MANUAL DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
DEM 02 V8

12-Feb-2021

Documento Publico

ELABORADO POR	REVISADO POR	APROBADO POR
Yulian Colmenares	Jairo López	Jairo López
Oficial de Seguridad de la Información	Gerente deTecnología	Gerente de Tecnología

1. POLÍTICA SGSI

OUTSOURCING S.A. 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 la norma ISO/IEC 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 S.A.

Esta política es general y aplica todas nuestras sedes: Calle 128, Caracas, Calle 22, Tres Elefantes, Cali, Pereira.

Teniendo en cuenta que la información es un activo muy importante para el negocio; OUTSOURCING S.A 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, sino también PCI DSS y 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 S.A., 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.

En el Manual del SGSI se encontrará, 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 S.A. 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 su uso es interno, por lo que puede ser mostrada a los terceros colaboradores, clientes, socios, gobierno 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 S.A., el incumplimiento de las obligaciones incluidas en la política tendrá las consecuencias disciplinarias a las que hubiere lugar.

2. ALCANCE SGSI

Outsourcing S.A., basa su actuar en tres (3) grandes procesos estratégicos en la cadena de valor (Comercial, Implementación y Operaciones) que relacionados entre sí, con actores (externos e internos), comparten información de carácter vital necesarios para apoyar la gestión y permanencia del negocio.

En este orden de ideas, el alcance del Sistema de Gestión de la Seguridad de la Información (SGSI) de Outsourcing S.A., se basa 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, Desarrollo de software y Compras de tecnología, en las diferentes sedes a nivel nacional.

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 nuestra organización el anexo A10 y los controles A14.2.7 y A18.1.5

3. OBJETIVOS SGSI

- Mantener la Confidencialidad, Integridad y Disponibilidad de la información que interviene en los diferentes procesos del negocio; así como de los sistemas que la soportan, aumentando la confianza de nuestros clientes y otras partes interesadas.

- Cumplir los requisitos legales, reglamentarios y contractuales que apliquen para cada uno de los proyectos institucionales.

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

- Garantizar el tratamiento de riesgos con el objeto de proteger los activos de información de la compañía y velar por la disponibilidad del servicio y la continuidad del negocio.

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

- Desarrollar, implantar y mantener actualizado un Plan de Continuidad del Negocio acorde a las necesidades de la empresa y que garantice la continuidad de los principios de seguridad de la información.

- Garantizar condiciones de servicio en las cuales la operatividad e información de los diferentes clientes cumpla con los requisitos de confidencialidad, integridad y disponibilidad

- Implementar, operar, medir y revisar de manera periódica los controles establecidos en la declaración de aplicabilidad.

4. POLÍTICAS

- ITL01 Política de Uso Aceptable de los Activos
- ITL02 Política de uso de los servicios de red
- ITL03 Política retiro de Activos
- ITL04 Política de Derechos de Propiedad Intelectual
- ITL05 Política de Escritorio Limpio y Pantalla Segura
- ITL06 Política de Uso del Data Center
- ITL07 Política de Acceso Remoto por VPN
- ITL08 Política Control de Acceso
- ITL09 Política de Reporte Oportuno de Eventos y Debilidades de la Seguridad de la Información
- ITL10 Política de backup
- ITL11 Objetivos y necesidades de seguridad de la información
- ITL12 Restricciones relevantes regulatorias actualizada
- ITL13 Política uso de transporte
- ITL14 Política Red Inalámbrica
- ITL15 Política de utilización de controles criptográficos
- ITL16 Aviso de Privacidad
- ITL17 Política y procedimientos de protección de datos personales
- ITL18 Política Gestión de Incidentes de Seguridad de la Información
- ITL19 Funciones y responsabilidades frente al SGSI
- ITL21 Política de teletrabajo
- ITL22 Política de transferencia de información
- ITL23 Política de Desarrollo Seguro
- ITL24 Política de uso de dispositivos móviles

5. PROCEDIMIENTOS

- ITP01 Procedimiento de mantenimiento
- ITP02 Procedimiento de Gestión de Incidentes y Soporte Servicios de TI
- ITP03 Procedimiento de Control de Cambios
- ITP04 Procedimiento de clasificación, etiquetado, manejo y almacenamiento de Información
- ITP05 Procedimiento de Reporte y Manejo de Incidentes de Seguridad de la Información
- ITP06 Procedimiento control de inventarios
- ITP07 Procedimiento Gestión de Riesgos y Oportunidades
- ITP09 Procedimiento Plan de Gestión de Continuidad del Negocio
- ITP11 Procedimiento de Revision del SGSI
- ITP13 V1 Procedimiento de Acuerdo Nivel de Servicio
- ITP14 Auditoria de Sistemas de información
- ITP16 Procedimiento de Desarrollo
- ITP18 Procedimiento Preventa
- ITP19 Procedimiento Gestión de Requerimientos
- ITP20 Procedimiento de Borrado Seguro de Equipos
- ITP21 Procedimiento de Servicios Profesionales
- ITP22 v1 Entrega y recepción de equipos WaH
- ITP28 Procedimiento para la instalación de software
- ITP29 Procedimiento para la gestión de medios removibles

6. INSTRUCTIVOS

- ITI02 Instructivo Consulta PCSistel
- ITI03 Instructivo Uso del CCTV Caracas
- ITI04 Instructivo Escalamiento de Casos en IT
- ITI06 Instructivo Control de Seguimiento y de Medición

- ITI08 Instructivo Manejo y Control del Aire Acondicionado para el Datacenter
- ITI09 Instructivo Manual de Configuración VPN
- ITI10 Guía para el Manejo de Incidentes de Seguridad de la Información
- ITI11 Guía para el aseguramiento de la Planta Física
- ITI13 Instructivo de Administración De Usuarios
- ITI15 v2 Proceso Acceso Remoto Laboratorios Heel
- ITI16 Descripción de roles y responsabilidades para implementar el SGSI
- ITI17 Intercambio de información a través de los límites
- ITI18 Alcance y límites desde la perspectiva de las TIC
- ITI20 Instructivo Aplicativo Mesa de Servicio
- ITI21 Instructivo Administración De Equipos
- ITI22 Instructivo Encendido Manual Planta Eléctrica
- ITI23 Instructivo de uso correo Zimbra
- ITI25 Instructivo llamadas no esperadas
- ITI27 Procedimiento Identificación y Actualización de Activos de Información
- ITI28 Procedimiento de custodia externa de medios
- ITI29 Manual de Service Observing
- ITI31 v1 ANS Alistamiento de equipos

7. FORMATOS

- ITF01 Plan de mantenimiento preventivo
- ITF02 Seguimiento de mantenimiento Preventivo
- ITF03 Examen SGSI
- ITF04 Cheklist de Centro de Datos
- ITF05 Relación Entrada Centro de Cómputo
- ITF06 Check list voz
- ITF07 Acta de Entrega Clave de llamadas
- ITF10 Entrega de elementos tecnológicos
- ITF11 Formato Acta de borrado seguro
- ITF13 Cheklist de Servidores
- ITF15 Informe Auditoria
- ITF16 Cheklist de Equipos
- ITF17 Cheklist de Bases de Datos
- ITF18 Diagrama ER - base de datos
- ITF19 Levantamiento de Requerimiento
- ITF20 Formato Pruebas
- ITF21 Acta de entrega
- ITF22 Documento conceptual especificación del requerimiento
- ITF27 Control Temperatura y Humedad
- ITF46 Formato de Pruebas a Puesto de Trabajo
- ITF48 Formato Informe De Incidentes de TI
- ITF49 Check List Equipo Nuevo-Reasignado-Formateado
- ITF50 Formato de Dimensionamiento de Recursos Tecnológicos
- ITF52 Formato Catalogo de Servicio de TI
- ITF53 Formato de solicitud de campaña outbound
- ITF54 Acta de Entrega Clave Aplicativo ACR-CSR
- ITF55 v1 Cheklist Alistamiento de Equipos WaH