Política Corporativa de Seguridad de la Información

(PL-SI-03) v16 202306
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/IEC 27000:2012].

Amenaza: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. [Fuente: Manual Metodología de Riesgos: Función Pública:2022].

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [Fuente: ISO/IEC 27000:2018].

Disponibilidad: Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada. [Fuente: ISO/IEC 27000:2018].

Gestión de Riesgos: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. [Fuente: Manual Metodología de Riesgos: Función Pública:2022].

Impacto: Las consecuencias que puede ocasionar a la organización la materialización del riesgo. [Fuente: Manual Metodología de Riesgos: Función Pública:2022].

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/IEC 27000:2018].

Integridad: Propiedad de la exactitud y la integridad. [Fuente: ISO/IEC 27000:2018].

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/IEC 27000:2018].

Plan de Continuidad del Negocio: Información documentada que guía a una organización para responder a una interrupción y reanudar, recuperar y restaurar la entrega de productos y servicios según sus objetivos de continuidad del negocio. [FUENTE: ISO 22300: 2018].

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. [Fuente: Manual Metodología de Riesgos: Función Pública:2022].
Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Seguridad de la Información: Preservar la confidencialidad, integridad y disponibilidad de la información. [Fuente: ISO/IEC 27000:2018].

Sistema de Gestión de la Seguridad de la Información - SGSI: parte del sistema de gestión general, basado en un enfoque de riesgo empresarial, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
Nota: El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos. [Fuente: ISO/IEC 27000:2012].

Sistema de Información: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información. [Fuente: ISO/IEC 27000:2018].

Sistema de Gestión: Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas y objetivos y procesos para alcanzar esos objetivos. [Fuente: ISO/IEC 27000:2018].

4. PROPÓSITO

Definir una directriz de alto nivel, que enmarque las pautas relacionadas con el diseño, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI para CONTENTO BPS, 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 la Norma ISO/IEC 27001:2013 Sistema de Gestión de Seguridad de la Información, en el requisito 5.2 POLÍTICA, la cual debe ser adecuado al propósito de la compañía, objetivos estratégicos e incluir el compromiso de la alta dirección frente a su cumplimiento y mejora continua.

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 aprobado la presente política.

7. IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

La implementación del SGSI permite la protección de los activos de información de la compañía y sus partes interesadas, mediante la gestión de riesgos y la adopción de una cultura de seguridad, garantizando la continuidad del negocio, la disminución de materialización de riesgos e incidentes y la optimización del retorno de inversiones y mayores oportunidades de negocio.

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

- **Confidencialidad**: Garantizar que la información sea accesible sólo a aquellas personas autorizadas dado su rol y privilegios asociados.

- **Integridad**: salvaguardar la exactitud y completitud de la información y los métodos de procesamiento.

- **Disponibilidad**: Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la esta, siempre 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, correo electrónico, video, dispositivos móviles, conversación, entre otros), independientemente de esto, siempre debe contar con los controles necesarios para su adecuada protección de acuerdo con su clasificación.

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 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

- Falencias en los planes de sensibilización a todas las partes interesadas identificadas.
- Falta de apoyo, liderazgo o 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 objetivos estratégicos, ha adquirido el compromiso de proteger la integridad, disponibilidad y confidencialidad de la información mediante el diseño, implementación, 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 de todas las partes interesadas frente al SGSI.

La implementación de nuevos proyectos que puedan representar riesgos de seguridad de la información debe contar con actividades de planeación, seguimiento y cierre que incluyan la seguridad de la información durante todo su ciclo de vida. Adicionalmente, como parte de las actividades del proceso de Seguridad de la Información, está el de garantizar el acompañamiento en el diseño, implementación, ejecución de pruebas y actualización del 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 Contento BPS frente a eventos que puedan interrumpir el normal desarrollo de los servicios prestados.

A continuación, se relacionan controles aplicables para todos los integrantes de la compañía.

1. Portar el Carné siempre que vaya a ingresar al edificio, en un lugar visible, que lo identifique como empleado de Contento BPS S.A., en caso de ser colaborador de alianzas, mostrar su respectivo carné de la empresa para la cual labora y respetar el debido proceso de registro en la recepción.

2. Antes de ingresar a su área de trabajo correspondiente, debe de guardar sus pertenencias en el locker asignado, en caso de no tener locker, debe reportarlo con su Jefe inmediato para que éste, lo manifieste ante la Líder de seguridad física y se le asigne uno. En caso de que se utilice un locker sin haberse notificado y autorizado, se procederá a romper el candado y al correspondiente desalojo, estos artículos que sean desalojados se deben reclamar al Líder de Seguridad física.

3. No se permite el ingreso de dispositivos móviles y de almacenamiento a la operación a todo el personal, con excepción de Gerentes y Ejecutivos de cuenta y personal autorizado por el Área de Seguridad de la Información, de igual forma se ratifica que las acciones dentro de la operación para temas personales con líneas no corporativas no serán permitidas, para los casos donde sea necesario chat web o algún tipo de herramienta de comunicación se deben gestionar una licencia corporativa.

Estos dispositivos incluyen

- Celulares
- Tablet
- Computadores
- Cámaras fotográficas
- USB
- Discos extraíbles

Al igual que el ingreso y uso de

- Cuadernos
- Revistas
- Hojas
- Apuntes físicos
- Lápices, lapiceros, marcadores
- Objetos cortopunzantes.

Para el personal de las Áreas de Apoyo (Compras, Gestión del Talento Organizacional, Gestión Documental, Gestión Financiera, Gestión Jurídica, Mantenimiento, Seguridad de la Información, Tecnología y Comunicaciones, BI, Formación, Unidad de Valoración de Experiencias, Calidad y demás administrativos), se autoriza el uso del celular siempre y cuando no intervenga por ningún motivo en los ambientes de Operación.

4. Guardar absoluta reserva de la información que se gestiona en la compañía en concordancia al acuerdo de confidencialidad que se firma cuando se ingresa a la organización

5. Garantizar que sus contraseñas no sean conocidos por nadie, estas son personales e intransferibles

6. Solo el personal de Tecnología y comunicaciones está autorizado para cambiar configuraciones a los PC asignados y/o movilizarlos (Pc, mouse, teclado, diademas) en sitios internos o externos dependiendo de las directrices recibidas. Los daños físicos malintencionados a estos componentes será incumplimiento a la política de dispositivos móviles y conexión remota.

7. No está permitido a ningún proceso comprometer la integridad de la información por medio de programas, solicitudes de edición de audios, o cualquier otra actividad que modifique, altere, adicione o suprima toda o parte de los datos, contenidos en CDR, grabaciones, reportes, indicadores, bases de datos o cualquier tipo de documentación de propiedad de la empresa o terceras partes.

8. Todo visitante debe registrarse en la recepción, si llega en vehículo, debe parquear en el sitio asignado y desplazarse a la recepción para realizar dicho registro y si llega con acompañantes, los mismos deben de bajar del vehículo en la portería para registrarse.

9. El personal externo a la compañía debe de ser acompañado por un empleado durante todo el tiempo que permanezca en las instalaciones.

10. Todo el personal debe informar a su jefe inmediato y éste al Líder de Seguridad de la Información, los eventos o incidentes detectados y que impliquen riesgo de incumplimiento a las normas de Seguridad de la Información.

11. No está permitido el ingreso a otras áreas diferentes a las estipuladas en el contrato con la compañía, únicamente tendrán el acceso configurado por la Líder de Seguridad Física.

12. No está permitido el ingreso de alimentos y bebidas a las estaciones de trabajo ya que pueden poner en riesgo los equipos y causar daño o deterioro. Únicamente se permite el ingreso de un termo con tapa segura y debe ser ubicado en un lugar retirado del equipo.

13. No se deben dejar documentos físicos en las impresoras o escáner; además no se pueden dejar archivos digitales en los computadores ni servidores con acceso público después de imprimir o escanear alguna información.

11. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Garantizar la integridad, confidencialidad y disponibilidad de la información, mediante la adecuada gestión de los activos de información propios y de las partes interesadas internas y externas, estableciendo una metodología de clasificación, etiquetado, transferencia, almacenamiento y uso, que permita minimizar el riesgo existente frente a estos.

- Minimizar la materialización de riesgos de seguridad de la información, continuidad del negocio y privacidad y protección de datos personales, mediante su gestión adecuada y oportuna, tomando como marco de referencia la norma ISO 31000 y 27005.
- Mejorar continuamente la conveniencia, adecuación y eficacia del Sistema de Gestión de Seguridad de la Información de Contento BPS, mediante la implementación de acciones correctivas eficaces, auditorías internas y externas objetivas, participación de las partes interesadas internas y externas y revisiones a intervalos planificados del proceso de seguridad de la información.

- Capacitar y sensibilizar a los integrantes, aliados, proveedores y demás personas vinculadas a la compañía, logrando la apropiación de una cultura de seguridad de información, reflejada en el nivel de cumplimiento de políticas, procedimientos y resultados de las evaluaciones del conocimiento adquirido en los ejercicios de formación.

- Gestionar de manera oportuna los incidentes, eventos y vulnerabilidades de seguridad de la información, adoptando procedimientos claros para el reporte, atención, tratamiento, seguimiento y aplicación de las lecciones aprendidas, con el fin de reducir la probabilidad e impacto de incidentes futuros.

- Disponer de los recursos financieros, humanos y de infraestructura necesarios para mantener el adecuado desempeño del Sistema de Gestión de Seguridad de la Información de Contento BPS, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información propia y de sus partes interesadas internas y externas.

12. COMUNICACIÓN

La Política Corporativa de Seguridad de Información se dará a conocer a todas las partes interesadas identificadas en el contexto organizacional, por medio de los canales dispuestos por la compañía y definidos en el procedimiento de comunicación interna y externa. La presente política estará disponible como información documentada.

13. REVISIÓN, ACTUALIZACIÓN Y SEGUIMIENTO

Esta política 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 integrantes, aliados, proveedores y demás partes interesadas, deberán dar cumplimiento al 100% de la política.

Dado en la ciudad de Medellín a los 30 días del mes de junio del 2023 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	Coordinadora de Seguridad de la Información	Doralba Sierra	Correo electrónico
Revisión			
Aprobación	Representante Legal	David Rodríguez	

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
15	2023-05	Actualización de objetivos, definiciones y redacción de la declaración de la política.
16	2023-06	Inclusión de controles para los integrantes de contento