OBJETIVO:	Establecer los lineamientos que regulan la Seguridad de la Información, según las necesidades e infraestructura de la compañía, en concordancia con la planeación estratégica de la organización.
ALCANCE:	Aplica para todos los colaboradores, partes interesadas de la compañía, que tengan acceso a los servicios y/o sistemas de información de BPM Consulting SAS, así como los usuarios que tienen custodia sobre los activos de información de BPM Consulting SAS.

ROLES Y RESPONSABILIDADES	
ROL (CARGO)	**RESPONSABILIDAD**
Gerente de Control, Mejora e Innovación	Responsable de crear y/o actualizar las políticas de seguridad de la información acorde a cambios que afecten a la confidencialidad, integridad y/o disponibilidad de la información en la organización, dando cumplimiento al SGSI.
Gerente de Tecnología e infraestructura	Responsable de validar el contenido técnico y asociado a seguridad de la información en las políticas creadas, conforme a los estándares de la norma.
Gerente General / Subgerente General	Generar directrices para toda la organización, realizar seguimientos a través del Comité Directivo del estado del sistema, revisar y/o aprobar las políticas.
Toda la organización	Aplicar las políticas y directrices establecidas para los sistemas de la organización; también pueden solicitar revisiones, asistir y participar de las socializaciones o divulgaciones de estas.

TERMINOS Y DEFINICIONES

Política: Declaración, intenciones y directrices de la compañía, expresadas por la dirección general.

Activo: Cualquier cosa que tenga un valor de importancia relevante para la organización. Entre los activos de una organización se encuentra hardware, software, documentos electrónicos o físicos, infraestructura, servicios, personal, entre otros. El término Activo es sinónimo de Activo de Información.

Amenaza: Es una fuente generadora de eventos o acciones que puede producir o causar un daño representativo al activo de información, generando un factor o escenario de riesgo que originaría a la organización pérdidas por riesgo de seguridad de la información. La amenaza es un contexto de seguridad de la información que se manifiesta a través de actos deliberados, intencionados o impredecibles y provocados por las personas, la tecnología, la infraestructura, acontecimientos externos, entre otros.

Confidencialidad: Propiedad de salvaguardar el activo de información de personas, procesos o entidades no autorizados.

Controles: Medidas de protección o salvaguardas dispuestas para reducir el nivel de riesgo. Pueden ser políticas, procedimientos, directrices, prácticas, estructuras de la organización, soluciones tecnológicas, entre otros.

Disponibilidad: Propiedad de garantizar que el activo de información sea accesible y utilizable en el momento que se requiera, por parte de las personas, procesos o entidades autorizadas.

Incidente de seguridad de la información: Uno o una serie de eventos de seguridad de la información indeseados o inesperados que afecta un activo de información y que tienen una probabilidad significativa de comprometer las operaciones del negocio y/o amenazar la seguridad de la información asociada con el mismo.

Integridad: Propiedad de salvaguardar la exactitud y estado completo del activo de información, de acuerdo con los diferentes métodos de proceso a que se exponga.

Propietario: Se refiere al dueño responsable del activo de información utilizado para el desarrollo y cumplimiento de sus funciones. Está encargado de garantizar la seguridad adecuada del mismo, con base a los principios básicos de seguridad a saber: confidencialidad, integridad y disponibilidad.

Proteger la organización: Reducción del riesgo a través de la implementación de acciones o medidas de control dirigidas a disminuir el impacto o severidad de las consecuencias del riesgo si éste ocurre.

Riesgo: Se entiende por riesgo, la posibilidad de incurrir en pérdidas económicas, operativas, legales o de imagen para la organización por deficiencias, fallas al no adecuado uso y/o manejo del activo de información, a causa de amenazas o vulnerabilidades que le altere su correcto funcionamiento u operatividad. Efecto de la incertidumbre en un resultado esperado.

Seguridad de la información: Preservación fundamental de la confidencialidad, integridad y disponibilidad del activo de información, además de otros criterios o propiedades tales como la autenticidad, no repudio, confiablidad, propiedad y/o responsabilidad, entre otros.

Sistema de Información: Es una disposición de personas, actividades o procedimientos y recursos tecnológicos integrados entre sí, para apoyar y mejorar las operaciones diarias de la organización, con la finalidad de satisfacer las necesidades de información en general y facilitar la toma de decisiones por parte de los directivos de la organización. Ejemplos aplicados: sistemas de automatización de oficina, sistemas de procesamiento de transacciones y sistemas de información de gestión.

Tratamiento del riesgo: Proceso de selección e implementación de controles o acciones para ajustar el nivel de riesgo del activo a los niveles aceptables para la Organización.

Sistema de gestión de seguridad de la información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza la compañía para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basado en un enfoque de gestión y de mejora a un colaborador o a los servicios de BPM Consulting.

PROCEDIMIENTO

	ACTIVIDAD	RESPONSABLE	TAREA	REGISTRO	CONTROL
#	Nombre de la actividad (Conjunto de tareas)	Cargo de quien realiza la tarea.	Tareas que se desarrollan secuencialmente dentro de una actividad	Documento que proporciona evidencia de la tarea desarrollada	Revisión que se le hace a una tarea
1	Definir las políticas de seguridad de la información	Gerente de control, mejora e innovación	Deberá definir las políticas, dando cumplimiento a la norma y a los requisitos del Anexo A de la ISO 27001, los requisitos del sistema integrado de gestión, los lineamientos de la compañía y entes de control.	Políticas del sistema de gestión de seguridad de la información	Revisión anual de las políticas
2	Validar las políticas	Gerente de Tecnología e infraestructura / Gerentes por procesos según aplique.	Los documentos asociados a políticas podrán ser revisadas con apoyo del Gerente de Tecnología y ayudarán con su aprobación o ajuste en su contenido.	Aprobación en el Sistema de Información	Nueva versión de los documentos del SGSI.
3	Notificar cambios	Gerente de control, mejora e innovación	Validar el contenido del documento, solicitar ajustes según corresponda y aprobar la política	Aprobación en el Sistema de Información	Nueva versión de los documentos del SGSI.
4	Autorizar socialización	Gerente de control, mejora e innovación	Publicar documento en repositorio documental	Políticas del sistema de gestión de seguridad de la información	Nueva versión de los documentos del SGSI disponible en el repositorio documental
5	Socializar información	Gerente de control, mejora e innovación / Líder de Formación y Bienestar/ Líder de Marketing	Comunicar y socializar las políticas de seguridad de la información a los colaboradores y partes interesadas	Políticas del sistema de gestión de seguridad de la información	Aseguramiento de que la información está publicada y los colaboradores/partes interesadas cuentan con acceso a la misma

	ACTIVIDAD	RESPONSABLE	TAREA	REGISTRO	CONTROL
7	Revisar cambios a la información publicada	Gerente de control, mejora e innovación / Gerencias por proceso.	Validar alguna novedad o modificaciones, según cambios legales, contractuales, organizacionales	Nuevos versionamientos en los documentos	Registro de revisión por la dirección
8	Generar cultura de seguridad de la información	Gerente de control, mejora e innovación / Todos los colaboradores de BPM Consulting	Implementar medios para lograr difundir y dar a conocer las buenas prácticas y los controles correspondientes acorde a cada proceso, proyecto o línea de negocio.	Inspecciones integrales / revisiones del sheriff de seguridad	Evidencias, fotos, notificaciones mediante correo electrónico.
9	Definir un plan de auditoria	Gerente de control, mejora e innovación	Diseñar un programa de auditoría del sistema de gestión de seguridad de la información donde se contemplen los requisitos de seguridad y las políticas asociadas.	Programa anual de auditorias	Ejecución de auditorias

OBJETIVOS DE SEGURIDAD DE LA INFORMACION

- Garantizar la protección de los activos críticos de la empresa
- Velar por la disponibilidad de los servicios
- Asegurar la continuidad del negocio
- Mantener el cumplimiento de los requerimientos contractuales para los proyectos
- Alcanzar la conformidad del SGSI según los requisitos de la ISO 27001
- Incluir tecnología que provea apoyo a la gestión del sistema de seguridad de la información.

POLITICA DE SEGURIDAD DE LA INFORMACION

BPM Consulting SAS decreta desde su política de alto nivel el compromiso con implementar, mantener y mejorar el sistema de seguridad de la información. Se entiende la importancia de una adecuada gestión de los activos y la información y está altamente comprometida con la implementación del SGSI; buscando establecer un marco de confianza en el desarrollo de las actividades internas y los servicios prestados enmarcados en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de nuestra organización.

La compañía está comprometida con aplicar y mantener los pilares de la seguridad:

- Confidencialidad.
- Integridad
- Disponibilidad

Para con la información y todos los activos. Se busca la disminución del impacto generado y los riesgos identificados, a través de la mejora continua, se espera mantener un nivel de exposición tolerable, que no genere impactos que afecten la reputación, ni buen nombre de la organización y que estén acorde con las necesidades de los diferentes grupos de interés.

A través del presente documento y de los estándares aplicables de la norma ISO 27001 se espera lograr:

- Mantener la satisfacción y confianza de los colaboradores, clientes y partes interesadas para con los sistemas, activos e información.
- La minimización del riesgo en los procesos internos y en los servicios prestados a los clientes.
- Dar cumplimiento a los principios de la seguridad de la información (confidencialidad, disponibilidad, integridad)
- Innovar en materia tecnológica.
- Crear, mantener, actualizar y divulgar las políticas, procedimientos e instructivos en materia de seguridad de la información.

Las políticas de seguridad de la información se fundamentan en los dominios y objetivos de control de la norma NTC-ISO/IEC 27001. Estas deben tener un dueño, responsable de las actividades de desarrollo, evaluación y revisión. La actividad de revisión debe incluir las oportunidades de mejoras, en respuesta a los cambios, entre otros: organizacionales, normativos, legales, tecnológicos.

ORGANIZACIÓN INTERNA

Dando continuidad al compromiso de la dirección con la seguridad de la información, se aprueba la creación de los siguientes componentes en la compañía:

- Asignación de un responsable de la seguridad de la información: Gerente de mejora e innovación o quien haga sus veces.
- Comité de seguridad de la Información: Tecnología de la infraestructura, operaciones y gerencia general o quien haga sus veces.
- Asignación de responsabilidades asociadas a la seguridad de la información de acuerdo con el cargo dentro de la compañía y las funciones de este, que se detallan en el perfil de cargo.

Roles y Responsabilidades

Gerencia General

- Dirección estratégica e impulso del SGSI.
- Definir los objetivos estratégicos.
- Compromiso en la asignación de recursos
- Aprobación de los lineamientos, políticas, mecanismos de supervisión y métricas
- Promover la implementación y aplicabilidad de los lineamientos y políticas de seguridad de la información en la organización.
- Verificar las evaluaciones de riesgo resultantes del BIA
- Supervisar el cumplimiento de las obligaciones regulatorias
- Aprobar y participar activamente en la implantación de la cultura de seguridad de la información en la compañía
- Revisar y aprobar los proyectos de seguridad de la información

Líderes de proceso (Gerentes por proceso)

- Participar activamente en la implementación de las políticas y controles de seguridad de la información.
- Facilitar la integración de sus equipos de trabajo para lograr la implementación exitosa del Sistema de Seguridad de la Información.
- Velar por la disponibilidad de los recursos y su uso apropiado.
- Compromiso en la asignación de recursos

Comité Directivo

El comité Directivo es un órgano de alto nivel, que está conformado por los gerentes de las siguientes áreas: Tecnología e Infraestructura, Operaciones, Talento Humano, Administración y Finanzas, Mercadeo y Ventas, Control, Mejora e Innovación y la Subgerencia General. Sesiona 1 vez al mes para abordar la gestión de cada área, temas que requieren toma de decisiones y actuaciones, definiciones en cuanto asignación de recursos, requerimientos particulares para cada proyecto/cliente, prospectos de nuevos clientes/ clientes nuevos.

En cuanto a la seguridad de la información se revisa periódicamente:

- Estado general del sistema de gestión de seguridad de la información
- Monitoreo y acciones para seguir en cuanto a la gestión de los incidentes de seguridad de la información.
- Comunicación sobre proyectos de seguridad de la información y sus avances en el proceso de implementación.
- Aprobación de lineamientos de seguridad de la información.
- Aprobación, seguimiento a actividades de formación, sensibilización.

Oficial de Seguridad de la Información

- Definir y actualizar los lineamientos, normas, procedimientos y estándares del Sistema de Gestión de Seguridad de la Información.
- Definir una metodología de riesgo adecuada y alineada con la estructura organizacional.
- Realizar el análisis de riesgo de los procesos críticos del negocio.
- Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad del negocio
- Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad de la información.
- Emitir lineamientos para controlar el acceso a los sistemas de información y la modificación de privilegios
- Promover la formación, educación y el entrenamiento para fortalecer la cultura de seguridad de la información al interior de la compañía.
- Mantenerse actualizado ante la evolución de las amenazas y vulnerabilidades existentes y las nuevas que surjan.
- Desarrollar e implementar el enfoque de monitoreo.
- Garantizar la identificación y cierre de las brechas.
- Desarrollar métodos y métricas para evaluar el rendimiento del SGSI.

Colaboradores

Los colaboradores son responsables del cumplimiento de las políticas de seguridad de la información.

Contratistas, proveedores y terceros

Los contratistas, proveedores y terceros que tengan acceso a los activos de información, están obligados a cumplir las políticas de la seguridad de la información de BPM Consulting SAS.

CONTACTO CON LAS AUTORIDADES

Se mantendrán los contactos apropiados con las autoridades pertinentes, en caso de encontrar violación a cualquier política de seguridad de la información.

Las siguientes autoridades listadas corresponden a las entidades competentes en caso de que se presentara un incidente de cualquier índole que pusiera en riesgo la confidencialidad, integridad, disponibilidad y privacidad de la información. En caso de requerirse el llamado a las autoridades mencionadas, sólo podrán hacerlo los funcionarios encargados (Gerente TI, Gerente Admin y Fin, Gerente TH o las personas que estos roles asignen para tal fin).

Descripción	Organización	Contacto
Acceso abusivo a sistemas informáticos	Centro Cibernético Policial (CCP)	http://www.ccp.gov.co/
Violación de Datos personales		
Uso de Software malicioso		
Suplantación de Sitios Web		
Transferencia no consentida de activos		
Hurto por medios informáticos		
Phishing		
Ingeniería Social		
Respuesta a Emergencias Cibernéticas de Colombia	COLSERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia	http://www.colcert.gov.co/
Atención a incidentes de seguridad informática colombiano	CSIRT-CCIT Centro de Coordinación Seguridad Informática Colombia	https://cc-csirt.policia.gov.co
Emergencia por Incendio	Bomberos	119
Robo	Policía Nacional	112
Antisecuestro y Antiextorsión	Gaula	165
Siniestros ambientales	Defensa Civil	144
Incidentes Laborales	Cruz Roja	132
Incidentes laborales	Centro Toxicológico	136
Robo	Dijin	157

CONTACTO CON GRUPOS DE INTERES ESPECIAL

Los grupos de interés son un elemento fundamental de la relación de la empresa con su entorno de actividad, están estrechamente vinculados con su capacidad para conseguir sus objetivos económicos. Se mantendrá contacto con los grupos de interés con la finalidad de compartir conocimientos, identificar oportunidades de mejora, mejores prácticas, recibir capacitación, compartir información relevante frente al sistema y sus cambios, obtener información:

Descripción	Organización	Contacto
Información sobre el sector	Asociación colombiana de Contac Center y BPO	https://www.bpro.org/
Tecnologías aplicadas y nuevas tecnologías		
Conferencias, charlas, capacitaciones		
Noticias		
Eventos		
Expertos en buenas prácticas de tecnología informática (seminarios, cursos, formaciones).	IT Service	https://itservice.com.co/
Proveedores de servicios de pruebas, inspección y certificación en temas de seguridad de la información.	CQR	https://cqr.com.co/

Descripción	Organización	Contacto
Tecnología omnicanal utilizada para la prestación del servicio.	Ucontact	https://www.ucontactcloud.com/es
Suministro de redes de internet, conectividad	Claro Movistar	Información detallada en cada contrato suscrito con un tercero

Se mantendrán los contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna, en el caso de que se presente un incidente de seguridad de la información.

Se debe mantener contacto permanente con las universidades, los grupos de investigación, entidades del gobierno y proveedores de tecnología que trabajan en pro de mantener actualizado a las personas que se desarrollan dentro del ámbito de la tecnología, para de esta manera mantenerse al tanto en amenazas, incidentes y soluciones.

Grupo de interés
Ministerio de Tecnologías de la Información y las Comunicaciones
Microsoft
Fortinet
ESET- Consejos de seguridad para el uso seguro del ordenador y de la información sensible y personal -Alertas ESET
www.welivesecurity.com
https://managedprotection.pandasecurity.com
Superintendencia de Industria y Comercio
Proveedores
Clientes

POLITICAS COMPLEMENTARIAS SEGURIDAD DE LA INFORMACIÓN

Dentro de las políticas establecidas y requeridas para la gestión correcta de la Seguridad de la Información, se han definido e implementado las siguientes:

- POLITICA DE DISPOSITIVOS MOVILES
- POLITICA DE CONTROL DE ACCESO LOGICO
- POLITICA DE CLASIFICACION ETIQUETADO Y MANEJO DE INFORMACION
- POLITICA DE CONTROLES CRIPTOGRÁFICOS Y GESTION DE LLAVES
- POLITICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA
- POLITICA DE SEGURIDAD EN LAS RELACIONES CON PROVEEDORES
- POLITICA DE DESARROLLO SEGURO
- LINEAMIENTOS DE SEGURIDAD DE LA INFORMACION PARA EL DESARROLLO DE SOFTWARE
- POLÍTICA DE CALIDAD OPERATIVA
- POLITICA DE CONTROL DE ACCESO FISICO

- POLITICA DE USO ACEPTABLE DE ACTIVOS
- POLITICA DE BACK UP DE LA INFORMACION
- POLITICA DE TELETRABAJO
- IMPLEMENTACION Y OPERACION DE SERVICIOS BPO
- POLITICA DEL SISTEMA INTEGRADO DE GESTIÓN
- POLITICA DE TRANSFERENCIA DE INFORMACION
- POLITICA PARA EL TRATAMIENTO DE DATOS PERSONALES

Nota: El contenido específico de cada una está indicado en la política particular a cada tema.

CUMPLIMIENTO

El cumplimiento de las políticas es obligatorio. En caso de que los colaboradores y terceras partes no se adhieran a estas, la organización se reserva el derecho de tomar las medidas correspondientes. Cualquier empleado que tenga conocimiento de alguna violación a estas políticas, debe informar a su jefe directo, a la Gerencia de Talento Humano o a la Gerencia de Control, Mejora e Innovación.

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA DE APROBACIÓN**	**DESCRIPCION**
01	16-02-2022	Creación del documento.
02	17-05-2022	Se adiciona listado de partes interesadas. Se describe brevemente la intensión de cada política que hace parte del sistema.
03	27-06-2023	Se ajustó la declaración de la política, se adicionan los objetivos y el responsable, se actualizan los ítems de las políticas que hay de seguridad.
04	02/01/2024	Cambio de la clasificación del documento, de Privado a Público.
05	06/03/2024	Actualización de los siguientes elementos: • Objetivo de la política general • Objetivos de Seguridad de la Información conforme revisión por la Dirección. • Exclusión de los textos detallados para cada política indicada en el documento. • Inclusión del listado de las políticas que aplican para el Sistema de Seguridad de la Información
06	07/05/2024	Actualización del capítulo Políticas complementarias Seguridad de la Información: • Exclusión de las políticas relacionadas con medio ambiente, seguridad y salud en el trabajo, diversidad, equidad e inclusión y desconexión laboral, dado que sus alcances no incluyen la seguridad de la información. • Inclusión del documento Lineamientos de seguridad de la información para el desarrollo de software