1. OBJETIVO

La Política de Seguridad de la Información de Viña Concha y Toro S.A y filiales (en adelante el "Holding" o la "Compañía"), define las **guías, acciones y disposiciones para preservar la seguridad de los datos e información** de la Compañía. Considera las actividades para asegurar la confidencialidad, integridad y disponibilidad de la información, con el fin de evitar los daños intencionales y/o accidentales de pérdida o mal uso de los activos de información (datos, equipos, documentación impresa, etc.), daños en la imagen pública de la compañía, y riesgos que afecten la continuidad del negocio en sus procesos y sistemas.

2. ALCANCE

Este documento aplica a todo el personal de Viña Concha y Toro y sus filiales nacionales y extranjeras, incluyendo colaboradores, contratistas, voluntarios y externos que tengan acceso a información de la Compañía.

Esta política comprende todo activo de información que la Compañía posea, en cualquier tipo de formato, de manera que la no inclusión explícita en el presente documento no constituye razón para no proteger activos de información que se encuentren en otros medios o formatos, sea que ésta se encuentre impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o usando medios electrónicos, incluso la conocida por medios verbales.

La seguridad de la información de la Viña estará abordada por los dominios de acuerdo a la norma ISO 27001, aplicando las definiciones que sean pertinentes en los casos particulares de esta norma que apliquen al negocio del Holding. Cabe destacar que el primer dominio corresponde a la Política de Seguridad de la Información que da el marco general para los dominios siguientes.

En esta política se enlazan aspectos individuales para la gestión y control de los recursos de seguridad de la información de la Compañía. A un nivel específico se incorporarán nuevas políticas, normas, procedimientos, implementación de controles, evaluaciones de riesgo, para abordar las necesidades de los dominios que se mencionan a continuación:

- Responsabilidades de los colaboradores y proveedores.
- Clasificación, custodia y uso de activos de información.
- Uso de Internet.
- Control de acceso.
- Seguridad física y del ambiente (evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información de la organización).
- Seguridad de las operaciones.

- Criptografía.
- Adquisición de sistemas, desarrollo y mantenimiento.
- Gestión de los incidentes de seguridad de la información.
- Aspectos de la seguridad de la información en la gestión de la Continuidad de Negocio (BCP).
- Cumplimiento con requerimientos legales y contractuales.

Esta Política incorpora los aspectos más relevantes para la Compañía en esta materia, definiendo directrices, ámbitos de acción, responsabilidades y obligaciones para todos los colaboradores de Viña Concha y Toro y sus filiales.

3. DEFINICIONES

Activo de información: Todos aquellos elementos relevantes que procesen, almacenen y distribuyan información de la compañía. Existen tres tipos de activos: (1) La información en sus múltiples formatos (papel, digital, imagen, texto, audio, video, entre otros); (2) los equipos o sistemas que la soportan y (3) las personas que utilizan esos activos.

Información: Toda información contenida en cualquier formato, digital, impreso u otros que contengan datos de la organización, relacionados con sus productos, servicios, desarrollo de tecnología e informática, sistemas, planes de trabajo y negocios, estrategias de precios y mercados, así como los antecedentes de sus colaboradores, directores, ejecutivos, proveedores, clientes.

Información Pública: Aquella información que está actualmente en conocimiento del mercado o del público en general y que, por lo tanto, su divulgación no presenta riesgos para la organización.

Información de Uso Interno: Toda aquella información utilizada por la organización para desarrollar normalmente sus operaciones, sin tener la característica de Información Confidencial, también estarán en esta categoría la información que no generen un daño o perjuicio a los procesos de la organización.

Información Confidencial: Toda aquella Información que de acuerdo con su naturaleza es privada, y su conocimiento por parte de terceras personas tiene el potencial de afectar el desarrollo de los negocios de la organización (por ejemplo, información de clientes, asociados, proveedores).

Información Altamente Confidencial: Toda aquella información cuya divulgación o uso en forma negligente puede causar un daño grave para la organización, sus directores o gerentes. Se entiende que es Información Altamente Confidencial, entre otras, las siguientes: los resultados financieros de la empresa antes de su publicación al mercado, los antecedentes sobre negociaciones en curso en las que se ha pactado expresamente confidencialidad con la contraparte, las actas de Directorio de la

sociedad, informes de gestión, de costo, de auditoría, configuraciones de sistemas, contraseñas a los sistemas, entre otras.

Ciberataque: Es una acción intencional que busca causar daños o interrupciones en sistemas informáticos, redes o dispositivos conectados a Internet. Puede incluir acciones como la introducción de virus, la obtención ilegal de información, el robo de identidad, la interrupción de servicios y la destrucción de datos.

Ciberdefensa: Conjunto de medidas y estrategias destinadas a proteger las redes, sistemas y dispositivos informáticos de una organización o país de posibles ciberataques.

Ciberespacio: Término utilizado para describir el espacio virtual existente en la red de Internet, en el cual los usuarios interactúan a través de dispositivos conectados a la red. Incluye todo tipo de contenido digital, desde sitios web, redes sociales, entre otros.

Infraestructura de la información: Aquella infraestructura conformada por las personas, procesos, procedimientos, herramientas, instalaciones y tecnologías que soportan la creación, uso, transporte, almacenamiento y destrucción de la información.

Infraestructuras críticas de la información: Las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad.

Correo electrónico: Sistema de comunicación que permite enviar y recibir mensajes mediante Internet.

Phishing: Técnica de fraude en línea con la cual se busca obtener información personal o financiera de una persona mediante la suplantación de identidad en correos electrónicos, sitios web o mensajes de texto.

Malware: Término general para el software malicioso que se utiliza para causar daño a un dispositivo o red. Incluye virus, gusanos, troyanos, ransomware y otros tipos de software malicioso.

Ransomware: Es un tipo de malware que cifra los archivos del sistema infectado y exige un rescate para recuperarlos.

Botnet: Término referido a varios equipos informáticos infectados y controlados por ciberdelincuentes de forma remota con un fin malicioso.

Firewall: Equipo de comunicaciones que permite conectar las redes internas de una empresa con la red pública Internet de forma segura, solo dejando ingresar/salir los datos previamente validados y permitiendo bloquear el acceso no autorizado a la red interna de la organización.

4. RESPONSABILIDADES

Viña Concha y Toro, ha establecido una estructura interna que le permite administrar la seguridad de la información al interior de ella, la cual define estrategias específicas para prevenir, detectar y responder apropiadamente a eventos de seguridad.

Colaboradores Internos: Conocer, entender, aplicar y cumplir los aspectos de la Política de Seguridad de la Información vigente, dentro de su ámbito de competencia. Tienen la responsabilidad de cumplir con lo establecido en este documento y aplicarlo en su entorno laboral. Tienen la obligación de alertar de manera oportuna y adecuada a su Jefatura y al Chief Information Security Officer (CISO), respecto a cualquier incidente que atente contra lo establecido en esta política (detallado en la sección 5. Fundamentos de la Política). Poner a disposición del área de Ciberseguridad, todos los antecedentes, información o datos que le sean solicitados.

Proveedores y Terceros: Empresas prestadoras de servicios, contratistas, subcontratistas y cualquiera que, por cuenta propia o de terceros, desarrolle trabajos para o por cuenta de "Viña Concha y Toro". En los casos que estos prestadores tengan acceso a información confidencial o altamente confidencial de la Compañía se deberán firmar acuerdos de responsabilidad y confidencialidad con estos.

Chief Information Security Officer (CISO): Es el principal responsable en la definición de criterios de seguridad y Ciberseguridad de la información en Viña Concha y Toro y filiales, para lo cual deberá analizar permanentemente el nivel de riesgo existente, además de mantener la vigencia de este documento, generando las modificaciones necesarias acorde con las nuevas amenazas y riesgos del entorno. Por otra parte, es responsable de publicar y dar a conocer nuevas versiones del documento dentro de la Compañía, informar al Comité de Ciberseguridad y a la alta Gerencia los riesgos asociados a la Ciberseguridad, establecer medidas de mitigación pertinentes y proponer los cambios al Comité para su posterior validación y aprobación. Por último, es clave dentro de su rol detectar la necesidad de inducción y/o capacitación en la comprensión y adopción de la política de seguridad de la información en los casos que sea necesario.

Comité de Ciberseguridad: Tiene por responsabilidad alinear la estrategia de Ciberseguridad con la estrategia del Holding, dándole prioridad a los proyectos, de acuerdo con los planes estratégicos propuestos por la Gerencia General y el Directorio, así como establecer los criterios de control apropiados para ser efectivos y eficientes, logrando confidencialidad e integridad, cumpliendo con las políticas y procedimientos de la Compañía. El Comité está conformado por la Gerencia Corporativa de Finanzas y Asuntos Corporativos, Gerencia de Comunicaciones Corporativas, Gerencia de Tecnología de la Información, Gerencia de Personas, Fiscalía y Auditoría Interna.

5. FUNDAMENTOS DE LA POLÍTICA

Viña Concha y Toro y sus filiales deben encargarse permanentemente de gestionar los riesgos de su negocio, cumpliendo con todas las regulaciones y exigencias que el mercado solicita. Todos los colaboradores están obligados a proteger la información de la Compañía. En esta política entregamos instrucciones a los colaboradores de cómo evitar infracciones de seguridad.

a) Clasificación de Información

La información es un activo para la Compañía, y su clasificación es esencial para garantizar la seguridad y la privacidad de esta. Toda información generada, recibida o almacenada por el Holding debe ser clasificada de acuerdo con su nivel de sensibilidad. Los niveles de clasificación incluyen: Pública, Uso Interno, Confidencial y Altamente Confidencial.

b) Uso responsable de la información

Toda información clasificada como Altamente Confidencial o Confidencial, debe ser tratada con la máxima precaución y seguridad. Se debe hacer uso responsable de la información que cada colaborador y usuario de los sistemas utiliza y administra. Está prohibido divulgar cualquier información clasificada como “Confidencial”, “Altamente Confidencial” o de “Uso Interno”, en cualquier medio, incluso verbal, salvo que sea explícitamente autorizado por escrito por el Fiscal de la Compañía. Todo aquello que no está expresamente permitido, está prohibido, siendo necesario exponer la situación en conflicto para que se otorgue autorización explícita a aquello que se necesita. Esto implica la inhabilitación de todo aquello que no sea necesario.

La información y sus recursos tecnológicos deben ser usados exclusivamente para propósitos relacionados con el negocio y el mismo debe ser autorizado por la jefatura correspondiente. Se deben aplicar criterios de uso responsable de los activos del Holding cuando no exista una política o normativa explícita para su utilización.

c) Comunicación e información de la Compañía hacia externos

En el caso de ser necesario, la comunicación de información interna de la Compañía hacia entidades externas (medios de comunicación, prensa en general, foros de discusión en la web, revistas, entre otros), debe canalizarse por los conductos y procedimientos regulares que establece la Gerencia de Comunicaciones de la Compañía, se debe solicitar autorización y establecer una estrategia que no perjudique la imagen corporativa del Holding, con el objetivo de evitar niveles de exposición indeseados al divulgar Información Confidencial o Altamente Confidencial sin previa autorización.

d) Uso de Internet

En Internet constantemente podemos estar expuestos a ciberataques que pueden generar perjuicio y afectar las operaciones y la infraestructura tecnológica de la Compañía. Para garantizar el uso seguro de Internet por parte de los colaboradores del Holding se deben establecer medidas que incluyen restricciones en el acceso a sitios web con contenido inapropiado o malicioso, así como la descarga de información prohibida o divulgación de información no autorizada.

Las directrices sobre el uso seguro de Internet se especifican en la PO-GCF-SI-02 Política de uso de Internet.

e) Impresión de documentos

No está permitido mantener sobre los escritorios documentos impresos clasificados como información “Confidencial”, “Altamente Confidencial” o “Uso Interno”, éstos se deben resguardar adecuadamente.

f) Eliminación de documentos

Todos los documentos e información clasificados como “Confidencial” o “Altamente Confidencial” deben ser eliminados de manera segura, y de acuerdo con las regulaciones o normas aplicables (si corresponde). Esto incluye la eliminación física de cualquier documento en papel y la eliminación segura de cualquier información almacenada en dispositivos electrónicos.

En caso de requerir la eliminación o destrucción de documentos impresos que contengan información “Confidencial” o “Altamente Confidencial”, se deberán utilizar técnicas de destrucción que imposibiliten su recuperación por parte de terceros (para esto es recomendable el uso de máquinas o herramientas picadoras de papel).

No se podrán eliminar ni destruir documentos legales que deben permanecer en la Compañía por los tiempos que establecen las leyes y normativas vigentes. En caso de duda, se debe consultar a Fiscalía.

g) Acceso a oficinas

El acceso físico a las oficinas debe ser restringido solo a personal autorizado. Todos los empleados, contratistas, externos y visitantes deben presentar una identificación válida antes de ingresar a las instalaciones de la Compañía. Además, todas las áreas de trabajo y salas de servidores deben estar protegidas para prevenir el acceso no autorizado. El personal de seguridad debe monitorear las entradas y salidas de las instalaciones, registrar y reportar cualquier actividad sospechosa.

h) Protección de dispositivos personales y de la Compañía

Cuando los colaboradores usan sus equipos personales para acceder al correo electrónico o a sus cuentas, tienen la responsabilidad de mantener sus equipos personales y los asignados por la Compañía (teléfono móvil, tablet o computador personal) de forma segura. Para lograr esto deben:

- Mantener todas las contraseñas de acceso protegidas.
- Mantener el antivirus actualizado.
- No dejar el dispositivo expuesto a terceros o sin atender.
- Instalar actualizaciones de seguridad del navegador web y de los sistemas, por lo menos 1 vez al mes o en la medida que las actualizaciones estén disponibles.
- Acceder a cuentas y sistemas de la Compañía solo a través de redes seguras y privadas.
- Bloquear sus dispositivos cuando abandonen sus escritorios o dejen sus equipos sin atender.
- Conectar dispositivos con conexión USB solo en caso de mouse y teclado, el resto de los dispositivos no está permitido.
- Instalar solo los programas autorizados por la Compañía (Listado Corporativo).

Adicionalmente, tienen prohibido acceder a cuentas y sistemas internos desde computadoras de otros usuarios y/o prestar su equipo asignado a otros colaboradores.

Con respecto a los nuevos ingresos, y los equipos que les son facilitados por la Compañía, deben seguir las siguientes instrucciones:

- Acceder a la red de la Compañía / sistema de desbloqueo-cambio contraseña.
- Uso de software para conexión remota.
- Acceder a los sistemas de la Compañía que le corresponden.
- Acceder al correo electrónico de la Compañía, utilizando un segundo factor de autenticación.

Las directrices sobre el uso seguro de equipo computacionales se especifican en la PO-GCF-SI-03 Política de uso de equipos computacionales (ver Política).

i) Uso seguro del correo electrónico

El correo electrónico a menudo recibe correos no deseados e inclusive intentos de estafas y software malicioso. Para evitar infección de algún virus o robo de datos, instruimos a los colaboradores a:

- No abrir documentos y hacer clic en links adjuntos cuando el contenido no está claramente explicado.
- Ser cauteloso ante títulos y/o contenido impactante o peticiones urgentes que inciten a actuar o realizar una acción de forma inmediata.
- Revisar correo y nombre de las personas que envían el correo para asegurar que son legítimos.
- Buscar inconsistencias en la redacción (por ej. errores gramaticales, letras mayúsculas, excesivo uso de signos de exclamación)

Si el colaborador no está convencido de que el correo que recibió es seguro, debe reportarlo por los canales dispuesto para ello por el área de Ciberseguridad.

Las directrices sobre el uso seguro del correo electrónico se especifican en el EST-GCF-SI-02 Estándar de uso de correo electrónico corporativo.

.

j) Administración adecuada de las contraseñas

Las contraseñas de acceso a los sistemas computacionales que provee la Compañía **son individuales, intransferibles y de responsabilidad única de la persona asignada**. La filtración o fuga de contraseñas puede comprometer toda la infraestructura de TI de la Compañía. Las contraseñas deben ser seguras, robustas y permanecer secretas, por esta razón, instruimos a nuestros colaboradores a:

- Elegir contraseñas con al menos 12 caracteres (incluyen letras minúsculas, mayúsculas, números y símbolos) y evitar información que sea fácil de adivinar (por ej. cumpleaños, nombres, etc.)
- Recordar las contraseñas en lugar de escribirlas. Si los colaboradores necesitan escribir sus contraseñas, están obligados a mantener el papel o archivo digital en forma confidencial y destruirlo cuando su trabajo haya finalizado.
- Cambiar sus contraseñas cada 60 días.

Las directrices sobre la administración adecuada de las contraseñas se especifican en el EST-GCF-SI-01 Estándar de contraseñas.

k) Transferencia segura de datos

La transferencia de datos genera riesgos de seguridad, por esta razón los colaboradores deben:

- No transferir Información "Confidencial" o "Altamente Confidencial" (por ej. información de clientes, registros de colaboradores entre otros), hacia otros dispositivos o cuentas. Cuando la transferencia de datos en forma masiva es necesaria, los colaboradores deben contactar al equipo de especialistas de TI y solicitar las autorizaciones correspondientes.
- Compartir información sólo a través de las herramientas y programas tecnológicos que la Compañía pone a disposición de todos los colaboradores (Listado Corporativo).
- Cuando sea estrictamente necesario, se debe compartir información confidencial o altamente confidencial solo a través de la Red/Sistemas de la Compañía, no a través de Internet pública, ni mediante dispositivos externos.
- Asegurar que los destinatarios de los datos están autorizados y tienen las políticas de seguridad adecuadas.
- Reportar estafas, infracciones de seguridad e intentos de ingreso no autorizado a los sistemas de la Compañía al área de Ciberseguridad (ciberseguridad@conchaytoro.cl).

El procesamiento de los datos por parte de la Compañía está basado en la normativa vigente de protección de datos personales, correspondiente a cada localidad.

l) Trabajo remoto de forma segura

Colaboradores trabajando a distancia (por ejemplo, desde sus casas, desde un hotel, desde un café, etc.) deben seguir los lineamientos planteados en esta política. El acceso a los sistemas de la Compañía a distancia debe ser realizado a través de una red privada segura (VPN); así como seguir todos los controles de cifrado de datos, estándares y configuración de protección.

6. INCUMPLIMIENTO Y SANCIONES

Las infracciones a la Política Corporativa de Seguridad de la Información serán evaluadas por el Comité de Ciberseguridad, para definir las eventuales sanciones con la Gerencia de Personas de la Compañía, áreas de compras, gestión de servicios externos o fiscalía, para el caso que corresponda, ajustándose a lo señalado en nuestro Reglamento Interno de Orden, Higiene y Seguridad (RIOHS).

Tales sanciones podrán incluir las de amonestación, registro de los hechos para su consideración en el desarrollo profesional futuro del infractor, el término del contrato en cuestión y la posible denuncia de los hechos a las autoridades respectivas. Todo lo anterior, según la naturaleza y gravedad de los hechos y sus consecuencias para la Compañía, sus accionistas y el mercado en general.

El incumplimiento a la Política Corporativa de Seguridad de la Información podrá constituir una infracción grave al Contrato de Trabajo, razón por la cual la Compañía se reserva el derecho de tomar medidas administrativas o legales que corresponda en contra de quienes no den cumplimiento a lo dispuesto en la presente política y en su documentación de referencia.

7. MANEJO DE EXCEPCIONES

La Política y demás normas sobre la Seguridad de la Información son de carácter obligatorio, por lo que no admiten excepciones.

8. MODIFICACIONES DEL DOCUMENTO

Versión 01 - Fecha de modificación: marzo 2018

- Se actualiza de manera integral la versión inicial de la Política Corporativa de Seguridad de la Información.
- Se incorpora codificación (PO-TI-SI-01) al documento de acuerdo a controles del Sistema de Gestión Documental.

**** Versión 02 - Fecha de modificación: septiembre de 2020***

- Se actualiza de manera integral la versión inicial de la Política Corporativa de Seguridad de la Información.
- Se incorporan los elementos de ciberseguridad.
- Se incorpora la comunicación hacia externos
- Se incorpora la política de uso de Internet.

**** Versión 03 - Fecha de modificación: enero de 2023***

- Se incorporan las responsabilidades del Chief Information Security Officer (CISO).
- Se cambia el Comité de Riesgos y Seguridad de la Información por el Comité de Ciberseguridad.
- Se actualizan las responsabilidades del Comité de Ciberseguridad.
- Se actualizan los parámetros de contraseñas.
- Se actualiza el correo de consultas por ciberseguridad@conchaytoro.cl.
- Se actualizan los miembros del Comité de Ciberseguridad (aprobadores).
- Se mejora la redacción de distintos puntos de la Política.

Modificado por: Alejandro Jofre - Chief Information Security Officer (CISO)