1 OBJETIVO

La Política de Seguridad de la Información ("Política" o "PSI") tiene como objetivo establecer pautas, principios y responsabilidades, además de orientar la ejecución de acciones relacionadas con el tratamiento de la información y el uso adecuado de los activos y/o información por parte del público objetivo, con el fin de mitigar cualquier riesgo relacionado con amenazas externas o internas, deliberadas o accidentales, que puedan afectar la información de V.tal con respecto a su integridad, confidencialidad y disponibilidad.

2 PÚBLICO OBJETIVO

Esta PSI es aplicable a todo V.tal, contemplando todo uso de dispositivos, acceso a servidores, conexiones a la red e internet y cualesquiera otros usos de recursos tecnológicos o que contengan información de V.tal. Por lo tanto, debe cumplirse y aplicarse en todas las áreas de la Compañía, incluidas todas las personas físicas o jurídicas, ya sean socios, directores, administradores, funcionarios, aprendices y pasantes ("Colaboradores Internos"), así como proveedores de servicios, terceros, proveedores y socios de la Compañía ("Colaboradores Externos") que, dentro del alcance de su relación con V.tal, pueden tener acceso a las áreas, equipos, información, archivos, redes y datos propiedad de la Compañía. A los efectos de interpretar esta Política, los Colaboradores Internos y los Colaboradores Externos se denominarán juntos simplemente "Colaboradores".

3 DIRECTRICES

La información es Patrimonio: toda la información y cualquier dato o activo generado, adquirido, manejado, almacenado, bajo custodia, transportado y/o desechado por los Colaboradores en las instalaciones y/o en los activos de la Compañía, debido a su vínculo con V.tal o al desempeño de sus actividades contratadas por la Compañía ("Información Protegida"), se consideran patrimonio de V.tal y deben usarse exclusivamente para intereses corporativos. V.tal cuenta con una Política de Clasificación de Datos dirigida a Colaboradores Internos y un Manual de Privacidad y Protección de Datos Personales para Terceros dirigido a Colaboradores Externos, que establecen normas y obligaciones específicas sobre el uso de la Información Protegida, aplicándose además de esta PSI.

La responsabilidad y el compromiso deben ser de todos: todos los Colaboradores son responsables de la protección y salvaguarda de la información protegida, así como de los entornos físicos e informáticos a los que tienen acceso, independientemente de las medidas de seguridad implementadas. El uso aceptable de la infraestructura y los servicios de red de la Compañía es siempre ético, honesto y respeta los derechos individuales, incluidos los derechos a la privacidad y la protección de datos.

Se debe gestionar el acceso a la información: se aprobará, controlará, registrará, almacenará y monitorizará el acceso lógico, el control de acceso físico y el uso de la información, con el fin de adaptar la Seguridad de la Información con la ejecución de las tareas inherentes a su cargo o función.

Las incidencias de seguridad deben ser prevenidas o combatidas: Las incidencias de seguridad de la información, cuando no puedan ser prevenidas, deben ser identificadas, monitoreadas, comunicadas y adecuadamente combatidas con el fin de reducir los riesgos en el medio ambiente, evitando la interrupción de las actividades, y no afectar el logro de los objetivos estratégicos de la Compañía y el servicio al cliente.

Los activos de V.tal y su uso pueden ser monitoreados: la Compañía puede, dentro de los límites de la ley aplicable y según sea necesario, monitorear, grabar y registrar el acceso y uso de sus activos tecnológicos, así como los entornos, servicios, equipos y sistemas de información, incluidos, entre otros, correos electrónicos, archivos, impresiones, historial de navegación y, en general, redes y computadoras, para que se detecten acciones no deseadas o no autorizadas.

V.tal podrá auditar el cumplimiento de las prácticas de seguridad: la Compañía podrá auditar periódicamente sin previo aviso, las prácticas de Seguridad de la Información, con el fin de evaluar el cumplimiento de las acciones de sus Colaboradores en relación con lo establecido en esta Política, en los demás lineamientos que la componen y en la legislación aplicable, incluso a través de las prácticas de monitoreo mencionadas en esta PSI.

3.1 Principios de Seguridad de la Información

Estas son las acciones de seguridad o líneas de conducta que actúan como guía para su implementación y la gestión de la Seguridad de la Información:

Establecer la seguridad de la información en todo V.tal: La seguridad de la información se maneja a nivel organizacional, de acuerdo con la toma de decisiones que tiene en cuenta todos los procesos comerciales críticos de V.tal.

Adoptar un enfoque basado en el riesgo: la seguridad de la información se basa en decisiones basadas en el riesgo, como la pérdida de ventaja competitiva, el cumplimiento, la responsabilidad civil, las interrupciones operativas, los daños a la reputación y las pérdidas financieras, el uso indebido, el fraude, el sabotaje, el robo y los ciberataques.

Promover un entorno positivo de seguridad: La Seguridad de la Información se estructura a partir del análisis del comportamiento humano, observando las crecientes necesidades de todos los grupos de interés, a través de la concientización, educación y madurez del capital humano, fortaleciendo uno de los elementos fundamentales para mantener el nivel adecuado de Seguridad de la Información.

3.2 Privacidad y Protección de Datos Personales

Esta PSI se aplica a los datos, incluidos los datos personales y los datos personales confidenciales, sobre los Colaboradores, clientes, clientes finales y prestadores de servicios relacionados con V.tal. Queda prohibido, sin la autorización previa de V.tal, el uso de estos datos para fines distintos de los que respaldaron la recopilación, uso, almacenamiento y cualquier otra hipótesis de procesamiento de datos, en los términos de esta PSI y otras políticas relacionadas con la privacidad y protección de datos personales.

V.tal utiliza proveedores de servicios externos. Si los datos que se procesan son personales, celebramos acuerdos contractuales apropiados y se implementan medidas organizativas de acuerdo con la legislación aplicable para garantizar la protección de datos.

El Colaborador garantiza que todos los datos personales a los que tenga acceso no serán divulgados o compartidos sin la autorización expresa de la Compañía, ni serán transmitidos o accedidos por terceros no autorizados. El Colaborador también garantiza que adoptará las mejores prácticas de Seguridad de la Información a lo largo del ciclo de vida de los datos dentro de V.tal, sin limitarse a las descritas en esta PSI.

3.3 Monitoreo y Auditoría del Entorno

Cada entorno físico y digital de V.tal es o puede ser monitoreado, respetando los límites establecidos en la legislación vigente, incluido el acceso, uso o tráfico de información en dicho entorno por cualquier medio (como, por ejemplo, correo electrónico) con el fin de verificar el cumplimiento de los estándares de seguridad y protección de datos de la Compañía.

Los Colaboradores son conscientes de que V.tal puede:

- Monitorear todos los servidores, redes, conexiones a Internet, software, equipos y dispositivos corporativos, móviles o no, conectados a la red corporativa;
- Realizar inspecciones físicas en los equipos y estaciones de trabajo del colaborador, periódicamente o bajo sospecha razonada de violación de las normas internas de la Compañía.

El Colaborador también es consciente de que el monitoreo puede identificarlo y presentar datos sobre su uso de la infraestructura técnica de V.tal y el material y contenido manejado por el Colaborador, teniendo la certeza de que toda la información recopilada en el curso del monitoreo se almacena en las copias de seguridad de la Compañía con fines de auditoría y puede usarse como evidencia de una posible violación de las reglas y condiciones establecidas por V.tal o por la legislación vigente. Si así lo solicitan los organismos competentes, esta información puede divulgarse en la medida en que exista una razón legal o una determinación judicial para hacerlo.

El Colaborador entiende que el monitoreo se lleva a cabo para salvaguardar la seguridad no solo de los sistemas de la Compañía y la Información Protegida, sino también del propio Colaborador. Los datos y la información monitoreados solo pueden ser accedidos por los departamentos competentes y con fines legítimos, como investigar denuncias y realizar investigaciones en el entorno de trabajo. Todos y cada uno de los tratamientos de datos para estos fines se basarán en el informe de auditoría u otro instrumento apropiado para este fin y cumplirán con las normas específicas sobre privacidad y protección de datos personales.

3.4 Manejo de Información Protegida

El Colaborador es responsable de su uso de la Información Protegida. Por lo tanto, se deben observar las reglas a continuación para garantizar un nivel mínimo de seguridad de la información.

3.4.1 Cuidados de Impresoras y Copiadoras

Los Colaboradores son conscientes de que cualquier y todo uso de equipos, como copiadoras e impresoras, debe hacerse exclusivamente dentro del alcance de sus actividades profesionales, y el uso para fines personales está prohibido. Debe evitarse imprimir documentos que contengan ciertos tipos de Información Protegida, dado que el Colaborador Interno debe seguir las pautas de la Política de Clasificación de Datos y el Colaborador Externo debe seguir las directrices del Manual de Privacidad y Protección de Datos Personales para Terceros. Cualquier tipo de documento impreso o copiado deberá ser retirado inmediatamente del equipo.

3.4.2 Uso de Información Protegida

El Colaborador debe tener el máximo cuidado con su uso de la Información Protegida, teniendo cuidado de no dejar notas o manipular documentos que contengan Información Protegida en lugares de circulación, como salas de reuniones o espacios públicos, como cafeterías y aviones. Queda prohibida la reutilización de borradores de documentos que contengan Información Protegida.

En los casos que impliquen la contratación de servicios de terceros que justifiquen la necesidad de compartir Información Protegida, solo podrán ser compartidos después de la firma de un acuerdo de confidencialidad u otros instrumentos contractuales relevantes firmados con dichos terceros.

3.4.3 Recepción, Envío y Compartición de Archivos

El Colaborador es responsable de los archivos que recibe, envía y comparte a través de medios electrónicos y la infraestructura tecnológica de la Compañía, ya sea equipo propiedad de la Compañía puesto a disposición para el uso del Colaborador, equipo propio del Colaborador o servicios *cloud* (nube).

Para garantizar niveles mínimos de seguridad de la infraestructura tecnológica de V.tal, el Colaborador tiene prohibido:

- **recibir, enviar y compartir archivos que**: (a) tengan fines diferentes y no estén relacionados con las actividades de interés de la Compañía o relacionadas con su negocio; (b) contengan pornografía o contenido de carácter racista, discriminatorio o de cualquier otra índole que viole la legislación vigente, la moral y las buenas costumbres; (c) violen los derechos de terceros, en particular los derechos de propiedad intelectual, los derechos de autor, los derechos de imagen, entre otros; (d) caractericen infracciones civiles o penales y/o puedan causar daños a V.tal y a terceros; y (e) constituyan competencia desleal o incumplimiento del secreto profesional;
- **enviar, compartir y descargar:** (a) archivos que contengan malware, como virus y otros códigos maliciosos; (b) información interna, confidencial o secreta en un entorno externo; y (c) cualquier archivo ejecutable (.exe) que no esté autorizado por V.tal.

3.4.4 Custodia y Transferencia de Información

Toda la Información Protegida que deba ser almacenada en forma física o digital, cuando sea almacenada por el Colaborador, deberá cumplir con las reglas del ciclo de vida de datos de V.tal, así como las siguientes precauciones, de acuerdo con la clasificación de la información:

- **Soporte físico**. Todos los documentos que contengan cierta Información Protegida deben almacenarse en sus propios archivos físicos indicados por V.tal, de acuerdo con los métodos de identificación del contenido, también indicados por la Compañía, incluida su fecha de archivado. Los documentos utilizados por el Colaborador en su estación de trabajo, cuando no se utilicen, siempre deben almacenarse en un cajón o gabinete, asegurando que dichos cajones y gabinetes permanezcan cerrados con llave cuando se trate de información más crítica. No se deben dejar anotaciones relacionadas con la Información Protegida en exhibición, ya sea en la mesa, en el ordenador o en particiones, incluso cuando el Colaborador esté presente. Cuando el Colaborador no se encuentre en las instalaciones de la Compañía, los documentos que contengan la información más crítica no deben exponerse.
- **Soporte digital**. Todos y cada uno de los archivos que contienen Información Protegida deben guardarse en la red corporativa de V.tal, en un directorio específico, lo que impide el acceso de Colaboradores no autorizados. Si el archivo se va a almacenar en un dispositivo móvil (como en ordenadores portátiles, debido a reuniones externas), es esencial que el colaborador elimine el archivo del dispositivo después de su uso.

Todos y cada uno de los documentos o archivos que contienen información protegida solo se pueden cambiar, copiar y/o mover si existe la posibilidad de recuperación, control de versiones o

análisis de los registros de dicho archivo o documento en caso de violaciones de seguridad que resulten en la pérdida o extravío de la Información Protegida.

3.4.5 Eliminación de la Información

La eliminación de un documento físico y/o la eliminación de un archivo digital de la red V.tal que contenga Información Protegida debe seguir las siguientes reglas de eliminación:

- **Soporte físico.** Los documentos que tienen información pública pueden ser desechados en la basura común; aquellos que tienen Información Protegida deben ser destruidos manualmente o, preferiblemente, por un dispositivo de fragmentación antes de su eliminación. En el caso de información más crítica, el uso de un dispositivo de fragmentación es obligatorio y, en ausencia de dicho dispositivo, el Colaborador debe llamar al gestor responsable para tomar las medidas apropiadas.
- **Soporte digital.** Los archivos que contengan Información Protegida y estén almacenados en soportes digitales flexibles, como CD o DVD, deberán ser destruidos mediante un dispositivo de fragmentación y, en ausencia de dicho dispositivo, el Colaborador deberá llamar al gestor responsable para que se tomen las medidas necesarias. Por otro lado, aquellos archivos almacenados en medios digitales duros, como disco duro (HD) y pen drive, deben enviarse al Departamento de Tecnología, en una caja sellada, para su correcta destrucción, según el procedimiento interno adoptado.

Solo la persona responsable de generar o almacenar el archivo o documento a descartar es competente para descartarlo o eliminarlo, a menos que la persona responsable otorgue expresamente autorización para que un tercero lo haga. Además, se debe registrar toda la disposición, con el fin de mantener un historial que permita realizar auditorías, si es necesario. En el caso de información que involucre datos personales, el Colaborador interno seguirá las pautas descritas en la Política de retención de datos de V.tal y el Colaborador externo seguirá el Manual de privacidad y protección de datos personales para terceros.

3.5 Correo Electrónico Corporativo

Las direcciones de correo electrónico proporcionadas por V.tal a los Colaboradores son individuales y están destinadas exclusivamente a fines corporativos y relacionadas con las actividades del Colaborador dentro de la Compañía. Los mensajes de correo electrónico siempre deben incluir la firma con el formato estándar de V.tal. Añadimos que los Colaboradores tienen prohibido usar el correo electrónico de V.tal para:

- enviar mensajes no solicitados a múltiples destinatarios, excepto si están relacionados con el uso legítimo de V.tal;
- enviar cualquier mensaje por medios electrónicos que haga que su remitente y/o V.tal y sus unidades sean vulnerables a procedimientos legales y/o administrativos;

- divulgar información no autorizada, incluyendo, sin limitación, imágenes de pantalla, sistemas, documentos y similares sin autorización expresa y formal otorgada por la persona responsable;
- falsificar la información de direccionamiento, alterar los encabezados para ocultar la identidad de los remitentes y/o destinatarios, con el fin de evitar los castigos previstos;
- eliminar mensajes de correo electrónico relevantes cuando cualquiera de las unidades o colaboradores de V.tal estén sujetos a cualquier tipo de investigación.

3.6 Internet

Todas las reglas de V.tal están orientadas básicamente al desarrollo de un comportamiento ético y profesional en el uso de internet. Para garantizar el uso racional de estos recursos, así como la seguridad de los datos y el software, la Compañía se reserva el derecho de utilizar herramientas para verificar el contenido de los correos electrónicos corporativos y monitorear el uso de Internet y la red corporativa.

Cualquier intento de cambiar los parámetros de seguridad, por parte de cualquier Colaborador, sin la debida acreditación y autorización para hacerlo, se considerará inadecuado y los riesgos relacionados se informarán al Colaborador y al gestor respectivo. El uso de cualquier recurso para actividades ilegales puede resultar en acciones administrativas y sanciones derivadas de procedimientos civiles y penales, y en estos casos, la Compañía cooperará activamente con las autoridades competentes.

Los colaboradores con acceso a Internet pueden descargar solo software aprobado en V.tal y directamente vinculado a sus actividades.

Los Colaboradores no pueden:

- utilizar los recursos de V.tal para descargar o distribuir software o datos sin las licencias adecuadas;
- cargar ("subir"), para sus clientes, socios y otros terceros, cualquier software licenciado a V.tal o datos de su propiedad, sin la autorización expresa de la persona responsable del software o los datos;

3.7 Redes Sociales y Correos Electrónicos Personales

V.tal puede suspender, sin previo aviso y a su entera discreción, el uso y acceso a las redes sociales, correos electrónicos personales y servicios de mensajería para fines personales, en las instalaciones y dispositivos físicos de la Compañía, por razones de gobernanza y/o Seguridad de la Información.

3.8 Acceso a la red de archivos

El acceso a la información almacenada en la infraestructura técnica de V.tal puede llevarse a cabo de manera diferente (por medios físicos, lógicos o remotos), dependiendo del tipo de formato. Para cada tipo de formato, se aplicarán diferentes reglas de conducta, a saber:

3.8.1 Acceso Físico a la Información

Los lugares donde se instalan o almacenan los centros de datos de los archivos físicos de la Compañía se consideran una parte crítica de su infraestructura tecnológica, por lo que se debe aumentar el cuidado con protección y seguridad. Hay diferentes tipos de accesos y, para cada uno de ellos, diferentes reglas y restricciones, como se muestra a continuación:

- **acceso permanente**: permitido solo a los colaboradores y colaboradores de la Compañía que tengan la necesidad de acceso autorizado para realizar sus actividades;
- **acceso esporádico**: permitido a otros Colaboradores o visitantes externos, previa autorización de V.tal, con acceso registrado (nombre, fecha y hora).
- **acceso externo**: permitido a aquellos que no son Colaboradores internos de la Compañía (contratistas externos), previa autorización y registro (nombre, fecha y hora), siempre que justifique este acceso.

3.8.2 Acceso Lógico

El acceso a la información almacenada en la infraestructura tecnológica de la Compañía estará restringido a cada Colaborador, dependiendo del perfil de acceso que le asigne el Departamento de Tecnología, de acuerdo con las reglas establecidas en el ítem 3.9 – *Identificación y Contraseñas*. Cada perfil presupone la liberación de acceso a ciertos directorios dentro de la red de la Compañía, que son asignados por el Departamento de Tecnología, para que se pueda acceder a la información de acuerdo con el nivel de acceso definido por V.tal.

3.8.3 Acceso Remoto

Cuando el Colaborador no se encuentra en las instalaciones de V.tal, puede acceder a la red privada de la Compañía de forma remota, a través de tecnologías autorizadas por V.tal, que pueden incluir el uso de VPN. El acceso remoto solo se otorgará al Colaborador en los casos en que exista una necesidad comprobada. Se ha comprobado la necesidad de acceso remoto y será otorgado por el sistema de gestión de accesos según el perfil del Colaborador.

Solo se permite el acceso remoto para la ejecución de las actividades profesionales del Colaborador que estén vinculadas a V.tal. El Colaborador es responsable de todas las actividades realizadas en acceso remoto, siendo responsable de cualquier uso irregular, incluso por parte de otra persona en posesión de su acceso. En caso de robo, hurto o pérdida de equipos

móviles que tengan configurado el acceso remoto a la VPN de la Compañía, el Colaborador deberá solicitar inmediatamente a una autoridad policial que elabore un informe policial y, posteriormente, denunciar el incidente al equipo de Tecnología, presentando copia del informe policial elaborado.

Todos los accesos remotos serán registrados por el equipo de Tecnología y dichos registros estarán disponibles para su consulta en caso de auditoría.

3.9 Identificación y Contraseñas

Todos los Colaboradores tienen ciertos privilegios para acceder a la Información Protegida, de acuerdo con su posición y deberes, de acuerdo con las reglas establecidas en el punto 3.8 – *Acceso a la Red de Archivos*. Algunos ejemplos de privilegios son el acceso externo al correo electrónico, las autorizaciones en el acceso a Internet y el acceso lógico, el uso externo de ciertos equipos V.tal, la liberación de espacio en el disco duro, el uso de dispositivos móviles, entre otros.

El Colaborador recibirá un login y una contraseña, según el perfil que se le asigne, que le permitirá ser identificado al acceder a la infraestructura de la Compañía. Por lo tanto, el Colaborador solo tendrá acceso a las áreas de infraestructura de V.tal que estén autorizadas considerando su perfil. V.tal se reserva el derecho de revisar, en cualquier momento y sin previo aviso, a través de los departamentos competentes, los privilegios de cualquier Colaborador, con el fin de salvaguardar los niveles de Seguridad de la Información de la Compañía.

El inicio de sesión y la contraseña del Colaborador son personales y, en consecuencia, el Colaborador es responsable del secreto y mantenimiento seguro de su contraseña vinculada al inicio de sesión, estando prohibido compartir el inicio de sesión y la contraseña con terceros, incluidos otros Colaboradores, bajo pena de soportar las sanciones no solo previstas en esta Política, sino también las sanciones civiles, penales y laborales, respondiendo, incluyendo, por cualquier y todo daño que cause a la Compañía.

Además del inicio de sesión del Colaborador, también recibirá una identificación física que le otorgará acceso a ciertas áreas físicas de la Compañía. Dicha identificación se realizará por medio de un distintivo, cuyo uso es personal e intransferible, y tendrá como finalidad dar de alta la entrada y salida de las instalaciones de V.tal.

3.10 Dispositivos

Los dispositivos físicos capaces de almacenar Información Protegida, tales como computadores, notebooks, tablets y otros, puestos a disposición de los Colaboradores para la ejecución de sus actividades, son propiedad de V.tal, y cada uno es responsable de utilizarlos y manejarlos correctamente para las actividades de interés para la Compañía, así como cumplir con las recomendaciones contenidas en los procedimientos operativos proporcionados por el Departamento de Tecnología.

El equipo debe identificarse individualmente, inventariarse y protegerse del acceso inadecuado. Los equipos deben tener la función de actualizaciones automáticas del sistema operativo habilitada de forma predeterminada y el software antivirus instalado, activado y actualizado con frecuencia. El usuario, en caso de sospecha de virus o problemas en la funcionalidad, debe llamar al Departamento de Tecnología.

Los archivos personales y/o archivos no relevantes para el negocio de V.tal (fotos, música, videos, etc.) no deben copiarse/trasladarse a unidades de red, ya que pueden sobrecargar el almacenamiento en el disco del computador. Si se identifica la existencia de estos archivos, se pueden eliminar permanentemente.

Los documentos esenciales para las actividades de los Colaboradores y/o para el negocio de la Compañía deben guardarse en un directorio con servicio de copia de seguridad y con disponibilidad de acceso. Dichos archivos, si se graban solo localmente en computadores (por ejemplo, en la unidad C:), no tendrán garantía de copia de seguridad y pueden perderse en caso de falla del computador, siendo por lo tanto responsabilidad del propio Colaborador.

El Colaborador entiende que es responsable de todos y cada uno de los daños que cause al equipo, por intención o culpa, y conoce y acepta observar las siguientes reglas:

- El Colaborador es responsable del equipo y se compromete a utilizar todos los cuidados necesarios, como si el dispositivo fuera suyo;
- Los dispositivos deben estar siempre a su alcance y no pueden dejarse en lugares públicos, en vehículos o en cualquier otro lugar, fuera de las instalaciones de V.tal, donde pueda haber acceso al equipo por personas no autorizadas, con el fin de evitar el robo y/o hurto de este equipo, así como la fuga de la Información Protegida contenida en el mismo;
- Los Colaboradores deben informar al departamento técnico de cualquier identificación de un dispositivo extraño conectado a su computador;
- Queda prohibida la apertura o manipulación de ordenadores u otros equipos informáticos para cualquier tipo de reparación que no sea realizada por un técnico de TI de V.tal o por terceros debidamente contratados para el servicio;
- El Colaborador debe mantener la configuración de los equipos puestos a disposición por V.tal, siguiendo los controles de seguridad adecuados requeridos por esta Política y por las reglas específicas de la Compañía, asumiendo la responsabilidad como custodio de la información. En caso de cambio/manipulación de la configuración, estará sujeta a las sanciones aplicables de acuerdo con el punto 3.14.
- Todos los dispositivos, incluidos los terminales informáticos y las impresoras, deben estar protegidos por contraseña (bloqueados) cuando no estén en uso;

- Todos los recursos tecnológicos adquiridos por V.tal deben cambiar inmediatamente sus contraseñas predeterminadas (default);
- Si, durante el uso del dispositivo, el Colaborador tiene dudas sobre su manejo o encuentra fallas que impliquen la necesidad de su reemplazo o mantenimiento, el Colaborador debe abrir una llamada con el Departamento de Tecnología que, a su vez, además de proporcionar las aclaraciones necesarias, debe guiarlo para entregar el equipo al lugar indicado para su reemplazo o reparación;
- Si el uso de un dispositivo es esporádico, el Colaborador debe devolverlo al Departamento de Tecnología en perfectas condiciones de uso, junto con los accesorios que le hayan sido entregados, como bolsas, estuches, películas, etc., tan pronto como finalice el período necesario para el uso. En caso de no devolución del equipo, dentro del tiempo y lugar determinados, el Colaborador será responsable de reembolsar los costos de dicho equipo a la Compañía, sin perjuicio de otras medidas legales y administrativas que V.tal deba tomar; y
- En caso de pérdida, robo, hurto o daño al equipo, el Colaborador deberá notificarlo inmediatamente al Departamento de Tecnología, que procederá a la eliminación del contenido corporativo contenido en el dispositivo.

El mal uso de los dispositivos de V.tal someterá al Empleado a las sanciones aplicables, en función de la gravedad de la conducta practicada. Hay algunas hipótesis de mal uso:

- Intentar u obtener acceso no autorizado a otro computador, servidor o red;
- Eludir cualquier sistema de seguridad;
- Acceder a información confidencial sin la autorización explícita del propietario;
- Observar secretamente a otros en busca de dispositivos electrónicos o software, como analizadores de paquetes (*sniffers)*;
- Interrumpir un servicio, servidor o red informática por cualquier método ilegal o no autorizado;
- Utilizar cualquier tipo de recurso tecnológico para cometer o ser cómplice de delitos o actos ilícitos, como acoso sexual, constreñimiento, hostigamiento *(stalking)* o manipulación o supresión de derechos de autor o propiedad intelectual sin la debida autorización legal del titular;
- Alojar pornografía, material racista o cualquier otro contenido que viole la legislación vigente en el país, la moral, las buenas costumbres y el orden público; y
- Utilizar software pirateado, actividad considerada delictiva según la legislación nacional.

3.11 Data Center y Cloud

V.tal utiliza diversos softwares propietarios y de terceros en el curso de sus operaciones y el Colaborador no podrá:

- utilizar dicho software para fines personales o de cualquier manera que comprometa la seguridad de la infraestructura de la Compañía;
- eliminar, modificar, copiar, transferir, realizar ingeniería inversa o asignar acceso a dicho software a terceros, o realizar cualquier acto que esté en desacuerdo con la ley aplicable;
- instalar en la red o en los dispositivos de la Compañía cualquier software pirateado, no licenciado o no autorizado por el área de TI, y cualquier software no autorizado descargado por el Colaborador será eliminado por el equipo de Tecnología.

V.tal pone a disposición únicamente el (los) recurso(s) para el almacenamiento externo de archivos, software y sistemas. Por lo tanto, está prohibido el uso por parte del Colaborador de servicios de almacenamiento en la nube que no estén disponibles a través de la infraestructura tecnológica de la Compañía.

3.12 Terminación o Movimiento del Colaborador

Al final del vínculo del Colaborador con V.tal, se revocará su acceso a la infraestructura tecnológica de la Compañía. El Colaborador debe devolver, en perfectas condiciones de uso, todos y cada uno de los dispositivos propiedad de V.tal que estén en su poder, junto con los accesorios que le hayan sido entregados. Las obligaciones de secreto y no reproducción de la Información Protegida, asumidas por el Colaborador en esta ISP, permanecerán vigentes incluso después del despido del Colaborador.

En caso de no devolución del equipo, dentro del tiempo y lugar determinado, el Colaborador será responsable de reembolsar los costos de dicho equipo a V.tal.

Si el Colaborador cambia de departamento o función dentro de V.tal, también debe revisar sus accesos, comenzando a ver solo los sistemas y carpetas de red necesarios para el desempeño de su nueva función.

3.13 Informe de Incidentes de Seguridad de la Información

Para evitar la exposición indebida de la Información Protegida, V.tal emplea medidas de seguridad, tanto internas como externas, que cumplen con las obligaciones legales vigentes. Sin embargo, es esencial que el Colaborador cumpla con las obligaciones de seguridad asumidas en esta Política, ya que tales incidentes pueden ocurrir debido a fallas humanas, tecnológicas o sistémicas.

Si el Colaborador tiene conocimiento o sospecha cualquier evento que viole las reglas de esta Política o ponga en peligro la seguridad de la información de la Compañía, debe comunicarse inmediatamente al Canal Confidencial. V.tal investigará las causas y efectos del incidente, para luego tomar las medidas de contención, evaluación de impacto y necesidad de comunicar sobre el incidente al organismo competente y/o a los titulares de la Información Protegida, de acuerdo con el Procedimiento de Respuesta a Incidentes de Seguridad de la Información que involucre Datos Personales de V.tal.

Para que se lleve a cabo una auditoría sobre el incidente, V.tal analizará toda la información, así como la evidencia disponible que pueda identificar la causa del problema. La información y las pruebas se compilarán y adjuntarán a un informe para formalizar lo sucedido.

3.14 Compromisos y Sanciones

Todas las garantías necesarias para cumplir con esta Política se establecen formalmente con los Colaboradores de V.tal.

El incumplimiento de la Política se considera una falta grave y puede dar lugar a la aplicación de las sanciones previstas por la ley, así como a advertencias, suspensiones o rescisión del contrato de trabajo, de acuerdo con los procedimientos internos y las disposiciones contractuales.

Todas las disposiciones legales y otras normas V.tal, como el Código de Ética y Conducta, deben ser estrictamente observadas.

3.15 Capacitación, Actualización y Divulgación

V.tal tiene un programa continuo de concientización sobre seguridad que tiene como objetivo crear conciencia, capacitar e instruir a las personas, siguiendo las mejores prácticas internacionales, contribuyendo a la difusión de la cultura de Seguridad de la Información para los Colaboradores de V.tal.

El contenido de la Política se actualiza y difunde amplia y frecuentemente. La relectura de esta Política, incluso si no se solicita directamente, debe hacerse periódicamente para una mejor comprensión.

3.16 Disposiciones Finales

Las excepciones a las reglas establecidas por esta Política para satisfacer cualquier demanda específica deben enviarse a V.tal para su evaluación y aprobación.

Esta Política puede ser revisada, actualizada y enmendada en cualquier momento, a la sola discreción de V.tal, siempre que cualquier hecho o evento relevante motive su revisión.

4 FUNCIONES Y RESPONSABILIDADES

Consejo de Administración

- Aprobar esta Política, reforzando el compromiso de la alta dirección con la mejora continua de los procesos de seguridad y designar en su estructura corporativa un director responsable de su gestión.

Área de Seguridad de la Información

- Gestionar, coordinar, orientar, evaluar y promover la implementación de acciones, actividades y proyectos relacionados con la Seguridad de la Información en V.tal, promoviendo acciones de interés para el negocio, programas educativos y sensibilización al capital humano.

Colaboradores

- Conocer y cumplir con las normas y lineamientos establecidos en esta Política y demás directrices que la componen;
- Informar situaciones que comprometan o puedan comprometer la seguridad de la información a través del Canal Confidencial puesto a disposición por V.tal a tal efecto;
- Toda la información creada, modificada en el ejercicio de funciones y cualquier información contenida en los mensajes de correo electrónico corporativo debe tratarse como referida al negocio de V.tal, y no debe considerarse como privada o confidencial, incluso si se archiva en la carpeta personal de los Colaboradores;
- Asegurar que la prohibición de compartir o intercambiar credenciales (ID, contraseñas, insignias, tokens y similares) sea conocida y cumplida;
- Revise sus accesos cada vez que cambie de departamento o función dentro de V.tal;
- Garantizar que los requisitos, políticas y procesos de seguridad de la información y protección de datos se incluyan en las adquisiciones y/o implementaciones tecnológicas y se mantengan durante todo su ciclo de vida.

5 REFERENCIAS

ABNT NBR ISO/IEC 27001:2013 Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Requisitos.

ABNT NBR ISO/IEC 27002:2013 Tecnología de la información — Técnicas de seguridad — Código de prácticas para los controles de seguridad de la información.

Canal Confidencial: 0800 721 0783 (https://www.canalconfidencial.com.br/vtal/)

NIST Cybersecurity Framework Version 1.1.

Política de Clasificación de datos

Política de Retención de Datos

Manual de Privacidad y Protección de Datos Personales para Terceros

6 GLOSARIO

- Autenticidad: garantía de la veracidad de la autoría de la información;
- Colaboradores: todos los Colaboradores Internos y Colaboradores Externos que, dentro del alcance de su relación con V.tal, puedan tener acceso a las áreas, equipos, información, archivos, redes y datos propiedad de la Compañía;
- Colaboradores externos: todos los colaboradores contratados indirectamente por la Compañía, ya sean proveedores de servicios, terceros, proveedores y socios de la Compañía;
- Colaboradores internos: todos los colaboradores contratados directamente por la Compañía, ya sean socios, directores, administradores, colaboradores, aprendices menores y pasantes;
- Confidencialidad: la información debe estar disponible y solo debe divulgarse a personas, entidades o procesos autorizados;
- Cumplimiento: proceso de garantizar el cumplimiento de un requisito, que pueden ser obligaciones comerciales con las partes interesadas (inversores, empleados, acreedores, etc.) y con aspectos legales y reglamentarios relacionados con la gestión de empresas, dentro de los principios éticos y de conducta establecidos por la Alta Administración;
- Disponibilidad: Las personas autorizadas tendrán acceso a la información y a los activos correspondientes cuando sea necesario.
- Integridad: salvaguardar la exactitud de la información y los métodos de procesamiento;
- Información: es la recopilación o conjunto de datos y conocimientos resultantes del tratamiento, manipulación y/o V.tal de datos, de tal forma que represente una modificación (cuantitativa o cualitativa) en el conocimiento del sistema (humano o máquina) que los recibe;
- Información Protegida: toda la información y cualquier dato o activo generado, adquirido, manejado, almacenado, bajo custodia, transportado y/o desechado por los Colaboradores en las instalaciones y/o activos de la Compañía, debido a su vínculo con V.tal o al desempeño de sus actividades contratadas por la Compañía.
- Incidente de seguridad de la información: todas y cada una de las violaciones de seguridad que, accidentalmente o no, conducen o son capaces de conducir a la destrucción, pérdida, alteración, bloqueo, divulgación o uso no autorizado o acceso a datos personales u otra información procesada por V.tal y los Colaboradores;

- Riesgo de seguridad de la información: riesgos asociados con la violación de la autenticidad, confidencialidad e integridad, así como la disponibilidad de información en medios físicos y digitales u otras propiedades de información;
- Seguridad de la Información (SI): es el conjunto de acciones y controles que tiene como objetivo preservar los aspectos de confidencialidad, integridad, disponibilidad, autenticidad y cumplimiento de la información, contribuyendo al cumplimiento de los objetivos estratégicos de V.tal y al servicio a sus clientes.

7 ANEXOS

No aplica

ESTE DOCUMENTO REVOCA VERSIONES ANTERIORES