Política de Relación con Proveedores

1. Objetivo

Establecer directrices y controles que garanticen el cumplimiento de los ANS y la protección de los Activos de Información a los que tengan acceso los proveedores de Contento BPS, en relación a la Confidencialidad, Integridad, Disponibilidad y Responsabilidad Legal.

2. Alcance

Esta política es aplicable a todos los proveedores y terceras partes vinculadas con Contento BPS, y que, en el cumplimiento del compromiso contractual, tengan acceso a la información interna y/o confidencial de la compañía.

3. Introducción

Contento BPS, como complemento a la Política Corporativa de Seguridad de la Información, implementa los presentes lineamientos con finalidad de asegurar la adecuada gestión de la Seguridad de los datos almacenados, procesados, y transferidos a través de los diferentes sistemas y medios para el desarrollo de las funciones contractuales con proveedores y/o terceros.

La gestión de los proveedores de Contento BPS, es una actividad que requiere tercerizar un servicio para el logro de los objetivos del negocio, el cual busca incrementar la productividad y mejorar los procesos por medio de estrategias que se proveen desde partes externas.

Finalmente los líderes de procesos mediante la gestión de proveedores, busca establecer relaciones de confianza y de valor agregado con terceras partes que signifiquen un retorno tangible en la promesa de prestación de los servicios con los clientes.

4. Definiciones

Proveedores vinculados: *Todos aquellas terceras partes que tienen una relación comercial activa o lo vincule un acuerdo de cumplimiento previamente firmado luego de la terminación de la relación contractual.*

SFTP: *Protocolo Seguro de Transferencia de Archivos.*

VPN: *Red Privada Virtual.*

Hosting: *Servicio de alojamiento externo de recursos de Tecnologías de Información.*

ANS: *Acuerdos de Niveles de Servicio.*

Contingencia: *Actividades de control que permite la continuidad de operaciones en eventos no programados que suspendan la funcionalidad del negocio.*

Intranet: *Servicio web corporativo interno*

Situación de crisis: *Es la pérdida de control sobre las operaciones de: Infraestructura física y tecnológica, soporte TIC y personal (Recurso Humano), por una falla inesperada o no programada de alguno de sus componentes en operación.*

Impacto: *El coste para la empresa de un incidente (de la escala que sea), que puede o no ser medido en términos estrictamente financieros ej., pérdida de reputación, implicaciones legales, etc.*

Análisis de Impacto al Negocio (BIA): *Análisis realizado a los procesos críticos de la compañía, donde se determina el impacto que puede ocasionar al negocio una irrupción a los mismos; permitiendo obtener información para el desarrollo de los planes de restauración de los servicios de los procesos de Infraestructura física y tecnológica, soporte TIC y personal (Recurso Humano) ofrecidos a los clientes de CONTENTO BPS.*

5. Propósito

Contento BPS establece directrices que permitan el relacionamiento con los proveedores, estableciendo como prioridad la seguridad de sus activos de información, de acuerdo a los objetivos establecidos por los procesos de la organización, generando confianza entre las partes.

6. Marcos de referencia

- *NTC – ISO/IEC – 27001: Sistema de Gestión de Seguridad de la Información. (A.15.Relacion con los proveedores)*
- *NTC – ISO – 22301: Sistema de Gestión de Continuidad del Negocio.*
- *NTC – ISO – 20000: Gestión de los Servicios de T.I*

7. Compromisos de la empresa

Contento BPS es consciente de la importancia de las buenas prácticas y acuerdos establecidos e implementados con los proveedores, dando cumplimiento mediante actividades de monitoreo, revisión y mejora continua para garantizar la satisfacción entre las partes.

8. Marco sancionatorio

El componente legal y las implicaciones del incumplimiento de la presente política serán analizados y ejecutados por el área Jurídica, Compras, Gerencia de TIC, Gestión del Talento Organizacional, la Alta Dirección, o cualquier responsable de administrar el proveedor.

9. Factores críticos de éxito

- *Desconocimiento de la presente Política por parte de los involucrados.*
- *Acuerdos de servicios establecidos sin protocolos y sin firmas.*
- *Incumplimiento de los ANS por las partes.*
- *Desconocimiento de los requisitos a cumplir entre las partes.*
- *Divulgación inoportuna de la Política y/o de cambios en la misma.*
- *Ausencia de acuerdos de confidencialidad y transferencia de información.*
- *Incumplimiento en la cláusula de auditoría y revisión a proveedores.*

10. Declaración de la política

Esta Política de Relación con Proveedores se integra a la normativa básica de la empresa, incluyendo su difusión y las sanciones correspondientes por incumplimiento de la misma.

Seguridad de la Información en las relaciones con los proveedores.

Para los servicios tercerizados de infraestructura, plataforma tecnológica, procesamiento y almacenamiento de información física o digital y recursos humanos, Contento BPS verifica que el proveedor cuenta con mecanismos de protección y controles de seguridad de información adecuados al objeto del servicio contratado.

Así mismo, se deberá realizar una evaluación de requisitos de seguridad asociados al servicio entregado por el proveedor, con la finalidad de identificar brechas que puedan ser potenciales vulnerabilidades que expongan la continuidad operativa de los procesos o puedan dañar la imagen Institucional. Ver Requisitos de proveedores.

- *Ver Formato de Requisitos a Proveedores de S.I.*

En materias de seguridad y tecnología

El Líder de Compras es el encargado de validar la oportuna y eficaz contratación de servicios o productos que tengan relación con el tratamiento, almacenamiento, manipulación, transmisión o resguardo de los activos de información, tales como almacenamiento de documentos, compra de servidores, adquisición de dispositivos móviles, construcción de sistemas, desarrollo de sitios Web, servicios de infraestructura tecnológica, softwares como servicio, y demás componentes relacionados.

Las validaciones estarán en relación al costo y al beneficio obtenido por Contento BPS, teniendo en cuenta el ciclo de vida de la relación.

Autorización y entrega de información adicional

En el caso en que un proveedor requiera información de la organización adicional a aquella establecida en los acuerdos contractuales, o que no sea inherente a la naturaleza del mismo, el propietario de la información analizará los motivos de dicho requerimiento y procederá a aprobar o rechazar la entrega de la misma con previo consentimiento del Líder de seguridad de la Información.

Acceso físico a los activos de información y equipos tecnológicos

El acceso físico por parte de los proveedores a los activos de información de Contento BPS, deberá ser controlado y supervisado por el personal de seguridad (vigilancia) y de tecnología asignado para esta labor. En las áreas protegidas o de alto riesgo, como es el caso del Datacenter, se establecen normas que tienen por objeto gestionar la forma en que se realizarán los trabajos en su interior, y restricciones preventivas, como el lector biométrico para el ingreso a la instalación.

El área de seguridad física debe controlar el acceso a empleados y terceros por medio de torniquetes en las operaciones y carnet en las áreas de apoyo, dependiendo de la finalidad de la prestación del servicio o una visita programada; Adicionalmente, se debe llevar un registro de estos controles, así como del personal que entra y sale, además de las actividades que realizan en las áreas identificadas como seguras para la compañía.

Acceso remoto a través de herramientas informáticas

Los proveedores podrán acceder en forma remota a los activos tecnológicos de Contento BPS únicamente a través de herramientas tales como SFTP o la Red Privada Virtual (VPN), cuando ello sea necesario para el cumplimiento de las obligaciones que resulten del respectivo contrato.

En caso contrario, deberá solicitarse una autorización especial al Líder de Seguridad de la Información, quien analizará los motivos de dicho requerimiento y procederá a otorgarlo o denegarlo.

En cualquier caso, dicho acceso será gestionado por el área correspondiente dueño del proveedor al área de Tecnología y Comunicaciones, prestando a su vez servicios de seguridad y/o monitoreo. Para garantizar lo anterior, la organización implementa controles que permitan limitar el acceso. (Ver Política de Control de Acceso)

Contratación de servicios tecnológicos

Cuando se requiera elaborar un contrato particular con proveedores que tenga relación con servicios de tratamiento, manipulación, transmisión o almacenamiento de activos de información, ya sea en formato físico o digital; se deberán incorporar cláusulas de seguridad que permitan garantizar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, tales como acuerdos de niveles de servicios (ANS), derechos de auditar los procesos involucrados, los procedimientos aplicados frente a incidentes de seguridad, cláusulas de confidencialidad y no divulgación de información (Ver acuerdo de Transferencia de Información), como también la extensión de las obligaciones de cumplimiento de empresas subcontratadas. (Gestión de Incidentes)

Gestión de Cambios en los Servicios de Proveedores *(A.15.2.2 Gestión de cambios en los servicios de los proveedores)*

Mediante el Procedimiento de Gestión de Cambios se establecen las condiciones en las cuales un cambio puede ser aceptable para su ejecución.
Ver – Procedimiento de Gestión de Cambios

Seguridad en la instalación y configuración de activos tecnológicos

Cuando los proveedores requieran hacer instalaciones de activos de información de carácter tecnológico, tales como servidores, equipos de red, equipos de soporte, entre otros, será requisito implementar configuraciones que cumplan con las políticas de seguridad de la información de Contento BPS, así como la entrega de un análisis de vulnerabilidad reciente a los mismos.

Igualmente, el área de TIC será responsable verificar y validar la configuración de los equipos instalados, así como también de reportar las debilidades y oportunidades de mejora al proveedor.

Posibilidad de inspeccionar y auditar las condiciones del servicio y la seguridad de la información

Para asegurar que los proveedores que prestan servicios a CONTENTO BPS, cuenten con estándares de industria en materia de seguridad; la organización se reserva el derecho de solicitar evidencia de la ejecución de auditorías independientes relacionadas al riesgo tecnológico, control interno, o auditorías de certificación relacionados con dicha materia, los cuales deben ser facilitados de manera confidencial y con el objeto de revisar el alcance del trabajo realizado y el detalle de los resultados obtenidos.

Adicionalmente, la organización también podrá realizar visitas programadas y supervisadas, así como solicitar auditorias para verificar el cumplimiento de los ANS, acuerdos de confidencialidad y demás controles de cara a la seguridad de la información a la que estos tienen acceso; todo esto coordinado con anterioridad.

Acuerdos de custodia y confidencialidad de la información *(A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores)*

En el caso en que se requiera entregar información a proveedores, o que producto de la prestación del servicio el proveedor acceda a información de la organización, se deberán aplicar acuerdos de confidencialidad y no divulgación entre Contento BPS y el proveedor, el que deberá especificar los responsables, la información en cuestión, las medidas mínimas de seguridad aplicadas, la forma de proceder frente a incidentes, la extensión del acuerdo a terceros subcontratados, la propiedad de los productos desarrollados, el tiempo de vigencia del acuerdo, la transferencia de información, el tratamiento de datos personales, las sanciones frente a su incumplimiento y su aceptación formal.

Seguridad en el intercambio de información con proveedores

En todo intercambio de información entre Contento BPS y los proveedores, se deberá implementar estándares y procedimientos formales asociados al intercambio de información, que permitan garantizar razonablemente la seguridad en el acceso y la transferencia de datos, considerando la aplicación de cifrado en las comunicaciones y la validación de identidad. (Ver Cifrado de Información y Política de Intercambio de información).

Para el caso en que existan proveedores que requieran acceder a información interna o confidencial a partir de una solicitud específica, se deberá hacer la entrega en los medios establecidos, que consideren mecanismos criptográficos basados en las políticas establecidas.

Requisitos de certificación de seguridad de los proveedores

Los proveedores que brinden sus servicios a la organización, deberán contar con certificaciones vigentes relativas a la seguridad de la información, aplicada a los procesos de servicios que se contraten. (Requisitos a Proveedores de S.I.)

Dichas certificaciones podrán contemplarse además como requerimientos y/o factores de evaluación en los procesos de licitación, así como también a los procesos internos para la adopción e incorporación de mejores prácticas aplicadas los procesos de compra. (Selección, Evaluación y Reevaluación de Proveedores)

Cadena de Suministro *(A.15.1.3 Cadena de suministro de tecnología de información y comunicación)*

Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación, garantizando de que los productos de tecnología de información y de comunicación funcionen en la forma esperada.

Se debe definir reglas para la comunicación de cualquier evento entre la organización y los proveedores, dando manejo adecuado a las inconsistencias e incidentes de Seguridad de la Información.

Manejo de incidentes de seguridad asociados a los servicios

Para los proveedores que tengan relación con almacenamiento, comunicación, infraestructura, plataforma o software que sean brindados a la Contento BPS en modalidad de servicio, también conocidos como servicios en la nube, además de los equipos tecnológicos que sean adquiridos o sistemas de información que sean desarrollados por terceros y sobre los cuales existan garantías del fabricante, se deberán establecer y documentar procedimientos para la gestión de incidentes de seguridad, los que serán gestionados a través de la mesa de ayuda, bajo los procedimientos internos ya definidos. (Ver Gestión de Incidentes)

Los procedimientos para la gestión de incidentes que estén relacionados con proveedores, en los términos referidos en el párrafo anterior, deberán ser comunicados y formalizados entre las partes. Así mismo Contento BPS, podrá solicitar informes relacionados a los incidentes de algún período, información que deberá estar disponible durante el tiempo de relación con el proveedor y la Organización. El procedimiento de seguridad para la gestión de incidentes en cada caso deberá señalar, la persona de contacto, así como el número telefónico y/o correo electrónico al cual habrá que dirigir las solicitudes. (Ver Formatos de Registro de Eventos e Incidentes de S.I)

Acuerdos de niveles de servicios (ANS) y los planes de recuperación

Contento BPS considera relevante mantener la disponibilidad permanente de los servicios entregados por los proveedores, para lo cual se deberán establecer acuerdos de niveles de servicio que permitan garantizar razonablemente este principio, los que deberán ser formalizados a través de bases de licitación, actos administrativos o acuerdos complementarios, siendo estos medidos y monitoreados permanentemente.

El área requirente del servicio, conjuntamente con el departamento técnico de la Organización, deberán verificar la existencia de planes de contingencia para efectos de validar que estos cumplen de buena forma con el criterio de disponibilidad del servicio y los datos.

Monitoreo sobre los servicios tecnológicos externalizados

Para el caso de servicios asociados a tecnología y sistemas, será responsabilidad del área de TIC incorporar en su control de monitoreo, la disponibilidad de los servicios tecnológicos, plataformas de infraestructura y los sistemas de información que sean entregados por el proveedor, con la finalidad de medir los niveles del servicio y gestionar de manera oportuna cualquier evento que puedan afectar el principio de disponibilidad.

En la medida que el área requirente necesite información detallada del servicio o sus equipos, podrá solicitar un informe sobre la disponibilidad del servicio dentro de un período determinado, incluyendo el rendimiento de los equipos en caso que se haya sido acordado previamente entre las partes.

Seguimiento y Revisión *(A.15.2.1 Seguimiento y revisión de los servicios de los proveedores)*

La Organización revisa periódicamente la prestación de los servicios contratados con los proveedores, para el cumplimiento de lo anterior, se establece el Procedimiento de Selección, Evaluación Y Reevaluación de Proveedores y el Formato de Evaluación Proveedores.

Entrega y difusión de las políticas de seguridad a proveedores

Para facilitar el acceso a estas normativas de seguridad por parte de los proveedores, Contento BPS establece las directrices acordadas con cada proveedor para su

conocimiento y aplicación, conservando el grado de responsabilidad y confidencialidad a los activos de información que se tenga accesos según el objetivo de la prestación de sus servicios.

11. Actualización

La actualización, el seguimiento y evaluación del nivel de cumplimiento de los requisitos de esta Política se realizará anualmente o en caso de cambios o modificaciones significativos en los procesos.

12. Vigencia

Esta política es aprobada por la alta dirección, comunicada y de cumplimiento según el alcance a partir de la fecha.

Dado en la ciudad de Medellín a los 12 días del mes de Abril de 2022 se aprueba por el Representante Legal.

DAVID RODRIGUEZ
Representante Legal

CRISTIAN SANCHEZ
Gerente de Compras

APROBACION Y OFICIALIZACION

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

MODIFICACIONES /ACTUALIZACIONES

VERSIÓN	FECHA (año- mes)	DESCRIPCIÓN RESUMIDA DE LA MODIFICACIÓN / ACTUALIZACIÓN / ANULACIÓN
00	*2018-09*	*Creación*
01	*2019-05*	*Actualización de información*
02	*2021-07*	*Migración del proceso seguridad de la información al proceso de Compras*
03	*2022-02*	*Actualización de información*
04	*2022-04*	*Actualización de información*