Política Corporativa de Seguridad de la Información

(PL-SI-03) v14 202209
Documento interno

1. Objetivo

Establecer el liderazgo y compromiso de la Alta Dirección frente al Sistema de Gestión de Seguridad de la Información – SGSI de CONTENTO BPS S.A, mediante el establecimiento de la Política Corporativa de Seguridad de la Información, con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información de la organización.

2. Alcance

La presente política aplica a todos los empleados, aliados y partes interesadas (internas y externas), que gestionan datos o hacen uso de los activos de información de CONTENTO BPS S.A.

3. Definiciones

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. [Fuente: ISO 27000]

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. [Fuente: ISO 27000]

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [Fuente: ISO 27000]

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. [Fuente: ISO 27000]

Gestión de Riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. [Fuente: ISO Guía 73:2009].

Impacto: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-. [Fuente: ISO 27000]

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [Fuente: ISO 27000]

Integridad: Propiedad de la información relativa a su exactitud y completitud. [Fuente: ISO 27000]

Parte Interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. [Fuente: ISO 27000]

Plan de Continuidad del Negocio: Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro. [Fuente: ISO 27000]

Riesgo: Efecto de la incertidumbre sobre los objetivos. El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización. [Fuente: ISO 27000]

Seguridad de la Información: Preservar la confidencialidad, integridad y disponibilidad de la información. [Fuente: ISO 27000]

Sistema de Gestión de la Seguridad de la Información - SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua. [Fuente: ISO 27000]

4. Propósito

Definir una directriz de alto nivel, que enmarque las pautas relacionadas con el establecimiento, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI para CONTENTO BPS S.A; y que, a su vez, sirva como un marco de referencia para el uso adecuado de los activos de información y la gestión de riesgos que se deriven de la utilización los mismos.

5. Marco de referencia

Esta Política está sustentada en lo establecido en el Normograma del SGSI; el cual recopila todos aquellos elementos normativos (requisitos legales, reglamentarios, contractuales y técnicos) que soportan el Sistema de Gestión de Seguridad de la Información de la compañía.

6. Compromiso de la Dirección

La Alta Dirección de Contento BPS S.A. está comprometida con el desarrollo y la implementación del Sistema de Gestión de Seguridad de la Información, así como el mantenimiento y mejora continua del mismo.

Como muestra de este compromiso ha autorizado el diseño e implementación del SGSI basado en la norma ISO 27001:2013, y aprueba la presente Política.

7. Importancia de la Seguridad de la Información

La Seguridad de la Información permite la protección de los activos de información mediante la gestión de riesgos y la adopción de una cultura de seguridad; lo que contribuye a la continuidad del negocio, la minimización de la probabilidad de ocurrencia de un riesgo

o sus impactos adversos y la maximización del retorno de inversiones y mayores oportunidades de negocio.

La seguridad de la información se enfoca en la preservación de las siguientes características:

- **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, cada vez que lo requieran.

Entendiendo que la información puede existir en diversas formas (física y digital) y puede estar contenida o trasmitirse por cualquier medio (papel, USB, computador, Tablet, correo electrónico, video, dispositivo móvil, conversación, entre otros), independientemente de lo que sea su forma o medio por el cual se comparte, procesa o almacena, siempre debe tener la protección adecuada.

8. Marco sancionatorio

El incumplimiento de la presente Política, dará lugar a la aplicación de las medidas disciplinarias o legales vigentes en la organización, con la intervención del área Jurídica, Gestión del Talento Organizacional y/o la Alta Dirección; de acuerdo con los procedimientos internos, el impacto que esto tenga para la empresa y demás lineamientos aplicables a la compañía.

9. Factores críticos de éxito

- Falta de capacitación a los colaboradores.
- Ausencia de planes de sensibilización a todas las partes interesadas identificadas.
- Falta de apoyo, liderazgo y compromiso por parte de la Alta Dirección.
- Incumplimiento de la presente política por desconocimiento.

10. Declaración de la Política de seguridad de la información

CONTENTO BPS consiente de la importancia de la seguridad de la información y la protección de sus activos para el cumplimiento de su misión, visión y propósitos corporativos, ha adquirido el compromiso de proteger la integridad, disponibilidad y confidencialidad de la información mediante el establecimiento, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información – SGSI, a través de la gestión de activos, incidentes y riesgos de seguridad de la información.

CONTENTO BPS se compromete a dar cumplimiento de los requisitos legales aplicables, además de promover una estrategia de seguridad de la información basada en las mejores

prácticas y adopción de los controles descritos en la norma ISO 27001:2013. De igual forma, establece las medidas requeridas para la formación de su personal y la toma de conciencia en todas las partes interesadas frente a la seguridad de la información.

La implementación de nuevos proyectos debe contar con actividades de Planeación que incluyan la Seguridad de la Información en todos sus componentes. Para el inicio de cualquier proyecto independientemente cual sea este, deberá contar con el aval del Líder de Seguridad de la Información como encargado de establecer y validar los controles aplicables para el proyecto.

Seguridad de la Información e informática será parte integral de cada etapa de los proyectos de la compañía, desde su concepción hasta su puesta en producción, evaluando y avalando los requerimientos de cada uno de estos, asegurando la participación en su Planificación, Ofertas, configuración, Pruebas y en propuestas de tercerización de proyectos.

Como parte de las actividades del proceso de Seguridad de la Información, CONTENTO BPS S.A. establece, implanta y mantiene actualizado un Plan de Continuidad de Negocio acorde a las necesidades de la Compañía y a los riesgos que puedan afectar el desempeño, respuesta u operación de la compañía frente a eventos que interrumpan el normal desarrollo de los servicios prestados.

11. Objetivos de Seguridad de la Información

- Garantizar la confidencialidad, integridad y disponibilidad de los activos de información, mediante la gestión de los riesgos de Seguridad de la Información, continuidad del negocio y datos personales.

- Promover la cultura de Seguridad de la Información en los empleados, aliados y demás personas vinculadas a la empresa, a través del diseño e implementación de programas de capacitación y sensibilización.

- Gestionar los incidentes de seguridad de la información y ciberseguridad, adoptando procedimientos claros para el registro, documentación, seguimiento, trazabilidad, respuesta y aplicación de las lecciones aprendidas, con el fin de reducir la probabilidad o el impacto de incidentes futuros

- Asegurar el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información - SGSI mediante la implementación de acciones correctivas y de mejora, derivadas de las revisiones al Sistema de Gestión de Seguridad de la Información.

- Gestionar los activos de información, mediante la adopción de procedimientos y herramientas que permitan identificar la criticidad de los mismos, el propietario y los riesgos que podrían surgir por el uso e importancia de los mismos para los procesos o la organización.

- Proveer los recursos financieros, humanos y de infraestructura, requeridos para mantener el Sistema de Gestión de Seguridad de la Información - SGSI.

12. Comunicación

La presente política se dará a conocer a todas las partes interesadas identificadas en el contexto organizacional, por los medios que disponga la compañía, y estará disponible como información.

13. Revisión, actualización y seguimiento

La Política de Seguridad de la Información será revisada anualmente o actualizarse en el momento en que existan modificaciones en el propósito, misión, visión, objetivos estratégicos o el contexto de la compañía; en el alcance del Sistema de Gestión de Seguridad de la Información - SGSI o cuando existan cambios legales, estatutarios o reglamentarios.

Se deberá hacer seguimiento periódico al cumplimiento de las disposiciones aquí contenidas, por lo menos una vez al año.

14. Cumplimiento

Todos los empleados, aliados, terceros y demás partes interesadas identificadas, deberán dar cumplimiento al 100% de la política.

Dado en la ciudad de Medellín a los 13 días del mes de septiembre de 2022 se aprueba por el Representante Legal.

DAVID RODRÍGUEZ
Representante Legal

DORALBA SIERRA
Líder de Seguridad de la Información

APROBACION Y OFICIALIZACION

FASES	CARGO RESPONSABLE	NOMBRE	MEDIO POR EL CUAL SE APROBÓ
Elaboración	Líder de Seguridad de la Información	Doralba Sierra	Correo electrónico
Revisión			
Aprobación	Representante Legal	David Rodriguez	

MODIFICACIONES /ACTUALIZACIONES

VERSIÓN	FECHA (año- mes)	DESCRIPCIÓN RESUMIDA DE LA MODIFICACIÓN / ACTUALIZACIÓN / ANULACIÓN
00	2011-05	Creación
01	2013-05	Actualización de Políticas por revisión anual
02	2015-03	Actualización de Políticas por revisión anual
03	2016-04	Actualización de Políticas por revisión anual
04	2016-12	Actualización de imagen corporativa
05	2018-01	Actualización de contenido
06	2018-09	Actualización de contenido
07	2018-12	Actualización de contenido

08	2019-04	Actualización de contenido
09	2019-05	Actualización de contenido
10	2020-09	Inclusión de disposiciones en cuanto a; Trabajo en casa, Teletrabajo, inclusión de Seguridad de la Información en todas las etapas de los proyectos emprendidos, y prohibiciones de uso de dispositivos personales para temas Corporativos
11	2021-09	Actualización de contenido
12	2022-02	Actualización de contenido
13	2022-04	Estructura del documento y actualización de contenido
14	2022-09	Actualización de contenido