POLÍTICA DE ASUNTOS INFORMÁTICOS

ALTO JARDÍN S.A.

Versión	Documentos	Fecha
2	Política de Asuntos Informáticos	06/05/2024

ÍNDICE DE CONTENIDO

POLÍTICA DE ASUNTOS INFORMÁTICOS

1. ASPECTOS GENERALES

1.1. Objetivo

La presente **Política de Asuntos Informáticos** (en adelante, la "*Política*") constituye la norma marco encargada de establecer los principios, valores y compromiso de Alto Jardín S.A. (en adelante, "*Alto Jardín*" o la "*Compañía*") en el cumplimiento de las regulaciones aplicables en materia de delitos informáticos, así como las obligaciones, objetivos y marco de actuación necesarios para el desarrollo de los procesos y actividades de la Compañía en un contexto de ética e integridad empresarial.

La presente Política, tiene con finalidad prevenir los delitos contemplados en la Ley N°21.595 sobre Delitos Económicos, la cual modificó una serie de cuerpos normativos entre los cuales podemos encontrar la Ley N°21.459 que "*Establece normas sobre Delitos Informáticos, deroga la Ley N°19.223 y modifica otros cuerpos legales con el objetivo de adecuarlos al Convenio de Budapest*" y la Ley N°20.393 que "*Establece la Responsabilidad Penal de las Personas Jurídicas en los Delitos que Indica*".

En general, las medidas más relevantes se relacionan con la tipificación de los siguientes delitos: (i) ataque a la integridad de un sistema informático; (ii) acceso ilícito; (iii) intercepción ilícita; (iv) ataque a la integridad de los datos informáticos; (v) falsificación informática; (vi) receptación de datos informáticos; (vii) fraude informático; y, (viii) abuso de dispositivos.

Esta política forma parte del Modelo de Prevención de Delitos de Alto Jardín y es complementaria a la Política de Compliance y las demás políticas empresariales y la normativa vigente.

1.2. Ámbito de aplicación

Cada una de las disposiciones y/o prohibiciones de la presente Política son aplicables a todos los integrantes de Alto Jardín, lo cual incluye trabajadores, socios, accionistas, directores, alta administración, gerentes, ejecutivos, empleados, personal temporal, prestadores de servicios, contratistas y asesores de la Compañía (en adelante, "*Personal de la Compañía*").

Es responsabilidad compartida de todo el Personal o colaborador de la Compañía entender esta Política y asegurar que se mantengan sus normas éticas. Todo el Personal de la Compañía tienen la responsabilidad de garantizar que todos los empleados de sus departamentos conozcan la Política y su contenido, y deberán proporcionar asistencia y orientación en su aplicación e interpretación. El **Encargado de Prevención de Delitos** también estará disponible para responder a cualquier pregunta o inquietud que pueda surgir.

Adicionalmente, aplica a todas las empresas, filiales y asociaciones en las que Alto Jardín S.A. tenga el control. En aquellos casos en que la Compañía carezca de dicho control o tenga igualdad de participación con otros asociados, se deberá instar a que se adopten e implementen políticas y medidas que contribuyan a impedir la comisión de delitos informáticos.

1.3. Definiciones

1. **Abuso de los Dispositivos: entregar u obtener** para la utilización, importar, difundir o realizar cualquier 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 informáticos.

2. **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.

3. **Ataque a la Integridad de los Datos Informáticos (Sabotaje de Datos):** alterar, dañar o suprimir indebidamente datos informáticos.

4. **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.

5. **Falsificación Informática:** introducción, alteración, daño o supresión de datos informáticos.

6. **Fraude Informático:** manipulación de 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.

7. **Intercepción Ilícita:** interrumpir, por medios técnicos, la transmisión no pública de información en un sistema informático.

8. **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.

9. **Prestadores de Servicios:** toda identidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de los mismos.

10. **Receptación de Datos Informáticos:** comercialización, transferencia o almacenamiento, proveniente de la realización de las conductas de acceso ilícito, interceptación ilícita y falsificación informática.

1.4. Marco Normativo Aplicable

La presente Política toma en consideración el marco normativo nacional e internacional aplicable a la Compañía al desempeñar sus actividades en Chile, dentro del cual cabe destacar las siguientes normas:

- Código Penal de Chile.
- Ley N°20.393 que "*Establece la responsabilidad penal de las personas jurídicas*".
- Ley N°21.595 "*Ley de Delitos Económicos*".
- Ley N°21.459 que establece "*Normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales, con el objeto de adecuarlos al Convenio de Budapest*".

Ante la verificación de una modificación legislativa que imponga pautas más severas de las expuestas en la presente Política, estas deberán prevalecer sobre el presente documento. Ante cualquier duda que pueda surgir a partir de la interpretación de las normas vigentes y su contenido, se deberá acudir al Encargado de Prevención de Delitos.

2. ACTIVOS DE INFORMACIÓN

Esta Política se extiende a todos los activos de información, tales como computadores, servidores, equipos de red, servicios en la nube, portables y sistemas de propiedad de Alto Jardín o sus filiales,

dispositivos de almacenamiento extraíbles, discos duros físicos y virtuales, independientemente de su formato o ubicación, que son fundamentales para nuestras operaciones y para cumplir con nuestros compromisos.

Los activos de información incluyen, pero no se limitan a:

2.1. **Datos y registros:** información recopilada y mantenida en nuestra base de datos de clientes, registros financieros, informes de cumplimiento normativo, informes de seguimiento de procesos de gestión de residuos y reciclaje, datos personales y cualquier otra información utilizada para respaldar las operaciones y el cumplimiento de las regulaciones pertinentes, ya sea ambientales, de libre competencia, responsabilidad penal de la persona jurídica, entre otras.

2.2. **Sistemas y aplicaciones:** sistemas informáticos y aplicaciones que se utiliza en la Empresa por los colaboradores, para gestionar y operar las actividades, incluyendo herramientas de análisis de datos, sistemas de gestión y cualquier otro sistema que maneje, almacene o procese información de las Compañías.

2.3. **Redes y comunicaciones:** se refiere a la infraestructura de red utilizada, incluyendo conexiones internas y externas, dispositivos de red, firewalls y otros componentes necesarios para el intercambio seguro de información dentro de las Compañías y con entidades externas.

2.4. **Equipos:** incluye todos los 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.

2.5. **Documentación:** comprende los documentos físicos o electrónicos que contienen información para las operaciones de las Compañías, como manuales de procedimientos, políticas internas, contratos, acuerdos de confidencialidad y cualquier otro documento que sea necesario para la gestión de la información.

3. RESPONSABILIDADES

3.1. Dirección

El Directorio es responsable de que los objetivos de seguridad de la información estén establecidos y sean compatibles con la dirección estratégica de Alto Jardín; mientras que la Alta Dirección tiene la responsabilidad de liderar y respaldar la implementación de la Política de Asuntos Informáticos. Esto implica proporcional los recursos necesarios, establecer objetivos y supervisar regularmente el desempeño del sistema de gestión de seguridad de la información.

Además, la Alta Dirección debe garantizar que se establezca en marco de gestión de riesgos de seguridad de la información y asuntos informáticos, asignar roles y responsabilidades claras dentro de la organización, así como de asegurarse de que se realicen revisiones periódicas del sistema de gestión de seguridad de la información para evaluar su eficacia y realizar mejoras continuas.

3.2. Propietarios de activos de información

Cada activo de información de Alto Jardín debe tener un propietario asignado que sea responsable de su protección y gestión adecuadas. Estos propietarios tienen la responsabilidad de:

(i) Identificar y clasificar los activos de información bajo su custodia, asegurándose de comprender su importancia y sensibilidad.

(ii) Establecer controles se seguridad adecuados para proteger los activos de información, basados en las evaluaciones de riesgos y los requisitos de seguridad.

(iii) Definir los requisitos de acceso ya autorización para los activos de información, asegurándose de que sólo se otorguen los privilegios necesarios para la ejecución de sus funciones.

(iv) Supervisar y revisar regularmente la efectividad de los controles de seguridad implementados y tomar medidas correctivas cuando sea necesario.

(v) Colaborar con otros propietarios de activos de información y con equipo de gestión de seguridad de la información para garantizar una gestión coherente y eficaz de los activos de información en toda la organización.

3.3. Colaboradores de Alto Jardín

Todos los colaboradores (trabajadores, socios, etc.) de Alto Jardín tienen responsabilidad en la seguridad de la información y deben cumplir con la presente Política y los procedimientos que de ella deriven. Esto incluye:

(i) Conocer, aceptar y cumplir la política y procedimientos se Asuntos Informáticos, incluida la clasificación de los activos de la información y el manejo adecuado de la información confidencial.

(ii) Participar en programas de capacitación y concientización sobre seguridad de la información para comprender los riesgos y las mejores prácticas de seguridad.

(iii) Informar cualquier incidente de seguridad o vulnerabilidad detectada a los responsables designados, y cooperar en la resolución de los incidentes.

(iv) Utilizar activos de información de manera responsable y asegurarse de protegerlos contra pérdidas, robos o daños físicos.

3.4. Prestadores de Servicios (contratistas, proveedores, asesores, entre otros)

Las medidas que contemplan a los prestadores de servicios de Alto Jardín son, a lo menos, las siguientes:

(i) **Acuerdos de Confidencialidad y Cláusulas de Seguridad**: se requerirá establecer acuerdos de confidencialidad que definan claramente la responsabilidad de los prestadores de servicios para proteger la información confidencial y cumplir con las políticas de Alto Jardín, considerando la Política de Asuntos Informáticos.

(ii) **Control de Acceso y Sensibilización: se proporcionará** capacitación sobre las políticas de seguridad de Alto Jardín y las mejores prácticas para proteger la información confidencial, según el tipo de prestación de servicio.

(iii) **Revisión de Prácticas de Seguridad: se realizarán** auditorías periódicas para verificar que los prestadores de servicios cumplan con las políticas de seguridad y las medidas acordadas.

(iv) **Cifrado y Protección de Datos: se deberá asegurar** que los datos estén encriptados adecuada y proporcionalmente, protegidos durante la manipulación y almacenamientos de los proveedores.

(v) Revocación de Acceso: se seguirá un procedimiento establecido para revocar el acceso a los prestadores de servicios cuando finalice la relación de servicio.

(vi) Informe de Brechas e Incidentes: se deberá contar con cláusulas en los acuerdos que exija a prestadores de servicios informar cualquier brecha o incidente de seguridad de manera inmediata.

(vii) Evaluación de Riesgos: se realizará una evaluación inicial de seguridad para los prestadores de servicios con el objeto de determinar si se ajustan a las medidas de seguridad según el nivel de riesgo o si se deben tomar medidas de resguardo especiales.

Estas medidas serán personalizadas según las características o naturaleza de los prestadores de servicios con los que trabaja Alto Jardín. El objetivo es garantizar la protección de la información confidencial y mantener una colaboración segura y confiable.

4. CONDUCTAS CONSTITUTIVAS DE DELITO Y PROHIBICIONES

4.1. **Ataque a la Integridad de un Sistema informático.** Está prohibido obstaculizar o impedir el normal funcionamiento, total o parcial, de un sistema informático de terceros **través** de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos.

4.2. **Acceso Ilícito.** Está prohibido acceder a un sistema informático sin autorización, o excediendo la autorización otorgada y superando barreras técnicas o medidas tecnológicas de seguridad. También se encuentra prohibido acceder a un sistema informático con el ánimo de apoderarse o usar la información contenida en él, así como también obtener y divulgar la información obtenida de esta manera.

4.3. **Interceptación Ilícita.** Está prohibido interceptar, interrumpir o interferir indebidamente, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de estos. sin autorización de su emisor. Además, está prohibido, sin contar con la debida autorización, captar, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas proveniente de los mismos.

4.4. **Ataque a la Integridad de los Datos Informáticos.** Está prohibido alterar, dañar o suprimir indebidamente datos informáticos, ya sea de la Compañía o de terceros, siempre que con ello se cause un daño grave al titular de los mismos.

4.5. **Falsificación Informática. Está prohibido introducir, alterar, dañar o suprimir datos informáticos, con la intención de que éstos sean tomados como auténticos o utilizados para generar documentos auténticos.**

4.6. **Receptación de Datos Informáticos. Está prohibido comercializar, transferir o almacenar a cualquier título datos informáticos provenientes de los delitos de acceso ilícito, interceptación ilícita y falsificación informática con el mismo objeto u otro fin ilícito, conociendo su origen ilícito o no pudiendo menos que conocerlo.**

La Compañía incorporará cláusulas en los contratos con Terceras Partes que permitan asegurar el origen lícito de los datos informáticos entregados a Alto Jardín por parte de las Terceras Partes con las cuales contrata.

4.7. **Fraude Informático.** Está prohibido 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, con la finalidad de obtener un beneficio económico para sí o para un tercero, causando perjuicio a otro. También está prohibido facilitar a otro los medios con que se comete el fraude informático.

4.8. **Abuso de Dispositivos.** Está prohibido entregar u obtener para su utilización, importar, difundir o realizar otra forma de puesta a disposición dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otro dato similar, creados o adaptados para cometer los delitos de ataque a la integridad de un sistema informático, acceso ilícito, interceptación ilícita y ataque a la integridad de los datos informáticos o de los delitos de uso fraudulento de tarjetas de pago y transacciones electrónicas de la ley N° 20.009.

5. MEDIDAS GENERALES DE CONTROL Y SEGURIDAD

Las medidas de Asuntos Informáticos de Alto Jardín, contemplará a lo menos lo siguiente: (i) acuerdos de confidencialidad, (ii) acceso controlado, (iii) plataformas seguras, (iv) auditorías regulares, (v) capacitación y sensibilización, (vi) gestión de contraseñas, (vii) control de versiones, (viii) notificación de incidentes.

6. CAPACITACIÓN Y DIFUSIÓN

Alto Jardín será responsable de poner en conocimiento de todos sus colaboradores la existencia y contenido del Modelo de Prevención de Delitos, del alcance de la Ley N° 20.393, de la Ley N° 21.595 y la presente Política, difusión que deberá ser hecha de manera didáctica y empleando un lenguaje claro.

Asimismo, Alto Jardín se compromete a realizar comunicados públicos señalando quién es el Encargado de Prevención de Delitos y cuáles son los canales que existen a disposición de los trabajadores para contactarlo.

Además, y para que esta política sea integrada a las labores cotidianas de cada integrante de Alto Jardín, se efectuarán capacitaciones en forma periódica, a lo menos una vez al año, para transmitir los conocimientos mínimos necesarios sobre la materia y la aplicación de sus procedimientos.

Siempre que exista alguna duda sobre el cumplimiento o posible incumplimiento de esta Política o de las políticas y procedimientos que forman parte del Modelo de Prevención de Delitos, deberá consultarse al Encargado de Prevención de Delitos o al Oficial de Cumplimiento, pidiendo su opinión en el tema sin necesidad que ésta sea emitida o enviada de manera formal.

Para otras situaciones que no están cubiertas en esta Política, las políticas y procedimientos que forman parte del Modelo de Prevención de Delitos o en las que se destinan o emplean recursos de la Compañía y están involucrados Funcionarios Públicos, el Encargado de Prevención de Delitos debe ser consultado para mayor orientación, antes de tomar una decisión o llevar a cabo la operación o actividad correspondiente.

7. CANAL DE DENUNCIAS

Si el Personal de la Compañía o Terceras Partes tuviesen motivos razonables o fundados para creer que alguna acción u omisión incumple esta Política o el Modelo de Prevención de Delitos, obligatoriamente debe comunicarlo inmediatamente a través de los siguientes canales:

(i) Denuncia directa y personal ante el Encargado de Prevención de Delitos.

(ii) Comunicación al superior jerárquico. El Personal de la Compañía puede comunicar por escrito a su superior jerárquico sobre cualquier violación a la presente Política. Estas denuncias serán derivadas al Encargado de Prevención de Delitos. El superior jerárquico tiene en estos casos el deber de preservar y garantizar la confidencialidad de la identidad del denunciante.

(iii) Denuncia anónima a través de la página web y al correo electrónico denuncias@altojardin.cl.

La denuncia será tramitada de acuerdo a lo determinado en el Protocolo de procedimiento de denuncias, investigación y sanciones.

Para aquello, se debe considerar como principio general que, frente a dudas o sospechas respecto a una posible cocción al Modelo de Prevención de Delitos, a normativa interna de la Compañía o a toda otra normativa que incida sobre la actividad de la misma, se solicita a todo empleado, colaborador de Alto Jardín o tercero que formule una denuncia mediante los Canales de Reportes establecidos.

Los empleados deberán prestar toda su colaboración en los procedimientos internos de investigación que se lleven a cabo dentro del marco del Modelo de Prevención de Delitos. Las políticas y procedimientos indicados en el Modelo de Prevención de Delitos son de obligatorio cumplimiento y se incorporan a las funciones y responsabilidades asignadas a cada empleado.

8. SANCIONES

Todo integrante de Alto Jardín debe conocer el contenido del Modelo de Prevención de Delitos y la presente política y deberá regirse por sus lineamientos en todo momento.

El incumplimiento de los términos del Modelo de Prevención de Delitos y de las Políticas de Alto Jardín por parte de los empleados o los integrantes de la Compañía podrá ser objeto de las sanciones que se establezcan en los instrumentos internos de la Compañía o que se indiquen en la normativa legal vigente.

En el caso de los asesores, contratistas o proveedores, el incumplimiento de los términos del Modelo de Prevención de Delitos y la presente política podrá ser causa de **término inmediato** del contrato que se mantenga vigente.