iOutsourcing | Transformamos Experiencias

Política general de seguridad de la información ITL001 V9

TABLA DE CONTENIDO

1. OJETIVO

Establecer una política de seguridad de la información basada en el estándar ISO/IEC 27001:2013

2. ALCANCE

Todas las partes interesadas de **OUTSOURCING S.A.S. BIC.**

3. RESPONSABLES

Todas las partes interesadas de **OUTSOURCING S.A.S. BIC.**

4. DEFINICIONES Y SIGLAS

No aplica

5. DESARROLLO DE LA POLÍTICA

5.1 Política

OUTSOURCING S.A.S. BIC en su empeño por generar mayor ventaja competitiva a sus clientes con factores de diferenciación, establece este Sistema de Gestión de la Seguridad de la Información basado en ISO 27001:2013 para ofrecer a los clientes internos y externos servicios de Contact Center y BPO niveles de seguridad de información adecuados, que les garanticen la protección de los datos confiados a OUTSOURCING SAS BIC

Esta política es general y aplica para todas nuestras sedes.

Teniendo en cuenta que la información es un activo muy importante para el negocio; OUTSOURCING SAS BIC se compromete a identificar y proteger los activos de información adecuadamente, incluyendo los datos

personales y financieros de nuestros clientes, cumpliendo con los lineamientos no sólo de ISO 27001, también otros requerimientos que sean exigidos para la industria BPO; manteniendo las mejores prácticas y empleando procedimientos, estructuras organizacionales y sistemas de información que cumplan ese objetivo.

Por la naturaleza del negocio de OUTSOURCING SAS BIC, en donde se manejan simultáneamente clientes del mismo sector de la economía y clientes que depositan su información crítica en nuestras manos, es un compromiso ineludible garantizar que esa información sea salvaguardada cumpliendo los requisitos de seguridad.

El marco de gestión de riesgos proporciona el contexto adecuado para identificar, evaluar y controlar los riesgos relacionados con la información mediante el mantenimiento del SGSI. La evaluación de riesgos, la declaración de aplicabilidad y el plan de tratamiento del riesgo, definirán cómo controlar los escenarios de riesgo de seguridad de la información. La Gerencia de Tecnología asume el liderazgo en la gestión y mantenimiento del plan de tratamiento del riesgo y mediante actividades de evaluación de riesgo se hará monitoreo a la efectividad de los controles implementados, así como de la aceptación del riesgo residual.

Dentro de la implementación del SGSI se encontrarán aspectos como la continuidad del negocio, gestión de incidentes y los procedimientos establecidos para el análisis del riesgo y su tratamiento.

El Sistema de Gestión de Seguridad de la información (SGSI), busca el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información de la organización y de sus clientes, entendiéndose estos como:

a) Confidencialidad: Asegurar que la información es accesible solo a aquellos autorizados a tener acceso.

b) Integridad: Salvaguardar la exactitud e integridad de la información y de los métodos de procesamiento.

c) Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información y activos asociados cuando lo requieran.

La Presidencia de OUTSOURCING SAS BIC se compromete a dar todo su apoyo en cuanto a los recursos necesarios para el diseño, la implantación, certificación, mantenimiento o mejora continua del Sistema de Gestión de la Seguridad de la Información, y en cuanto al compromiso de motivar todas las Gerencias de la compañía para que se involucren en las actividades que sean necesarias para sacarlo adelante.

A través del comité del SGSI, se revisará el contenido del documento del SGSI para confirmar la vigencia o actualización y de esta manera realizar todo el ciclo de mejora continua establecido en este Sistema. Esta política se revisará para responder ante cambios y modificaciones derivados del análisis de riesgos, de nuevos negocios o del plan de tratamiento de riesgos y, en cualquier caso, al menos una vez al año.

La Política del SGSI estará disponible para todos los miembros de la organización en la Intranet corporativa, no contiene información confidencial y es de etiquetado público, por lo que puede ser mostrada a los terceros colaboradores, clientes y proveedores cuando sea necesario.

En la inducción corporativa se deberá definir un espacio para que los nuevos funcionarios queden informados, concienciados y sensibilizados sobre esta política;

de igual manera esta se debe dar a conocer a los clientes, proveedores y terceros de OUTSOURCING SAS BIC, el incumplimiento de las obligaciones incluidas en la política tendrá las consecuencias disciplinarias a las que hubiere lugar.

En resumen, la política de seguridad de la información de Outsourcing S.AS. BIC es el compromiso de proteger los datos de sus partes interesadas: clientes, accionistas, colaboradores, proveedores, gobierno.

5.2 Alcance SGSI

Outsourcing SAS BIC basa su alcance del sistema de gestión de la seguridad de la información (SGSI) en los tres procesos estratégicos de la cadena de valor (comercial, implementación y operaciones) usados en la prestación de servicios de centro de contacto y tercerización de procesos de negocio, así como sus procesos de apoyo: tecnología, gestión del talento humano, gestión administrativa y desarrollo de software.

Para dar cumplimiento a los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) se debe prestar especial atención a los siguientes aspectos del entorno en el que se mueve la organización:

Nivel Interno:

-Llegada de nuevos clientes a la organización.
-Ajustes en la cultura corporativa.
-Cambios en la estructura organizativa.
-Adquisición de nuevos activos de información.
-Problemas económicos de la compañía.

Nivel Externo:

- Normatividad del sector de las telecomunicaciones a nivel nacional e internacional cuando se tengan clientes que tengan su operación fuera del país.
- Leyes que promulgue el Gobierno Nacional frente a la operación de los Centros de Contacto y la tercerización de servicios.
- Situación política, social y económica del país.
- Situación financiera y organizativa de los clientes de la organización.
- Situación financiera y organizativa de los proveedores de la organización.

Exclusiones:

- No aplican para la organización los controles a 10.1.2, A14.2.7 y A18.1.5

5.3 Objetivos SGSI

- Establecer mecanismos de seguimiento y medición, análisis y evaluación del sistema de gestión para garantizar su conformidad y eficacia.

- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables para la organización.

- Sensibilizar a todos los funcionarios en las mejores prácticas de seguridad de la información.

- Gestionar y mantener la continuidad de negocio en la organización.

- Gestionar los incidentes de seguridad de la información que surjan en la organización.

6. DOCUMENTOS DE REFERENCIA

Norma ISO/IEC 27001:2013

7. CONTROL DE VERSIONES

Versión	Descripción de los cambios	Elaboró (Nombre - Cargo -Fecha)	Revisó (Nombre - Cargo -Fecha)	Aprobó (Nombre - Cargo -Fecha)
9	Se migra la política a la nueva plantilla documental y se actualiza para los requisitos de la Norma ISO/IEC 27001:2013	**Yulian Colmenares** Oficial de Seguridad de la Información 15/Ene/2023	**Yulian Colmenares** Oficial de Seguridad de la Información 15/Ene/2023	**Jairo López** Gerente de Tecnología 15/Ene/2023

iOutsourcing | Transformamos Experiencias

Política general de seguridad de la información ITL001 V9

Outsourcing

IT-L-001

www.outsourcing.com.co

Outsourcing S.A.S. BIC · Enero 2023

Para cualquier duda, por favor contactarse con el departamento de Mercadeo.