SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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 del documento, se incorpora cláusula de Ciberseguridad
14/06/2024	06	Todas	Gerente General	Se realiza mejora a la estructura y se reubican puntos de las políticas en otros documentos del SGSI.

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 de la Información de ITQ LATAM, es responsabilidad de todo el personal, tanto interno como externo, incluyendo Empresas Filiales, Sucursales y Proveedores que haga uso de ésta y que participen en todas las actividades y servicios declarados en el alcance. Por tal razón, las políticas planteadas en este documento son de conocimiento y cumplimiento obligado para todo el personal involucrado.

4. Referencia Normativa

Norma ISO/IEC 27001. “Seguridad de la información, Ciberseguridad y protección de la intimidad- Sistema de Gestión de la Seguridad de la Información. Requisitos.

Norma ISO/IEC 27002. “Seguridad de la información, ciberseguridad y protección de la privacidad”. Control de la seguridad de la información.

Norma ISO/IEC 27701 Técnicas de seguridad — Extensión de ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información de privacidad — Requisitos y directrices

Norma ISO/IEC 27017 Técnicas de seguridad — Extensión de ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información de privacidad — Requisitos y directrices.

Norma ISO/IEC 27018 Técnicas de seguridad — Extensión de ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información de privacidad — Requisitos y directrices

Requisitos / Controles:

- Req. 5.2 Política.
- 5.1 Políticas para la seguridad de la información.
- 5.34 Privacidad y protección de datos de carácter personal (DCP).

Control ISO 2017:

- CLD.6.3.1 Roles y responsabilidades compartidos dentro de un entorno de computación en la nube

Control ISO 27018:

- A.2 Legitimidad y Especificación del propósito.
- A.5 Limitación de uso retención y Divulgación.
- A.9 Contabilidad.

5. Responsabilidades del Sistema de Gestión de Seguridad de la Información

- Definidas en el Procedimiento **PRO46_Procedimiento de Roles y Responsabilidades SGSI.**

6. Descripción de la Política

6.1. Objetivos de Seguridad de la Información.

- Definir el marco global para la gestión de la Seguridad de la Información en ITQ LATAM y sus empresas colaboradoras, estableciendo los lineamientos, para la protección y preservación de la confidencialidad, integridad y disponibilidad de la información de la organización y de sus clientes.

- Asegurar la privacidad y protección de la información basándonos en metodologías específicas de gestión en seguridad de la información, controles de seguridad para servicios Cloud y privacidad en la nube cuando aplique.

- Establecer metodología y gobierno de riesgos para gestión de procesos asociados a la seguridad de la información y privacidad de datos tanto en ITQ LATAM durante la prestación de los servicios y gestión de procesos operacionales para cumplirlos.

- Establecer estrategias de gestión para protección eficientemente los activos de información de la organización y los servicios involucrados, 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.

- Implementar gestión de los requisitos y condiciones generales de protección 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 y empresas con acuerdos de colaboración:

a) Cumplir con las políticas y normas de seguridad establecidas por ITQ LATAM en relación con la información y los flujos de comunicación.
b) Mantener la confidencialidad de toda la información de ITQ LATAM y protegerla adecuadamente. Esto incluye informes, datos, proyecciones, métodos, estrategias, configuraciones de software, diagramas de hardware y red, entre otros
c) Evitar exponer los registros y archivos electrónicos de manera innecesaria
d) Cumplir con todas las políticas que definen el uso aceptable de los activos, redes e información de ITQ LATAM.
e) Mantener los espacios destinados al almacenamiento de información, tanto físicos como electrónicos, en condiciones adecuadas.
f) Utilizar de manera apropiada los perfiles informáticos asignados por ITQ LATAM o clientes para los servicios correspondientes.
g) Participar en investigaciones relacionadas con delitos o faltas que se desarrollen en ITQ LATAM en relación con el uso de información y sistemas de información.
h) Participar activamente en la gestión de incidentes en los que esté involucrado o que presencie.

Está prohibido para el colaborador de ITQ, de todas sus empresas filiales, sucursales y proveedores que presten servicios dentro del alcance del SGSI que manejen información de uso interno, confidencial e información identificada como personal (IIP) lo siguiente:

i) Confidencialidad de la información: Es fundamental no divulgar ni entregar a personas ajenas a ITQ LATAM, ni reproducir en su presencia, ningún tipo de información que pueda afectar a la empresa en términos legales, técnicos, comerciales o de imagen, sin el consentimiento explícito y formal de ITQ LATAM.

j) Uso responsable de la información y recursos: Es importante actuar con diligencia en el uso de la información institucional, evitando cualquier acción negligente que pueda llevar a la inutilización o destrucción de los recursos computacionales y de información de la empresa.

k) Acceso y uso autorizado de los recursos electrónicos: Se debe evitar el acceso o uso no autorizado de canales electrónicos, datos sensibles, equipos computacionales, informes y otros documentos. Esto implica no hacer uso indebido de claves y contraseñas, respetando las políticas y normativas establecidas por ITQ LATAM.

Estas directrices son esenciales para garantizar la seguridad de la información y proteger los activos de ITQ LATAM. Al cumplir con estas políticas, contribuimos a mantener la integridad y confidencialidad de los datos, así como a salvaguardar la reputación y el éxito de la empresa.

6.3. 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 POL18-Política de Privacidad y Protección de Datos que indica como la organización se preocupa de la privacidad y protección de información de identificación personal. Esta política se encuentra publicada para el conocimiento de los stakeholders internos y externos de la organización y es 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 de forma anual o ante un cambio significativo dentro de la organización o en los esquemas regulatorios, legales o contractuales que impacten los procesos que, estas modificaciones serán aprobadas con la revisión de la alta dirección.

6.4. Ciberseguridad

ITQ LATAM, sus empresas colaboradoras, sus empresas filiales, sucursales y proveedores que presten servicios dentro del alcance del SGSI, asumen el compromiso de 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 tecnologías y metodologías para la aplicación de esta para definir estrategias para 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 LATAM 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.

6.5. Implicancias de no cumplimiento.

Se definen desde esta política la obligación por parte de los colaboradores de ITQ, de todas sus empresas filiales, empresas colaboradoras, sucursales y proveedores que presten servicios dentro del alcance del SGSI y en virtud de los acuerdos trazados de forma legal o contractual.

Toda infracción al Sistema de Gestión de Seguridad de la información y/o a sus políticas estarán sujetas a las siguientes acciones:

a) Procesos de llamados de atención de acuerdo con lo establecido en el Reglamento interno y/o acuerdo de colaboración

b) Análisis de causa raíz y planes de acción y medición de eficacia de estas acciones.

c) Toma de decisiones importantes enmarcadas en los acuerdos contractuales o de servicios establecidos.

6.6. Difusión de la Política de Seguridad de la Información

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, proveedores críticos y empresas colaboradoras 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 las principales stakeholders en la página web de la Empresa www.itqlatam.com, además se enviará un correo corporativo ITQ LATAM con los cambios y modificaciones relevantes.

6.7. 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.

6.8. Anexos

No Aplica

Nestor Straube E