconstruye, incluyendo conexiones internas y externas, dispositivos de red, firewalls, y otros componentes necesarios para el intercambio seguro de información dentro de la organización y con entidades externas.

- **Equipos**: Equipos físicos utilizados para recopilar, almacenar, procesar o transmitir información, como servidores, ordenadores, portátiles, dispositivos móviles, unidades de almacenamiento y cualquier otro dispositivo que albergue datos o se utilice para acceder a ellos.

- **Documentación**: Documentos físicos o electrónicos que contienen información crítica para las operaciones de Iconstruye, incluyendo manuales de procedimientos, políticas internas, contratos, acuerdos de confidencialidad y cualquier otro documento que sea necesario para la gestión de la información.

4. PREVENCIÓN DE DELITOS INFORMÁTICOS

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

Como se indicó previamente, el objetivo de este protocolo es que los accionistas, directores, ejecutivos, trabajadores, proveedores, y terceros que tengan algún tipo de relación con la organización, tomen conocimiento respecto de aquellas conductas que constituyan Delitos Informáticos, de manera que puedan identificar y evitar cualquiera de dichas conductas, así como también denunciarlas al Encargado de Cumplimiento según los protocolos que se contemplan en este documento.

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.

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.

Un ejemplo de esta conducta, es la introducción de un malware en los dispositivos de la empresa, que impida a los usuarios acceder a sus sistemas o archivos, exigiendo el pago de un rescate para recuperar el acceso ("secuestro de sistemas").

b) Acceso ilícito.

Consiste en acceder a un sistema informático superando barreras técnicas o medidas tecnológicas de seguridad, sin autorización o excediendo la autorización que se posee. Por ejemplo, el uso de credenciales de un tercero sin autorización, para acceder a un sistema o archivo.

La conducta es aún más gravosa cuando el acceso se efectúa con el ánimo de apoderarse o usar la información obtenida, o bien, con el propósito de divulgar la información a la cual se accedió ilícitamente.

c) Interceptación ilícita.

Consiste en interceptar, interrumpir o interferir la transmisión no pública de información en un sistema informático o entre dos o más sistemas informáticos, de forma indebida; o captar, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas que de éstos provienen.

Por ejemplo, interceptar mediante softwares el tráfico o comunicaciones que se realizan dentro de la empresa (también conocido como "sniffing").

d) Ataque a la integridad de los datos informáticos.

Consiste en alterar, dañar o suprimir indebidamente datos informáticos, siempre que con ello se cause un daño grave a su titular.

A diferencia de la hipótesis contemplada en la letra a) anterior, en este caso la conducta se ejecuta en contra de un componente específico de un sistema informático, esto es, los datos almacenados en su interior, por ejemplo, mediante la introducción de un malware en los dispositivos de la empresa, que encripte o elimine datos confidenciales de los usuarios.

e) Falsificación informática.

Consiste en la introducción, alteración, daño o supresión de datos informáticos, de forma indebida, con la intención de que aquellos sean considerados como auténticos o sean utilizados para generar documentos auténticos.

Por ejemplo, la suplantación de identidad o "*spoofing*", en donde un tercero se hace pasar por una entidad institucional u oficial, ya sea por correo electrónico, vía telefónica u otra, a través de la falsificación de los datos en la comunicación.

f) <u>Receptación de datos informáticos</u>.

Consiste en comercializar, transferir o almacenar a cualquier título, datos informáticos provenientes de acceso ilícito, interceptación ilícita o falsificación informática, conociendo o no pudiendo menos que conocer el origen ilícito de dichos datos.

Por ejemplo, adquirir y/o almacenar una base de datos obtenida a través de un acceso ilícito de otro sistema informático.

g) <u>Fraude informático</u>.

Consiste en manipular un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos, o a través de cualquier interferencia en el funcionamiento del sistema informático, con el propósito de obtener un beneficio económico propio o para un tercero, y a su vez, ocasionando un perjuicio.

Por ejemplo, "*pishing*", es decir, el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar, como, por ejemplo, traspaso de fondos a cuentas falsas, o pago de facturas fraudulentas.

h) <u>Abuso de los dispositivos</u>.

Consiste en facilitar los medios tecnológicos y herramientas informáticas (dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso), para la comisión de los Delitos Informáticos descritos precedentemente. Por ejemplo, copia ilegal de información, o la entrega indebida de información confidencial a la que un colaborador ha tenido acceso en virtud de las tareas que le fueron encomendadas.

Adicionalmente, la ley contempla ciertas circunstancias agravantes:

- Cometer el delito abusando de una posición de confianza en la administración del sistema informático o ser el custodio de los datos informáticos contenidos en el sistema, por el cargo o función que tiene la persona.

- Cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores.

5. PROTECCIÓN DE DATOS PERSONALES

Iconstruye reconoce la importancia de la protección de Datos Personales y el debido resguardo de la privacidad. Por lo anterior, todos aquellos Datos Personales que la

organización obtenga, genere, o almacene, serán considerados bienes relevantes, y activos estratégicos para Iconstruye.

Para estos efectos, se entiende por "**Datos Personales**" cualquier información concerniente a personas naturales, identificadas o identificables, tales como su nombre y apellido, cédula de identidad, dirección, número de teléfono, fecha de nacimiento, entre otros.

Cualquier persona de la organización que tenga a acceso a Datos Personales dentro del ejercicio de las actividades de Iconstruye, será responsable de usarlos y protegerlos adecuadamente, y se encontrará obligada a guardar la debida confidencialidad de la misma. Esta obligación no terminará por haber cesado sus actividades o funciones dentro de la empresa.

En el mismo sentido, Iconstruye deberá obtener el consentimiento escrito del titular de los Datos Personales para efectuar cualquier operación destinada a recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar dichos datos, o utilizarlos en cualquier otra forma. Lo anterior, salvo que se trate de Datos Personales que provengan o se recolecten de fuentes accesibles al público.

Adicionalmente, Iconstruye tomará las medidas necesarias para resguardar los Datos Personales contra el tratamiento no autorizado o ilícito, y garantizará el ejercicio de los derechos de los titulares de los Datos Personales, incluidos el derecho de acceso, rectificación, cancelación y oposición, de acuerdo con lo establecido en la Ley N°19.628, sobre Protección de la Vida Privada.

6. ENCARGADO DE CUMPLIMIENTO.

El Encargado de Cumplimiento de Iconstruye será quien esté encargado de velar por la correcta aplicación y cumplimiento del presente protocolo, y deberá reportar directamente al Directorio y al Comité de Riesgos en su reporte.

El Encargado de Cumplimiento tendrá la responsabilidad específica de desarrollar, implementar y supervisar un sistema integral de gestión para evaluar y manejar las conductas de cumplimiento en Iconstruye, en concordancia con su estructura Corporativa, tomando en consideración sus diversas áreas.

En su rol, el Encargado de Cumplimiento deberá fomentar la formulación de políticas, procedimientos y buenas prácticas en todos los procesos que presenten riesgos de incumplimiento de normas contempladas en la Ley N°21.459, sobre Delitos Informáticos y en la Ley N°19.628, sobre Protección de la Vida Privada

El Encargado de Cumplimiento deberá ejecutar el presente protocolo de manera de prevenir eficazmente la ocurrencia de situaciones que puedan violar las normas contempladas en la Ley N°21.459, sobre Delitos Informáticos y en la Ley N°19.628, sobre Protección de la Vida Privada, así como los principios y políticas de Iconstruye.

El Encargado de Cumplimiento, cuenta con los recursos, habilidades y posición adecuados, además de autoridad e independencia. Tiene acceso directo al Directorio y al Comité Riesgos para informar sobre el seguimiento y abordar contingencias o asuntos que requieran atención a esos niveles.

Entre sus responsabilidades se encuentran:

a) Supervisar el diseño, actualización e implementación del presente protocolo.
b) Comunicar, capacitar, asesorar y guiar a los trabajadores, en todas las materias que incumben el presente protocolo.
c) Efectuar las observaciones que le merezcan a las autorizaciones de operaciones de los trabajadores, de acuerdo con las políticas y procedimientos vigentes, así como otorgar su autorización cuando corresponda.
d) Conocer y resolver respecto de sanciones aplicables en caso de denuncias e incumplimientos del Protocolo de Delitos Informáticos y Protección de Datos Personales y velar por que no existan represalias en caso de denuncias.
e) Gestionar las auditorías internas y externas del sistema de cumplimento de Iconstruye.

7. PROCEDIMIENTO DE DENUNCIA

En el evento de que alguno de los accionistas, directores, ejecutivos, trabajadores, o colaboradores de Iconstruye, tomare conocimiento de hechos o conductas que revistan o puedan revestir incumplimientos a lo indicado en el presente protocolo, deberán iniciar un proceso de denuncia.

Para efectos de lo anterior se ha dispuesto en la intranet y vía correo electrónico (compliance@iconstruye.com) un canal de denuncias interno, disponible 24/7, y a disposición pública.

Para quien quiera realizar a denuncia de manera anónima, se garantizará la total confidencialidad de las comunicaciones que se realicen en este contexto.

El Canal de Denuncias y el contacto con el Encargado de Cumplimiento podrán ser utilizados también para aclarar cualquier duda que los trabajadores y ejecutivos puedan tener en relación con la normativa relativa a Delitos Informáticos y Protección de Datos Personales, su aplicación y alcance.

Toda denuncia deberá ser planteada de forma seria y de buena fe.

Los denunciantes pueden respaldar su denuncia a través de los siguientes antecedentes:

- Descripción de la conducta denunciada, fecha y lugar referenciales.
- Descripción de las personas involucradas en la conducta.
- Forma en que el denunciante tomó conocimiento de los hechos denunciados.
- Documentos físicos y electrónicos que sean pertinentes en la denuncia.

En virtud de la relevancia de la información presentada, el Encargado de Cumplimiento determinará si es apropiado iniciar una investigación interna, la cual tendrá una duración máxima de 60 días. Durante este periodo, el denunciante tendrá la oportunidad de mantener comunicación con el Encargado de Cumplimiento y dar seguimiento a la denuncia presentada. Al concluir los 60 días, el Encargado de Cumplimiento decidirá si es pertinente informar el incidente al Directorio de Iconstruye para evaluar posibles medidas preventivas, correctivas y sancionatorias que puedan aplicarse a las personas vinculadas con la situación denunciada.

Esto se realiza sin perjuicio de las acciones legales que pueda emprender Iconstruye. Se garantizará la confidencialidad de la información y el anonimato del denunciante, si así lo solicita.

8. SANCIONES POR INCUMPLIMIENTO DE ESTE PROTOCOLO

El incumplimiento de la presente Protocolo de Delitos Informáticos, la ley de Protección de Datos Personales y, sobre todo, la comisión de alguna conducta constitutiva de delitos, conforme a la Ley N°21.459, o a la ley 19.628 sobre Protección de la Vida Privada han de conllevar las sanciones previstas en la ley, en los contratos de trabajo y en el Reglamento Interno de Orden, Higiene y Seguridad de Iconstruye, las que podrán ir desde amonestaciones hasta la terminación del contrato de trabajo.

En el caso de proveedores y terceros, habrá de aplicarse sanciones de censura por escrito comunicada a la administración o representante legal del proveedor, o bien de terminación inmediata del contrato con el proveedor en caso de infracciones graves.

Todo lo anterior es sin perjuicio de las eventuales sanciones laborales, civiles, administrativas y/o penales que puedan afectar al infractor.

9. MEDIDAS DE SEGURIDAD QUE ADOPTA ICONSTRUYE

Los directores, ejecutivos principales, trabajadores, y colaborares de Iconstruye deberán seguir las siguientes políticas para evitar cualquier conducta que pueda constituir un Delito Informático, conforme a la Ley N°21.459, o vulnerar la protección de Datos Personales, conforme a la Ley N°19.628.

• **Acuerdos de Confidencialidad (NDA):** Suscripción de contratos o acuerdos de confidencialidad con proveedores, clientes, o cualquier tercero antes de compartir información confidencial.

• **Acceso Controlado:** Acceso a información confidencial solo a las personas que realmente necesitan conocerla. Adicionalmente, se implementan sistemas de autenticación y autorización sólidos para asegurar que sólo los usuarios autorizados tengan acceso a la información sensible y/o confidencial.

• **Encriptación:** Encriptación de datos confidenciales, con el propósito de prevenir que terceros no autorizados accedan a información confidencial.

• **Consentimiento y Registro de Datos Personales:** Obtener el consentimiento escrito de los titulares de datos personales antes de recopilarlos, almacenarlos, procesarlos, o utilizarlos en cualquier otra forma. Adicionalmente, mantener un registro ordenado y actualizado de los datos personales a los que se tiene acceso y/o son almacenados por la empresa.

• **Auditorías Regulares:** Auditorías periódicas para evaluar la seguridad de la información compartida con terceros, con el objeto de identificar posibles vulnerabilidades o puntos débiles en el sistema.

• **Capacitaciones:** Formación regular a los trabajadores y colaboradores sobre las mejores prácticas de seguridad de la información, para prevenir amenazas internas y/o errores dentro de la organización.

• **Antivirus y antimalware**: Implementación de mecanismos antivirus y antimalware actualizados y eficaces en todos los sistemas y dispositivos utilizados en Iconstruye, plataformas, sitios web, aplicaciones.

• **Perímetro de seguridad**: Implementación de dispositivos de seguridad de red para controlar y monitorear el tráfico entrante y saliente, y para prevenir ataques externos no autorizados.

• **Detección y prevención de intrusiones**: Utilización de sistemas de detección y prevención de intrusiones para monitorear y analizar el tráfico de red en busca de actividades sospechosas y/o maliciosas.

10. ACTUALIZACIÓN DEL PROTOCOLO

El presente protocolo se revisará y actualizará de manera anual, o en su defecto, cuando existan cambios normativos que exijan su modificación.

PREGUNTAS Y RESPUESTAS.

Como se ha indicado en el Manual de Prevención de Delitos ("MPD") de Iconstruye, uno de los elementos más importante de la Ley de Responsabilidad Penal de las Personas Jurídicas y la Ley de Delitos Económicos, es que el MPD se encuentre debidamente implementado, y gran parte de dicha implementación está en que todos los Trabajadores, conozcan y sepan identificar situaciones de riesgo y que puedan llevar a realizar ciertos actos que puedan revestir características de delitos.
Por lo anterior, a continuación, hemos preparados para los Trabajadores material didáctico consistente en diversas preguntas y situaciones en las que se podría encontrar un Trabajador de Iconstruye que, sumado al MPD, permitirá que estos se familiaricen tanto con los conceptos y conductas que implican la comisión de los delitos, así como con ciertas conductas respecto de las cuales deben estar atentos para denunciar oportunamente al Encargado de Cumplimiento.

Se indica con un * la respuesta correcta.

1. **¿Qué es un ataque a la integridad de un sistema informático?**

   a) Acceder a un sistema informático sin autorización.
   b) Interceptar comunicaciones no públicas.
   c) Obstaculizar o impedir el normal funcionamiento de un sistema informático mediante la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos.*
   d) Comercializar datos obtenidos ilícitamente.

2. **Usted descubre que alguien ha accedido a los archivos confidenciales de la empresa utilizando credenciales robadas. ¿Qué hace usted?**

   a) Guardar silencio para evitar problemas.
   b) Notificar al Encargado de Cumplimiento.*
   c) Hablar directamente con el responsable del acceso.
   d) Cambiar sus propias credenciales de acceso.

3. **¿Qué se considera acceso ilícito a un sistema informático?**

   a) Acceder a un sistema informático sin superar barreras técnicas.
   b) Acceder a un sistema informático sin autorización o excediendo la autorización que se posee. *
   c) Consultar información pública en internet.
   d) Utilizar dispositivos de almacenamiento extraíbles.

4. **Usted recibe un correo electrónico sospechoso solicitando información confidencial haciéndose pasar por un ejecutivo de la empresa. ¿Qué hace usted?**

   a) Responder al correo solicitando más información.
   b) Eliminar el correo sin reportarlo.
   c) Informar al Encargado de Cumplimiento y no responder al correo.*
   d) Reenviar el correo a sus compañeros de trabajo para advertirles.

5. **¿Qué implica la interceptación ilícita?**

   a) Acceder a un sistema informático con autorización.
   b) Interrumpir la transmisión pública de información.
   c) Interceptar, interrumpir o interferir la transmisión no pública de información en un sistema informático de forma indebida.*
   d) Utilizar una red Wi-Fi pública.

6. **Usted se da cuenta de que se están interceptando las comunicaciones internas de la empresa.? ¿Qué hace usted?**

   a) Ignorar la situación.
   b) Informar al Encargado de Cumplimiento.*
   c) Consultar con un abogado externo.
   d) Hablar con sus compañeros sobre el problema.

7. **¿Qué constituye un ataque a la integridad de los datos informáticos?**

   a) Consultar datos confidenciales sin autorización.
   b) Alterar, dañar o suprimir indebidamente datos informáticos, causando un daño grave a su titular.*
   c) Compartir datos informáticos públicamente.
   d) Almacenar datos en la nube.

8. **Usted detecta que se ha introducido un malware en los dispositivos de la empresa, impidiendo el acceso a los sistemas. ¿Qué hace usted?**

   a) Ignorar el problema y seguir trabajando.
   b) Informar al Encargado de Cumplimiento.*
   c) Reiniciar los dispositivos y esperar que el problema se solucione.
   d) Intentar eliminar el malware por su cuenta.

9. **¿Qué es la falsificación informática?**

   a) Modificar datos con autorización.
   b) Introducir, alterar, dañar o suprimir datos informáticos con la intención de que sean considerados auténticos.*
   c) Almacenar datos en un servidor seguro.
   d) Compartir información con sus compañeros de trabajo.

10. **Usted se da cuenta que alguien ha alterado datos financieros importantes, causando un daño significativo a la empresa. ¿Qué hace usted?**

   a) Intentar corregir los datos por su cuenta.
   b) Hablar con el responsable de la alteración.
   c) Informar al Encargado de Cumplimiento.*
   d) Guardar una copia de los datos alterados.