

	Política Seguridad de la Información	Versión: 01 Páginas: 1 de 6
---	---	--------------------------------

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CONTEXTO

Actualmente, y desde 2010, Champiñones Abrantes forma parte del conglomerado de Empresas Sutil, la que, junto a un grupo de socios, dio origen a Champiñones Abrantes S.A. En ese contexto, Champiñones Abrantes comparte los principios, valores, políticas y directrices del resto del conglomerado y, por ende, adhiere a su Código de Ética y Conducta, así como a su Manual y Política de Prevención de Delitos, participa de su Procedimiento de Denuncias y hace suyos el resto de los documentos de lineamiento de gestión de seguridad empresarial.

INTRODUCCIÓN

En plena vorágine de la era digital, donde toda la información se maneja digitalizada en plataformas tecnológicas, una política de Seguridad de la Información debe, necesariamente, abordarse desde esa perspectiva. La presente política describe pautas y disposiciones de Champiñones Abrantes S.A. para reservar la seguridad de su infraestructura de datos y tecnología.

Cuanto más dependemos de la tecnología para recopilar, almacenar y administrar información, más vulnerables nos volvemos a sufrir graves violaciones de seguridad. Los errores humanos, los ataques de piratas informáticos y el mal funcionamiento del sistema podrían causar un gran daño financiero y poner en peligro la reputación de nuestra empresa.

Por esta razón, hemos implementado una serie de medidas de seguridad. También hemos preparado instrucciones que pueden ayudar a mitigar los riesgos de seguridad. Hemos esbozado ambas disposiciones en esta política.

OBJETIVOS

El objetivo de esta política es establecer los principios y directrices respecto de la información de Champiñones Abrantes S.A. que, en su conjunto, permitan crear un ambiente propicio para desarrollar prácticas que garanticen la Seguridad de la Información, entendiéndose por ello su confidencialidad, integridad, disponibilidad, legalidad y confiabilidad, en cualquier forma o medio, frente a cualquier amenaza, riesgo o daño que pueda sufrir.

Elaborado por:	Gerente de Ventas Pablo Gárate	Fecha Creación:	Julio 2022
----------------	--------------------------------	-----------------	------------

ALCANCES

Toda la información entregada a Champiñones Abrantes S.A. será tratada con estricta reserva y absoluta confidencialidad, se entiende que esto aplica a información sobre datos de clientes, información y estados financieros, y cualquier tipo de información que se comparta con Champiñones Abrantes S.A.

Esta política se aplica a todos nuestros colaboradores y contratistas, así como a cualquier persona que tenga acceso permanente o temporal a nuestros sistemas y hardware.

RESPONSABILIDAD DE LOS USUARIOS

1. Información confidencial

Los datos confidenciales constituyen información privada y valiosa. Dentro de esta se puede mencionar:

- Información financiera, contable y corporativa de Champiñones Abrantes S.A. o sus clientes y / o Proveedores.
- Datos de clientes y sus socios o accionistas, respecto de los cuales se opera en conformidad con la ley N°19.628 de Protección de datos de carácter personal.
- Datos de proveedores.
- Listas de clientes (existentes y prospectivos)
- Datos personales de los colaboradores de Champiñones Abrantes S.A. respecto de los cuales se opera en conformidad con la ley N°19.628 de Protección de datos de carácter personal.

Todos los colaboradores están obligados a proteger estrictamente estos datos y respetar la legislación en torno a esta materia según acuerdo de confidencialidad establecido en los contratos de trabajo y, en función del cual:

“El empleado se obliga a guardar la más absoluta reserva respecto de toda información o antecedentes a que se tenga acceso o que conozca con motivo u ocasión de sus funciones, o por otras razones, o que diga relación con operaciones o proyectos de empleador, sus accionistas y/o de sus sociedades relacionadas. Dicha información y antecedentes se refieren especialmente, pero no excluyentemente, a negocios, operaciones y faena, operaciones comerciales, litigios judiciales o administrativos, bienes y estado patrimonial, estrategias comerciales, publicidad, comunicaciones internas o externas, procedimientos, métodos de trabajo y de organización, respecto del empleador, sus accionistas y sus empresas filiales y/o relacionadas. Este deber deberá ser cumplido por el empleado incluso después de haber dejado de trabajar para el empleador. La inobservancia de este

compromiso constituirá grave falta a las obligaciones que impone el presente contrato, sin perjuicio de la responsabilidad que le haya lugar por cualquier daño o perjuicio que cause con su incumplimiento”.

2. Protección de los dispositivos personales y de la empresa

Cuando los empleados usan sus dispositivos digitales para acceder a cuentas o correos electrónicos de la empresa, introducen un riesgo de seguridad para nuestros datos. Aconsejamos a nuestros colaboradores que mantengan seguros tanto sus computadoras personales como teléfonos celulares. Para esto es importante que cada uno se ocupe de:

- Mantener todos los dispositivos protegidos con contraseña.
- Se asegure de no dejar sus dispositivos expuestos o desatendidos.
- Iniciar sesión en las cuentas y sistemas de la empresa solo a través de redes seguras y privadas (conocidas).
- Seguir las directrices del área de soporte de Champiñones Abrantes S.A, 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 Champiñones Abrantes S.A, software que no tengan licencia a favor de la Empresa. Asimismo, se obliga a no utilizar software de propiedad de terceros en los computadores de la Empresa sin la expresa autorización del Empleador.

3. Seguridad de los correos electrónicos

Los correos electrónicos pueden ser objeto de estafas y software malicioso (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.
- Sospechar de los títulos de “clickbait” o “ciberanzuelo” (por ejemplo, ofreciendo premios, consejos).
- En caso de no estar seguro de que un correo electrónico recibido sea seguro, puede consultar al área de soporte de Champiñones Abrantes S.A.
- Nuestros especialistas en seguridad son responsables de asesorar a los empleados sobre cómo detectar correos electrónicos fraudulentos. Alentamos a nuestros empleados a contactarlos con cualquier pregunta o inquietud.

Procedimiento para marcar correo como SPAM.

En ocasiones, ciertos correos externos podrán traspasar la barrera antispam con que cuenta nuestro servicio de Google Workspace. Estos correos en general contienen publicidad y ocasiones pueden contener contenido malicioso.

Para marcar estos correos como Spam y no recibirlos en nuestra bandeja de entrada seguir el siguiente proceso:

Elaborado por:	Gerente de Ventas Pablo Gárate	Fecha Creación:	Julio 2022
----------------	--------------------------------	-----------------	------------

- Marcar el correo en la bandeja de entrada, una vez seleccionado presionar el botón derecho del mouse, seleccionar correo no deseado opción bloquear remitente.
- Los correos del remitente serán bloqueados y automáticamente enviados a la carpeta de no deseados.
- En caso de tener dudas o consultas respecto de un correo electrónico y/o su contenido, podrá ser analizado por nuestro soporte.

4. Gestionar contraseñas correctamente

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 lo siguiente a nuestros colaboradores:

- Elegir contraseñas con al menos siete caracteres (incluyendo letras mayúsculas y minúsculas, números y símbolos) y evite información que pueda adivinarse fácilmente (por ejemplo, cumpleaños).
- Procurar recordar contraseñas en lugar de escribirlas. Si necesitan escribir sus contraseñas, están obligados a mantener la confidencialidad del documento en papel o digital.
- Intercambiar credenciales solo cuando sea absolutamente necesario. Cuando no sea posible intercambiarlos en persona, los empleados deben preferir el teléfono en lugar del correo electrónico, y solo si reconocen personalmente a la persona con la que están hablando.
- Cambiar sus contraseñas cada un tiempo razonable (6 meses) .
- No usar la misma contraseña en los accesos a sistemas o sitios de carácter personal.

5. Respaldo de información

Equipos:

Cada colaborador es responsable del adecuado respaldo de la información de sus equipos, según lo programado por nuestra área de soporte técnico de Champiñones Abrantes S.A.

No obstante, para determinados usuarios que cumplen funciones críticas, se ha adoptado un esquema de respaldo periódico que funciona de modo automático.

Correos electrónicos:

Los colaboradores de Champiñones Abrantes S.A. son los responsables de la administración y correcto almacenamiento de sus correos. Para esto se ha puesto a su disposición una cuenta Gmail con 20 GB de capacidad. Es responsabilidad de cada uno la correcta gestión de correos para no sobrepasar el límite definido y solicitar ayuda al área de soporte técnico, ante cualquier problema referente a esto.

6. Medidas adicionales

Para reducir la probabilidad de violaciones de seguridad, también instruimos a nuestros empleados a:

- Apagar sus pantallas y bloquear sus dispositivos al salir de sus escritorios.
- Informe el equipo robado o dañado lo antes posible al [Departamento de Recursos Humanos / Soporte técnico].

- Cambie todas las contraseñas de la cuenta de una vez cuando le roben un dispositivo.
- Informar una amenaza percibida o una posible debilidad de seguridad en los sistemas de la compañía.
- Abstenerse de descargar software sospechoso, no autorizado o ilegal en el equipo de su empresa.
- Evitar conectarse a redes públicas de wifi. En casos de urgencia compartir la señal de internet móvil de los teléfonos.
- Evite acceder a sitios web sospechosos.

RESPONSABILIDAD AREA DE SOPORTE INFORMÁTICO

El área de soporte técnico de Champiñones Abrantes S.A. es la responsable 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 respaldos de sistemas de información de modo se asegure la integridad de los datos y la continuidad del negocio.
- Respaldo de datos de equipos de usuarios críticos.
- 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 organización respecto a dudas o implementación de estas prácticas.
- Creación / modificación de usuarios en los sistemas, según requerimiento.

RESPONSABILIDAD DE LA ORGANIZACIÓN

- Se entiende incorporado en esta política la cláusula de confidencialidad de la información establecida en los contratos del personal y colaboradores de Champiñones Abrantes S.A., antes incluida, extendiendo su responsabilidad y cumplimiento para todos los colaboradores al uso de recursos informáticos dentro y fuera de las dependencias de la empresa.
- Capacitar a los colaboradores de Champiñones Abrantes S.A. respecto al valor de la Seguridad de la Información y los riesgos asociados, reforzando esta política de manera permanente, por medio de charlas y capacitaciones con miras a crear una cultura activa de la Ciberseguridad en Champiñones Abrantes S.A.
- Proporcionar los recursos y herramientas para el cumplimiento de esta política.

	Política Seguridad de la Información	Versión: 01 Páginas: 6 de 6
---	---	--------------------------------

La política aquí descrita aplica a todos nuestros colaboradores. El no cumplimiento de ella es motivo de sanciones según lo establecido en el Reglamento Interno de Orden Higiene y Seguridad.

RESGUARDO DE LA INFORMACIÓN DE CLIENTES/PROVEEDORES

La información de nuestros socios comerciales, ya sean clientes o proveedores, se maneja de manera privada en el software de Planificación de Recursos Empresariales (ERP, por sus siglas en inglés Enterprise Resource Planning) conforme la facturación es electrónica. La información se mantiene almacenada por un plazo calendario de 1 año, con miras a poder dar respuesta de manera oportuna en caso de auditorías internas, o Fiscalizaciones del Servicio de Impuestos Internos (SII).

La información de nuestros clientes no se divulga con ninguna empresa privada. Sólo se comparte la información de ventas y datos comerciales con el SII.

CANALES DE COMUNICACIÓN

Champiñones Abrantes S.A. tiene una serie de canales de comunicación para todos sus clientes y posibles clientes, con el objetivo de fortalecer la cercanía y el vínculo de estos. Lo anterior, para efectos de entregar una atención y apoyo personalizado.

Los canales disponibles son los siguientes:

Correo electrónico: pgarate@abrantes.cl

Número telefónico: +569 8549 7464

Página web: www.abrantes.cl

Elaborado por:	Gerente de Ventas Pablo Gárate	Fecha Creación:	Julio 2022
----------------	--------------------------------	-----------------	------------