OBJETIVO:	Establecer las actividades y controles para gestionar las políticas de seguridad de la información, según las necesidades e infraestructura y su relación ante los lineamientos estratégicos de BPM Consulting SAS.
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 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	Generar directrices para toda la organización, realizar seguimientos a través de la mesa directiva del estado del sistema, revisar y/o aprobar las políticas.
Toda la organización	Debe 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.

Software: En computación, término inglés que hace referencia a todo lo lógico, es todo programa o aplicación, programado para realizar tareas específicas.

Acuerdo de Confidencialidad: Es un convenio que crea obligaciones a una o a ambas partes que intervienen, con respecto al uso, manejo y divulgación de la información, con el propósito de preservar la confidencialidad, integridad y disponibilidad de esta, como parte de una relación contractual o comercial.

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.

Equipamiento: El equipamiento de procesamiento de la información incluye todo tipo de elemento físico soportado para el desarrollo de las actividades diarias del negocio. Estos elementos pueden ser entre otros: computadores de escritorio o personales, organizadores físicos, teléfonos móviles, escáneres, impresoras, tóner, fotocopiadoras, dispositivos USB, discos removibles, papel, entre otros.

Evento de seguridad de la información: Es la ocurrencia identificada de un estado del activo de información (sistema, servicio, red, entre otros) que indica un incumplimiento posible de la política de seguridad de la información, una falla de controles existentes, o una situación previamente desconocida que puede ser pertinente para la seguridad

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.

Perímetro de seguridad física: Corresponde a un mecanismo o división implementada e identificable, que permite limitar o aislar un área segura o crítica de la organización con el propósito de brindar niveles de seguridad adecuados para el acceso o restricción al área respectiva.

Procesamiento de Información: Es la capacidad que tiene un sistema de información de efectuar cálculos con base a una secuencia de operaciones preestablecidas y permitiendo la transformación de datos fuentes en información para ser utilizada en la toma de decisiones.

Programa de concientización en seguridad de la información: Conjunto de estrategias que busca que todos los Colaboradores de la Compañía y los Colaboradores provistos por terceras partes interioricen y adopten las políticas, normas, procedimientos y guías existentes al interior de la Institución dentro de sus labores diarias.

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.

Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar recursos informáticos, sistemas operativos, redes de datos o sistemas de información.

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.

Vulnerabilidad: Es la debilidad o incapacidad de resistencia de un activo de información frente a una amenaza.

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 de BPM	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

	ACTIVIDAD	RESPONSABLE	TAREA	REGISTRO	CONTROL
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.	Soportes de ejecución, de aprobación o rechazo.	Nueva versión de los documentos del SGSI.
3	Notificar al Gerente General	Gerente de control, mejora e innovación	El personal encargado de crear las políticas de seguridad de la información informara al gerente general con el fin de validar su aprobación por la alta dirección.	Políticas del sistema de gestión de seguridad de la información. Soportes de ejecución, de aprobación o rechazo.	Si el gerente aprueba las políticas establecidas, iniciar su socialización. Si el gerente notifica algún cambio, ejecutarlo hasta su aprobación.
4	Autorizar socialización	Gerente General / Gerente de control, mejora e innovación	El gerente general o el representante de la alta dirección podrán dar visto bueno para iniciar la socialización de las políticas y procedimientos creados. Dejando como responsables a los solicitantes.	Políticas del sistema de gestión de seguridad de la información	Divulgaciones
5	Realizar socialización de políticas	Gerente de control, mejora e innovación /	Comunicar y socializar las políticas de seguridad de la información a los colaboradores y socios interesados a	Políticas del sistema de gestión de seguridad de	Registro de actividades

	ACTIVIDAD	RESPONSABLE	TAREA	REGISTRO	CONTROL
		Formación	través de herramientas de sensibilización, capacitación o medios autorizados.	la información	
6	Publicar en el sistema de gestión definido	Gerente de mejora e innovación	Publicar la versión final de las políticas, procedimientos pertinentes para ser notificados como información de uso interno en BPM Consulting.	Políticas del sistema de gestión de seguridad de la información	Publicación en sistema documental interno y en la página web la que aplique.
7	Revisar documentación anual	Gerente de control, mejora e innovación / Gerencias por proceso.	Validar alguna novedad o cambio anualmente o si es solicitado por la alta dirección. Si la documentación requiere ajustes, debe tener en cuenta la estructura organizacional, el contexto externo, condiciones legales o el ambiente técnico de infraestructura. En caso de que la documentación no requiera cambios, dar inicio con los esquemas de cultura y auditoria.	Políticas del sistema de gestión de seguridad de la información	Registro de revisión por la dirección

	ACTIVIDAD	RESPONSABLE	TAREA	REGISTRO	CONTROL
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.	Plan anual de auditorias Plan de auditorias	Ejecución de auditorias

OBJETIVOS DE SI

Objetivos de seguridad de la información BPM Consulting	Indicador de medición	Proceso
Velar por la satisfacción de los clientes frente al SGSI.	Mesa de soporte con meta del **80%** de cumplimiento frente a solicitudes recibidas	Tecnología e infraestructura
Garantizar el adecuado funcionamiento de los equipos que hacen parte de la prestación de los servicios tecnológicos.	Mantenimientos preventivos: N° de actividades ejecutadas / N° de actividades planeadas con meta de cumplimiento del **85%**	Tecnología e infraestructura
Alcanzar la conformidad del SGSI según los requisitos de la ISO 27001	Auditorias programadas / Auditorias ejecutadas con meta de cumplimiento del **100%**	Control, mejora e innovación
Incentivar la adopción de tecnología que permita la automatización y optimización de actividades en los procesos corporativos.	*Creación de BOT soporte nivel 1 *Creación de App inventario tecnológico.	Tecnología e infraestructura

POLITICA DE SEGURIDAD DE LA INFORMACION BPM CONSULTING

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.
- 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 Interdisciplinario 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.

Funciones del Comité de Seguridad de la información

El comité de seguridad de la información estará conformado por el equipo de Tecnología de la infraestructura, operaciones y gerencia general o quien haga sus veces y según la necesidad estarán los miembros de alto nivel de los procesos de BPM Consulting SAS. El comité deberá cumplir de forma organizada y coherente con las siguientes funciones:

- Debe revisar el estado general de la seguridad de la información periódicamente.
- Revisar y monitorear los incidentes de seguridad de la información.
- Revisar y aprobar los proyectos de seguridad de la información.
- Aprobar las modificaciones o nuevos lineamientos de seguridad de la información.
- Aprobar y participar activamente en la implantación de la cultura de seguridad de la información en la compañía.
- Coordinación de la seguridad de la información.
- La gerencia es responsable de que los colaboradores de alto nivel bajo su cargo conozcan y apliquen los lineamientos y políticas de seguridad de la información y realicen una adecuada retroalimentación a sus grupos de trabajo.
- BPM Consulting SAS, deberá contar con un cargo, que asuma las tareas y responsabilidades que conlleva el sistema de seguridad en la compañía.

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
- Verificar las evaluaciones de riesgo resultantes del BIA
- Supervisar el cumplimiento de las obligaciones regulatorias
- Definir y desarrollar el plan de seguridad de la información.

Líderes de proceso (Gerentes por proceso):

- Participar activamente en la implementación de los programas de seguridad de la información.
- Facilitar la integración entre los diferentes dueños de procesos de negocio para lograr la implementación del programa.
- Velar por la disponibilidad de los recursos y su uso apropiado.
- Compromiso en la asignación de recursos

Oficial de Seguridad de la Información:

- Definir y desarrollar el plan 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.
- Realizar estudios de penetración y pruebas de seguridad en todos los ambientes (Desarrollo, pruebas, producción y contingencia).
- 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.

Oficial de Privacidad de la Información:

- Identificar y servir en la dirección, implantación, desarrollo, y mantenimiento de estrategias, procedimientos y políticas de privacidad y confidencialidad.
- He de asegurar que se mantienen políticas y formularios (consentimientos, autorizaciones, entre otros) de privacidad, confidencialidad y seguridad de información.
- Liderar las actualizaciones de contenido para divulgación a personal interno, contratistas y terceros relacionados con la institución acerca de la privacidad y confidencialidad de la información del Servicio.
- Implantar protocolos de acceso a la información del servicio protegida dentro y fuera de la compañía (según lo requiera la ley) y delimitar el acceso solamente al personal calificado y con necesidad de revisar dicha información.
- Exigir el cumplimiento de los lineamientos de privacidad y confidencialidad, aplicando las sanciones ante el incumplimiento de dichas directrices, por parte de TODOS los miembros de BPM Consulting SAS, con el apoyo de los procesos de talento humano, la Gerencia General y los demás involucrados según sea el caso.
- Colaborar con el personal designado para asegurarse que los lineamientos y procedimientos relacionados a la confidencialidad y seguridad de la información (en particular la que se comparte por medio de comunicaciones electrónicas), se cumplan de acuerdo con los programas, equipos y sistemas de protección de la organización.

Administradores de los sistemas de información

Los administradores de los diferentes sistemas deben en forma activa implementar las normas, estándares, formatos y procedimientos, para brindar un nivel apropiado de seguridad de la información.

Colaboradores (Colaborador directos o en misión)

Los colaboradores son responsables del cumplimiento de las políticas de seguridad de la información. Adicionalmente cada colaborador tiene el compromiso de reportar al oficial de seguridad cualquier incidente de seguridad de la información del que tenga conocimiento.

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.

Custodio
Tienen la responsabilidad de monitorear el cumplimiento de las actividades encargadas.

Usuario o Propietario
Debe verificar la integridad de la información y velar por que se mantenga la disponibilidad y confiabilidad de esta.

Asignación de responsabilidades para la seguridad de la información.

Las responsabilidades de la seguridad de la información están definidas y asignadas de acuerdo con la clasificación dada a la información.

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.

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/

Descripción	Organización	Contacto
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 interés 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 Tecnologías aplicadas y nuevas tecnologías Conferencias, charlas, capacitaciones Noticias Eventos	Asociación colombiana de Contac center y BPO	https://www.bpro.org/
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/
Tecnología omnicanal utilizada para la prestación del servicio.	Inconcert	https://info.inconcertcc.com/p/SL/landing?gclid=EAIaIQobChMIobyCrrPn9wIVkfvjBx0NggroEAAYAiAAEgICrfD_BwE
Suministro de redes de internet, conectividad.	Claro Movistar	https://www.claro.com.co/empresas/ https://www.movistar.com.co/

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.

El oficial de seguridad de la información será el encargado de coordinar los conocimientos disponibles en BPM Consulting SAS, a fin de brindar ayuda en la toma de decisiones en materia de seguridad, éste podrá obtener asesoramiento de otros organismos.

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
Kaspersky
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

El **comité de seguridad de la Información** debe revisar anualmente y prever el tratamiento en caso de los cambios no planeados, a efectos de mantener actualizadas las políticas. Además, efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como, por ejemplo, cambios tecnológicos, variación del costo de los controles o el impacto de los incidentes de seguridad.

Dentro de las políticas establecidas encontramos:

Uso aceptable de activos

El uso de los activos de información pertenecientes a la organización es responsabilidad del propietario asignado; es su deber proteger y mantener la confidencialidad, integridad y disponibilidad de los activos de información.

Subtítulos descritos en la política:

- Directrices generales
- Directrices de uso de internet
- Asignación de equipos y usuarios
- Directrices de uso de equipos de escritorio (PC) y portátiles (laptops)
- Uso de mensajería instantánea
- Directrices de uso de información escrita y verbal
- Directrices para el uso de bases de datos
- Directrices de devolución de activos

Clasificación etiquetado y manejo de información

- La información debe ser clasificada por su propietario y éste a su vez debe informar a la organización sobre su clasificación de manera que se tomen las medidas requeridas para preservar la confidencialidad e integridad de esta.
- El propietario de la información es responsable por la actualización de la clasificación de la información de acuerdo con los cambios de la organización.
- Se deben utilizar los mecanismos apropiados de control de acceso a la información dependiendo de su nivel de clasificación.

Clasificación de la Información: Realizar clasificación teniendo en cuenta los siguientes criterios:

- **Público**: Información declarada de conocimiento público que puede ser entregada o publicada sin restricciones a cualquier persona (incluso fuera de la compañía) sin que implique daños a terceros, a las finanzas ni a la imagen de la compañía.
- **Privado:** Es toda aquella información que no es pública y debe ser usada exclusivamente por grupos específicos de usuarios al interior de la organización. El conocimiento de esta información por parte de personas no autorizadas puede afectar las finanzas de la compañía y la imagen

frente al público.

- **Confidencial:** Información que es en extremo sensible y que debe ser usada únicamente por ciertos individuos dentro de la compañía. Debe estar en el nivel más alto de vigilancia y protección, ya que es el fundamento de la subsistencia de la compañía. El conocimiento de esta información por parte de personas no autorizadas puede afectar las finanzas, la imagen y la estabilidad misma de la compañía.

Etiquetado de la información: Se relacionan los etiquetados por tipo y presentación de documentos de la siguiente manera:

- Etiquetado de documentos digitales
- Etiquetado de información física

Manejo de la información: Para cada nivel de clasificación se debe tener en cuenta los siguientes elementos.

- Seguridad de la documentación de sistemas
- Mecanismos de distribución de la información
- Personal con acceso a la información

Escritorio y pantalla limpia

Escritorio limpio:

- Los puestos de trabajo deben permanecer limpios y ordenados
- Al levantarse del puesto de trabajo y al finalizar la jornada laboral, los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles que contengan información pública, privada o confidencial.
- Cuando se imprima o digitalice documentos con información confidencial, deben retirarse inmediatamente de dichos dispositivos.
- Los dispositivos de impresión y digitalización deben permanecer limpios de documentos.
- Los gabinetes, cajones y archivadores de contengan documentos y/o medios extraíbles con información confidencial deben dejarse cerrados durante la hora de almuerzo y al finalizar la jornada laboral.

Pantalla limpia:

- La pantalla del computador (escritorio) no debe contener ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias

para que los colaboradores o contratistas ejerzan sus funciones o cumplan sus obligaciones contractuales, según el caso.

- Los documentos electrónicos que producen los colaboradores o contratistas en el ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales, según el caso, deben guardarse conforme a las indicaciones suministradas por el área de tecnología.

Equipo de usuario desatendido:

- Al levantarse del puesto de trabajo, se debe bloquear la sesión de los equipos de cómputo mediante las teclas Windows + L para para proteger el acceso a las aplicaciones y servicios de organización.
- El área de tecnología implementa el bloqueo automático de la sesión de usuario mediante el directorio activo al transcurrir 5 minutos de inactividad en el equipo de cómputo.

Ética y conflictos de intereses

Ética en la conducción de los negocios

Con el fin de mantener el Good Will de la compañía, garantizar el manejo confidencial de nuestra información, proteger nuestros activos y propender por un buen ambiente laboral, todas las acciones de los trabajadores de BPM Consulting. se fundamentarán en las siguientes disposiciones:

- Protección de activos
- Manejo de la información
- Cumplimiento de las diferentes normas y códigos
- Manejo de los recursos para la operación de los trabajadores
- Compromiso con la calidad
- Relación con nuestros accionistas
- Compromiso con los empleados
- Compromiso con nuestros clientes
- Compromiso con nuestros proveedores
- Compromiso con la sociedad
- Compromiso con el medio ambiente

Conflicto de intereses

Nuestros lineamientos derivan de la definición legal de “conflicto de intereses” que establece: “el trabajador debe excusarse de intervenir en la atención, tramitación o resolución de asuntos en los que tenga interés o beneficio personal, familiar (cónyuge, parientes consanguíneos hasta el cuarto grado, parientes por afinidad

hasta el cuarto grado, parientes civiles) o de negocios (terceros con los que tenga relaciones profesionales o de negocios o para socios o sociedades de las que el trabajador o los familiares mencionados formen o hayan formado parte)".

Tratamiento de datos personales

BPM Consulting SAS, sociedad por acciones simplificadas, identificada con el NIT 900.011.395-6, con domicilio principal en la Carrera 17 No. 164 - 25. de la ciudad de Bogotá, República de Colombia. Página https://www.bpmconsulting.com.co/, Teléfono 7569094 en la ciudad de Bogotá D.C.

Los datos personales respecto de los cuales BPM Consulting asume el carácter de responsable son incluidos en bases de datos y serán utilizados para el desempeño propio de las actividades comerciales de la compañía.

BPM Consulting, alineado con las disposiciones dadas por la Ley 1581 de 2012, establece los siguientes numerales dentro de la política:

- Excepciones para la autorización de uso de datos personales
- Derechos de los titulares de los datos personales
- Datos de menores de edad
- Datos sensibles
- Atención a peticiones, consultas y reclamos
- Procedimiento para ejercer los derechos de titulares a conocer, actualizar, rectificar, suprimir información y revocar la autorización.
- Medidas de seguridad del tratamiento de datos personales
- Confidencialidad de la información de datos personales
- Vigencia.

Dispositivos móviles

- No se debe modificar la configuración establecida por el área de Tecnología en los dispositivos móviles; esto incluye los mecanismos de seguridad asignados por la organización (antivirus, firewall, configuración del sistema operativo, programas, aplicaciones, entre otros), ni desinstalar el software provisto al momento de su entrega.
- Se prohíbe la instalación de software o aplicaciones adicionales a los incluidos en el dispositivo móvil. En caso de que se requiera una aplicación o un software adicional, se deberá solicitar su aceptación e instalación al área de tecnología de la organización.

- La asignación de dispositivos móviles y planes de telefonía celular para los colaboradores se realiza de acuerdo con las responsabilidades propias de su cargo.
- Los dispositivos móviles deberán tener un sistema de control de acceso como los siguientes: PIN, usuario y contraseña, patrón de bloqueo, desbloqueo a través de huella digital.
- El área de Tecnología tiene bajo su responsabilidad el suministrar soporte para la instalación y configuración de aplicaciones, software y servicios autorizados por la organización en los dispositivos móviles.
  Nota: Si se requiere de un soporte adicional como por ejemplo garantías o servicio técnico debe ser tramitado a través del área administrativa y/o de tecnología según corresponda
- Los colaboradores que usen el servicio de telefonía celular (planes de voz y/o datos), asignados por la organización, deben darle un uso racional y estrictamente laboral.
- Los colaboradores con dispositivos móviles de la organización deben acogerse las disposiciones de navegación definidas por la empresa, las cuales prohíben, entre otros, la consulta de páginas violentas, pornográficas o que atenten contra los principios de la ética y la moral.
- El colaborador que se desvincule laboralmente de la compañía deberá devolver los dispositivos móviles y los accesorios que le hayan sido asignados.

Se entregan directrices para garantizar la seguridad de los equipos fuera de las instalaciones y el uso de dispositivos personales de los colaboradores (empleados y contratistas) dentro de las instalaciones de BPM Consulting SAS.

Trabajo Remoto

El entorno de trabajo remoto, para colaboradores y contratistas con equipos suministrados por la organización debe considerar, entre otros:

- Sistema operativo y aplicaciones actualizadas.
- Software antivirus.
- Cuentas de usuario sin permisos para instalar software.
- Controles de acceso lógico al equipo
- Controles de navegación
- Bloqueo automático por inactividad.
- Software original.

- Cifrado del disco.

Se dictan las recomendaciones para el trabajo que se realice en equipos de propiedad del colaborador o contratista.

Se dan las recomendaciones de la propiedad física de los equipos.

Se dan los lineamientos para uso de tablets y smartphones.

Se establecen los lineamientos en cuanto a:

- Comunicaciones
- Copias de seguridad
- Cifrado de disco duro

Control de acceso lógico

Todos los colaboradores que accedan a los sistemas de información de la organización deben contar con usuario y contraseña los cuáles son personales e intransferibles, con excepción de sistemas con información de bajo riesgo en la que se permite el acceso mediante usuarios grupales.

Registro de usuarios:

- Todos los colaboradores con acceso a los sistemas de información de la compañía deben registrar su usuario parar acceder a los distintos servicios de la red.

Gestión de privilegios:

- En los sistemas de la organización los usuarios solo ven lo que necesitan, cuando lo necesitan. El uso inapropiado de los privilegios de administración del sistema (cualquier dispositivo o medio de un sistema de información que permite al usuario superar los controles del sistema o aplicación) acarreará acciones disciplinarias.
- Los contratistas y terceros con acceso a los sistemas de información de la organización deberán cumplir con lo estipulado en la presente política.

Gestión de claves:

- Los sistemas de información de bajo impacto en términos de seguridad de la información podrán contar con claves genéricas. Estas claves serán asignadas por el área de tecnología. Los demás

sistemas de información deben contar con una clave que pueda ser cambiada por el colaborador.

Revisión de los derechos de acceso del usuario:

- El área de tecnología deberá revisar los derechos de acceso de los usuarios de forma periódica teniendo en cuenta la información registrada en la matriz de acceso lógico.

Responsabilidad del usuario:

- Todos los usuarios de sistemas de información de la organización deberán reportar el acceso no autorizado a los sistemas de información, el robo de información o cualquier incidente de seguridad en materia de acceso lógico. En los casos en que se presente esta situación se deberá cumplir con lo estipulado en el procedimiento de reporte de incidentes de seguridad.
- La gestión del acceso (solicitud, autorización, asignación y remoción de derechos de acceso a la información contenida en los sistemas de información de la compañía) se realizará con base en las necesidades y funciones de cada cargo en la organización. En ningún caso se podrá acceder con credenciales diferentes a quien ingresa al sistema de información.

Uso de claves secretas:

- Los colaboradores de la compañía con acceso a los sistemas de información de esta deberán cumplir las siguientes recomendaciones con relación al uso de las claves secretas:
  - Evitar mantener un registro en papeles
  - Cambio de claves de forma periódica o cuando exista una amenaza que ponga en peligro la información contenida en el sistema.

Acceso a redes:

- El área de tecnología determinará las redes a las cuales tendrán acceso los colaboradores y terceras partes en función de sus actividades laborales
  - Red LAN
  - Red Inalámbrica
  - Redes visitantes
  - VPN

- El acceso a las redes de la organización para visitantes se deberá solicitar mediante caso a Mesa de Ayuda. El área de tecnología junto con el Coordinador del SIG o quien haga las veces de oficial de seguridad de la información, evaluarán dicha solicitud. El área de tecnología utilizará medios técnicos para impedir acceso a las redes de la organización. (DHCP)

- Todos los accesos a los sistemas de información deben ser removidos una vez se termina la relación laboral o contractual con la organización.
- Es responsabilidad del área de gestión humana reportar oportunamente la finalización de un contrato de trabajo al área de tecnología.
- Los accesos de proveedores a sistemas de información de la organización serán autorizados por el área de tecnología con el visto bueno del Coordinador del SIG, el oficial de seguridad de la información o quien haga sus veces.

Controles criptográficos y gestión de llaves

Todo cifrado de información en BPM Consulting se realizará con herramientas criptográficas y criterios de cifrado de la información aceptados y aprobados por la dirección de tecnología de la organización, en conjunto con el oficial de seguridad de la información o quien haga sus veces.

Toda información transportada en dispositivos removibles, que tenga carácter confidencial, deberá protegerse mediante herramientas de encriptación.

Se deberá tener en cuenta las siguientes disposiciones para la gestión de llaves:

- ***Uso:***
  - En ningún caso la longitud de las llaves simétricas será inferior a 128 bits. La longitud de llaves asimétricas deberá contar con fortaleza equivalente.
  - Los requisitos de longitud de llaves de cifrado en nuevos sistemas de la organización deberán ser definidos por la dirección de tecnología de la organización.
  - Los algoritmos usados en la organización deberán cumplir con la legislación colombiana y extranjera que le sea aplicable.
  - En la generación de llaves se deben generar claves y contraseñas seguras. Para lograrlo es necesario:
    - Emplear una mezcla de símbolos y caracteres sin coherencia lógica

- Ayudarse de nemotecnias e imágenes mentales conocidas únicamente por quien establece la contraseña segura
- Evitar utilizar información personal tal como fecha de nacimiento y similares

- ***Distribución:*** La forma como llega las llaves puede ser:
  - Distribución Manual: La clave se envía mediante canales distintos a la línea de comunicación mediante la cual se mandan mensajes cifrados, por ejemplo: Carta certificada; vía telefónica; mensaje de texto, etc.
  - Distribución central: Las partes interesadas en el intercambio seguro de datos establecen una conexión cifrada por un tercero. Este elemento se encarga de entregar las claves cifradas seguras de comunicación a ambos extremos.
  - Distribución certificada por:
    - Transferencia de clave
      - El Emisor genera una clave asimétrica con la llave pública del Receptor (criptografía asimétrica)
    - Intercambio o acuerdo de clave
      - El Emisor y el Receptor conocen de antemano la clave (criptografía simétrica)
- ***Protocolo de Recuperación de llaves***
  Cuando la herramienta de cifrado lo permita, la organización debe contar con mecanismos para gestionar la recuperación de contraseñas en caso de olvido de la clave o contraseña que se generó. Algunas opciones para activar este protocolo son las siguientes:
  - Recuperación de Clave o Contraseña
  - Restablecimiento de Clave o Contraseña
- ***Protección y Almacenamiento: Las llaves de cifrado deberán protegerse mediante al menos uno de los siguientes controles:***
  - Respaldo de información
  - Almacenamiento en repositorios seguros que proporcionen protección adecuada y que impidan su divulgación.
  - En ningún caso se tendrán listas de llaves criptográficas en textos planos o archivos en los que no se tenga ninguna protección
- ***Tiempo de vida:***
  - En ningún caso las llaves serán usadas de forma indefinida.
  - La disposición de llaves criptográficas obsoletas se realizará mediante alguno de los siguientes mecanismos:

- Disposición por Expiración: Establecimiento del tiempo máximo de vida útil de claves y contraseñas.
- Disposición por Revocación: Ocurre cuando el Administrador de Sistema detecta compromiso en las claves y contraseñas, y para asegurar la integridad de la data, procede a su descontinuación inmediata. También se revoca una clave o contraseña por fuerza mayor (despido, deceso o redefinición de privilegios de usuario; actualizaciones; restructuraciones, etc.).

Transferencia de información

Intercambio de Información entre los colaboradores de la organización:

La información de la organización solo intercambiará de entre colaboradores cuando dicho intercambio corresponda a actividades relacionadas con el desarrollo de sus labores. Siempre que se realice intercambio de información catalogada como confidencial, dicho intercambio se realizará mediante las herramientas de comunicación suministradas por la organización.

Intercambio de información con terceros:

Todo intercambio de información confidencial perteneciente a la organización con sus terceros debe ser respaldado con un acuerdo (convenio o contrato), que incluya una cláusula de confidencialidad y no divulgación de la información proporcionada.

Se exceptúa toda aquella información que deba ser transferida a entidades de control y autoridades que la soliciten

El intercambio de información digital clasificada como confidencial o personal, debe realizarse mediante mecanismos que permitan el cifrado de dicha información y que garanticen la protección de su confidencialidad, acorde con la política de controles criptográficos y gestión de llaves de la organización. La solicitud de envío de este tipo de información se debe hacer al área de T.I. a través de la mesa de ayuda.

Intercambio de Información Física:

El intercambio de información que se encuentre en formatos físicos debe hacerse mediante transporte o servicios de mensajería confiables.

Se deben transportar estos mediante mecanismos que protejan al activo de amenazas ambientales.

Control de acceso físico

- El ingreso de personas a las instalaciones de la organización se realizará mediante controles de acceso que permitan registrar la fecha y hora de dicho ingreso (Lector biométrico, tarjeta de acceso, área de recepción, etc.).
- En todos los casos los colaboradores de la organización deberán registrarse de forma individual mediante los mecanismos previstos por la empresa. No está permitido el ingreso de colaboradores o terceros sin que antes se haya validado su identidad mediante los mecanismos de control de acceso dispuestos por la organización.
- Las fallas de funcionamiento en los sistemas de control de acceso deben ser reportadas de manera inmediata al área Administrativa y Financiera mediante correo electrónico.
- Los sistemas de control de acceso de la organización deberán contar con mecanismos que permitan su suspensión en caso de falla o emergencia.
- Los centros de procesamiento de datos y cuartos de equipos deberán estar en áreas protegidas físicamente contra el acceso no autorizado.
- Los equipos de cómputo y de comunicaciones que no sean propiedad de la organización, deberán registrarse antes de su ingreso a las instalaciones de la compañía, indicando la fecha, hora de entrada, hora de salida, nombre y apellido, marca, serial y firma.
- Los equipos de propiedad de la organización que por razones de negocio deban retirarse con frecuencia de las oficinas, contarán con una autorización global la cual le permitirá ser transportados por sus propietarios sin que sea necesario su registro. No obstante, el personal de vigilancia de la organización deberá verificar que el equipo se encuentre autorizado para salir de las instalaciones de la organización y sea su propietario quien lo retire.
- Ningún equipo de cómputo o comunicaciones podrá salir de la organización sin que exista una autorización.
- El ingreso de visitantes será controlado por el personal de recepción previa autorización del colaborador a quien visitan. En todos los casos los visitantes deberán registrarse en el formato destinado para tal fin.

- Todos los visitantes de la organización serán acompañados en todo momento por el colaborador responsable de dicha visita o por quien haya sido designado para hacerlo. Los visitantes solo tendrán acceso para propósitos específicos autorizados.
- El acceso a las ***Zonas Seguras*** de la organización (Data center, cuartos de comunicaciones, archivo, etc.) estará restringido al personal autorizado. El ingreso a dichas zonas deberá registrarse en el formato destinado a tal fin.
- Solamente se permitiría el acceso a proveedores que deban realizar labores dentro de la infraestructura de la organización. En ninguna circunstancia los proveedores realizarán trabajos sin el acompañamiento de un colaborador de la organización.
- La recolección y entrega de documentos y mercancías se realizará en las áreas de recepción que disponga organización, con excepción de equipos o paquetes que por su tamaño requieran del transporte del proveedor. En este último caso será necesario que un colaborador de la organización acompañe a los visitantes durante toda su estancia en las instalaciones de la empresa.
- Todos los visitantes deberán anunciar su llegada mediante los mecanismos dispuestos por la organización, con excepción de aquellos que se encuentren en compañía de un colaborador de la empresa, con quien se haya anunciado previamente.
- El personal ajeno a la organización deberá portar una identificación en un lugar visible mientras permanezca en las instalaciones de la empresa.
- Todos los colaboradores que se encuentren dentro de las instalaciones de la organización están obligados a portar su carnet en forma visible para su identificación como trabajador.
- La presencia de personas sin identificación y/o sin la compañía de colaboradores de la organización deberá ser reportada de inmediato al personal de seguridad y/o Coordinador del Sistema Integrado de Gestión.

Seguridad en las relaciones con proveedores

Los siguientes aspectos se deben tener en cuenta dentro de los acuerdos proveedores:

- BPM CONSULTING acordará los requisitos de seguridad mínimos que deben cumplir los productos y los servicios que se adquieren.

- Dentro de los acuerdos con proveedores se deberá definir las responsabilidades concretas de ambas partes.
- Cuando la organización lo determine, establecerá acuerdos de niveles de servicio (ANS).
- La organización determinará los controles de seguridad que son de obligatorio cumplimiento en las relaciones con los proveedores de servicios tecnológicos. Cuando sea necesario, dichos controles se deben registrar en el acuerdo.
- Cuando la organización así lo determine exigirá a sus proveedores certificaciones que garanticen la calidad en materia de seguridad de ciertos servicios contratados de especial criticidad.
- BPM CONSULTING. implementará mecanismos de seguimiento y revisión a los servicios de proveedores.
- Cuando sea factible la organización realizará Auditoría de los servicios contratados.
- Cuando BPM CONSULTING lo determine se deberán incluir cláusulas en las que el proveedor suministre información oportuna con relación a los incidentes de seguridad que afecten los productos y/o servicios que suministra a la empresa.
- Proveedores y terceros solo deben tener acceso a la información, sistemas de información o instalaciones que son indispensables para el cumplimiento de su objeto contractual.
- Cuando la organización lo determine se deberán incluir cláusulas a fin de que los proveedores y sus terceros cumplan con la reglamentación en materia de derechos de autor y propiedad intelectual, incluido, pero no limitado al uso de información y software.
- Los proveedores y terceros que presten sus servicios en la organización no están autorizados para utilizar los recursos de información y tecnología de la organización para propósitos diferentes a los necesarios para el cumplimiento del objeto contractual suscrito.
- No está autorizada la ejecución de cambios sobre la infraestructura de información y comunicaciones de BPM CONSULTING sin contar con la autorización formal y expresa de la organización.
- No está autorizada la modificación o desactivación de los controles de seguridad instalados en los componentes de información y tecnología de BPM CONSULTING sin contar con autorización del área de Tecnológica.

Compras

- Para iniciar el procedimiento de compras, desde un área diferente a Administrativa y Financiera, se deberá crear la requisición de compras a través del aplicativo MANTIS, esta solicitud debe ser diligenciada por administradores de proceso exclusivamente.
- Para aprobar un requerimiento se debe dar la especificación detallada sobre las características de la solicitud de compra, con el fin de obtener la satisfacción por parte del cliente interno.
- El envío de la requisición de compra al área Administrativa y Financiera cumplirá su trámite de recepción y análisis del producto y/o servicio solicitado. Si la requisición está asignada, es aprobada, caso contrario se cerrará el proceso adjuntando una nota con la causa de su rechazo.
- Los proveedores críticos que estén bajo contrato por demanda y/o acuerdo comercial, que nos provean los mismos insumos mes a mes, serán: seleccionados, inscritos y evaluados solo la primera vez que se vaya a contratar el servicio y/o producto.
- Todo proveedor excepto los CRÍTICOS de BPM CONSULTING SAS deberán cumplir con las 3 fases propuestas para poder brindar productos y servicios a la compañía cada vez que se requieran. Estas fases son: SELECCIÓN DE PROVEEDOR, INSCRIPCIÓN DE PROVEEDOR Y REEVALUACIÓN DE PROVEEDOR.
- En caso de no recibir novedades, una vez confirmado el recibido a satisfacción se procederá a cerrar la requisición de compra desde el área Administrativa y Financiera en el aplicativo MANTIS.

Las solicitudes de compra están sujetas a unos tiempos de respuesta según la prioridad:

Tiempos de Respuestas en las Solicitudes de Compra para Productos y/o Servicios	
Prioridad	**Días Hábiles**
Inmediato	De 0 días a <= 6 días
Urgente	> 7 días a <= 8 días
Alta	> 9 días a <= 10 días
Normal	> 11 días a <= 12 días
Baja	> 13 días a <= 14 días
Ninguna	<= 15 días

Nota: Cuando se trate de servicios como los canales dedicados y renta de inmuebles se contará con un plazo máximo de 40 días hábiles.

Dentro de los lineamientos del proceso se encuentra:

- Selección y Evaluación de proveedores, clasificando estos en dos categorías:
    - Proveedor No Crítico
    - Proveedor Crítico

Reevaluación de proveedores

- La reevaluación de proveedores se hará en el software **KAWAK – Módulo Proveedores – Evaluar Proveedores**. Los criterios para evaluar son TIEMPO DE ENTREGA DE COTIZACIONES, CALIDAD DEL PRODUCTO O SERVICIO PRESTADO, TIEMPO DE ENTREGA DEL PRODUCTO Y/O SERVICIO SOLICITADO, FACTURACION. La calificación se hará una vez realizada la primera compra con un sistema de puntuación de 1 a 100.
- Si la calificación obtenida por el proveedor en la evaluación es inferior o igual a 69, su desempeño se considera deficiente, y se realizará una reevaluación en la siguiente compra con el fin de efectuar un nuevo seguimiento a su desempeño, sin embargo, si reincide en una calificación inaceptable el proveedor es removido de la base de datos y se buscará un reemplazo en no más de tres meses para dar continuidad a la prestación del servicio dentro de la operación.
- Se les informará a los proveedores con un resultado deficiente en su evaluación esperando que se realice una mejoría en su desempeño.
- Si la calificación obtenida por el proveedor en la evaluación es superior a 70 e inferior o igual a 89 su desempeño se considera aceptable, y se realizará una reevaluación de forma semestral.
- Si la calificación obtenida por el proveedor en la evaluación es superior a 90 su desempeño se considera excelente, y se realizará una reevaluación de forma anual.

Anticorrupción

- Todo tercero que inicie un proceso de negociación con BPM Consulting debe ser consultado dentro de las listas restrictivas determinadas por la organización.
- Se prohíbe el aceptar suvenir de cualquier tipo de corrupción y/o soborno.
- No aceptar regalos o invitaciones que comprometan la toma de decisión frente al bien o servicio que se está negociando

- Se prohíbe ofrecer o recibir coimas para buscar un beneficio propio o para la empresa.
- Se declara impedido todo oferente que tenga vínculos familiares con los colaboradores de la compañía, hasta un quinto grado de consanguinidad.
- Los colaboradores de BPM Consulting S.A.S., deberán comprometerse a identificar y reportar las situaciones de soborno o corrupción que puedan presentarse a cualquier nivel, en los procesos de la compañía, con el fin de actualizar la matriz de riesgo de Corrupción y Soborno, dando cumplimiento al indicador para alcanzar la meta propuesta.

Canal De Reporte:

BPM CONSULTING S.A.S., en su interés por recibir la información, reportes de posibles casos, a dispuesto a través de su página web https://www.bpmconsulting.com.co/ el módulo de PQRSF mediante el cual los colaboradores, socios de negocio y partes interesadas pueden contactar e instaurar los reportes de la(s) situación(es) de corrupción en la que se vea involucrado(a), con el fin de ofrecer confianza y seguridad frente a cualquier eventualidad que se considere como un hecho irregular.

Es importante que se indique el contexto y los datos de contacto de la persona que está presentando la novedad, buscando de esta manera, darle un manejo adecuado a la situación presentada.

SAGRILAFT

El alcance de las acciones y estrategias que ha implementado BPM Consulting para el cumplimiento del sistema SAGRILAFT, abarca todos los niveles en la estructura organizacional y que se efectúa por la cooperación en cada proceso de la empresa a través de sus colaboradores, así como enlaces con el oficial de cumplimiento.

El comité es el órgano responsable de poner en marcha y garantizar la efectividad del SAGRILAFT y tiene las siguientes funciones:

- Establecer las políticas para la prevención y control del riesgo integral de lavado de activos, financiación del terrorismo y financiamiento de la proliferación de armas de destrucción masiva – SAGRILAFT.
- Designar el Oficial de Cumplimiento y su respectivo suplente, cuando sea procedente.
- Analizar oportunamente los reportes y solicitudes presentados por el representante legal.

- Efectuar los pronunciamientos sobre los informes presentados por la Revisoría Fiscal o las auditorías interna y externa, que tengan relación con la implementación y el funcionamiento del SAGRILAFT.
- Hacer el seguimiento y avances periódicos del sistema.
- Presentar, los reportes, solicitudes y alertas que consideren que deban ser tratados y que estén relacionados con el SAGRILAFT.
- Ordenar y garantizar los recursos técnicos, logísticos y humanos necesarios para implementar y mantener el buen funcionamiento del SAGRILAFT.
- Establecer los criterios para aprobar la vinculación de Contrapartes cuando sea una PEP (Persona Expuesta Políticamente).
- Instituir pautas y determinar los responsables de realizar auditorías sobre el cumplimiento y efectividad del SAGRILAFT.
- Constatar que la Compañía, el Oficial de Cumplimiento, el representante legal y sus trabajadores, desarrollen las actividades designadas en el presente Manual.

La gerencia general de BPM Consulting designa como oficial de cumplimiento a la gerencia de control, mejora e innovación. Quien será el encargado de velar por el eficiente y oportuno funcionamiento del sistema de administración de riesgos integrales LA/FT-FPADM, mediante la realización de las siguientes actividades:

- Participar activamente en los procedimientos de diseño, dirección, implementación, auditoría, verificación del cumplimiento y monitoreo del SAGRILAFT.
- Contar con conocimientos suficientes en materia de administración de riesgos, entender el giro ordinario de las actividades de la empresa y estar en capacidad de tomar decisiones frente a la gestión del Riesgo LA/FT/FPADM.
- Fungir como Oficial de Cumplimiento para BPM Consulting garantizando que no hay de por medio conflicto de intereses.
- Velar por el cumplimiento efectivo, eficiente y oportuno del SAGRILAFT.
- Certificar ante la Superintendencia de Sociedades el cumplimiento del sistema.
- He de asegurar que los documentos del sistema SAGRILAFT (formatos, políticas, procedimientos y autorizaciones de consulta) cuentan con la privacidad, confidencialidad y seguridad de información.
- Detectar operaciones sospechosas, evaluarlas, controlarlas y monitorearlas.
- Reportar operaciones sospechosas a la Unidad de Información y Análisis Financiera (UIAF), cuando las adviertan dentro del giro ordinario de sus labores, en cumplimiento del numeral 10 del art. 207 del Código de Comercio. Para tal efecto, debe registrarse en la plataforma Sistema de

Reporte en Línea (SIREL), administrado por la UIAF para efectuar el reporte de operaciones sospechosas.

La Compañía, dentro del Sistema de Administración de Riesgo de Lavado de Activos, Financiación del Terrorismo, Financiamiento de la Proliferación de Armas de Destrucción Masiva LA/FT/FPADM, comprende las etapas de identificación, medición, control y monitoreo.

- Identificación del riesgo
- Determinación de criterios del riesgo
- Monitoreo del riesgo

Los empleados de la Compañía, proveedores o cualquier parte interesada, que detecten una operación inusual o intentada deberán informar por medio de la página web de la organización, al Oficial de Cumplimiento de forma inmediata, el cual a su vez evaluará y analizará las operaciones reportadas con el propósito de establecer si en efecto se trata o no de una operación inusual o intentada.

Adicionalmente, se llevará una base de registros sobre operaciones internas inusuales y sospechosas para dejar constancia de aquellas situaciones en las cuales se considera que se pudo haber materializado un riesgo de LA/FT y el análisis y resultados obtenidos en cada una de ellas.

El canal que utiliza la Compañía para poner a disposición de las clientes y usuarios es:

URL: https://www.bpmconsulting.com.co/

Módulo de: PQRS

Desarrollo seguro

1. Directrices

a. Las etapas de diseño y construcción de software y aplicaciones, así como la etapa de pruebas, deben efectuarse en los ambientes dispuestos para ello por la organización o terceros contratados.
b. Durante el diseño de software y aplicaciones, los colaboradores de la organización y/o terceros especializados deberán identificar y aprobar los requerimientos de seguridad a incorporar durante las etapas de construcción e implementación.
c. La organización debe asegurar que se realice el análisis e implementación de los requerimientos de seguridad en el software y aplicaciones que se desarrollen.
d. En el análisis de factibilidad de los requerimientos, se deberá considerar el nivel de criticidad del sistema, además del nivel de protección de seguridad que requerirán los datos y las aplicaciones que lo compongan.

e. La organización definirá las metodologías de desarrollo seguro que aseguren la implementación de controles de seguridad en el desarrollo.
f. BPM Consulting o Terceros Especializados dispondrán de herramientas que permitan almacenar el código fuente de forma segura, en repositorios locales o en la nube, y con los cuales se pueda hacer control de versiones.
g. Todos los desarrollos realizados por la organización o sus proveedores deben contener controles para la protección de datos personales.
h. Todos los desarrollos realizados por la organización o sus proveedores deberán tener un proceso de pruebas que garantice la calidad del producto y la seguridad de la información.
i. El acceso a la documentación de los Desarrollos, bibliotecas de códigos fuentes y programas ejecutables, debe estar habilitado sólo a los colaboradores autorizados. La excepción a esta política, son los manuales de usuario, manuales de capacitación, u otros documentos destinados a los clientes de la organización.
j. Previo a cualquier cambio, actualización, o reconfiguración, planificada, en los servidores, bases de datos, u otros equipos asociados al desarrollo de software, se deberá gestionar los cambios de tal forma que se realicen las actividades de gestión del cambio, donde se evalúen los impactos y riesgos que puedan generar dichas actividades.
k. Se deberán planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, plan de retorno y aceptación del cambio.
l. Para propósitos de desarrollo y pruebas de software, se deberán generar datos de prueba distintos a los que se encuentran en el ambiente de producción y/o datos que no sean reales.
m. Si se requiere el uso de cifrado de datos, este deberá ceñirse a los lineamientos descritos en la Política del uso de controles criptográficos y gestión de llaves.
n. Todos los programas críticos deberán incluir la generación de registros de auditoría, considerando como mínimo la identidad del usuario que inactiva escribe, o actualiza, el tipo de evento y la fecha y hora de dicho evento. Estos registros deben ser protegidos contra la manipulación no autorizada.
o. No está permitido modificar programas sin que quede registrado o documentado el cambio. En caso de requerirse la implementación de un cambio, este deberá ceñirse a procedimientos de gestión de cambios.

p. No está permitido escribir o modificar código autocopiaste o cualquier otro tipo de código malicioso (virus y gusanos), así como funciones u operaciones no documentadas o no autorizadas en los programas.
q. En lo posible, las pruebas del sistema deberán incluir: instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante errores.
r. Se deberán tener las siguientes consideraciones con relación a los datos de entrada y salida de los sistemas de información:
    - Realizar las validaciones de datos de entrada y salida en un sistema confiable (por ejemplo: un servidor).
    - Validar la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como tipos de datos, rangos válidos y longitud, entre otros.
    - Validar el intento de ingreso de bytes nulos, caracteres de nueva línea o caracteres de alteración de rutas.
    - Limpiar las salidas de datos no confiables hacia consultas SQL, XML y LDAP o hacia comandos del sistema operativo.
s. Se deberán establecer los siguientes controles para la autenticación en los sistemas de información:
    - Realizar los controles de autenticación en un sistema confiable (por ejemplo, un servidor).
    - Si la aplicación administra un almacenamiento de credenciales, asegurar que únicamente se almacena el hash de las contraseñas.
    - Validar los datos de autenticación, luego de haber completado todos los datos de entrada.
t. Se deberá realizar una gestión de las sesiones, que tenga en cuenta los siguientes aspectos:
    - Realizar la creación de identificadores de sesión en un sistema en cual se confíe (por ejemplo: el servidor).
    - Garantizar la existencia de opciones de desconexión o cierre de sesión de los aplicativos (logout) que permita terminar completamente con la conexión asociada.
    - No exponer los identificadores de sesión en URL, mensajes de error ni logs, y no transmitirlos como parámetros.

- He de asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- He de asegurar que la sesión expire después de cierto tiempo.
- No permitir la apertura de sesiones simultaneas con el mismo usuario.

u. Todas las funciones de criptografía de las aplicaciones desarrolladas deben ser implementadas en sistemas confiables (por ejemplo: el servidor).
v. Se deben considerar los siguientes aspectos en el manejo de errores:
   - Garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios. Los mensajes de error deben ser genéricos.
   - En el manejo de archivos se deberá prevenir la revelación de la estructura de directorios de los sistemas construidos.
w. Para el establecimiento de conexión a las bases de datos se deberán considerar los siguientes aspectos:
   - No incluir las cadenas de conexión a las bases de datos en el código de los aplicativos.
   - Cerrar la conexión a las bases de datos desde los aplicativos, tan pronto como estas no sean requeridas.
x. Se deberán desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación y almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos.
y. No se deberá incluir en parámetros, nombres de directorios o rutas de archivos. En su lugar, se deben utilizar índices que internamente se asocien a directorios o rutas predefinidas.
z. Se deberá garantizar la protección del código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

2. Normas de seguridad para la documentación del software

a. El diccionario de datos, o repositorio de metadatos, deberá mantener una descripción actualizada de las definiciones de datos.
b. Si el desarrollador incluye comentarios en el programa fuente, estos no deben divulgar información de configuración innecesaria.

c. La documentación de los desarrollos deberá:
   - Generarse para todos los desarrollos de la organización.
   - Ser revisada por los usuarios finales del sistema en desarrollo
   - Actualizarse si el programa cambia alguna de sus funcionalidades.
   - Almacenarse en un sitio centralizado.

3. Restricciones del Cambio a los Paquetes de software

a. La introducción de nuevas funcionalidades y cambios importantes en los desarrollos de la organización, deberán contar con un proceso de gestión del cambio.
b. En los casos en que sea necesario realizar cambios en paquetes de software suministrados por proveedores, de se deberán tener en cuenta las siguientes condiciones:
   - Demostrar que el cambio es necesario para la organización.
   - Analizar los términos y condiciones de la licencia de uso, a fin de determinar si las modificaciones se encuentran autorizadas.
   - Aplicar los procedimientos de gestión del cambio en la organización.
c. En todos los casos se deberá mantener una versión del software original. Los cambios se realizarán sobre una copia perfectamente identificada.
d. Todos los cambios en paquetes de software que han sido suministrados por proveedores deberán ser validados, revisados y/o documentados.

4. Desarrollo contratado externamente

BPM Consulting podrá contratar desarrollos externos para dar cumplimiento a los requisitos de la organización. Para los casos en que se considere la tercerización del desarrollo de software, se establecerán las siguientes directrices dentro de los acuerdos firmados con el proveedor:

a. Cláusulas con relación al licenciamiento, propiedad de código y derechos de propiedad Intelectual.
b. Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
c. Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos.

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 talento humano o al gerente de mejora e innovación o quien haga sus veces.

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 ajusto la declaración de la política, se adicionan los objetivos y el responsable, se actualizan los ítems de las políticas que hay de seguridad.