

REQUISITOS GENERALES
SEGURIDAD DE LA INFORMACIÓN
Estos requerimientos se basan en lo establecido en la CE 029/2014 de la SFC, la cual es de obligatorio cumplimiento
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 S.A. 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 y la ciberseguridad, para lo cual podrán tener como referencia los estándares ISO 27001 -ISO 27032, o el que lo sustituya
Disponer que el envío de información confidencial y de los instrumentos para la realización de operaciones los clientes de Previsora, se haga en condiciones de seguridad. Cuando dicha información se envíe como parte de, o adjunta a un correo electrónico, mensajería instantánea o cualquier otra modalidad de comunicación electrónica, ésta debe estar cifrada. 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.
Proteger las claves de acceso a los sistemas de información. Se debe evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo debe ser única y personalizada.
PROVEEDORES CRÍTICOS
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:
a) Data center alternativo: En el que se repliquen todos los aplicativos, bases de datos, etc., que apalancan los servicios prestados a la compañía
b) Canales de comunicación de contingencia: Deben cumplir los mismos requisitos de seguridad que los canales de comunicación principales Principal Previsora - Principal Proveedor DRP Previsora - DRP Proveedor DRP Previsora - Principal Proveedor Principal Previsora - DRP Proveedor