# SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

IVAN GONZALO TORO OLAVARRIA

Firmado digitalmente por IVAN GONZALO TORO OLAVARRIA
Fecha: 2023.05.24 19:41:06 -04'00'

*NOTA DE CONFIDENCIALIDAD*

## Tabla de Contenido

## 1. Control de Cambios

| Fecha | Versión | Página | Aprobación | Modificación |
|---|---|---|---|---|
| 02/05/2019 | 01 | Todas | Gerencia de Administración y Finanzas | Versión inicial del documento |
| 20/04/2020 | 02 | Todas | Gerencia de Administración y Finanzas | Versión inicial del documento |
| 18/05/2020 | 03 | Todas | Gerencia de Administración y Finanzas | Se agrega el principio de segregación de tareas para ITQ, agrega puntos de las normas 27017 y 27018 |
| 30/06/2022 | 04 | Todas | Comité de Seguridad de la Información | Se agrega objetivos a la Política cumpliendo con el apartado 5.2 la norma ISO 27001 |
| 11/04/2023 | 05 | Todas | Comité de Seguridad de la Información | Se realiza actualización de estructura de documento, se incorpora cláusula de Ciberseguridad |

La presente versión substituye completamente a todas las precedentes, de manera que este sea el único documento válido de entre todos los de la serie.

## 2. Objetivo

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

## 3. Alcance

La Seguridad Informática de ITQ LATAM, es responsabilidad de todo el personal, tanto interno como externo, que haga uso de ésta. Por tal razón, las políticas planteadas en este documento son de conocimiento y cumplimiento obligado para todo el personal interno y externo de la empresa.

## 4. Referencia Normativa

Norma ISO/IEC 27001. “Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos”

Norma ISO/IEC 27002. “Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Código de Prácticas para los controles de seguridad de la información”

**Requisitos y Controles Anexo A:**

- Req. 5.2 Política.

## 5. Responsables

| Rol | Responsabilidades |
|---|---|
| Comité de Seguridad | Es el Comité encargado de la Seguridad de la Información, en el cual se sustente el Plan de Seguridad de la Información de ITQ LATAM. Este comité debe analizar la administración de problemas de seguridad y se definan las estrategias a implementar que permitan controlar el entorno lógico y físico de la información de ITQ LATAM. |

- Supervisar el desarrollo inicial de las políticas de seguridad al interior de su organización y el control de su implementación, y velar por su correcta aplicación.
- Gestionar la respuesta a incidentes que afecten a los activos de información institucionales.
- Impulsar las políticas, normas y procedimientos de seguridad de la información basado en las leyes y regulaciones locales vigentes, mejores prácticas de mercado y necesidades del negocio.
- Proponer, organizar y supervisar el plan de capacitación y sensibilización de seguridad de la información para los colaboradores de ITQ LATAM.
- Realizar seguimiento al plan de seguridad de la información y generar nuevas iniciativas de seguridad de la información.
- Comunicar e involucrar a la organización en las iniciativas de seguridad la Información a fin de asegurar su efectiva implementación a nivel de ITQ LATAM.
- Apoyar en el análisis del riesgo asociado a la implementación de los distintos proyectos, productos y servicios y entregar las recomendaciones para el tratamiento de riesgos y vulnerabilidades.
- Apoyar en la definición, desarrollo e implementación de planes de mejoras en el ámbito de seguridad de la información para los distintos procesos, productos y servicios en la organización.
- Manejar una visión integral de la seguridad de la información de ITQ LATAM, teniendo roles y responsabilidades en otras políticas relacionadas a seguridad de la información.
- Promover actividades de gestión de riesgos y, en particular, para la aceptación de los riesgos residuales.

Este comité debe sesionar al menos semestralmente o cuando un evento de seguridad así lo amerite, debe estar conformado por las siguientes personas:

- ✓ Gerencia de Recursos Humanos.
- ✓ Gerencia de Finanzas.
- ✓ Gerencia de Ingeniería.
- ✓ Gerencia de Ciberseguridad.

| | |
|---|---|
| | ✓ Gerencia de Proyectos.<br>✓ Gerencia de Servicios.<br>✓ Gerencia Comercial.<br>✓ Gerencia de Marketing.<br>✓ Representante de la Dirección.<br>✓ Oficial de Seguridad. |
| Oficial de Seguridad | • Encargado de administrar y controlar el proceso o plan de implementación de las normativas y controles establecidos por el Comité de Seguridad y definidas en las Políticas de Seguridad de la Información.<br>• Monitorear permanentemente el cumplimiento de las políticas de seguridad de la información.<br>• Verificar la implementación de los distintos mecanismos de registros de eventos y demás parámetros de seguridad a nivel de sistemas operativos y de apoyo.<br>• Analizar e informar formalmente al Comité de Seguridad de cualquier evento que atente contra la seguridad de la información.<br>• Contar y gestionar el contacto con terceros, de otras empresas, especialmente de empresas de servicio que pudieran apoyar a ITQ LATAM ante la problemática de administración de seguridad. |
| Área de Compliance | Es la unidad organizacional responsable de definir y mantener la presente política de acuerdo con las mejores prácticas y recomendaciones evaluando los riegos y estableciendo el plan de acción en conjunto con todas las áreas involucradas en la política y sus funciones son las siguientes:<br>• Tener a su cargo el desarrollo de las políticas de seguridad al interior de la organización y el control de su implementación, y velar por su correcta aplicación.<br>• Coordinar la respuesta a incidentes que afecten a los activos de información de la organización.<br>• Impulsar las políticas, normas y procedimientos de seguridad de la información basado en las leyes y regulaciones locales vigentes, mejores prácticas de mercado y necesidades del negocio.<br>• Proponer, organizar y supervisar el plan de capacitación y sensibilización de seguridad de la información para los colaboradores de ITQ LATAM. |

| | |
|---|---|
| | • Realizar seguimiento al plan de seguridad de la información y generar nuevas iniciativas de seguridad de la información.<br>• Apoyar la comunicación e involucramiento de la organización en las iniciativas de seguridad la Información a fin de asegurar su efectiva implementación<br>• Analizar el riesgo asociado a la implementación de los distintos proyectos, productos y servicios y entregar las recomendaciones para el tratamiento de riesgos y vulnerabilidades.<br>• Apoyar en la definición, desarrollo e implementación de planes de mejoras en el ámbito de seguridad de la información para los distintos procesos, productos y servicios en la organización.<br>• Mantener informado a las Gerencias y al Comité de Seguridad de los niveles de riesgo de seguridad de la información y tecnología.<br>• Convocar, registrar en actas las reuniones del Comité de Seguridad de la información de ITQ LATAM.<br>• Establecer puntos de enlace con encargados de seguridad de otros organismos públicos, privados y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes. |
| Gerentes de ITQ LATAM | • Asegurar el cumplimiento de la Política de Seguridad de la Información al interior de su área, y tomar conocimiento de las políticas en incumplimiento y excepciones.<br>• Velar por la protección de la confidencialidad, integridad y disponibilidad de la información que se procese, transmita y almacene en los procesos y los ámbitos bajo su responsabilidad.<br>• Velar por la protección de la confidencialidad, integridad y disponibilidad de la información de los Activos Individuales, y llevar a cabo procesos de seguridad de la información específicos. |
| Colaboradores y Proveedores Críticos | Son responsables del cumplimiento de estas políticas. Como así mismo deben saber que se podrá supervisar violaciones a las políticas mediante controles automáticos registrados en logs, o cualquier otro medio disponible para dichos efectos, en base a los cuales se pueden tomar medidas disciplinarias. |

## 6. Descripción de la Política

### 6.1 Objetivos

- Definir el marco global para la gestión de la Seguridad de la Información en ITQ LATAM, estableciendo los lineamientos, para la protección y preservación de la confidencialidad, integridad y disponibilidad de la información de ITQ LATAM y de sus clientes en forma consistente con las estrategias de ITQ LATAM.

- Asegurar la privacidad y protección de la información basándonos en las normas ISO 27001 seguridad de la información, ISO 27017 controles de seguridad para servicios Cloud y ISO 27018 privacidad en la nube.

- Minimizar el riesgo en los procesos asociados a la seguridad de la información y privacidad de datos tanto en ITQ LATAM como en los servicios prestados.

- Proteger eficientemente los activos de información de ITQ LATAM, asegurando la triada de la seguridad de la información en cuanto a la confidencialidad, integridad y disponibilidad.

- Establecer políticas, procedimientos e instructivos que refuercen los procesos contenidos en el sistema de seguridad de la información, para que la información cumpla con los niveles de acceso, autorización y responsabilidad correspondientes para su utilización, divulgación, administración, seguimiento y custodia

- Fortalecer la cultura de seguridad de la información en los trabajadores de ITQ LATAM, que permita la concientización y sensibilización a través capacitaciones, charlas etc., para la mejora continua del SGSI.

- Todos los colaboradores de ITQ LATAM tienen el compromiso de contribuir a la seguridad de la información y resguardo de los activos de información; y deben tener el conocimiento y familiaridad con el contenido de esta política, para el cumplimiento de la normativa que se imparta y que se deba aplicar en cada caso.

- Establecer los requisitos y condiciones generales de protección y resguardo y resguardo de ciberseguridad a los que se encuentra sujeto ITQ LATAM, de acuerdo con las normas

legales y reglamentarias pertinentes, así como los riesgos a que están expuestos los activos de información de la organización.

## 6.2 La Seguridad de la información y uso de bienes y servicios informáticos.

ITQ LATAM, considera la información como un recurso estratégico y uno de sus activos más importantes. Para salvaguardar este activo y no exponerlo a riesgos, se establecen políticas, normas, estándares técnicos y procedimientos de seguridad de la información, a las que deben adherirse todos los trabajadores de la empresa. Lo anterior supone un marco normativo, que comprende las regulaciones, restricciones y prohibiciones necesarias indicadas en los puntos siguientes, para proteger la información de amenaza que atenten contra la confidencialidad, integridad y disponibilidad de la información.

Será responsabilidad de cada colaborador leer, conocer y entender en detalle todas las políticas, normas, estándares y procedimientos de seguridad de la información que se publiquen en intranet o cualquier medio de comunicación interna.

Es exclusiva responsabilidad de cada trabajador:

a) Cumplir con las políticas y normas de seguridad que ITQ LATAM defina, difunda y notifique respecto de la información y los flujos de comunicación de ésta.
b) Mantener absoluta confidencialidad, proteger y resguardar toda información de ITQ LATAM que disponga o administre, sean estos informes, datos, proyecciones, métodos, estrategias, configuraciones de software, diagramas de hardware y red u otro que se estime importante para el cumplimiento de los fines de ITQ LATAM, así como de las materias propias del área específica donde se desempeña, respecto de las cuales haya tomado conocimiento producto del ejercicio de sus labores.
c) Cuidar los registros y archivos electrónicos por medio de respaldos periódicos de información.
d) La destrucción de material impreso con información confidencial y estratégica de ITQ LATAM, cuando ello sea procedente.
e) El mantenimiento adecuado de espacios destinados al almacenamiento de información, físicos y electrónicos (computadores personales).
f) Garantizar el uso apropiado de los perfiles informáticos de usuario asignados por ITQ LATAM a cada trabajador, lo cual implica, entre otras obligaciones:

- Cambiar periódicamente sus contraseñas, las contraseñas deben cumplir con la Política de Claves de ITQ LATAM.
- Solicitar la eliminación (o transferencia) de aquellas cuentas o accesos que ya no requiera por cambios de funciones.

g) Dar facilidades a las investigaciones de delitos o faltas que se desarrollen en ITQ LATAM con relación con la utilización de información y el uso de sistemas de información.
h) No dejar expuesta información confidencial o sensible en áreas sin supervisión (como impresoras, escritorios desatendidos, salas de reuniones, sala de recepción, etc.).

Está prohibido para el colaborador:

a) Divulgar o entregar a personas ajenas a ITQ LATAM, o reproducir en presencia de estas, de ninguna forma y medio, sea en soporte material, verbal o virtual, datos, valores, procedimientos, técnicas, estadísticas, instructivos, manuales, datos de empleados de ITQ LATAM, en general, cualquier tipo de información que pudiera afectar a ITQ LATAM en términos legales, técnicos, comerciales o imagen, sin el consentimiento explícito y formal de ITQ LATAM.
b) Actuar negligentemente en el uso de información institucional o provocando la inutilización o destrucción de recursos computacionales y de información.
c) Acceder o usar, sin autorización, canales electrónicos, datos sensibles, equipos computacionales, informes y otros documentos, haciendo uso indebido de claves y contraseñas.

***Nota:*** La desobediencia a cualquiera de las normas señaladas anteriormente en este mandato, se considerará una infracción grave a las obligaciones que emanan del contrato de trabajo.

## 6. 3 Acceso y uso de internet, intranet y aplicaciones informáticas

El acceso a Internet e Intranet por los trabajadores queda sujeto a las siguientes condiciones y limitaciones:

a) El personal debe dar uso responsable y profesional a las plataformas de conectividad a servicios de internet.

b) El personal debe hacer uso de las aplicaciones informáticas internas de ITQ LATAM, diseñadas y perfiladas en conformidad con las funciones del respectivo cargo.
c) Los usuarios de Internet e Intranet deben respetar en todo momento el derecho de propiedad intelectual, la seguridad de los sistemas de terceros y la privacidad ajena.
d) Los usuarios deben cumplir con todos los procedimientos de acceso establecidos por ITQ LATAM, incluyendo el uso de sistemas de autentificación de usuario asignado. Está prohibida la cesión de contraseñas que permiten la autentificación y el acceso a sistemas informáticos de ITQ LATAM, cuentas de correo electrónico, o cualquier tipo de aplicación instalada en los computadores asignados en el ejercicio del cargo. Tampoco pueden utilizarse de forma compartida entre dos o más colaboradores de la empresa.
e) Los usuarios deberán hacer uso de software debidamente licenciado por ITQ LATAM. Está prohibido ejecutar descargas, instalaciones de software o ejecutar copias de aplicaciones licenciadas sin la aprobación formal y por escrito de la Gerencia de Ingeniería de ITQ LATAM.
f) Está prohibido hacer uso de aplicaciones de televisión o radio en línea que utilicen como soporte Internet, debido al alto consumo de la capacidad de la red que ello representa.
g) ITQ LATAM posee el derecho de restringir el acceso a contenidos y materiales en internet o Intranet que pongan en riesgo las redes y plataformas informáticas de ITQ LATAM, lo que no implica un deber de regular el contenido de la Información en Internet. En todo caso, la ausencia de dichas restricciones no implica una autorización para acceder a tal material.
h) La información confidencial o sensible para las actividades de ITQ LATAM, patentada o interna, sólo puede ser transmitida a través de internet previa autorización formal y por escrito de la Gerencia de Ingeniería de ITQ LATAM y del área responsable por el contenido del Activo de Información correspondiente.
i) ITQ LATAM se reserva el derecho de acceso o monitoreo a través de las redes informáticas de ITQ LATAM, sin previo aviso, de cualquier uso de Internet o Intranet, incluyendo la revisión de archivos individuales (no privados) mantenidos por los usuarios en los equipos asignados por ITQ LATAM.
j) Se prohíben los comentarios, bromas, insultos y obscenidades sexuales, raciales u otras, ofensivas o ilegales a través de Internet o Intranet. Asimismo, el uso de Internet o Intranet para observar, tener acceso, cargar, descargar, almacenar, transmitir, crear o manipular en otra forma materiales ofensivos, pornográficos o sexualmente explícitos.
k) Está prohibido utilizar o informar, en forma regular o recurrente, cuentas de correo asignadas por ITQ LATAM para fines personales o ajenos a los intereses de ITQ LATAM.

l) Está prohibido hacer públicas listas de distribución de correos electrónicos de personal de ITQ LATAM.
m) Se prohíbe el envío de correos electrónicos masivos como cadenas, spams, bromas u otros. Los envíos masivos de correos electrónicos institucionales serán ejecutados conforme a los procedimientos que indique la Gerencia de Ingeniería.

***Nota:*** La desobediencia a cualquiera de las normas señaladas anteriormente en este mandato, se considerará una infracción grave a las obligaciones que emanan del contrato de trabajo.

## 6. 4 Uso del equipamiento computacional

El uso responsable y profesional que los colaboradores deben dar al equipamiento computacional asignado por ITQ LATAM implica los siguientes deberes, sin estar limitados a éstos.

Deberes del personal que tenga asignado y que utiliza equipamiento computacional:

a) Validar el correcto funcionamiento del antivirus de ITQ LATAM.
b) Mantener las actualizaciones de parches de seguridad al día, reiniciado el equipo cada vez solicite una nueva instalación.
c) Reportar cualquier falla o anomalía a la Mesa de Soporte de la Gerencia de Ingeniería de ITQ LATAM.

Prohibiciones:

a) Manipular en los equipos computacionales su configuración de hardware (memoria, disco duro, etc.), software (sistema operativo, nombre de equipo, etc.). Sólo personal autorizado por la de Ingeniería de ITQ LATAM o por quien ella designe pueden intervenir el equipamiento.
b) Intercambiar recursos computacionales con trabajadores de otras dependencias.
c) Cambiar la ubicación física de éstos sin la previa autorización del jefe directo. Todos los documentos creados, archivados o comunicados a través del equipamiento computacional de ITQ LATAM, sean estos asignados a usuarios finales o no, son susceptibles a ser auditados.

***Nota:*** La desobediencia a cualquiera de las normas señaladas anteriormente en este mandato, se considerará una infracción grave a las obligaciones que emanan del contrato de trabajo.

## 6.5 Privacidad y Protección de la información de identificación personal

Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda.

Se desarrolla e implementa la Política que indica como la organización se preocupa de la privacidad y protección de información de identificación personal. Esta política debe ser comunicada a todas las personas involucradas en el tratamiento de la información de identificación personal.

Todas las políticas y procedimientos relacionado con el PII serán revisadas al igual que para la norma 27001, 27018 y 27017 una vez al año o cuando exista un cambio significativo dentro de la organización, estas modificaciones serán aprobadas con la revisión de la alta dirección.

Otro tema importante que debe administrar es que los sistemas de información siempre deben crear archivos temporales en el curso normal de su funcionamiento. Dichos archivos son específicos del sistema o aplicación, pero pueden incluir diarios de reversión del sistema de archivos y archivos temporales asociados con la actualización de bases de datos y el funcionamiento de otro software de aplicación. Los archivos temporales no son necesarios una vez finalizada la tarea de procesamiento de la información relacionada, pero hay circunstancias en las que es posible que no se eliminen. El tiempo durante el cual estos archivos permanecen en uso no siempre es determinista.

Los sistemas de información de procesamiento de PII implementado en ITQ LATAM, es una vez al año donde se eliminará los archivos temporales no utilizados por encima de una edad específica.

## 6.6 Administración de Proyectos

Se deber integrar la seguridad de la información en los métodos de administración de proyectos de ITQ LATAM, para asegurarse de que se identifican y abordan los riesgos de seguridad de la información como parte de un proyecto, sin importar su carácter o tipo.

El encargado de la **Oficina de PMO** de ITQ LATAM, es el encargado de definir y asignar las responsabilidades para la seguridad de la información a los roles especificados definidos en los métodos de administración y gestión de proyectos.

Los métodos de administración de proyectos en uso deben requerir que:

a) Se incluyan los objetivos de seguridad de la información en los objetivos del proyecto.
b) Se realice una evaluación de riesgos de seguridad de la información en una etapa temprana del proyecto.
c) La seguridad de la información sea parte de todas las fases de la metodología aplicada del proyecto.

## 6.7 Segregación de Tareas

Separación de responsabilidades de la diversidad de actividades que intervienen en la consecución del sistema de gestión de seguridad de la información, con el fin de reducir el riesgo de manipulación de activos por terceros.

La segregación de funciones es un control interno que busca evitar que un mismo colaborador tenga control sobre dos o más proceso del SGSI sensibles e incompatibles. Es decir, según este principio, una misma persona no debería poder realizar dos tareas cuya combinación pudiera resultar en un riesgo potencial que afectase o pudiera significar un riesgo para la organización.

ITQ LATAM establece que los roles y responsabilidades sobre una función deben ser divididos de tal manera que un único colaborador no tenga acceso a los procesos del sistema de gestión de seguridad de la información de principio a fin. De esta manera el riesgo se ve reducido

## 6.8 Seguridad de la información para Servicios Cloud.

Las políticas de seguridad de la información para servicios Cloud en ITQ LATAM, están definidas como parte de esta política. Uno de los puntos más importantes es poder asegurar la información para servicios Cloud y para esto se debe solicitar al gerente de ingeniería que el asigne los accesos, ya que en él reside la responsabilidad de estos, siguiendo políticas de acceso ya establecidas. Los respaldos siguen siendo responsabilidad de ITQ LATAM, bajo los procedimientos y las políticas definidas por la organización, de lo contrario, existe el riesgo de que el proveedor de servicios en la nube se deba hacerse cargo de esta información y asumir en caso de pérdida de datos.

Se deberá siempre acordar con el proveedor del servicio en la nube, la asignación adecuada de roles y responsabilidades de seguridad de la información en Cloud.

El proveedor de servicios de la nube es responsable de la seguridad de la información establecida como parte del contrato de servicios en la nube.

La implementación y el aprovisionamiento de la seguridad de la información en la nube deben realizarse de acuerdo con las funciones y responsabilidades determinadas dentro de la organización del proveedor. Los datos y archivos en los sistemas del proveedor de servicios en la nube que se crean o modifican durante el uso del servicio en la nube pueden ser críticos para la operación segura, la recuperación y la continuidad del servicio.

ITQ LATAM como cliente del servicio en la nube debe identificar y gestionar su relación con la función de atención del proveedor.

## 6.9 Seguridad de la información para la protección de la información de identificación personal (PII) en la nuble Pública.

Las políticas de seguridad de la información para la protección de la información de identificación personal cualquier información que pueda usarse para establecer un vínculo entre la información y la persona física a la que se refiere dicha información, o pueda estar vinculada directa o indirectamente a una persona física.

El procesador de PII en la nube pública debe designar un punto de contacto para que lo utilice el cliente del servicio en la nube con respecto al procesamiento de la PII según el contrato.

Los acuerdos contractuales deben asignar claramente las responsabilidades entre el procesador de PII en la nube pública, sus subcontratistas y el cliente del servicio en la nube, teniendo en cuenta el tipo de servicio en la nube en cuestión (por ejemplo, un servicio de una categoría IaaS, PaaS o SaaS de la referencia de computación en la nube). Por ejemplo, la asignación de responsabilidad para los controles de la capa de aplicación puede diferir dependiendo de si el procesador de PII en la nube pública está proporcionando un servicio SaaS o más bien está proporcionando un servicio PaaS o IaaS en el que el cliente del servicio en la nube puede construir o superponer sus propias aplicaciones.

## 6.10 Notificación de divulgación de PII

El procesador de PII en la nube pública debe notificar a ITQ de acuerdo con cualquier procedimiento y períodos de tiempo acordados en el contrato de:

1. Rechazar cualquier solicitud de divulgación de PII que no sea legalmente vinculante;
2. Consultar con ITQ LATAM cuando sea legalmente permitido antes de realizar cualquier divulgación de PII
3. Aceptar cualquier solicitud de divulgación de PII acordada contractualmente que esté autorizada por ITQ LATAM.

## 6.11 Registro de divulgaciones de PII

Las divulgaciones de PII a terceros deben registrarse, incluida la PII que se ha divulgado, a quién y en qué momento.

La PII se puede revelar durante el curso de las operaciones normales. Estas divulgaciones deben registrarse. También debe registrarse cualquier divulgación adicional a terceros, como las que surjan de investigaciones legales o auditorías externas. Los registros deben incluir la fuente de la divulgación y la fuente de la autoridad para realizar la divulgación.

## 6.12 Ciberseguridad

ITQ LATAM considera que la ciberseguridad está orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos de la empresa, así como los activos que participan en los procesos.

La ciberseguridad tiene como objetivo garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, y cumplir con las Leyes y Reglamentaciones vigentes en cada

momento, manteniendo un equilibrio entre los niveles de riesgo y un uso eficiente de los recursos, con criterios de proporcionalidad, para ello se establece los siguientes principios básicos:

- Garantiza que los Sistemas de Información y Telecomunicaciones que dispone ITQ LATAM poseen el adecuado nivel de ciberseguridad y resiliencia.
- Sensibiliza a todos los colaboradores, acerca de los riesgos de ciberseguridad y garantiza que disponen de los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para sustentar los objetivos de ciberseguridad.
- Potencia las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a nuevas amenazas.
- Se dota de procedimientos y herramientas que permiten adaptarse con agilidad a las condiciones cambiantes del entorno tecnológico y las nuevas amenazas.

ITQ LTD se basa en un modelo de ciberseguridad que se define de la siguiente manera:

- Un marco para la gestión de las medidas de ciberseguridad aplicables mediante el establecimiento de una metodología de riesgos aprobada por la dirección en la que se fijen los objetivos y las metas de seguridad y ciberseguridad, así como los principios de la ciberseguridad alineados con la estrategia y los objetivos de negocio y coherente con el contexto dónde se desarrollan las actividades de la compañía.
- Mecanismos para reaccionar frente a los incidentes que se produzcan tanto en la gestión del sistema como en los procedimientos operativos que dependen del mismo.
- La existencia de un conjunto de funciones y responsabilidades en materia de ciberseguridad claramente definidas y asignadas en el organigrama corporativo.
- Un proceso de revisión y actualización continua del modelo de gestión de la ciberseguridad para adecuarlo en todo momento a las ciber amenazas que van surgiendo y puedan afectar a ITQ LATAM.

## 6.13 Sanciones

Las partes comparecientes acuerdan que cualquier infracción por parte del colaborador a las obligaciones que asumen en virtud del presente acuerdo de confidencialidad que se suministró con el contrato de cada colaborador, dará lugar a los derechos que concede la legislación chilena en caso de incumplimiento contractual. Toda infracción al presente acuerdo podrá ser sancionada en la siguiente forma:

a) Amonestación verbal

b) En caso de reincidencia, con amonestación escrita con copia a la hoja de vida y a la Inspección del Trabajo.

c) En caso de una segunda reincidencia, se castigará con la causal de termino de contrato de trabajo contenida en el N°7 del art. 160 del código del trabajo “incumplimiento grave a las obligaciones que impone el contrato”.

En el caso que el trabajador no respete a cabalidad la prohibición contenida en este acuerdo, será responsable de todos los perjuicios y daños que ocasionare al colaborador sin perjuicio de las responsabilidades legales de cualquier naturaleza, configurándose en materia laboral la causal de termino de contrato de trabajo contenida en el N°7 del art. 160 del código del trabajo “incumplimiento grave a las obligaciones que impone el contrato”.

## 6.14 Difusión de la Política de Seguridad de la Información

La presente política de seguridad de la información ha sido elaborada de acorde a los objetivos de la organización y los objetivos de seguridad de la información por la alta dirección y comité de seguridad de ITQ LATAM.

Las políticas y procedimientos de ITQ LATAM, así como cualquier modificación de estas, deberán ser aprobadas por las jerarquías pertinentes, definidos en los acuerdos del Comité de Seguridad de la Información. No así la política de la seguridad de la información que deberá ser revisada y aprobada por la alta dirección.

Todas las políticas de Seguridad de la Información deberán ser comunicadas a los colaboradores de ITQ LATAM de manera pertinente, accesible y comprensible, dejándose constancia de ello.

Los mecanismos de divulgación. El texto íntegro y actualizado de la presente política se pondrá y mantendrá a disposición de los colaboradores en la página web de la Empresa www.itqlatam.com, además se enviará un correo corporativo ITQ LATAM con los cambios y modificaciones relevantes.

## 6.15 Vigencia, Revisión y Retención

La Política de Seguridad de la Información y todo su contenido tendrán vigencia a contar de su fecha de aprobación y puesta en marcha, y tendrá duración indefinida en tanto la Gerencia General de ITQ LATAM no adopte otra resolución al respecto.

La presente política será evaluada y revisada, al menos una vez al año, cuando el oficial de Seguridad de la Información o el Comité de Seguridad de la Información lo requiera, para asegurar su continuidad e idoneidad, considerando cambios externos o internos que puedan afectarla.

La presente versión sustituye completamente a todas las precedentes, de manera que este sea el único documento válido de entre todos los de la serie. Lo anterior, una vez que sea aprobado por la alta directiva

Se realizará cada año la revisión de la documentación para verificar si requiere un control de cambio para que sea actualizada y la retención de toda la documentación de las normas 27001, 27017 y 27018 es de 2 años.

## 7. Anexos

No Aplica