ANEXO 2. ALCANCE AL CUMPLIMIENTO DE LAS NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA EL RELACIONAMIENTO CON EL PROVEEDOR DE SERVICIOS TECNOLÓGICOS EN SERVICIOS POSTALES NACIONALES S.A.

El oferente se compromete al cumplimiento de las normas de seguridad y ciberseguridad de SERVICIOS POSTALES NACIONALES S.A. bajo el siguiente alcance:

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Definir, aprobar, formalizar, publicar y comunicar hacia todos los empleados las políticas y directrices corporativas relacionadas con la seguridad de la información, esta política debe ser creada considerando las buenas prácticas y contener cómo mínimo los siguientes temas: Control de acceso, control de cambios, clasificación y manejo de la información, seguridad física y ambiental, roles y responsabilidades con la seguridad de la información, gestión de eventos e incidentes de seguridad, escritorios y pantallas limpias, equipos desatendidos, gestión segura de contraseñas, uso aceptable de la red, los canales de comunicaciones, el internet, el correo electrónico, el software, los recursos informáticos, entre otros. Con base en esta política se deberá establecer un conjunto de estándares, técnicas o procedimientos necesarios para tratar adecuadamente todos los aspectos de seguridad de la información presentados en dicha política.

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Garantizar la identificación, el análisis, la evaluación y el tratamiento de los riesgos de seguridad de la información propios y de sus terceros subcontratados que hacen parte de la cadena de suministros de los servicios prestados a SERVICIOS POSTALES NACIONALES S.A.

Exigir el manejo adecuado y seguro de los servicios tecnológicos a los terceros subcontratados, cuando estos pueden o tiene el acceso a la información de SERVICIOS POSTALES NACIONALES S.A. Contar con la metodología y los procedimientos adecuados para identificar y gestionar oportunamente los riesgos sobre la información cuando esta es conocida y manejada por terceros.

Informar una vez durante la vigencia del contrato o cada vez que SERVICIOS POSTALES NACIONALES S.A. lo requiera, los riesgos identificados junto con su análisis de criticidad y planes de tratamiento, esto con el fin de actualizar el panorama de riesgos y tener el entendimiento de los impactos que estos tendrán sobre el negocio y las operaciones.

Como parte de la gestión de riesgos se debe contar con un repositorio de eventos e incidentes, los cuales deben ser analizados y tratados oportunamente.

CONCIENCIACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Brindar a los empleados vinculados a los servicios que son prestados a SERVICIOS POSTALES NACIONALES S.A., la educación y la formación apropiada en seguridad de la información y ciberseguridad, cuyos programas deberán dictarse por lo menos una vez al

año y ser impartidas en el proceso de inducción de los nuevos colaboradores. Los programas de capacitación deberán evidenciarse a través de los registros de participación y evaluación.

SEGURIDAD DEL RECURSO HUMANO

Realizar las verificaciones de antecedentes de todos los candidatos a un empleo, considerando las leyes, regulaciones y la ética pertinente. Estas verificaciones deben ser proporcionales a los requisitos del negocio y a la clasificación o sensibilidad de la información a ser utilizada por el cargo.

Los acuerdos contractuales con los empleados y contratistas deben establecer las consideraciones y responsabilidades de seguridad de la información.

Los empleados o el personal a cargo del proveedor deben recibir la educación y la formación apropiada en concienciación de seguridad y ciberseguridad, recibiendo regularmente las actualizaciones de las políticas y de los procedimientos de seguridad de la información que sean aplicables al cargo que se está desempeñando.

Contar con un proceso formal y comunicado hacia el interior de su organización, para emprender acciones contra los empleados que hayan cometido violaciones a la seguridad de la información.

Las responsabilidades y los deberes de los empleados o contratistas para con la seguridad o la confidencialidad de la información después de la terminación o el cambio de funciones laborales deben estar definidos, comunicados y aceptados. Es común encontrar estos requisitos en los clausulados de los contratos laborales.

CONTROL DE ACCESO

Los derechos o permisos de acceso a las instalaciones de procesamiento de datos de los empleados, usuarios externos y proveedores subcontratados deben ser restringidos de acuerdo con las necesidades de acceso requeridas para el desarrollo de las funciones laborales y deben ser deshabilitados, eliminados o modificados una vez haya terminado o cambiado el acuerdo contractual laboral.

ADMINISTRACIÓN DE LOS SISTEMAS

Proporcionar los recursos de seguridad necesarios para impedir que la información de SERVICIOS POSTALES NACIONALES S.A. sea extraída en medios de almacenamiento externos.

Implementar un comprensivo y aprobado proceso de gestión de incidentes sobre los sistemas y la información, que incluya: la identificación, respuesta, recuperación y la revisión posterior a la implementación de los planes de acción o tratamiento. Los eventos que afecten la operación de los servicios prestados a SERVICIOS POSTALES NACIONALES S.A. deben ser notificados a través de los canales definidos y establecidos por SERVICIOS POSTALES NACIONALES S.A. Este proceso debe incluir la identificación y gestión de los eventos e incidentes de ciberseguridad.

Contar con controles y alarmas que informen sobre el estado de los canales y las aplicaciones o sistemas utilizados en la operación, permitiendo a su vez identificar y corregir las fallas oportunamente. (Funciones de monitorización sobre la plataforma tecnológica)

Establecer los procedimientos de seguridad a seguir cuando se encuentre evidencia de la alteración o manipulación de los dispositivos o de la información.

SEGURIDAD FÍSICA

El acceso a las instalaciones y oficinas debe ser controlado en pro de proteger la información sensible o confidencial y prevenir el robo de documentos y equipos.

El acceso a las áreas de procesamiento de datos, los centros de cableado y a las zonas de alto uso de información confidencial deber ser restringido y monitoreado.

Proteger a: las instalaciones, los centros de procesamiento de datos y cableado, los equipos y los servicios de tecnología, contra ataques maliciosos, daños accidentales, amenazas naturales y acceso físico no autorizado.

CIBERSEGURIDAD

Contar con las capacidades y recursos idóneos para la atención oportuna de eventos e incidentes de ciberseguridad que puedan afectar los servicios prestados a SERVICIOS POSTALES NACIONALES S.A. El proceso de gestión de incidentes de seguridad debe contar con actividades para la prevención, protección, detección, respuesta, comunicaciones, recuperación y aprendizaje de dichos eventos e incidentes.

Notificar oportunamente a SERVICIOS POSTALES NACIONALES S.A. cuando se materialicen ataques cibernéticos que afecten la disponibilidad de los servicios prestados al cliente.

Reportar los incidentes de ciberseguridad a SERVICIOS POSTALES NACIONALES S.A. al momento que se presentara alguno, así como la gestión y solución realizada, de acuerdo al alcance establecido en el contrato.

Contar con los mecanismos de seguridad apropiados para evitar el ingreso y la proliferación de software malicioso (malware) proveniente del ciberespacio que puedan llegar a afectar la disponibilidad de la plataforma tecnológica y la confidencialidad de los datos allí almacenados.

AUDITORÍAS DE CUMPLIMIENTO

Permitir la realización coordinada de revisiones o auditorías gestionadas directamente por el personal de seguridad de la información de SERVICIOS POSTALES NACIONALES S.A. una (1) durante la vigencia de contrato y/o cada año a costo de SERVICIOS POSTALES NACIONALES S.A.

MONITOREO DE SEGURIDAD Y RESPUESTA

Monitorear periódicamente el desempeño de seguridad de los sistemas y las redes utilizados dentro de los servicios ofrecidos a SERVICIOS POSTALES NACIONALES S.A..,

esto se puede lograr empleando sistemas de detección de intrusos y el registro y análisis consistente de los eventos de seguridad.

SERVICIOS POSTALES NACIONALES S.A. podrá realizar pruebas de vulnerabilidad y penetración sobre la plataforma tecnológica dispuesta para la prestación del servicio. En caso de presentarse vulnerabilidades críticas que pongan en riesgo los servicios prestados a SERVICIOS POSTALES NACIONALES S.A. y su información, se deberán aplicar medidas correctivas de mitigación que acaten los procesos establecidos por el proveedor para la gestión de cambios.

Estas pruebas de seguridad serán ejecutadas por SERVICIOS POSTALES NACIONALES S.A. asumiendo su correspondiente costo; serán ejecutadas una vez al año bajo común acuerdo entre las partes haciendo uso de la técnica: Caja Negra y/o Caja Gris.

SEGURIDAD DE LAS OPERACIONES

Hacer seguimiento y monitoreo al uso de los recursos, con el objetivo de garantizar la disponibilidad del servicio prestado a SERVICIOS POSTALES NACIONALES S.A.

Dotar a sus terminales, equipos de cómputo y redes locales de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de los clientes o de las operaciones de SERVICIOS POSTALES NACIONALES S.A. dentro de los servicios prestados.

Establecer los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo sólo puedan ser realizados por personal debidamente autorizado.

CONTINUIDAD DEL NEGOCIO

Garantizar la continuidad del servicio y la integridad de los datos durante las interrupciones que afecten los servicios prestados a SERVICIOS POSTALES NACIONALES S.A., tales como las provocadas por fallas o no acceso a la infraestructura física donde se presta el servicio, fallas en el suministro de energía eléctrica, los imperfectos o las fallas en los equipos de cómputo, fallas de los sistemas telefónicos o en los canales de comunicaciones, ausencia de personas críticas para la operación del servicio, ausencia o incumplimiento de los terceros requeridos para la presentación del servicio.

Disponer de planes de continuidad debidamente documentados y que respondan a la recuperación de los servicios ofrecidos.

Revisar y establecer de forma conjunta con SERVICIOS POSTALES NACIONALES S.A. el tiempo de recuperación (RTO) requerido y ofertado para la operación del servicio contratado.

Asegurar ante un evento de interrupción de los servicios prestados y que sea a causa de falla propias de los procesos o servicios del proveedor, se deberá garantizar la prestación del servicio manteniendo los niveles de servicio preestablecidos.

Realizar durante la vigencia del contrato una prueba de continuidad de los servicios prestados a SERVICIOS POSTALES NACIONALES S.A.., estas deberán ser previamente informadas y coordinadas de forma conjunta con el fin de establecer si se debe involucrar

a colaboradores de SERVICIOS POSTALES NACIONALES S.A. como observadores o como participantes.

Tomar las medidas requeridas para coordinar y administrar todos los recursos necesarios durante la contingencia del servicio prestado. Entre otras actividades, tales como:

- Reemplazo o reparación de componentes o partes de los equipos que soportan el servicio.
- Personal idóneo, con la formación, capacitación y habilidades necesarias para operar los servicios prestados.
- Garantizar que los terceros requeridos para la operación del servicio tengan unos acuerdos de niveles de servicio alineados con las necesidades de la operación y se realice seguimiento para verificar su eficacia y cumplimiento.
- Garantizar los niveles de seguridad suficientes para proteger los servicios prestados a SERVICIOS POSTALES NACIONALES S.A. desde el ambiente de contingencia.

Se deberá definir durante la vigencia del contrato a un funcionario que sea el contacto directo para atender situaciones de crisis y/o de interrupción de servicios, quien estará disponible durante las situaciones en mención y adicionalmente tendrá conocimientos técnicos específicos del servicio prestado y capacidad para toma de decisiones en este tipo de situaciones.

CONTINGENCIAS TECNOLÓGICAS

Los recursos tecnológicos utilizados en la operación de los servicios prestados a SERVICIOS POSTALES NACIONALES S.A., deben contar con la capacidad suficiente para soportar la demanda actual, deben estar soportados en esquemas de alta disponibilidad y recuperación ante desastres incluyendo la operación en ambiente de contingencia en caso de ser necesario según la criticidad del servicio prestado. Considerando y aplicando las medidas de seguridad y ciberseguridad pertinentes para la protección de la información.

RESPONSABILIDAD DEMOSTRADA FRENTE AL TRATAMIENTO DE DATOS PERSONALES EN CONFORMIDAD CON LA LEY 1581 DE 2012

De acuerdo con lo establecido en la Ley 1581 de 2012 y el decreto reglamentario 1377 de 2013, se deben garantizar los controles de seguridad informática, información y ciberdefensa suficientes para proteger el acceso físico y lógico a la información privada y sensible de los clientes, como de las instalaciones y equipos de almacenamiento de datos, en pro del cumplimiento del principio de seguridad de dicho requisito legal.