POLÍTICA SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	Francisco Javier Hidalgo Zelada, Sistemas y Ciberseguridad
Revisado por:	George Fotinos, Gerente de Tecnologías de la Información/ Consuelo Herrera, Gerente de Auditoría y Compliance /BCP Abogados / AJ Consulting
Aprobado por:	Directorio en sesión de 14 de septiembre de 2023
Alcance:	Interno y externo

Introducción

En la Corporación Sistema Colectivo de Gestión de Envases y Embalajes ReSimple, en adelante "ReSimple" o la "Corporación", como organización dedicada al reciclaje y comprometida con la protección del medio ambiente, reconocemos la importancia de los activos de información para el funcionamiento eficiente y seguro de nuestras operaciones.

La Política de Seguridad la Información, en adelante la "Política", establece los principios y directrices que debemos 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.

Los activos de información en ReSimple abarcan una amplia gama de recursos, como bases de datos de clientes, información financiera, informes de cumplimiento normativo y comunicaciones internas. Entendemos que la correcta gestión de estos activos es fundamental para mantener la confianza de nuestros clientes, cumplir con las regulaciones de libre competencia y ambientales y garantizar la continuidad de nuestras operaciones.

Nuestra Política establece los lineamientos para identificar y evaluar los activos de información críticos para nuestra empresa, 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.

En ReSimple nos comprometemos a implementar controles de seguridad adecuados para proteger nuestros 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, estableceremos medidas técnicas, físicas y administrativas para salvaguardar la información y promover prácticas seguras en toda la organización.

La gestión adecuada de los activos de información no solo contribuye a la protección de nuestra Corporación y nuestros clientes, sino que también refuerza nuestro compromiso con la sostenibilidad, el respeto por el medio ambiente y la legislación vigente, en especial en materia de libre competencia. Al asegurar la disponibilidad de la información necesaria para tomar decisiones informadas, podemos mejorar continuamente nuestros procesos y maximizar nuestra eficiencia operativa.

En resumen, esta Política refuerza nuestra dedicación a la seguridad, integridad y disponibilidad de los activos de información que respaldan nuestras operaciones de reciclaje, al tiempo que reafirma nuestro compromiso con el cumplimiento normativo y la protección del medio ambiente.

Alcance de la Política de Seguridad de la Información de ReSimple

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

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 para nuestras operaciones y para cumplir con nuestros compromisos.

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

Datos y registros: Esto abarca 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 nuestras operaciones y el cumplimiento de las regulaciones ambientales, de libre competencia y de responsabilidad penal de la persona jurídica, entre otras.

Sistemas y aplicaciones: Engloba los sistemas informáticos y aplicaciones que utilizamos para gestionar y operar nuestras actividades de reciclaje, incluyendo software de seguimiento de inventario, plataforma de declaración de línea base y patio trasero, software de trazabilidad y tracking, herramientas de análisis de datos, sistemas de gestión de residuos y cualquier otro sistema que maneje, almacene o procese información crítica para nuestra organización.

Redes y comunicaciones: Se refiere a la infraestructura de red utilizada en ReSimple, 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: 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.

Documentación: Esto comprende todos los documentos físicos o electrónicos que contienen información crítica para nuestras operaciones, como manuales de procedimientos, políticas internas, contratos, acuerdos de confidencialidad y cualquier otro documento que sea necesario para la gestión de la información en ReSimple.

Esta Política se aplica a todos los activos de información, independientemente de su ubicación física o digital, dentro de nuestras instalaciones, en dispositivos móviles o en la nube.

En resumen, esta política tiene como objetivo garantizar una gestión adecuada de todos los activos de información en ReSimple, abarcando desde los datos y sistemas hasta la infraestructura de red, equipos y documentación. Al aplicar esta Política, buscamos salvaguardar la información crítica para nuestras operaciones, garantizar el cumplimiento normativo y proteger la confidencialidad, integridad y disponibilidad de nuestros activos de información.

Principios de Seguridad de la Información

ReSimple, se rige por los siguientes principios en relación con la seguridad de la información:

Confidencialidad: La Corporación 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 ReSimple, debiendo ser guardada como Información Confidencial y no será revelada ni divulgada a terceros sin autorización previa, escrita y expresa de ReSimple.

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

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

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

Gestión de riesgos: Se identificarán, evaluarán y mitigarán los riesgos de seguridad de la información a través de un enfoque basado en evaluaciones de riesgos y mejores prácticas La Corporación tendrá una tabla de criterios de aceptación de riesgos, donde se especificará la probabilidad de ocurrencia y cuantificará el impacto de este (limitaciones de servicio, pérdida de datos, continuidad operativa, daños reputacionales, entre otros), asignándole un nivel de riesgo. Todos los riesgos identificados contarán con un propietario del riesgo, quien deberá proponer un plan de tratamiento de los riesgos identificados y asegurar la ejecución del plan

para mitigar los mismos. El propietario del riesgo será el Ingeniero asignado por el área de Ciberseguridad, bajo responsabilidad del Gerente de TI.

Responsabilidad: Toda persona que ocupa un cargo, función o posición en ReSimple, incluyendo directores, ejecutivos principales, trabajadores y todos aquellos que presten servicios a la corporación como contratistas, gestores de residuos, proveedores o asesores, así como los terceros que acceden, utilizan o manejan activos de información de ReSimple son responsable de cumplir con las políticas y procedimientos de seguridad de la información establecidos por ReSimple. A los socios de la Corporación se les enviará una vez por año, una guía de buenas prácticas de ciberseguridad, entendiendo que cada socio cuenta con sus propias políticas.

Responsabilidades

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 la ReSimple; mientras que la Alta Dirección tiene la responsabilidad de liderar y respaldar la implementación de la Política de la Seguridad de la Información. Esto implica proporcionar los recursos necesarios, establecer objetivos y supervisar regularmente el desempeño del sistema de gestión de seguridad de la información (SGSI).

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

2. Propietarios de activos de información:

En ReSimple, cada activo de información debe tener un propietario designado que sea responsable de su protección y gestión adecuadas. Estos propietarios tienen la responsabilidad de:

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

- Establecer controles de seguridad adecuados para proteger los activos de información, basados en las evaluaciones de riesgos y los requisitos de seguridad.

- Definir los requisitos de acceso y autorización para los activos de información, asegurándose de que sólo se otorguen los privilegios necesarios para la ejecución de sus funciones.

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

- Colaborar con otros propietarios de activos de información y con el 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. Trabajadores de ReSimple:

Todos tienen responsabilidades en la seguridad de la información y deben cumplir con esta Política y los procedimientos que de ella deriven. Esto incluye:

- Conocer y cumplir la Política y procedimientos de seguridad de la información de ReSimple, incluida la clasificación de los activos de la información y el manejo adecuado de la información confidencial.

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

- Informar cualquier incidente de seguridad o vulnerabilidad detectada a los responsables designados (Líder de equipo y Gerente de TI) y cooperar en la resolución de dichos incidentes.

- Utilizar los activos de información de manera responsable y asegurarse de protegerlos contra pérdidas, robos o daños físicos.

4. Prestadores de servicios (contratistas, gestores de residuos, proveedores o asesores).

Es importante establecer medidas de seguridad de la información para los prestadores de servicios que interactúan con ReSimple, como contratistas, gestores de residuos, proveedores o asesores, las que considerarán a lo menos:

- 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.

Ejemplo: Un contratista que se encarga del desarrollo de software firmará un Acuerdo de Confidencialidad que incluye cláusulas sobre cómo manejar los datos y el código fuente confidencial compartido.

- Control de Acceso y Autenticación: Los prestadores de servicios deben acceder solo a los recursos y datos necesarios para llevar a cabo sus funciones. Se debe implementar autenticación segura y control de acceso basado en roles.

Ejemplo: Un proveedor de servicios de TI tendrá acceso limitado solo a los sistemas específicos que necesita para brindar soporte técnico.

- Capacitación y Sensibilización: Proporcionamos capacitación sobre las políticas de seguridad de la Corporación y las mejores prácticas para proteger la información confidencial, según el tipo de prestación de servicio.

Ejemplo: Antes de comenzar a trabajar con gestores de residuos externos, se les proporcionará un módulo de capacitación en línea.

- Revisión de Prácticas de Seguridad: Realizamos de 1 a 2 auditorías anuales para verificar que los prestadores de servicios cumplan con las políticas de seguridad y las medidas acordadas.

Ejemplo: Un asesor legal externo permitirá a nuestro equipo de seguridad de la información realizar una revisión anual de sus prácticas de seguridad y gestión de datos de ReSimple.

- Cifrado y Protección de Datos: Nos aseguramos de que nuestros datos estén encriptados adecuadamente y protegidos durante la manipulación y almacenamiento de nuestros proveedores.

Ejemplo: Un contratista que maneja datos de clientes en su software implementará el cifrado de extremo a extremo para asegurar la privacidad de los datos.

- Revocar de Acceso: Contamos con un procedimiento para revocar el acceso a los prestadores de servicios cuando finalice la relación de servicio.

Ejemplo: Cuando el contrato con un asesor concluya, se desactivarán de inmediato sus cuentas y accesos a los sistemas (correo, acceso a documentos compartidos) de nuestra organización.

- Informe de Brechas e Incidentes: Contamos con cláusulas en los acuerdos que exija a los prestadores de servicios informar cualquier brecha o incidente de seguridad de manera inmediata.

Ejemplo: Un proveedor de servicios de gestión de residuos nos notificará en un plazo máximo de 24 horas si se produce una filtración de documentos confidenciales.

- Evaluación de Riesgos: Realizamos una evaluación inicial de seguridad para los prestadores de servicios con el objeto de determinar si se ajustan a nuestras medidas de seguridad según el nivel de riesgo o si debemos tomar medidas de resguardos especiales.

Ejemplo: Antes de contratar a un nuevo proveedor de servicios de marketing digital, evaluamos sus prácticas de seguridad y establecemos medidas adecuadas en función de la sensibilidad de los datos a los que accederán.

Estas medidas son personalizadas según las características o naturaleza de nuestros prestadores de servicios con los que trabajamos. La clave es garantizar la protección de la información confidencial y mantener una colaboración segura y confiable.

5. Socios de la Corporación

El trabajo seguro con socios de ReSimple implica un enfoque holístico de seguridad de la información. Pese a que nuestros socios suelen tener sus propias políticas de seguridad, trabajar juntos para establecer estándares compartidos y asegurar la protección de los datos confidenciales es fundamental para mantener la confianza y la integridad en la relación entre las partes.

Las medidas tomadas son las siguientes:

- Acuerdos de Confidencialidad (NDA): Acuerdos de confidencialidad sólidos (Non-Disclosure Agreements) con nuestros socios antes de compartir cualquier información confidencial. Esto crea una base legal para asegurar que la información no será compartida o utilizada de manera inapropiada.
- Acceso Controlado: Otorgamos acceso a la información confidencial solo a las personas que realmente necesitan conocerla. Utilizamos sistemas de autenticación y autorización sólidos para asegurarte de que solo los usuarios autorizados tengan acceso.
- Encriptación: Encriptamos los datos confidenciales tanto en tránsito (en proceso de envío en el caso de un correo) como en reposo (guardados en nuestros equipos). Esto ayudará a prevenir que terceros no autorizados accedan a la información incluso si logran interceptarla.
- Plataformas Seguras: Utilizamos plataformas y servicios seguros para compartir información confidencial. Esto lo determina nuestra Gerencia de TI y con el equipo o encargado de Ciberseguridad quien revisa las plataformas y poniendo énfasis en las versiones, actualizaciones, protocolos, estándares, entre otros detalles.
- Auditorías Regulares: Realizamos auditorías periódicas para evaluar la seguridad de la información compartida con los socios. Esto nos ayuda a identificar posibles vulnerabilidades o puntos débiles en el sistema.

- **Capacitación y Sensibilización:** Realizamos capacitaciones regular a los empleados y socios sobre las mejores prácticas de seguridad de la información. La sensibilización es fundamental para prevenir amenazas internas y errores accidentales, como se menciona en el en el ítem de "Responsabilidades" en el punto 3 en las responsabilidades de los trabajadores de la corporación.
- **Gestión de Contraseñas:** Damos credenciales de acceso al "Portal Empresa" de forma controlada, asegurándonos de que las contraseñas sean seguras, cambiables periódicamente (2 veces al año), enviando recordatorio y realizando monitoreo a los "Log Access" y votando sesión según tiempo de inactividad máximo 30 min.
- **Control de Versiones:** Utilizamos un sistema de control de versiones para rastrear cambios y asegurar de que solo las versiones autorizadas estén disponibles, almacenando nuestras versiones oficiales en Sharepoint con acceso restringido solo a personal autorizado.
- **Notificación de Brechas:** Contamos con un plan de acción claro en caso de una violación de seguridad. Esto incluye notificar a las partes afectadas y tomar medidas para mitigar los daños.

6. Equipo de Gestión de la Seguridad de la Información:

El Gerente de Tecnologías de la Información encabeza un equipo de Gestión de la Seguridad de la Información encargado de la estrategia de seguridad de la información de la Corporación y de supervisar y monitorear las actividades relacionadas con la Política de Seguridad de la información. Este equipo tiene las siguientes responsabilidades:

- Desarrollar y mantener el SGSI de acuerdo con los requisitos de la norma ISO 27001.

- Coordinar la identificación y clasificación de activos de información y asegurarse de que se asignen propietarios responsables.

- Establecer controles de seguridad apropiados y evaluar regularmente su efectividad.

- Realizar evaluaciones de riesgos y gestionar las vulnerabilidades y amenazas identificadas.

- Realizar evaluaciones de riesgos y gestionar las vulnerabilidades y amenazas identificadas, implementando medidas de mitigación adecuadas.

- Establecer y mantener políticas y procedimientos de seguridad de la información, asegurándose de que sean consistentes con los requisitos de la norma ISO 27001 y otras regulaciones aplicables.

- Supervisar el cumplimiento de las políticas de seguridad de la información y realizar al menos una auditoría interna periódica para identificar debilidades, proponer mejoras continuas, validar si las políticas se están cumpliendo y prepararnos para una auditoría externa.

- Mantenerse actualizado sobre las mejores prácticas y avances en seguridad de la información, y proponer mejoras y actualizaciones en el SGSI según sea necesario.

- Actuar como punto focal para la gestión de incidentes de seguridad de la información, coordinando la respuesta a incidentes, investigando y documentando los incidentes, y tomando medidas correctivas para evitar futuras incidencias.

- Fomentar una cultura de seguridad de la información en toda la organización a través de programas de capacitación al personal que se integre a los distintos equipos de Corporación, plan de concientización y promoción de buenas prácticas de seguridad con actividades, como charlas, correos informativos y evaluaciones. De estas actividades deberá mantener un registro y archivo quedarán con el objeto de poder reutilizar dicho material para inducciones u otras instancias.

- Mantener una comunicación efectiva con la alta dirección y otras unidades y equipos relevantes para garantizar la alineación de estos con las Política de Seguridad de la Información.

El Gerente de Tecnologías de la Información designará un responsable de la operatoria diaria para asegurar la implementación efectiva de la presente Política.

El equipo de gestión de seguridad de la información desempeña un papel fundamental en la implementación y mantenimiento de un entorno seguro para los activos de información de ReSimple. Su experiencia y conocimiento en seguridad de la información ayudan a garantizar que se apliquen medidas adecuadas y se tomen acciones proactivas para proteger la confidencialidad, integridad y disponibilidad de los activos de información, y para cumplir con los requisitos de la norma ISO 27001 y otras regulaciones pertinentes.

7. Consecuencias del incumplimiento

Toda infracción o incumplimiento a esta política será considerado incumplimiento grave de las obligaciones que impone el contrato de trabajo a los colaboradores de ReSimple. El incumplimiento de esta política faculta a ReSimple a aplicar las sanciones que se contemplan el Reglamento Interno de Higiene, Orden y Seguridad, sin perjuicio de las acciones judiciales que puedan dirigirse contra el transgresor para hacer efectiva su responsabilidad tanto civil como penal.

Toda infracción o incumplimiento de esta Política por parte de los socios de la Corporación puede resultar en medidas disciplinarias contempladas en los estatutos de ReSimple, determinadas por la Comisión de Ética previa investigación de la Gerencia de Auditoría y Compliance, sin perjuicio de las acciones judiciales que puedan dirigirse para hacer efectiva la responsabilidad tanto civil como penal.

Toda infracción o incumplimiento de esta Política por parte todos aquellos que presten servicios a la Corporación como contratistas, gestores de residuos, proveedores o asesores, así como los terceros que acceden, utilizan o manejan activos de información de ReSimple, puede resultar en sanciones o consecuencias de acuerdo con lo previsto en los respectivos contratos, sin perjuicio de las acciones judiciales que puedan dirigirse para hacer efectiva la responsabilidad tanto civil como penal.

Medidas de Seguridad

1. Acceso y control de la información:

Identificación y autenticación: Implementamos mecanismos de identificación y autenticación para garantizar que solo los usuarios autorizados puedan acceder a los activos de información. Esto incluye el uso de contraseñas seguras, autenticación multifactorial y el control de accesos basado en roles.

Control de acceso: Establecimos políticas y procedimientos para gestionar los permisos de acceso a los activos de información, asegurando que los usuarios tengan los derechos y privilegios adecuados según sus funciones y responsabilidades. Además, se revisarán y actualizarán regularmente los derechos de acceso para evitar privilegios innecesarios o no autorizados.

Gestión de sesiones: Implementamos controles para gestionar y controlar las sesiones de usuario, incluyendo el cierre automático de sesiones inactivas, el registro de actividad de inicio de sesión y la detección de actividades sospechosas.

2. Protección contra software malicioso:

Antivirus y antimalware: Implementamos soluciones antivirus y antimalware actualizadas y eficaces en todos los sistemas y dispositivos utilizados en ReSimple. Estas soluciones se configurarán para realizar escaneos periódicos, mantener las definiciones de virus actualizadas y generar alertas en caso de detección de amenazas.

Actualizaciones y parches de seguridad: Mantenemos un programa de gestión de parches y actualizaciones para garantizar que todos los sistemas y aplicaciones utilizados en ReSimple estén actualizados con las últimas correcciones de seguridad. Esto incluye la aplicación

oportuna de parches críticos y la realización de pruebas de seguridad posteriores a la implementación.

Concientización y capacitación: Realizamos capacitaciones de manera regular a los trabajadores de ReSimple sobre la importancia de la seguridad informática, incluyendo la detección de software malicioso, el manejo seguro de archivos adjuntos y enlaces, y las prácticas recomendadas para evitar infecciones.

3. Seguridad de la red:

Perímetro de seguridad: Implementamos firewalls y dispositivos de seguridad de red para controlar y monitorear el tráfico entrante y saliente, y para prevenir ataques externos no autorizados. Se establecerán políticas de filtrado para permitir únicamente el tráfico legítimo y se realizarán pruebas periódicas de penetración para evaluar la efectividad de las medidas de seguridad.

Detección y prevención de intrusiones: Utilizamos sistemas de detección y prevención de intrusiones (IDS/IPS) para monitorear y analizar el tráfico de red en busca de actividades sospechosas o maliciosas. Estos sistemas generarán alertas en tiempo real y tomarán medidas preventivas para mitigar cualquier intento de intrusión.

Seguridad inalámbrica: Implementaremos medidas de seguridad adecuadas para proteger nuestras redes inalámbricas, como el uso de autenticación segura, encriptación de datos y segmentación de redes. También se establecerán políticas y procedimientos para el uso seguro de dispositivos móviles y la conexión a redes externas.

En línea con las mejores prácticas de la norma ISO 27001, estas medidas de seguridad proporcionan una base sólida para proteger los activos de información en ReSimple.

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 ReSimple y sus asociados, 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 ReSimple, incluyendo directores, ejecutivos principales y trabajadores, además de los socios de la Corporación, y todos aquellos que presten servicios a la Corporación como contratistas, gestores de residuos, proveedores o asesores, así como los terceros que acceden, utilizan o manejan activos de información de ReSimple, 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.

1. 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).

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. 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).

3. 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).

4. 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).

5. 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).

6. 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).

7. 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).

8. 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).

Comunicación de la Política

Para asegurar la efectiva implementación de esta Política, es fundamental que todo el personal esté al tanto de su contenido, además de conocer los aspectos relevantes de la normativa aplicable. Asimismo, es necesario que todos los colaboradores comprometan su adhesión a la ésta.

Con el fin de asegurar que todos los colaboradores de la corporación estén debidamente informados sobre esta materia, además de las disposiciones incorporadas a sus contratos de trabajo, ReSimple ha dispuesto las siguientes medidas de comunicación:

a) La información relacionada a la presente Política estará disponible para todo el personal de ReSimple en sus redes de comunicación internas y externas;

b) Difusión sobre buenas prácticas, controles, obligaciones y prohibiciones para prevenir la comisión de delitos; y

c) Capacitación regular y continua.

Actualización y revisión continua de la Política

Esta Política se revisará y actualizará anualmente o cuando sucedan cambios en ReSimple que justifiquen su modificación.