Política General de Seguridad de la Información y Ciberseguridad

Contenido

1 Introducción

La presente "Política General de Seguridad de la Información y Ciberseguridad" es un instrumento que permite a **Corporate Compliance & Risk** declarar de manera formal su entendimiento y compromiso con todas las medidas y esfuerzos que sean necesarios para garantizar una debida protección de la confidencialidad, integridad y disponibilidad que requieran las distintas categorías de información y los activos relacionados.

Las medidas y acciones que se definan e implementen para proteger la información buscan la disminución del impacto eventual que se genere sobre las personas y/o los activos de información, debido a la materialización de los riesgos presentes en el ciberespacio o cualquier otro que pudiera afectar a la información o la infraestructura asociada.

Dado lo anterior, en este documento se establecerán los objetivos, principios y compromisos que **Corporate Compliance & Risk** define como esenciales para el debido tratamiento de los riesgos mencionados, apoyando las estrategias de la organización y los requerimientos que surgen de las Partes Interesadas que apliquen a este ámbito.

2 Objetivos

La presente Política define lineamientos generales que permitan a **Corporate Compliance & Risk** garantizar el logro de los objetivos conducentes a dar cumplimiento y satisfacer los requisitos derivados de las necesidades de las Partes Interesadas relacionadas, manteniendo su alineación a las estrategias de la organización.

En particular, se definen los siguientes objetivos:

- Cumplir con los Principios de Seguridad de la Información y Ciberseguridad.
- Mantener la confianza de sus clientes, socios, empleados y proveedores.
- Minimizar los riesgos que pudieran afectar a las personas y los activos de información.

3 Principios de Seguridad de la Información y Ciberseguridad.

- **Corporate Compliance & Risk** se compromete a proteger la información de propiedad de sus clientes y/o asociados que haya sido declarada como confidencial o sensible, y se encuentre siendo procesada o resguardada por sus procesos de negocio, su infraestructura tecnológica y/o las personas pertenecientes a la organización o terceros a los que **Corporate Compliance & Risk** les otorgue acceso como resultado de un servicio outsourcing.
- Las responsabilidades de Seguridad de la Información y Ciberseguridad serán, según corresponda, definidas, publicadas, compartidas y/o aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

4 Alcance

La presente "Política de Seguridad de la Información y Ciberseguridad" aplica a todos los empleados, proveedores y socios de negocio de **Corporate Compliance & Risk** que participen o tengan acceso a la información (determinada en los "Principios de Seguridad de la Información Ciberseguridad") y/o los activos relacionados, a través de la generación, procesamiento y transmisión de la misma, o bien tengan acceso a los repositorios donde ésta se encuentre almacenada.

5 Revisión y Actualización

Este documento deberá ser revisado anualmente, generando las actualizaciones eventuales que se desprendan de este análisis.

Adicionalmente, en caso de producirse cambios relevantes en los contextos internos o externos, también se deberán incorporar modificaciones si fuese necesario.

6 Referencias

- Norma ISO/IEC 27001
- Norma ISO/IEC 27002
- Norma ISO/IEC 27032
- Código de Ética.
- Reglamento Interno de Orden, Higiene y Seguridad.

7 Partes Interesadas

Para efectos de la presente Política y en concordancia son lo establecido en la Norma ISO 27001, se podrán considerar Partes Interesadas todas las personas u organizaciones internas o externas, públicas o privadas que, directa o indirectamente, puedan influir o impactar en el objetivo de Seguridad de la Información y Ciberseguridad de **Corporate Compliance & Risk** establecido en esta Política.

Dado lo anterior, **Corporate Compliance & Risk** ha definido las siguientes partes interesadas según contexto:

- Contexto Interno:
  - Socios Consultores
  - Empleados
  - Consultores
- Contexto externo:
  - Clientes
  - Partners o Asociados
  - Proveedores

A partir de esta definición, se establecen las siguientes necesidades o requisitos:

- Protección de las personas, la información y los activos relacionados.
- Privacidad de los datos personales.
- Monitoreo y gestión de riesgos de Seguridad de la Información y Ciberseguridad.
- Continuidad de las operaciones.

8 Roles y Responsabilidades

A continuación, se establecen los roles y responsabilidades necesarios para la correcta implementación y operación de la "Política General de Seguridad de la Información y Ciberseguridad"

1. Socios Consultores:
   - Velar por el establecimiento y difusión de esta Política y supervisar su cumplimiento.
   - Implementar y/o generar las condiciones necesarias para su implementación, de todas las medidas y controles que se requieran para asegurar el cumplimiento de esta Política.
   - Serán, por defecto, los que ejerzan el rol de "Dueño" o "Responsable" de la información clasificada como "Confidencial".

2. Empleados
    - Dar cumplimiento cabal a las disposiciones establecidas en esta Política.
    - Informar de inmediato sobre cualquier incidente o brecha de seguridad detectada u observada.

3. Proveedores, Partners o Asociados
    - Dar cumplimiento cabal a las disposiciones establecidas en esta Política y que les apliquen.
    - Difundir dentro de sus organizaciones o a quienes corresponda las disposiciones establecidas en este documento.
    - Informar de inmediato sobre cualquier incidente o brecha de seguridad detectada u observada.

9 Lineamientos de Seguridad de la Información y Ciberseguridad

9.1 Clasificación y Control de la Información

- Para la clasificación de la información se han determinado 3 categorías:
  - Confidencial
  - Uso Interno
  - Pública
- Toda aquella información de propiedad de clientes y/o asociados de **Corporate Compliance & Risk** que haya sido declarada como confidencial o sensible deberá ser clasificada y tratada como "Confidencial", no importando el medio en que se registre o se despliegue.
- Aquella información que no cuente con una clasificación explicita será considerada como de "Uso Interno".
- Para la información clasificada como "Confidencial", se deberá establecer el rol de "Dueño" o "Responsable" al interior de la organización, entidad que podrá autorizar los accesos asociados a la información respectiva.

9.2 Seguridad de los Recursos Humanos

- Se deberá mantener una adecuada seguridad en la administración de los Recursos Humanos, la que considera implementar controles o verificaciones:
  1. En la contratación, realizando una debida verificación de antecedentes.
  2. Durante el empleo, con campañas de difusión y sensibilización en temas de seguridad y ciberseguridad.
  3. En la finalización del empleo o cambio de puesto, rol o responsabilidad, asegurando la desactivación de todos los accesos (o aquellos que ya no se requieran) y la devolución o entrega de la información o activos que correspondan.

9.3 Seguridad Física y Ambiental

- Se deberán mantener controles para evitar accesos físicos no autorizados o cualquier otro daño (asociado a la acción física) a los activos de información.
- Esto incluye los controles de acceso a las dependencias (edificio, oficinas), computadores u otros dispositivos de la compañía (o contratados para fines

corporativos) que mantengan, transmitan o procesen información o interacción con el ciberespacio.

- Los equipos portátiles deberán contar con sistema de anclado ("candado") que permita prevenir la sustracción de éstos.
- Se deberá asegurar el mantenimiento de principios de "Escritorio limpio". Para esto:
    - Todos los equipos deberán tener configurado un bloqueo automático de la pantalla. Adicionalmente, cada usuario deberá bloquear sus dispositivos cuando estos queden desatendidos.
    - El puesto de trabajo deberá mantenerse despejado de papeles, medios de almacenamiento desmontables y equipos móviles que no estén anclados o asegurados físicamente.

9.4 Seguridad de los Accesos

- Para la gestión de accesos a información o recursos se deberá considerar como principio básico la "*necesidad de conocer*", elemento estrictamente necesario para la aprobación de accesos por parte de los "Dueños" o "Responsables" internos.
- Se deberán ejecutar todas las acciones necesarias para garantizar que todos los derechos de acceso sean removidos cuando ya no sean necesarios.
- Respecto del manejo de contraseñas asociadas a las credenciales de acceso:
    - Son estrictamente confidenciales, personales e intransferibles, incluidas las OTP.
    - A excepción de las OTP, las contraseñas deberán tener un largo mínimo de 8 caracteres, ser alfanuméricas y con una vigencia máxima de 12 meses.
    - A excepción de las OTP, las contraseñas deberán ser cambiadas ante cualquier sospecha de haber sido comprometidas.

9.5 Seguridad de las Operaciones

9.5.1 Protección ante el software malicioso

- Con el objetivo de asegurar que los recursos de información y la información propiamente tal están protegidos contra el malware (software malicioso), todos los equipos computacionales, incluidos los teléfonos inteligentes, deberán contar con alguna solución antimalware que prevenga y/o contenga estas amenazas.

- En aquellos casos en que los equipamientos sean contratados como servicio, se deberá asegurar que se verificó que el proveedor respectivo mantiene los debidos controles anti malware.

9.5.2 Hardening de equipos

- Los equipos utilizados para las operaciones de los procesos de negocio y/o que almacenen información sensible deberán mantener los Sistemas Operativos y Aplicaciones debidamente actualizadas y "parchadas".
- En aquellos casos en que los softwares sean contratados como servicio, se deberá asegurar que se verificó que el proveedor respectivo mantiene los controles necesarios de actualización y "parchado".

9.5.3 Copias de respaldo

- Se deberán realizar copias de respaldo de la información que permita evitar la pérdida de datos, en especial, aquellos de mayor sensibilidad.
- Estos respaldos podrán hacerse directamente sobre dispositivos de almacenamiento específico o utilizando servicios tipo Cloud que mantengan sincronizada y protegida la información de los equipos.

9.6 Seguridad de Proveedores y Servicios

- Se deberá asegurar la protección de la información y los activos de la organización a los que accedan los proveedores, estableciendo "Acuerdos de Confidencialidad" o de "No Revelación" que cubran las necesidades de protección de la información confidencial.
- Estos acuerdos deberán utilizar términos legalmente exigibles.
- Las plataformas o servicios de software (SaaS) deberán garantizar que la seguridad de la información sea parte integral de estos, por lo que se deberá verificar previamente la declaración de cumplimiento respectiva.

9.7 Gestión de Incidentes de Seguridad de la Información y Ciberseguridad

- Cualquier evento que, producto de la violación de la presente Política o de las leyes aplicables, dañé la confidencialidad, integridad y/o disponibilidad de la información de propiedad de alguna de las Partes Interesadas declaradas en esta Política, deberá ser inmediatamente atendido para contener los posibles impactos que pudieran producirse.
- Adicionalmente, **Corporate Compliance & Risk** se compromete a informar a las Partes Interesadas afectadas con la mayor celeridad posible.

- Los trabajadores deben alertar de cualquier incidente y/o situación que afecte o pueda afectar la seguridad de la información o la ciberseguridad.

9.8 Cumplimiento de los requisitos legales

- **Corporate Compliance & Risk** se compromete a dar cumplimiento cabal a todas las disposiciones legales establecidas y vigentes que tengan relación con el uso de información, datos personales y sistemas informáticos, incluidos aquellos requisitos establecidos en los compromisos contractuales como también aquellos asociados a los Derechos de Propiedad Intelectual.