ANEXO N. 3 – REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DEL NEGOCIO

El proveedor debe tener en cuenta el desarrollo de los siguientes lineamientos de seguridad y continuidad del negocio, requeridos para la implementación de los servicios a prestar:

REQUISITOS GENERALES

SEGURIDAD DE LA INFORMACIÓN

- Toda la información que gestione el proveedor en el marco del contrato con Previsora es de propiedad de Previsora y debe solamente ser usada para el propósito establecido en el contrato.
- El proveedor debe realizar la entrega de toda la información manejada durante la ejecución del contrato y la destruir de la misma una vez finalizado el servicio.
- La Previsora Seguros podrá revisar los procesos que lleva a cabo el proveedor o sus subcontratistas en cualquier momento a fin de verificar los controles de seguridad implementados
- Cualquier incidente de seguridad de la información que afecte a Previsora Seguros o que involucre la información de Previsora debe ser reportado inmediatamente al supervisor del contrato y a la mesa de ayuda de Previsora.
- El proveedor debe seguir los lineamientos establecidos por la compañía para la gestión de accesos a sistemas de información, bases de datos, aplicaciones, áreas seguras, entre otras
- El contratista debe proporcionar mecanismos de protección contra códigos maliciosos a los equipos que se disponen para el servicio de previsora
- Gestionar la seguridad de la información, para lo cual podrán tener como referencia los estándares ISO 17799 y 27001, o el último estándar disponible.
- Si se va a remitir información a los clientes que sea de carácter privado mediante el correo electrónico, ésta deberá estar cifrada.
- Implementar controles de seguridad para la información privada de la Previsora, que se maneja en los equipos y redes del proveedor.
- Velar por que la información gestionada de Previsora esté libre de software malicioso.
- Dotar a sus terminales o equipos de cómputo de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.
- Velar porque los niveles de seguridad de los elementos usados en los canales no se vean disminuidos durante toda su vida útil.
- El proveedor deberá contar con planes de contingencia y continuidad aplicables a los servicios o productos prestados, debidamente documentados y probados
- "Los planes de continuidad del negocio deben cubrir por lo menos los siguientes aspectos:
  - Identificación de los riesgos que pueden afectar la operación
  - Análisis de Impacto al Negocio (BIA), especificando RTO y RPO

    - Actividades a realizar cuando se presentan fallas
    - Alternativas de operación y
    - Regreso a la actividad normal."
- El proveedor faculta a la Previsora a revisar el PCN y DRP del proveedor, con el fin de validar que los servicios convenidos funcionen en las condiciones pactadas.
- Planes de Contingencia tecnológica: Específicamente sobre la infraestructura tecnológica que apoya los servicios contratados con Previsora: Los requisitos específicos deben ser definidos por la Gerencia de TI, de acuerdo con el servicio que se contrate. En términos generales son los siguientes:
    - Estructura tecnológica de contingencia:
        - Data center alterno: En el que se repliquen todos los aplicativos, bases de datos, etc., que apalancan los servicios prestados a la compañía
        - Canales de comunicación de contingencia:
            - Principal Previsora - Principal Proveedor
            - DRP Previsora - DRP Proveedor
            - DRP Previsora - Principal Proveedor
            - Principal Previsora - DRP Proveedor"

REQUISITOS PARA SISTEMAS DE INFORMACIÓN, DESARROLLO O ADQUISICIÓN

- El proveedor debe dar garantía que los requisitos de seguridad de la información se tuvieron en cuenta antes, durante y después de la puesta en producción del sistema de información.
- El proveedor debe definir la matriz de roles y perfiles del sistema de información a proveer a Previsora
- El sistema de información debe surtir el proceso de pruebas de Ethical Hacking en la fase de pruebas y producción.
- El sistema de información debe cumplir con los requisitos de OWASP (Para aplicaciones web)
- El sistema de información debe generar trazabilidad de los eventos que se generen ya sea a nivel de aplicación o por los usuarios de la aplicación.
- Mantener documentada y actualizada, al menos, la siguiente información: parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones; versión de los programas y aplicativos en uso; soportes de las pruebas realizadas a los sistemas de información; y procedimientos de instalación del software.
- Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura.
- Realizar como mínimo dos veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de transacciones por este aplicativo. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del aplicativo, deberá realizarse una prueba

adicional; el supervisor del contrato validará el cumplimiento de este requisito cuando lo considere necesario.

- Promover y poner a disposición mecanismos que reduzcan la posibilidad de que la información de Previsora y sus transacciones pueda ser capturada por terceros no autorizados durante cada sesión.
- Configurar 15 minutos como tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.
- Informar al usuario, al inicio de cada sesión, la fecha y hora del último ingreso a este aplicativo.
- Implementar mecanismos que permitan a la Previsora verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.
- Mantener tres ambientes independientes: uno para el desarrollo de software, otro para la realización de pruebas, y un tercer ambiente para los sistemas en producción. En todo caso, el desempeño y la seguridad de un ambiente no podrá influir en los demás.
- Implementar procedimientos que permitan verificar que las versiones de los programas del ambiente de producción corresponden a las versiones de programas fuentes catalogadas.
- Cuando se necesite tomar copias de la información de los usuarios para la realización de pruebas, se deberán establecer los controles necesarios para garantizar su destrucción, una vez concluidas las mismas.
- Contar con procedimientos y controles para el paso de programas a producción. El software en operación deberá estar catalogado.
- Contar con interfaz para los usuarios que cumplan con los criterios de seguridad y calidad, de tal manera que puedan hacer uso de ellas de una forma simple e intuitiva.
- Si dentro del servicio adquirido se incluye algún aspecto como: Aplicación y/o Sitio Web, Base de datos, Sistema operativo, Motor Web, Configuraciones de RED, se debe validar el cumplimiento del documento: Lista Verificación Cumplimiento Lineamientos de Seguridad.xlsx publicada en Isolución de la Organización
- Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus operaciones monetarias pueda ser capturada por terceros no autorizados durante cada sesión.

ADICIONALES

- Definir ANS con para la prestación del servicio
- Incluir cláusulas de propiedad de la información
- Cumplir con la obligación de reportar incidentes de seguridad de la información
- Permitir la realización de auditorías de revisión de cumplimiento de los requisitos de seguridad de la información establecidos por la Entidad.

- Para los contratos que involucren desarrollo de sistemas de información se debe incluir una obligación que los requisitos de seguridad de la información se tuvieron en cuenta antes, durante y después de la puesta en producción del sistema de información y se deben definir matrices de perfiles del sistema de información.
- Cumplimiento de las disposiciones de la normatividad colombiana incluyendo la circular 052 de 2007, 007 de 2018 y 008 de 2018 expedida por la Superintendencia Financiera de Colombia y la Ley 1581 de protección de datos personales.
- Incluir cláusulas de protección de datos personales