El **PROVEEDOR Y/O CONTRATISTA** con base al alcance de los servicios contratados y/o productos entregados, como oferente se compromete cumplir con los siguientes requisitos transversales para la seguridad de la información de SISA, bajo el siguiente alcance:

1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El PROVEEDOR Y/O CONTRATISTA debe 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.

2. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El PROVEEDOR Y/O CONTRATISTA debe garantizar la identificación, el análisis, la evaluación y el tratamiento de los riesgos de seguridad propios y de sus terceros subcontratados que hacen parte de la cadena de suministros de los servicios prestados a SISA.

Se debe 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 SISA.

Se debe contar con la metodología y los procedimientos adecuados para identificar y gestionar oportunamente los riesgos sobre la información que hacen parte de la cadena de suministros de los servicios prestados a SISA.

Se debe informar a SISA cada mes durante la vigencia del contrato los riesgos de la información 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 podrían tener sobre el negocio y las operaciones de SISA.

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.

3. CONCIENCIACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Es responsabilidad del PROVEEDOR Y/O CONTRATISTA brindar la educación y la formación apropiada en seguridad de la información por lo menos una vez al año y ser impartidas en el proceso de inducción a todos sus empleados que puedan participar en la prestación del servicio a SISA.

Los programas de capacitación deberán evidenciarse a través de los registros de participación y evaluación.

4. SEGURIDAD DEL RECURSO HUMANO

El PROVEEDOR Y/O CONTRATISTA debe 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 que se desempeñe para los servicios prestados a SISA.

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

El PROVEEDOR Y/O CONTRATISTA debe 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.

El PROVEEDOR Y/O CONTRATISTA debe establecer 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.

5. CONTROL DE ACCESO

El PROVEEDOR Y/O CONTRATISTA debe asignar los derechos o permisos de acceso a las instalaciones de procesamiento de datos frente a los empleados, usuarios externos y proveedores subcontratados.

Las áreas deben ser restringidas 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.

6. ADMINISTRACIÓN DE LOS SISTEMAS

El PROVEEDOR Y/O CONTRATISTA debe proporcionar los recursos de seguridad necesarios para impedir que la información de SISA sea extraída en medios de almacenamiento externos.

Así mismo debe 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 SISA deben ser notificados a través de los canales definidos y establecidos por SISA, **seguridad_informacion@sisa.com.co**. 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.

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

7. SEGURIDAD FÍSICA

El PROVEEDOR Y/O CONTRATISTA debe controlar el acceso a las instalaciones y oficinas 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 las zonas de alto uso de información confidencial deber ser restringido y monitoreado en caso de afectar los servicios prestados a SISA. Así mismo debe se debe garantizar la protección contra ataques maliciosos, daños accidentales, amenazas naturales y acceso físico no autorizado.

8. CIBERSEGURIDAD

El PROVEEDOR Y/O CONTRATISTA debe contar con las capacidades y recursos idóneos para la atención oportuna de eventos e incidentes de ciberseguridad que puedan afectar los servicios prestados a SISA.

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 de seguridad informática y ciberseguridad.

También debe notificar oportunamente al área de Seguridad de la Información de SISA, a través del correo **seguridad_informacion@sisa.com.co**, cuando se materialicen ataques cibernéticos que afecten la integridad, disponibilidad y confidencialidad de los servicios prestados a SISA.

Se debe reportar inmediatamente a SISA los incidentes de ciberseguridad al momento que se presentara alguno, así como la gestión y solución realizada con base a la metodología definida por el proveedor o contratista.

Se debe contar con los mecanismos de seguridad y ciberseguridad apropiados para evitar el ingreso y la proliferación de software malicioso (*malware)* proveniente del ciberespacio que puedan llegar a afectar la seguridad, integridad y disponibilidad de los servicios proporcionados y la confidencialidad de los datos almacenados de SISA.

9. AUDITORÍAS O REVISIONES DE CUMPLIMIENTO

El PROVEEDOR Y/O CONTRATISTA debe permitir la realización coordinada de revisiones y/o auditorías en gestionadas directamente por el personal de Seguridad de la Información y Ciberseguridad de SISA como mínimo (1) vez cada año y/o durante la vigencia del contrato.

10. MONITOREO DE SEGURIDAD Y RESPUESTA

El PROVEEDOR Y/O CONTRATISTA debe realizar monitoreo periódicamente sobre el desempeño de seguridad de los sistemas, la infraestructura tecnológica y las redes utilizados dentro de los servicios ofrecidos y/o interconectados a SISA, esto se puede lograr empleando sistemas de detección de intrusos y el registro y análisis consistente de los eventos de seguridad y el descubrimiento, análisis y gestión de vulnerabilidades para su respectiva remediación con el fin de mitigar los riesgos emergentes relacionados a la seguridad de la información, privacidad de los datos y la ciberseguridad.

SISA de manera coordinada con el PROVEEDOR Y/O CONTRATISTA 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 SISA y su información, se deberán aplicar medidas correctivas de mitigación que acaten los procesos y procedimientos establecidos por el PROVEEDOR Y/O CONTRATISTA para la gestión y control de cambios.

11. SEGURIDAD DE LAS OPERACIONES

El PROVEEDOR Y/O CONTRATISTA debe hacer seguimiento y monitoreo al uso de los recursos, con el objetivo de garantizar la disponibilidad del servicio prestado a SISA.

Además debe 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 SISA dentro de los servicios prestados.

12. CONTINUIDAD DEL NEGOCIO

El PROVEEDOR Y/O CONTRATISTA debe garantizar la continuidad del servicio y la integridad de los datos durante las interrupciones que afecten los servicios prestados a SISA, tales como las provocadas por: fallas en el suministro de energía eléctrica, fallas en los equipos de cómputo o de infraestructura tecnológica, amenazas ambientales o de acceso a la infraestructura física donde se presta el servicio, fallas de las redes o en los

canales de comunicaciones, ausencia de personas críticas para la operación del servicio, ausencia o incumplimiento de los terceros requeridos para la prestación del servicio.

Con lo anterior se debe disponer de planes de continuidad debidamente documentados y que respondan a la recuperación de los servicios ofrecidos a SISA.

Se debe revisar y establecer de forma conjunta con SISA, ANS (Acuerdo de niveles de Servicio), tiempos resolución de eventos e incidentes en el marco del tiempo de recuperación (RTO) requerido y ofertado para la operación del servicio contratado.

Se deberá definir durante la vigencia del contrato a un colaborador que sea el contacto directo para atender situaciones de crisis y/o de interrupción de los servicios prestados a SISA, 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.

13. CONTINGENCIAS TECNOLÓGICAS

El PROVEEDOR Y/O CONTRATISTA debe asegurar que los recursos tecnológicos utilizados en la operación de los servicios prestados a SISA 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.

14. RESPONSABILIDAD DEMOSTRADA 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, el PROVEEDOR Y/O CONTRATISTA debe garantizar los controles, políticas y procedimientos de tratamiento de datos personales, seguridad y privacidad suficientes para proteger el acceso físico y lógico a las instalaciones y sistemas de información para la protección, aseguramiento y tratamiento de la información personal y demás clasificaciones según los señalado en la ley 1581 de 2012. A través de la implementación de la seguridad tecnológica necesaria, teniendo en cuenta todos los aspectos técnicos, administrativos, operativos y humanos; que en términos de integridad y confidencialidad garanticen la protección de los datos privados, personal y sensibles en equipos de almacenamiento de datos; en pro del cumplimiento del principio de seguridad de los requisitos legales vigentes para la protección y tratamiento de los datos personales y en cumplimiento de la política de tratamiento de datos personales de SISA.

Para los casos que el PROVEEDOR Y/O CONTRATISTA tenga acceso compartido sea a nivel de consulta, lectura o procesamiento de datos personales, privados o sensibles en el marco de los servicios proporcionados a SISA, debe actuar y cumplir la figura como encargado del tratamiento de estos datos o de la información personal, de tal forma que cumpla con las obligaciones y funciones que señala la ley 1581 de 2012.

El PROVEEDOR Y/O CONTRATISTA no podrá hacer uso de los datos personales que tenga acceso en el marco de los servicios prestados a SISA para promover campañas, realizar mercadeo o para cualquier otra razón o circunstancia, sin antes contar con la debida autorización por parte del responsable del tratamiento de los datos que es SISA y en efecto de manera previa con la autorización por parte de los titulares de la información personal.

Ante cualquier inquietud o duda de lo indicado anteriormente con base a lo normado para el cumplimiento de la Ley 1581 de 2012, puede solicitar detalle o ampliación de la información al correo proteccioninformacionpersonal@sisa.com.co

15. ACEPTACIÓN Y CONOCIMIENTO

Confirmo que he leído y entendido los requisitos de Seguridad de la Información que SISA aborda con el PROVEEDOR Y/O CONTRATISTA

Firma Proveedor:

_____

NOMBRE:

ID:

FECHA DE ACEPTACIÓN: