POLÍTICA CORPORATIVA: SEGURIDAD DE LA INFORMACIÓN EMPRESAS SUTIL S.A. Y FILIALES

Empresas Sutil S.A. y Filiales

Índice

I. OBJETIVO **3**

II. ALCANCE **3**

III. DEFINICIONES **3**

IV. PRINCIPIOS **4**

V. RESPONSABILIDADES **5**

VI. POLÍTICAS – MARCO NORMATIVO **6**

A. POLÍTICA DE PROTECCIÓN DE ACTIVOS DE INFORMACIÓN 6
B. POLÍTICA REFERIDA A LA GESTIÓN DE LAS PERSONAS RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN QUE GENERAN Y UTILIZAN 9
C. POLÍTICA REFERIDA AL CUMPLIMIENTO DE LAS DISPOSICIONES LEGALES, REGULATORIAS O CONTRACTUALES 11

VII. RESPONSABILIDAD GERENCIAS, DEPARTAMENTOS, ENCARGADOS DE TECNOLOGÍA DE LA INFORMACIÓN (TI) **13**

VIII. VIGENCIA Y MODIFICACIONES **14**

ANEXO N°1 ..... ¡Error! Marcador no definido.

I. OBJETIVO

El objetivo de esta Política Corporativa de Seguridad de la Información (en adelante, la "**Política**") es establecer los lineamientos corporativos, criterios y principios generales sobre la gestión de Seguridad de la Información, aplicables en Empresas Sutil S.A. y Filiales.

La Política tiene como propósito garantizar la protección de la información de las compañías en todas sus formas y medios, evitando su uso no autorizado, divulgación indebida o interrupción. De este modo, se busca asegurar la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, y coherencia de la información con los requisitos del negocio, las leyes y normativas pertinentes. Asimismo, esta Política contribuye al cumplimiento del Modelo de Prevención de Delitos, en virtud de lo dispuesto en la Ley N°20.393 que establece la responsabilidad penal de las personas jurídicas.

La Política ha sido confeccionada en virtud de la Norma ISO 27002:2022 vigente, específicamente en relación con las directrices establecidas en el punto 5 de dicha norma.

II. ALCANCE

La presente Política es aplicable y de cumplimiento obligatorio para cualquier persona que ejerza un cargo, función o posición al interior de Empresas Sutil S.A. y sus filiales (en adelante, los "**Colaboradores**"). De esta forma, la Política se aplicará para las siguientes sociedades: (i) Empresas Sutil S.A., (ii) Coagra S.A., (iii) Banagro S.A. y Afiliada, (iv) Coagra Agroindustrial S.A., (v) Pacific Nut Company Chile S.A. y Afiliadas, (vi) Frutícola Olmué SpA y Afiliadas, (vii) Champiñones Abrantes S.A., (viii) Agrícola Sutil S.A. y Afiliadas, (ix) Top Wine Group S.A., y (x) Hotel Viña La Playa (en adelante, todas juntas, "**Grupo Sutil**" o la "**Compañía**").

Asimismo, Grupo Sutil procurará que cualquier persona natural o jurídica que preste servicios gestionando asuntos en nombre de Grupo Sutil, aunque no tenga poder de representación (en adelante, los "**Terceros Relacionados**"), conozcan y compartan los principios de esta Política.

III. DEFINICIONES

Activo: Es el conjunto de bienes y derechos necesarios para el mantenimiento de las actividades de la Compañía.

Activo de Información: Se entiende por activo de información todo elemento que posee valor para el desarrollo y continuidad de las actividades de la Compañía. Esto incluye documentos, sistemas, infraestructura y personas que participan en la generación, almacenamiento, comunicación, visualización y recuperación de información relevante para las sociedades que forman parte de Grupo Sutil. Estos activos se clasifican en tres niveles:

i. Información propiamente tal, en cualquiera de sus formatos (papel, digital, texto, imagen, audio, video), sin importar su medio de almacenamiento o transmisión, ya sea físico o electrónico.
ii. Equipos, sistemas e infraestructura que soportan y permiten el manejo seguro y eficiente de la información.
iii. Personas que utilizan, gestionan y resguardan la información, y que poseen conocimiento de los procesos institucionales asociados.

Amenaza: Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o proceso.

Disponibilidad: Es el principio que establece que la información debe ser accesible y utilizable oportunamente por las personas o procesos autorizados, en el formato requerido para su procesamiento.

Dueño de la información: Es el autor de la información, responsable por clasificar e identificar controles necesarios para mantener la seguridad de la información.

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 series de eventos de seguridad de la información, no deseados o inesperados, que compromete la seguridad la información y amenazan la operación del negocio.

Riesgo: Es la posibilidad de que ocurra uno o más eventos que afecten adversamente el logro de los objetivos de Grupo Sutil. Se mide combinando las consecuencias del evento (impacto) y su probabilidad de ocurrencia.

Seguridad de la información: Conjunto de acciones para la preservación de la confidencialidad, integridad y disponibilidad de la información de la Compañía.

Usuario: Incluye cualquier persona que esté autorizada para ingresar a los sistemas de información o a los servicios de sistemas TI de Grupo Sutil.

Vulnerabilidad: Es una debilidad de cualquier activo de un grupo de activos que puede ser explotado por una o más amenazas**.**

IV. PRINCIPIOS

a) Confidencialidad: Para garantizar que la información solo sea accesible a las personas autorizadas. Esto implica proteger los datos sensibles y la información confidencial de nuestros Colaboradores, clientes y Terceros Relacionados para evitar el acceso no autorizado, ya sea interno o externo.

b) Integridad: Para asegurar que los datos y la información no sean alterados de manera no autorizada, ya sea de forma intencionada o accidental. La integridad asegura que los datos sean precisos, completos y fiables.

c) Disponibilidad: Para mantener los sistemas, servicios y datos accesibles cuando sean requeridos por los usuarios autorizados. Esto incluye medidas de continuidad de negocio y recuperación ante desastres para asegurar la operación continua en caso de fallos o ataques.

d) **Autenticidad:** Para verificar que tanto los usuarios como las fuentes de información sean legítimos. Esto implica establecer mecanismos de autenticación, como contraseñas seguras y dobles factores de autenticación para confirmar identidades.

e) **Seguridad por diseño:** Para incluir medidas de seguridad desde las primeras etapas de diseño y desarrollo de sistemas y aplicaciones, en lugar de agregarlas como un complemento posterior. Esto asegura que la seguridad esté integrada en la arquitectura del sistema.

f) **Cifrado:** Utilizando técnicas de cifrado para proteger la información durante su almacenamiento y transmisión, asegurando que solo las partes autorizadas puedan descifrar los datos.

g) **Gestión de riesgos:** Para identificar, evaluar y mitigar los riesgos relacionados con la seguridad de la información de forma proactiva. Esto incluye realizar evaluaciones periódicas para adaptar las medidas de seguridad a nuevas amenazas y vulnerabilidades.

V. RESPONSABILIDADES

Todos los Colaboradores que desarrollen actividades, permanentes o transitorias, en alguna de las sociedades de Grupo Sutil, o quienes actúen en su representación, son responsables de la seguridad de la información a que tuviesen acceso, producto de las funciones que en el desempeño de sus actividades les corresponda realizar, debiendo desarrollar una aplicación irrestricta de su clasificación y precaución de uso de acuerdo a su criticidad, durabilidad y disposición en cualquier forma y medio.

a) Directorios

Es de responsabilidad de los comités ejecutivos y la alta administración de cada sociedad de Grupo Sutil apoyar esta Política y las normas internas, asegurando su implementación, facilitando el cumplimiento y su aplicación.

b) Gerencias, Departamentos, Encargados de Tecnología de la Información (TI)

Tienen la responsabilidad permanente de la gestión de la seguridad de la información a través de:

- El desarrollo, implementación de protocolos, estándares, procedimientos y manuales que propicien la seguridad de la información.
- Dar las directrices para el desarrollo de la infraestructura de TI Segura (información y sistemas).
- Planear, desarrollar, delegar y monitorear los planes de acción para cumplir con lo definido por esta política.
- Analizar y actuar en casos de incidentes de Seguridad.
- Capacitar en seguridad de la información y uso de herramientas tecnológicas.

c) Gerentes y Jefaturas

Estos tienen una responsabilidad adicional, al operar dentro de los límites de esta Política, lo que incluye:

- Tener un comportamiento ejemplar con relación a la Seguridad de la Información.

- Monitorear, reportar y responder a los incidentes de seguridad, desviaciones en la conducta y amenazas del negocio.
- Evaluar, analizar y tratar los riesgos y respectivas vulnerabilidades de la infraestructura y procesos de las sociedades del Grupo.

d) Colaboradores

Todos los Colaboradores se comprometen a cumplir con esta Política. Siempre que tienen acceso a recursos e información deben adherir y cumplir con los principios de esta Política, informar de manera inmediata la existencia de cualquier brecha, incidente o violación de ésta, como así también acciones que pongan en riesgo la seguridad de la información de dominio de Grupo Sutil.

VI. POLÍTICAS – MARCO NORMATIVO

Las políticas que se describen a continuación se establecen y consideran como parte del marco normativo de Seguridad de la Información, esto es, como políticas específicas de la seguridad de la información del Grupo.

De acuerdo a los criterios definidos en la norma ISO 27002:2022, estas políticas se han agrupado en tres grandes grupos:

a) Políticas referidas a los Activos de información.
b) Políticas referidas a la gestión de personas respecto de la seguridad de la información que generan y utilizan.
c) Políticas referidas al cumplimiento de disposiciones legales, regulatorias o contractuales.

A. POLÍTICA DE PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

El objeto de esta política es la protección de los activos de Grupo Sutil, esto es, los sistemas, tecnología, información y servicios, contra amenazas internas y/o externas, o de acciones intencionales, tales como fraudes que puedan causar daño a la confidencialidad, integridad y disponibilidad de la información propietaria.

Por tanto, se instruye a las Compañías que forman el Grupo Sutil a:

i. Realizar un levantamiento de todos los activos de información con los que cuenta cada sociedad.

ii. Clasificar toda la información de acuerdo con su criticidad, y/o dependiendo de su tratamiento en los procesos, sistemas, almacenamiento, divulgación y transmisión, para asegurar que la información tenga el nivel que amerite el proyecto.

Para estos efectos, la información puede clasificarse en:

1. Información Confidencial:

a. Información financiera, contable y corporativa de Grupo Sutil.
b. Datos de clientes y sus socios o accionistas, respecto de los cuales se ha entregado la

correspondiente autorización de conformidad con la Ley N°19.628 y la Ley N°21.719, que regula la protección y el tratamiento de datos personales.

c. Datos de proveedores.
d. Datos de clientes.
e. Datos de Empresas Relacionadas y sus respectivos contactos.
f. Datos personales de los Colaboradores de Grupo Sutil respecto de los cuales se ha entregado la correspondiente autorización de conformidad con la ley.

2. **Información Privada:** Información que incluye datos, registros, documentos y detalles que están destinados exclusivamente para uso interno o para un grupo específico de Colaboradores o partes interesadas, y no están destinadas a ser compartidas públicamente. Esta información a menudo incluye datos comerciales confidenciales, como estrategias, planes, políticas, secretos comerciales, información de clientes y cualquier otra información que la Compañía considere de naturaleza estratégica.

3. **Información Pública:** Información que puede ser divulgada fuera de la Compañía, pues su divulgación pública está alineada con la decisión estratégica de comunicación de la Compañía y no causa ningún daño o impacto para usuarios, clientes o la Compañía. Incluye información de reportes e indicadores financieros, contables, balances y demostrativos financieros publicados en el mercado; informaciones reglamentarias; certificaciones; premios nombrados a la organización y materiales de comunicación con el público externo.

4. **Información Sensible:** Información de uso restringido, que, en caso de divulgación indiscriminada, ocasiona o puede ocasionar serios perjuicios y/o consecuencias en los ámbitos de negocio, financiero, legal y/o estratégico para la Compañía, sus Colaboradores, Terceros Relacionados y/o partners. Incluye información de datos personales sensibles (de acuerdo con las leyes de protección de datos personales), datos de niños y adolescentes, datos financieros del titular, y datos estratégicos del negocio.

La información de las sociedades de Grupo Sutil solamente puede ser entregada y distribuida internamente para fines apropiados, respetando su confidencialidad y protegiendo la seguridad de la misma, conforme las medidas, condiciones y protecciones definidas por las áreas de TI de cada empresa de Grupo Sutil.

Todos los recursos informáticos de Grupo Sutil deben contar con un software anti-malware, actualizado y sus definiciones (por ejemplo, lista de virus y motores de búsqueda), independientemente del sistema operativo instalado y siempre que sea técnicamente posible.

Todos los recursos informáticos deben ser físicamente asegurados. El acceso físico a los sistemas incluyendo la infraestructura de red, debe mantenerse en un área de acceso restringido y controlado.

iii. Proteger los dispositivos personales y de la Compañía: El uso por parte de nuestros Colaboradores de sus dispositivos digitales para acceder a cuentas de correos electrónicos de la Compañía, infiere un riesgo de seguridad en los datos administrados, por lo cual se aconseja el manejo seguro de las computadoras personales y equipos móviles. Por lo anterior, se debe:

- Mantener todos los dispositivos protegidos con contraseña.
- No dejar sus dispositivos expuestos o desatendidos.
- Iniciar sesión en las cuentas y sistemas de la Compañía sólo a través de redes seguras y privadas (conocidas). Nunca usar la cuenta corporativa para iniciar sesión en sitios ajenos al de uso laboral, ya que las bases de datos se comparten y aumenta la factibilidad de envíos de spam.
- Seguir las directrices de las áreas de TI de cada filial para proteger sus dispositivos y consultar a los especialistas de esta área en caso de cualquier duda.
- Queda absolutamente prohibido incorporar a los equipos computacionales de propiedad de Grupo Sutil softwares que no tengan licencia.
- Generar procedimientos de seguridad física de los servidores, control de acceso, control de temperaturas, extintor, etc.
- Generar procedimientos de seguridad y respaldo de los servidores alojados en la nube.
- El uso de los equipos debe ser sólo para uso laboral y no personal.

Asimismo, se obliga a no utilizar softwares de propiedad de terceros en los computadores de la Compañía sin la expresa autorización del Empleador.

iv. Respaldo de información:

1. **Equipos:** Cada Colaborador es responsable del adecuado respaldo de la información de sus equipos, lo cual se sugiere realizar de forma mensual. Para hacer esto pueden solicitar ayuda al área de TI de la filial a la cual pertenece. No obstante, para determinados usuarios que cumplen funciones críticas, la filial debe contar con esquemas de respaldo periódico diario. Es importante recalcar no se debe tener información confidencial de clientes, de Terceros Relacionados o de la Compañía en los laptops (almacenamiento local). Esta debe ser almacenada en los drives / sitios que las sociedades de Grupo Sutil disponen para eso.

2. **Correos electrónicos:** Los Colaboradores de cada filial de Grupo Sutil son los responsables de la administración y correcto almacenamiento de sus correos. Para esto se ha puesto a su disposición una cuenta con capacidad definida por la filial. Será responsabilidad de cada uno la correcta gestión de correos para no sobrepasar el límite definido y solicitar ayuda al área de TI ante cualquier problema referente a esto.

3. **Servidores:** Las áreas de TI serán responsables por la implementación de un sistema de respaldo periódico, el cual debe contener el 100% de los servidores utilizados por la filial sean estos físicos o de almacenamiento Cloud.

4. **Robo de equipos:** Se debe generar un procedimiento donde se indique de manera clara qué debe realizar el Colaborador si su equipo es robado, como, por ejemplo; informar el equipo robado o dañado lo antes posible y cambiar todas las contraseñas de las cuentas de forma inmediata. Lo anterior se encuentra definido en la Política de Propiedades, Planta y Equipo corporativa.

v. Medidas adicionales: Para reducir la probabilidad de violaciones de seguridad, también se debe instruir a nuestros Colaboradores a:

- Apagar sus pantallas y bloquear sus dispositivos al salir de sus escritorios temporalmente.
- Al finalizar la jornada laboral, los equipos deben quedar apagados.
- En caso de robo, informar lo antes posible al Departamento de Recursos Humanos y/o TI.
- Cambie todas las contraseñas de la cuenta, en caso de que roben un dispositivo.
- Informar una amenaza percibida o una posible debilidad de seguridad en los sistemas de la Compañía.
- Abstenerse de descargar softwares sospechosos, no autorizados o ilegales en el equipo de la Compañía.
- Evitar conectarse a redes públicas de wifi (de acceso público o libre). En casos de urgencia, compartir la señal de internet móvil de los teléfonos.
- Evite acceder a sitios web sospechosos.

B. POLÍTICA REFERIDA A LA GESTIÓN DE LAS PERSONAS RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN QUE GENERAN Y UTILIZAN

Todos los Colaboradores que interactúan directa o indirectamente con los sistemas de información, infraestructura tecnológica o procesos de negocio -ya sea de forma habitual u ocasional- deben recibir capacitación por parte de los responsables de seguridad de la información. Esta formación debe impartirse al momento de su incorporación a la Compañía y actualizarse periódicamente, especialmente cuando se introduzcan cambios relevantes en la Política.

i. Gestionar contraseñas correctamente

La identificación (contraseña) de cualquier usuario, en cualquiera de los sistemas de información administrados por las empresas de Grupo Sutil, debe ser única, personal e intransferible, cualificándolo como responsable de las acciones realizadas. La composición, administración y uso de contraseñas forma parte esencial de los procesos de autenticación para acceder a los recursos, sistemas e infraestructura tecnológica de las sociedades que integran Grupo Sutil.

Las fugas de contraseña son peligrosas, ya que pueden comprometer toda nuestra información. Las contraseñas no sólo deben ser seguras para que no sean fácilmente pirateadas, sino que también deben permanecer en secreto. Por esta razón, aconsejamos a nuestros Colaboradores a:

- Elegir contraseñas con al menos siete caracteres (incluyendo letras mayúsculas y minúsculas, números y símbolos) y evitar información que pueda adivinarse fácilmente (por ejemplo, fecha de cumpleaños).
- Cambiar sus contraseñas cada tres (3) meses.
- No usar la misma contraseña en los accesos a sistemas o sitios de carácter personal.

En el caso de contar con sistemas con doble control de autentificación, por ejemplo, cuentas de correos, estas sí o sí deben ser activadas, con la finalidad de prevenir el hackeo.

ii. Proceso de control de contraseñas

Se instruye a Grupo Sutil el uso de herramientas de monitoreo del grado de fortaleza y antigüedad de las contraseñas de los usuarios creados.

Para garantizar la integridad y confidencialidad en el momento de la autenticación, los usuarios y contraseñas no pueden ser compartidos o escritos, de modo de no facilitar su divulgación a terceros.

iii. Mantener y aplicar la seguridad de los correos electrónicos

Los correos electrónicos pueden ser objeto de estafas y softwares maliciosos (por ejemplo, virus, ransomware, malwares, etc.).

Para evitar la infección de virus o el secuestro de datos, instruimos a nuestros Colaboradores a:

- Evitar abrir archivos adjuntos y hacer clic en los enlaces cuando el contenido no se explica adecuadamente (por ejemplo, "*mire este video, es increíble*").
- Verificar la dirección del correo electrónico y los nombres de las personas de quienes recibió un mensaje para asegurarse de que sean legítimos. La recepción de correos electrónicos falsos en los que se ha suplantado la identidad de un gerente o Director es cada vez más común. Si bien el nombre y la firma puede parecer auténtica, la dirección de email no es una corporativa (por ejemplo, securmailsmtp@pm.me).
- Sospechar de los títulos de “clickbait” o “ciberanzuelo” (por ejemplo, ofreciendo premios, consejos, ofertas, descuentos).
- En caso de no estar seguro de que un correo electrónico recibido sea seguro, puede consultar al área de TI de su Filial. Nuestros especialistas en seguridad son responsables de asesorar a los Colaboradores sobre cómo detectar correos electrónicos fraudulentos. Alentamos a nuestros Colaboradores a contactarlos con cualquier pregunta o inquietud.
- Ante la detección o recepción de un correo electrónico sospechoso o fraudulento, la persona que lo identifique deberá notificar de forma inmediata a Auditoría Interna, quien será responsable de comunicar y alertar oportunamente a las áreas y personas correspondientes del Grupo Sutil, con el propósito de mitigar riesgos y prevenir eventuales incidentes de seguridad.

El uso de correo institucional debe ser exclusivo para el desarrollo de las funciones propias de sus cargos.

Los usuarios sólo deben contar con los privilegios necesarios para realizar su función en los sistemas implementados por cada una de las sociedades de Grupo Sutil. Toda la información debe ser entregada y distribuida respetando la confidencialidad, e implementando los controles necesarios para asegurar que solo se acceda a ella en el nivel mínimo requerido para el cumplimiento de las funciones asignadas.

Los usuarios que por el desarrollo de sus funciones tengan acceso, usen y/o generen información confidencial, deberán reflejar la responsabilidad que esto conlleva en su contrato de trabajo, en una cláusula especial que refleje el resguardo de las compañías del Grupo frente a una eventual filtración de ésta y la responsabilidad del Colaborador.

Las actividades de cada usuario deben asignarse con la debida **"segregación de funciones"**, para prevenir o detectar los errores e irregularidades, asignando por separado la responsabilidad a los usuarios de iniciar y registrar transacciones, y la custodia de activos.

C. POLÍTICA REFERIDA AL CUMPLIMIENTO DE LAS DISPOSICIONES LEGALES, REGULATORIAS O CONTRACTUALES

i. Protección de Datos Personales

Toda la información personal, debe ser manejada en forma segura, y según lo establecido en la regulación chilena vigente (Ley N°19.628 sobre la Protección de la Vida Privada, la Ley N°21.096, que consagra el derecho constitucional de la protección de los datos personales y la Ley N°21.719 que regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales).

Las personas dentro de Grupo Sutil, que trabajen en el tratamiento de los datos personales están obligadas a guardar el secreto irrestricto de los mismos.

Cada sociedad de Grupo Sutil es responsable de implementar controles para la protección de datos personales, por ejemplo, en aquellos casos donde se desee intercambiar determinados datos personales con proveedores, será requisito contar previamente con la autorización otorgada por escrito del Gerente General y con un acuerdo de confidencialidad suscrito, el cual deberá ser elaborado por cada sociedad de Grupo Sutil.

ii. Uso de herramientas tecnológicas y redes

Los teléfonos, sistemas computacionales, correo electrónico, conexión a internet y otros medios electrónicos proporcionados a los Colaboradores por Grupo Sutil (en adelante también las "**Herramientas Tecnológicas**"), sea que estas se utilicen en el lugar de trabajo o fuera de este, son de propiedad de la Compañía y, por lo tanto, los documentos, archivos, copias de seguridad, comunicaciones, imágenes y grabaciones que se creen, manejen o almacenen mediante las Herramientas Tecnológicas son de propiedad de Grupo Sutil. Por tal motivo, estas deben ser debidamente utilizadas y protegidas contra el acceso no autorizado y la divulgación no deliberada.

Las Herramientas Tecnológicas se proporcionan a los Colaboradores como instrumentos de trabajo, es por ello que deben ser destinadas exclusivamente para el desempeño laboral. De esta forma, se deja expresa constancia que todo correo electrónico enviado por los Colaboradores desde las cuentas de correo proporcionadas por la Compañía podrá ser copiado en forma automática y depositado en una base de respaldo de propiedad de Grupo Sutil, no teniendo por tanto el carácter de comunicación privada, sino que, de registro de la Compañía, la que se encuentra plenamente facultada para monitorear y conocer dichos correos electrónicos.

La información debe estar disponible en el momento que se le requiera al Colaborador, para ello debe asegurarse que el ambiente puede ser recuperado dentro de los plazos establecidos por los planes de continuidad para reducir impactos de las fallas en infraestructura de tecnología y reducir así los riesgos de cada negocio y las respectivas vulnerabilidades. Toda la información, cualquiera

sea su forma de almacenamiento debe contar con su debido respaldo, que permita frente una eventual pérdida, acceder a ella sin restricción.

Queda prohibido, divulgar y utilizar fotografías o videos de plantas, faenas productivas, u otros aspectos que afecten tanto la privacidad de nuestros Colaboradores como la propiedad física e intelectual de Grupo Sutil.

Todos los accesos a Internet a través de las Herramientas Tecnológicas de la Compañía podrán ser supervisados y monitoreados. De esta manera, los registros históricos de accesos a Internet de todos los computadores de Grupo Sutil, cualquiera sea la persona que los utilice, podrán ser revisados por la administración de esta. Esta medida de control de carácter preventivo se realizará de manera general y despersonalizada, con el único fin de otorgar seguridad tanto para los Colaboradores como para la Compañía.

En virtud de lo anterior, los Colaboradores deberán dar cumplimiento a los siguientes lineamientos:

Respecto del uso de correo electrónico corporativo:

- Cada casilla de correo electrónico estará vinculada al Colaborador para el cual fue creada, quien será responsable del contenido escrito o adjunto.
- Los usuarios son responsables de todas las actividades realizadas desde su cuenta y deben cumplir en todo momento con la normativa vigente.
- Se debe utilizar un lenguaje respetuoso en los mensajes internos y externos. Está prohibido enviar contenido difamatorio, insultante, injurioso, amenazante, ofensivo, obsceno, racista o sexista.
- Se prohíbe el envío de información con fines de proselitismo político, religioso, gremial u otros similares.
- Los usuarios deben abstenerse de enviar o recibir contenidos no relacionados con su trabajo (por ejemplo, videos, imágenes, archivos de audio, etc.).
- Está prohibido enviar o recibir material ilícito, incluyendo contenido relacionado con delitos como terrorismo, piratería, infracción de derechos de autor, pornografía, estafas u otros.

Respecto del uso de teléfono móvil corporativo:

En caso de que la Compañía entregue un teléfono móvil, este será considerado exclusivamente como herramienta de trabajo. El Colaborador deberá cumplir con las siguientes disposiciones:

- El uso del teléfono móvil se limita a comunicaciones necesarias para el desarrollo de funciones (llamadas, mensajes, correos electrónicos). Se desalienta el uso para redes sociales durante el horario laboral.
- Está prohibido utilizar cámaras o grabadoras para capturar información confidencial de las empresas de Grupo Sutil o de terceros.
- No se permite el envío o recepción de material ilícito, acoso a terceros ni almacenamiento de información confidencial de otras compañías.
- El teléfono móvil puede utilizarse para gestionar contactos laborales, no personales.
- Si el equipo es provisto por Grupo Sutil, la Compañía podrá publicar el número para facilitar la comunicación interna.

- El dispositivo debe estar protegido con contraseña.
- Se recomienda mantener separadas las líneas personales y laborales.

iii. Cumplimiento legal Ley N°21.459 que define los delitos informáticos:

La Ley N°21.459, establece los Delitos Informáticos en línea con el Modelo de Prevención de Delitos de Grupo Sutil. Los delitos informáticos que debemos prevenir y alertar, en caso de brechas o riesgos, son:

a) **Ataque a la integridad de un sistema informático:** Este delito sanciona a quien obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático a través de la introducción, transmisión, daño, deterioro, alteración o suspensión de los datos informáticos.

b) **Acceso ilícito:** Este delito sanciona a quien, sin autorización y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático.

c) **Interceptación ilícita:** Este delito sanciona a quien indebidamente intercepte, interrumpa o interfiera, por medio técnicos, la transmisión no pública de información de un sistema informático entre dos o más de aquellos.

d) **Ataque a la integridad de datos informáticos:** Este delito sanciona a quien introduce, altera, daña o suprime datos informáticos.

e) **Falsificación informática:** Este delito sanciona a quien introduce, altera, daña o suprime datos informáticos con la intención de que sean tomados como antecedentes auténticos o usados para generar documentos auténticos.

f) **Receptación de datos informático:** Este delito sanciona a quien comercialice, transfiera o almacene datos informáticos de origen ilícito (por ejemplo, obtenidos a través de la realización de alguno de los delitos señalados precedentemente).

g) **Fraude informático:** Este delito sanciona a quien manipula un sistema informático, mediante la introducción, alteración, daño o supresión de datos con el objetivo de obtener un beneficio económico.

h) **Abuso de los dispositivos:** Este delito sanciona a quien 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 los delitos señalados.

VII. RESPONSABILIDAD GERENCIAS, DEPARTAMENTOS, ENCARGADOS DE TECNOLOGÍA DE LA INFORMACIÓN (TI)

Las áreas de TI de cada filial de Grupo Sutil serán responsables de:

- Seguir las disposiciones de esta Política al igual que todos los Colaboradores.

- Asegurar disponibilidad, integridad y confidencialidad de la información, así los usuarios puedan acceder a los recursos informáticos cuando lo requieran y obtener la información de forma rápida, segura y confiable.
- Elaborar, implementar y ejecutar protocolos de respaldos de sistemas de información de modo se asegurar la integridad de los datos y la continuidad del negocio.
- Respaldar datos de equipos de usuarios críticos, según el protocolo definido.
- Evaluar y proponer mejoras a mecanismos de respaldos y administración de perfiles.
- Informar a los usuarios regularmente sobre nuevos correos electrónicos o virus fraudulentos y formas de combatirlos.
- Asistir al resto de la Compañía respecto a dudas o implementación de estas prácticas.
- Elaborar y cumplir procedimiento para la administración de perfiles donde se establezcan para cada sistema la información accesible para cada perfil.
- Cumplir con protocolo para la creación / modificación de usuarios en los sistemas.

VIII. VIGENCIA Y MODIFICACIONES

Responsable:	Auditoría Interna
Revisado por:	Gerencia de Auditoría Interna Áreas específicas Filiales Comité de Auditoría
Aprobado por:	Comité de Auditoría

Versión	Motivo	Responsable	Fecha
2020-1	Confección	Auditoría interna	31-07-2020
2022-1	Incorporación de los delitos tipificados por Ley N° 21.459.	Auditoría interna	31-07-2022
2022-1	Revisión áreas especializadas Filiales	Áreas específicas Filiales	31-07-2022
2022-1	Aprobación y entrada en vigencia	Auditoría interna	01-10-2022
2025-2	Actualización Ley N° 21.595	Auditoría interna	10-11-2025