OBJETIVO:	Establecer los lineamientos relacionados con la gestión de la Seguridad de la Información, que deben ser cumplidos por los proveedores que suministran productos/servicios a la organización.
ALCANCE:	Aplica para todos productos/servicios entregados por los proveedores y que puedan afectar la confidencialidad, integridad y disponibilidad de la información/servicios de BPM Consulting SAS. Incluye los proveedores de servicio en la nube, TIC, componentes de infraestructura TIC, equipos de cómputo, sistemas de información, plataformas, aplicaciones, servicios de vigilancia y seguridad, servicios públicos, mantenimientos a la infraestructura física.
DOCUMENTOS ASOCIADOS:	Política de Control de Acceso Lógico Política de Control de Acceso Físico Política Transferencia de Información Procedimiento de Back Up y transferencia de información Procedimiento Gestión del Cambio Acuerdo de Confidencialidad

TERMINOS Y DEFINICIONES

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.

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

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.

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.

Acuerdos de Nivel de Servicio (ANS): Es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.

ESPECIFICACIONES DE LA POLITICA

Alcance en la prestación del servicio y Definición de ANS

- El contrato firmado entre las partes debe definir los tipos de componentes y servicios que proporciona el proveedor y que pueda afectar la confidencialidad, integridad y disponibilidad de la información de la organización y/o del servicio.

- BPM Consulting y el proveedor deben definir con claridad y de manera explicita los Acuerdos de Niveles de Servicio técnicos, operativos, de manejo de información (incluye copias de seguridad periódicas, back up al final del servicio, borrado seguro, transferencia de datos), administrativos (ej. entrega de informes periódicos, reuniones de seguimiento, revisión periódica de controles de seguridad) y de personal, que son necesarios para abordar la prestación/entrega de los productos/servicios, que el proveedor suministrará a la organización. Estos ANS deben quedar escritos en el contrato o en los anexos que hagan parte integral de este.

- En la definición del alcance del servicio se requiere que BPM Consulting y el proveedor determinen, según el tipo de servicio a prestar, el acceso a:

  - Información sensible de los clientes / usuarios del cliente / información privada o confidencial de la empresa.
  - Infraestructura física /lógica sensible que impacta en la prestación de los servicios de BPM Consulting o la operación interna de la organización.

Dichas definiciones deberán hacer parte del alcance indicado en el contrato o sus anexos técnicos y deben servir para dar claridad sobre la información, servicios TIC, infraestructura física a la cual el proveedor podrá acceder, utilizar y/o administrar según sea el caso. Deberán seguirse las políticas de control de acceso lógico y control de acceso físico de BPM Consulting, según sea el caso.

- Toda instalación, configuración o mantenimiento por parte de proveedores a la infraestructura tecnológica de la compañía, tales como servidores, equipos de red, equipos de soporte, cableado estructurado, de energía, entre otros, deberá cumplir con los requerimientos establecidos por la Gerencia de Tecnología e Infraestructura y la Gerencia Administrativa y Financiera (para los mantenimientos en la infraestructura física de las instalaciones). Estas áreas serán responsables de verificar y validar estas configuraciones y/o mantenimientos, así como también de reportar las debilidades y oportunidades de mejora al proveedor. En los casos que corresponda, BPM Consulting deberá seguir las indicaciones determinadas en el procedimiento de Gestión del Cambio de la organización.

Uso de la información y de los recursos

- El proveedor deberá incluir en su contrato la debida cláusula de confidencialidad y de igual manera firmar el documento “Acuerdo de Confidencialidad” entregado por BPM Consulting.

- Toda información confidencial de la organización que deba ser intercambiada o transferida por parte del proveedor deberá realizarse de forma segura, utilizando mecanismos de cifrado, por medios seguros y autorizados por el Gerente de Tecnología e Infraestructura. Se deberán seguir los lineamientos determinados en la política de transferencia de información señalada por BPM Consulting.

- El proveedor es responsable por la confidencialidad de la información de BPM Consulting a la que acceden sus colaboradores y deberá mantener con ellos acuerdos de no divulgación de la información. El acceso de estos colaboradores se define como temporal y por ello no existe derecho alguno de titularidad o copia sobre dicha información. Entendiendo lo anterior,

el proveedor deberá devolver toda la información facilitada por BPM Consulting, inmediatamente después de la finalización de las tareas que han originado el uso temporal de la información y, en cualquier caso, a la finalización de la relación contractual.

- En caso de que el proveedor requiera información de los sistemas de información/plataformas de BPM Consulting, adicional a la autorizada o establecida en el acuerdo contractual o que no esté relacionada con el objeto de su servicio, deberá notificar por correo electrónico al Gerente de Tecnología e Infraestructura, quien dará tratamiento a esta solicitud conforme las definiciones de la política de control de accesos lógicos. En los casos de información física, queda a potestad del propietario del activo de información habilitar los accesos pertinentes. No obstante lo anterior deberá quedar un registro por escrito de la solicitud y su respuesta, la cual deberá ser compartida con el Oficial de Seguridad.

- En caso de que el proveedor requiera acceso a herramientas o activos tecnológicos de BPM Consulting, deberá gestionar a través del propietario del activo una solicitud de excepción de seguridad, que deberá quedar por escrito con la respectiva respuesta (aprobación/negación) y siguiendo las directrices de la política de control de acceso lógico.

- BPM Consulting prohíbe de manera expresa, el uso de los recursos proporcionados por la organización, para actividades no relacionadas con el servicio contratado. Así mismo, prohíbe conectar en la red de la compañía cualquier tipo de malware (programas, macros, etc.), dispositivos lógicos, dispositivos físicos o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos y sistemas de información.

Gestión y Tratamiento de los Riesgos

- BPM Consulting solicitará al proveedor las definiciones que ha determinado para el tratamiento de sus riesgos de seguridad de la información, asociados con los productos/servicios contratados y también, aquellos riesgos relacionados con su cadena de suministro (se deben incluir las personas como un componente del riesgo), y que afecten la continuidad, disponibilidad e integridad de la información y el servicio ofrecido. Lo anterior con el fin de validar que el proveedor ha contemplado los riesgos de su cadena de valor, que pueden impactar en la prestación a conformidad de los servicios contratados por la organización.

- BPM Consulting podrá sugerir acciones o controles conforme el resultado de la operación de los servicios contratados/entregados.

Gestión de incidentes, escalamiento funcional y jerárquico

- El proveedor que suministre servicios relacionados con almacenamiento de información, comunicación, infraestructura tecnológica (física/lógica), plataformas o sistemas de información deberá establecer y documentar procedimientos para la gestión de incidentes de seguridad y ciberseguridad. Estos procedimientos deben ser notificados por escrito a

BPM Consulting, para que la organización conozca con exactitud los mecanismos definidos para la notificación, escalamiento, tiempos de respuesta, tiempos de solución y puntos de contacto (persona de contacto, # telefónico y/o correcto electrónico) en la gestión de los incidentes.

- El proveedor deberá reportar en un tiempo no mayor a 24 horas luego de identificado el incidente, al Gerente de Tecnología e Infraestructura, así como al Oficial de Seguridad de BPM Consulting, cualquier evento sospechoso o incidente de seguridad de la información que comprometa la confidencialidad, disponibilidad e integridad del servicio prestado por los proveedores y/o la información de propiedad de la BPM Consulting, sus clientes y/o usuarios finales.

- BPM Consulting podrá solicitar informes o evidencias que permitan conocer el incidente, validar el tratamiento y solución dado, al igual que las lecciones aprendidas que se identifiquen en el proceso de gestión del incidente. Estas evidencias deberán conservarse por un tiempo mínimo de 6 meses y de ser necesario, se solicitará al proveedor la implementación de un plan de atención al incidente, para disminuir la probabilidad de reincidir en el mismo o que existan eventos de similares características.

- En el caso de incidentes mayores, además del escalamiento funcional, el proveedor deberá dar a conocer al inicio de la relación contractual, los datos de los colaboradores a los cuales debe dirigirse BPM Consulting para el tratamiento inmediato de las situaciones (ej. Gerente de Proyecto, Gerente de TI, Subgerente, Gerente).

Borrado Seguro de la Información

- En los casos que aplique y conforme el alcance del servicio contratado, el proveedor deberá garantizar el borrado seguro de la información propiedad de BPM Consulting conforme los ANS establecidos entre las partes. Este borrado deberá ser ejecutado una vez finalice la relación contractual y también de forma adicional por solicitud expresa de BPM Consulting, en cualquier momento de la relación contractual. En cualquiera de los casos, deberá entregar un reporte que demuestre las evidencia de borrado con las fechas correspondientes (ej. logs, print screen).

- Previo al borrado seguro, el proveedor garantizará la entrega de una copia (back up) con toda la información a BPM Consulting. El medio dispuesto para la entrega de esta copia será en común acuerdo entre las partes.

Continuidad del Negocio

- Para garantizar la disponibilidad del servicio contratado, el proveedor deberá contar con un plan de continuidad del servicio debidamente documentado, probado y actualizado (por lo menos una vez al año), que tendrá disponible para el momento en que BPM Consulting considere pertinente su solicitud y consulta.

Multas, sanciones, penalizaciones

- BPM Consulting trasladará las multas, sanciones y/o penalizaciones impuestas por sus clientes, producto de los incumplimientos en cualquiera de los ANS pactados con el proveedor y que afecten la confidencialidad, integridad y disponibilidad del servicio y/o información de clientes/usuarios finales de la organización,

Acceso a las instalaciones

- En caso de que el proveedor deba tener colaboradores en las oficinas de BPM Consulting para el desarrollo de labor, deberá informar con días de antelación a la Gerencia Administrativa y Financiera mediante correo electrónico, el motivo de la visita, las fechas y horarios de asistencia en las instalaciones, los elementos informáticos requeridos, los accesos a áreas restringidas (en caso de que la labor lo amerite), el o los responsables de su estadía en las instalaciones, al igual que la respectiva identificación de las personas que asistirán. Estas personas deberán estar debidamente identificadas durante su permanencia en las instalaciones de la Compañía, portando en un lugar visible su identificación, en cumplimiento de la política de Seguridad de Control de Acceso Físico de BPM Consulting.

Reuniones de seguimiento y control, Auditoria a Proveedores

- BPM Consulting verificará las condiciones de seguridad implementadas por el proveedor, teniendo en cuenta el alcance del contrato y sus anexos, a través de reuniones de seguimiento y control que serán concertadas entre las partes y ejecutadas como parte de la gestión del contrato. Producto de estas reuniones podrán existir compromisos entre el proveedor y el cliente que deberán ser gestionados y tramitados en aras de minimizar los riesgos y garantizar la confidencialidad, disponibilidad e integridad de la información y/o los servicios entregados.

- De igual manera, podrá realizar auditorías de segunda parte, con el fin de supervisar el cumplimiento de los requisitos de Seguridad de la Información determinados por el proveedor, especialmente para aquellos proveedores que son considerados críticos para la organización.

Finalización de la relación contractual

- Al concluir la relación contractual, el colaborador responsable de la gestión y administración del contrato debe notificar la culminación de la relación contractual a la Gerencia de Tecnología e Infraestructura, Gerencia Administrativa y Financiera, Gerencia de Talento Humano y Cultura, con el fin de asegurar los siguientes elementos:

    - Retiro de los derechos de acceso
    - Tratamiento de la información
    - Titularidad de la propiedad intelectual desarrollada durante la relación contractual
    - Portabilidad de la información en caso de cambio de proveedor o de recurso interno (insourcing)

- Gestión de documentos
- Devolución de activos
- Eliminación segura de la información y otros activos asociados
- Requisitos de confidencialidad
- Evaluación /Reevaluación del proveedor, según corresponda
- Cierre de procesos de facturación, de ser necesario
- Culminación de procesos de vinculación de colaboradores

Tratamiento de Datos

Conforme lo determina la Política de Tratamiento de Datos que se encuentra disponible para las partes interesadas en la página web corporativa https://www.bpmconsulting.com.co/ , los datos de los proveedores son tratados para: solicitar bienes o servicios, gestionar la entrega de insumos adquiridos, retroalimentar sobre su desempeño y gestionar las actividades de pago.

Divulgación de la presente política

Esta política estará disponible para consulta de las partes interesadas en la pagina web corporativa https://www.bpmconsulting.com.co/ . No obstante lo anterior. BPM Consulting establecerá los canales de comunicación que considere apropiados, para entregar a cada proveedor el presente documento.

Peticiones, Quejas, Reclamos, Solicitudes, Felicitaciones

BPM Consulting ha dispuesto a través de su pagina web corporativa https://www.bpmconsulting.com.co/ , la sección de PQRSF para que el proveedor presente sus solicitudes, conforme lo considere pertinente. Para identificar el requerimiento, por favor indicar en el campo asunto, la palabra ***"proveedor".***

CUMPLIMIENTO

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

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA DE APROBACIÓN**	**CONTROL DE CAMBIOS**
01	16-11-2020	Creación de la política
02	02-04-2024	Actualización del documento en todo su contenido.