Capacitación Terceros

2024

Aseguradora Solidaria de Colombia
¡ Siempre junto a ti !

Gerencia de Riesgos y Gobierno Corporativo

Contenido

Aseguradora Solidaria de Colombia
¡ Siempre junto a ti !

Gerencia de Riesgos y Gobierno Corporativo

Normativa Aplicable a la relación con Terceros

Circular Externa 018 -2021

- La cual dicta todas las disposiciones en cuanto Sistema Integral para la Administración de Riesgos (SIAR), que incluye el riesgo de crédito, mercado, de seguros y operacional, entre otros.

Circular Externa 018 -2021

- Acorde a la normativa mencionada: "Las entidades deben diseñar, programar y coordinar planes de capacitación sobre el SARO dirigidos a todas las áreas y terceros que tengan relaciones contractuales y desempeñen funciones de la entidad. "

Circular Externa 007-2018

La cual dicta los requerimientos e instrucciones mínimos para la gestión de la Ciberseguridad incluyendo a los terceros que esta considere relevantes dentro de las políticas.

Circular Externa 005-2019

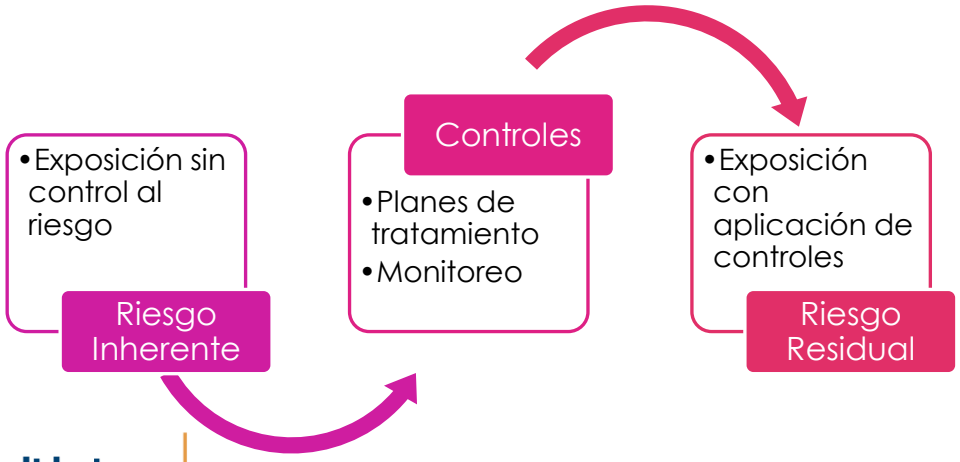
Servicios de computación en la nube deben contemplar como mínimo los siguientes elementos: Las condiciones referentes a capacidad, disponibilidad, tiempos de recuperación, la existencia de planes de continuidad, resolución de incidentes y horarios de atención del proveedor del servicio, las cuales deben prever niveles de servicio

Gestión de Riesgos Operacionales

Las obligaciones como terceros frente a Riesgo Operacional son:

	MENOR	MODERADO	MAYOR	GRAN IMPACTO
CASI CIERTO				RI
PROBABLE				
POSIBLE				
RARO			RR	

- Identificar y gestionar los riesgos de la operación tercerizada de acuerdo con las políticas y procedimientos de la Compañía
- Contrato formal que indique las obligaciones de las partes y acuerdos de niveles de servicio
- Acuerdo de prácticas comerciales y acuerdo de confidencialidad debidamente firmados
- Documentación de cómo se ejecutan las actividades del proceso en situaciones contingentes
- Reportar eventos de Riesgo Operacional



Aseguradora Solidaria de Colombia
¡ Siempre junto a ti !

Gerencia de Riesgos y Gobierno Corporativo

Como Tercero puedo incurrir en…

1. Riesgos de Seguridad de la Información
2. Riesgos de Fraude
3. Incumplimientos de ANS
4. Eventos de Contingencia y Continuidad

Estos son algunos riesgos asociados a los proveedores que afectan a nuestros procesos

Aseguradora Solidaria de Colombia
¡ Siempre junto a ti !

Gerencia de Riesgos y Gobierno Corporativo

Línea de Ética

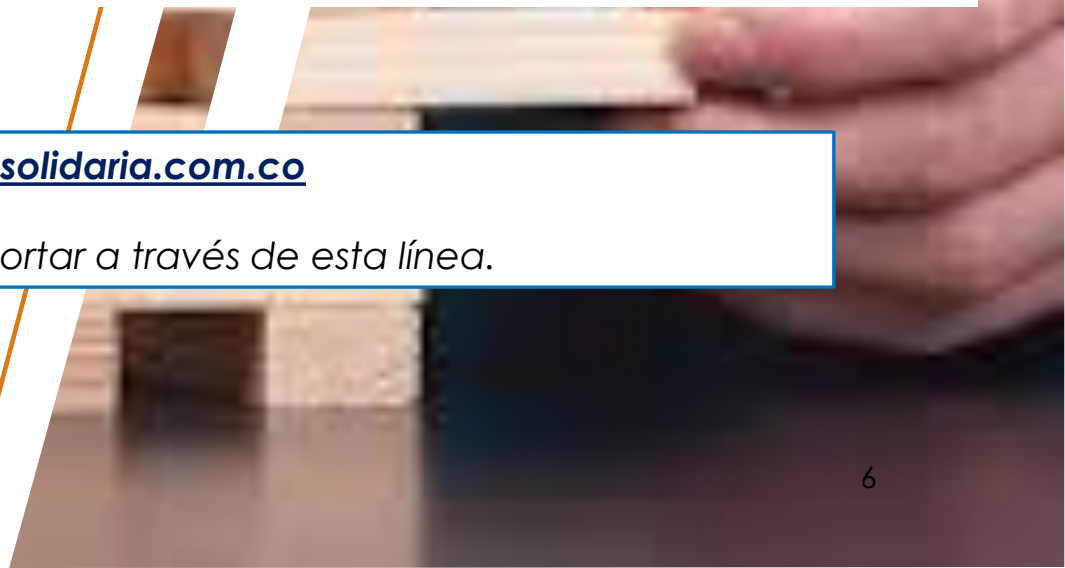
En la Línea Ética se podrá reportar cualquier evento del que se tenga conocimiento respecto a

Conductas no éticas o que comprometan la integridad de la Aseguradora y sus valores.

Cualquier actividad que pueda ser un evento de riesgo de fraude.

Las actuaciones que supongan una práctica ilegal de la profesión.

Cualquier actividad que pueda ser un evento de riesgo de protección de datos personales



Reportar a través de: ***www.aseguradorasolidaria.com.co***

Si se identifica un conflicto de interés se puede reportar a través de esta línea.

ACUERDOS DE PRÁCTICAS COMERCIALES DE

ASEGURADORA SOLIDARIA DE COLOMBIA

Aseguradora Solidaria de Colombia
¡ Siempre junto a ti !

Gerencia de Riesgos y Gobierno Corporativo

Acuerdo de Prácticas Comerciales

Identificación de Desviaciones / Riesgos

Cualquier impedimento a la prestación del servicio debe ser reportado a SOLIDARIA, para que su impacto sea analizado y comunicado internamente.

Gobierno Corporativo

Cumplir el Código de Ética y Conducta y el Código de Buen Gobierno Corporativo y políticas definidas por Solidaria.

Sistema de Gestión de Riesgos

Cumplir las políticas y normas establecidas en los sistemas de gestión de riesgos de Solidaria.

Participar en los programas de capacitación y/o **divulgación.**

Protección de datos personales

Sera obligación del contratista suministrar datos personales del representante legal, así como también podrá hacer uso del tratamiento de los datos suministrados por Solidaria.

Se debe reportar cualquier evento o queja al correo: tratamientodatos@solidaria.com.co

Acuerdo de Prácticas Comerciales

Los sistemas de información proporcionados para el uso de los empleados de **SOLIDARIA** y/o sus clientes, deben ofrecer garantías de seguridad de la información

Los Proveedores de **SOLIDARIA** no pueden reconfigurar o cambiar las capacidades y restricciones definidas en los equipos y recursos tecnológicos de propiedad de **SOLIDARIA.**

Uso aceptable de activos y recursos

SOLIDARIA se reserva el derecho de realizar análisis de seguridad.

Acuerdo de Prácticas Comerciales

Gestión de Seguridad de la Información

- Cumplir con las políticas de seguridad de la información y ciberseguridad.
- Implementar normas y procedimientos asociados a seguridad de la información.
- Informar el retiro del personal involucrado en las actividades contratadas.
- Informar cualquier evento de riesgo o incidente de seguridad a través del correo **SIC@solidaria.com.co**.

Devolución y/o destrucción de los activos de información.

- Firmar el formato de inventario de información certificando la entrega y/o devolución de la información suministrada.
- No se procederá con la destrucción de la información cuando exista una previsión legal que exija su conservación.

Software empleado

- Abstenerse de reproducir, distribuir y comercializar software de propiedad de Solidaria, así mismo, evitara que personas no autorizadas por solidaria tengan acceso al software.

Acuerdo de Prácticas Comerciales

Informe de eventos/incidentes de seguridad de la información

- Reportar eventos que puedan interferir con el rendimiento contratado o comportamientos anómalos de los recursos de TI que puedan afectar el servicio con la aseguradora.
- Puedes reportar estos eventos a: SIC@solidaria.com.co

Confidencialidad y propiedad de la información

- Toda Información entregada será de **carácter confidencial** a excepción de la que será de conocimiento público y la información recibida por parte de un tercero que no tenga acuerdos de confidencialidad.

Gestión de Seguridad de la Información y Ciberseguridad

Riesgo de ciberseguridad: El tercero puede ser víctima de un ataque cibernético que comprometa la seguridad de los datos o sistemas compartidos con la organización.

Las **auditorías regulares** son esenciales para garantizar que los proveedores cumplan con las políticas de seguridad establecidas. La evaluación de su seguridad física, controles técnicos, y su gestión de políticas de seguridad es importante para determinar el cumplimiento de las políticas.

La capacitación y concienciación son esenciales para crear una cultura de Seguridad de la Información. Los colaboradores deben estar capacitados en las políticas y procedimientos de Seguridad de la Información de la compañía. Además, deben ser conscientes de los riesgos de seguridad de la información y cómo prevenirlos

Gestión de Seguridad de la Información y Ciberseguridad

Herramientas de detección de eventos y pruebas de intrusión

Contar con herramientas que permitan detectar, prevenir o mitigar incidentes de seguridad. Las cuales se encuentran implementadas en la infraestructura de la compañía.

Realizar análisis semestrales con un tercero para la detección de amenazas en la infraestructura tecnológica.

Procedimientos

Contar con procedimientos para afrontar ataques cibernéticos, equipos de respuesta ante un incidente de seguridad, cláusulas de gestión de riesgos de seguridad de la información y ciberseguridad, gestión de usuarios y contraseñas.

Uso de doble factor de autenticación

Hacer uso del doble factor de autenticación en el correo electrónico corporativo y para el acceso a la red corporativa.

Cifrado de información en tránsito y reposo

La información clasificada como confidencial en tránsito o reposo debe estar cifrada bajo estándares y algoritmos como AES, RSA o 3DES.

Inventario de activos de información

Contar con un inventario de activos de la información que contemple los responsables, actualizaciones y monitoreo de controles seguridad de estos, además de la identificación de activos sin soporte en el último año y su porcentaje.

Herramienta de borrado seguro

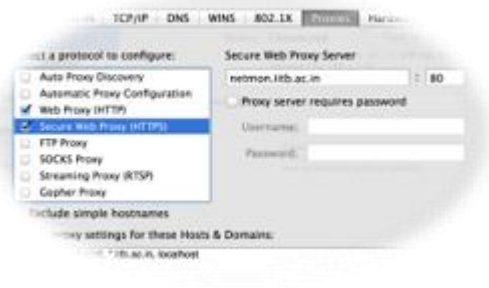
Contar con una herramienta de borrado seguro que elimine la información sin dejar huellas digitales cuando termina el contrato con un tercero.

Antispam en el correo

Hacer uso de herramientas o filtros de seguridad para mitigar los riesgos como el phishing, malware o posibles correos maliciosos.

Evaluación de Seguridad de la información y Ciberseguridad

¡Recuerda! Al diligenciar el formulario para la evaluación de seguridad enviar el soporte de las herramientas de seguridad y documentación de las observaciones realizadas. Esto nos permite validar la información diligenciada y el cumplimiento con la aseguradora.



Acuerdo de Prácticas Comerciales

Continuidad de Negocio

- Disponer de planes de Contingencia y continuidad de negocio. El contratista participará de las pruebas periódicas de continuidad y planes de recuperación en los que se requieran.

Compartir regularmente resultados de pruebas para la ejecución de planes de continuidad y/o recuperación ante desastres relacionados con el alcance de los productos y servicios del contrato, para demostrar el cumplimiento del proceso, entregas y tiempos acordados con SOLIDARIA

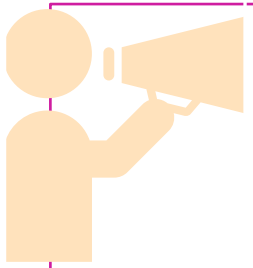
Evaluación al Plan de Continuidad de Negocio de Terceros

- Contar con tiempos máximos de interrupción toler able establecidos: RTO, MTO y RPO
- Realizar pruebas documentadas al Plan de Continuidad de Negocio con periodicidad establecida (min 1 vez al año) y socializar los resultados con AD
- Contar con una política de Continuidad que contenga: Objetivo, alcance, recursos, estructura, roles y responsabilidades, y periodicidad de actualización
- Estructurar Planes de acción derivado de las pruebas o evaluaciones periódicas al Plan de Continuidad de Negocio
- Contar con metodología y planes de concientización y capacitación

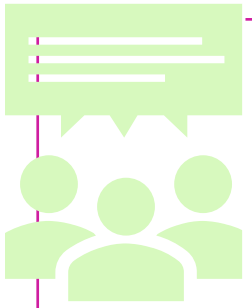
Evaluación al Plan de Continuidad de Negocio de Terceros

- Contar con estrategias y/o planes para afrontar las suspensiones de las actividades del negocio como: Planes de recuperación, DRP, Seguridad Física, Plan de Emergencia
- Contar con una metodología y un análisis de los riesgos que puedan afectar la continuidad del negocio y establecer los escenarios pertinentes
- Contar con la documentación de los procedimientos para la notificación y activación del Plan de Continuidad de Negocio
- Identificar los procesos y recursos críticos (Personas, Infraestructura, proveedores, ETC.)
- Contar con una metodología y un análisis de impacto al negocio (BIA)

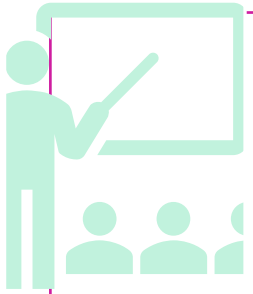
Responsabilidades de los Terceros



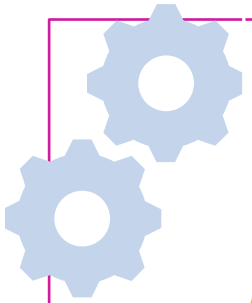
Notificar a la Aseguradora cuando se presente un evento de interrupción de los servicios



Socializar el resultado de las pruebas realizadas, así como el cumplimento al plan de acción establecido



Participar de las evaluaciones realizadas por la Aseguradora



Garantizar el cumplimiento de los acuerdos de nivel de servicios pactados

GRACIAS