POLÍTICA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON PROVEEDORES

Introducción

Para Coopetraban la gestión de las relaciones con proveedores es un aspecto clave para la prestación de sus diferentes servicios. La gestión de las relaciones con un proveedor no inicia ni termina con la compra de un producto /o servicio, la gestión de las relaciones de proveedores comprende todas las interacciones desde antes de iniciar un acuerdo contractual, continua con la compra de un servicio y/o producto, posteriormente la entrega del servicio y producto con las condiciones especificadas, el monitoreo de la prestación de los servicios y las gestiones a realizar una vez finalizado un contrato.

Los proveedores pueden originar oportunidades y riesgos que pueden llegar a afectar la seguridad y la continuidad de la organización; es por esto que es necesario implementar políticas y controles que permitan gestionar la seguridad de la información en las relaciones con los proveedores, que ayuden a conservar la confidencialidad, integridad, autenticidad y disponibilidad de la información.

1. Objetivo y Alcance

Establecer los requisitos y directrices a aplicar para la gestión de la seguridad de la información en las relaciones con proveedores, así como dar a conocer cuáles son los requisitos mínimos de seguridad de la información que se desarrolla en la Cooperativa, con el fin de que todos los involucrados en la operación o que prestan servicios relacionados con procesos críticos de la entidad o procesos de tecnologías de información y comunicaciones, garanticen el buen uso de los sistemas, herramientas, recursos y datos a los que tienen acceso, así como la idoneidad de los controles a implementar.

La presente política es aplicable a todo el personal de la Cooperativa., y proveedores que presten servicios tecnológicos relacionados con almacenamiento, transferencia o procesamiento de cualquier tipo de información sensible dentro el alcance del sistema de gestión de seguridad de la información (SGSI).

2. Referencias Normativas

- Norma ISO/IEC 27001:2013, A.15
- Ley 1581 de 2012.
- Circular externa No 36 de la Supersolidaria

3. Política General

COOPETRABAN establece los requisitos de seguridad de la información pertinentes para la contratación de los proveedores de servicios TIC los cuales deben garantizar la seguridad en el acceso, procesamiento, almacenamiento, comunicación o suministro de componentes de infraestructura de TI con el fin de asegurar el tratamiento de los riesgos de seguridad de la información asociados con los productos y servicios de tecnologías de información y comunicación. Coopetraban realizará seguimiento con el fin de revisar y/o auditar con regularidad la prestación de los servicios de TI por parte de los proveedores, adicionalmente gestionará los cambios en el suministro de servicios por parte de estos, así como el mantenimiento y la mejora de las políticas, procedimientos y controles existentes, teniendo en cuenta la criticidad y la valoración de los riesgos de seguridad de la información y teniendo en cuenta los requisitos aplicables según normatividad vigente de la Superintendencia de la Economía Solidaria y otras normas y leyes aplicables.

3.1 Políticas Específicas

- Toda información reservada o confidencial suministrada por parte Coopetraban, deberá ser tratada de acuerdo con la política y procedimiento de transferencia de la información de Coopetraban y/o ley 1581 de 2012.
- COOPETRABAN define, establece, monitorea y mejora procesos, procedimientos y controles para la gestión de la seguridad en las relaciones con los proveedores y de cada uno de los servicios prestados, los cuales estarán alineados al sistema de gestión de seguridad de la información.
- COOPETRABAN establece todos los requisitos mínimos para la seguridad de la información con los proveedores que tienen acceso a las instalaciones, almacenan, procesan, o transmiten información.
- COOPETRABAN establece los requisitos y criterios para cada tipo de proveedor, los cuales se encuentran definidos dentro del procedimiento de compras con el fin de satisfacer los requisitos de la seguridad de la información, entre Coopetraban y sus proveedores.

- COOPETRABAN incorpora en cada contrato con los proveedores de TI, un acuerdo de confidencialidad para restringir el uso o la divulgación de la información que Coopetraban pueda proporcionar al proveedor. Adicionalmente en los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.
- COOPETRABAN establece cláusulas en sus diferentes acuerdos y/o contratos con proveedores de las condiciones mínimas de seguridad que deberán cumplir en la prestación de servicios. En los contratos o acuerdos de servicios se incluyen los requisitos y condiciones requeridas para el intercambio de información. Cuando existan cambios en los servicios que prestan las terceras partes, estos deben ser documentados e incluidos en los acuerdos de servicios o contratos.
- COOPETRABAN en cada contrato y/o acuerdo que celebra queda explícito los requisitos que seguridad que los proveedores deben cumplir. Se describen los detalles sobre los recursos de Tecnologías de información que cada una de las partes pondrá a disposición de la otra y los controles de seguridad que se establecerán.
- Los empleados de las organizaciones y de las empresas aliadas deben estar cubiertos con acuerdos de confidencialidad y, por lo tanto, serán responsables de la entrega de información no autorizada.
- Coopetraban se asegura que los proveedores conocen las disposiciones de seguridad que tienen que establecer, que comprenden y están de acuerdo con lo que implican tales disposiciones.
- Coopetraban identifica, analiza, valora, gestiona y documenta los riesgos que se aplican a cada relación de trabajo y/o servicios prestados por proveedores que por el tipo de servicio o producto que ofrecen puedan impactar la seguridad de los activos de información o los servicios críticos de la entidad.
- Coopetraban establece y mantiene actualizada una clasificación de sus servicios críticos y las consideraciones de seguridad que se deben implementar para asegurar la confidencialidad, integridad y disponibilidad de estos.
- Coopetraban establece controles para garantizar la protección de los activos de información de la organización a los que tienen acceso los proveedores, así como de los servicios que son prestados por proveedores.
- Coopetraban no permite intercambiar información con entidades externas sin la debida autorización y/o acuerdos de confidencialidad que garantice los tratamientos de información pertinentes.
- En caso de ser necesario el envío y la recepción de información confidencial con los terceros contratados, se debe proteger con mecanismos de cifrado fuerte.

- Todas las conexiones a aplicaciones de terceros deben estar en mecanismos seguros de conexión como son VPN, canales exclusivos, con el registro de IP por parte de entidades para evitar acceder desde lugares remotos sin la debida seguridad y/o autorización pertinente.
- Las comunicaciones con terceras partes para la prestación de servicios del negocio, deben utilizar mecanismos de encriptación fuertes.
- La comunicación con entidades externas para el intercambio de información crítica se debe hacer a través de canales dedicados, con mecanismos de seguridad, como son VPN o webservices y debe ser configurado por personal de la Cooperativa.
- Coopetraban tendrá actualizada la información correspondiente de la persona de contacto de los proveedores.
- Para toda adquisición de software y hardware que se realice, es responsabilidad del área de Tecnología definir los requisitos de seguridad.
- Para la adquisición de software, el proveedor deberá realizar las pruebas pertinentes siguiendo los parámetros establecidos por Coopetraban.
- Todo proveedor que trate información confidencial y/o sensible, que haya sido suministrada por Coopetraban al finalizar la relación contractual deberá ejecutar un procedimiento de borrado seguro, contando con la participación del líder de TI de la Cooperativa.
- Los contratistas no podrán tener acceso a área, zonas o aplicaciones donde se encuentre información sensible de la Cooperativa. En caso de ser necesario su ingreso se debe contar con la autorización por parte del Gerente de agencia, encargado de oficina o Líder de Tecnología.
- Coopetraban mantiene actualizado el listado de proveedores de servicios de TI, el cual es administrado por el Líder de Tecnología en el formato “Listado maestro de proveedores”
- Coopetraban planea ejecuta y evalúa acciones preventivas, correctivas y de mejora cómo parte de sus procesos de mejora continua en aspectos de la gestión de seguridad de la información en las relaciones con Proveedores.
- Coopetraban podrá realizar o solicitar auditorías sobre los servicios contratados con los proveedores TIC para garantizar el cumplimiento de los parámetros establecidos en la relación contractual.
- Coopetraban realizará evaluaciones (mínimo una vez al año) a los proveedores que prestan servicios críticos para garantizar el cumplimiento de los acuerdos y condiciones acordadas con referencia a las condiciones de seguridad requeridas para los servicios vigentes contratados.

- Coopetraban mínimo una vez al año realiza un análisis de seguridad, de conveniencia e idoneidad de los servicios contratados con proveedores, evaluando como mínimo el cumplimiento en aspectos de confidencialidad, integridad y disponibilidad y calidad del servicio.
- Coopetraban realiza un registro completo de los diferentes incidentes de seguridad relacionados con la gestión de seguridad de la información en las relaciones con proveedores.
- Coopetraban planea ejecuta y evalúa acciones correctivas que sean necesarias para dar solución a errores técnicos o procedimentales de los sistemas, tecnologías y servicios prestados por proveedores y evitar que se vuelvan a producir errores o incidentes.
- Coopetraban establece y documenta procesos, procedimientos para dar cumplimiento a esta política.
- COOPETRABAN establece y documenta los roles, responsabilidades y cargos encargados de dar cumplimiento a estas políticas.

4. Cláusulas de Seguridad para Proveedores

Cuando se redacte un contrato con un proveedor de servicios TIC, es necesario tener en cuenta las siguientes cláusulas y definir cuales se incluirán en el contrato, adicionalmente el contrato debe ser revisado por el área jurídica:

1. Información sobre el servicio prestado, detallar la información que se pondrá a disposición para este objetivo y cómo se clasificará.
2. Si el proveedor tiene derecho a tomar subcontratistas; si puede hacerlo, debe obtener el consentimiento escrito de parte de la organización con un detalle de controles que deben cumplir los subcontratistas.
3. Una definición de información clasificada y cómo se regula el secreto comercial.
4. La duración del acuerdo y la obligación de mantener de forma confidencial y clasificada la información y/o los secretos comerciales luego del vencimiento del contrato (al redactar este artículo, se debe tener en cuenta cómo se garantizará la continuidad de negocio en la organización).
5. El derecho de la organización a acceder a información almacenada o procesada por el proveedor.
6. El derecho de auditar o verificar el uso de información confidencial y de controlar la ejecución del contrato en las instalaciones del proveedor, y si las auditorías pueden ser realizadas por terceros. Especificar los derechos de los auditores.

7. Las acciones requeridas luego del vencimiento del contrato (devolución, destrucción o borrado de información confidencial, devolución de equipos, etc.) para garantizar la protección de información confidencial y para asegurar la continuidad de negocio en la organización.
8. Identificación y uso de controles clave para garantizar la protección de los activos de la organización; por ej., controles físicos, controles para protección contra códigos maliciosos, controles de protección física, controles para proteger la integridad, disponibilidad y confidencialidad de la información, controles para asegurar la devolución o destrucción de activos de información después de ser utilizados, controles para evitar la copia y distribución de información.
9. Garantizar el acceso a informes financieros, a informes de auditores internos y externos y a otros informes relacionados con las actividades de negocio de los proveedores que puedan ser importantes para la organización.
10. Responsabilidades y acciones de las partes para evitar que personas no autorizadas accedan al contrato.
11. Identificar al propietario de la información y cómo se reglamentan los derechos de propiedad intelectual.
12. Uso permitido de información clasificada; es decir, el método establecido para manejar ese tipo de información.
13. Proceso para notificar a la otra parte del acuerdo sobre el acceso no autorizado a la información, violaciones a la confidencialidad o cualquier otro incidente.
14. Definir el tiempo de respuesta a los incidentes y establecer un proceso de escalamiento para la resolución de problemas e incidentes.
15. Acciones resultantes por incumplimiento de contrato, responsabilidad del proveedor por transacciones y demás actividades contratadas no ejecutadas o ejecutadas a destiempo o de forma incorrecta.
16. Conocimiento del proveedor sobre políticas y procedimientos clave de la organización.
17. Obligación de los proveedores de capacitar a los empleados para todas las actividades en las que están involucrados.
18. Comprobar que los proveedores sean conscientes de la necesidad de seguridad.
19. Prohibir que los empleados de la organización pasen a trabajar para los proveedores en un tiempo mínimo de un año después de terminar la relación contractual. La contratación podrá realizarse si ambas partes están de acuerdo.
20. Nivel de servicio deseado y nivel de servicio no aceptable.
21. Definición de los criterios de prestación de servicio, control y emisión de informes.
22. Un proceso de gestión de cambios claramente definido.

23. Sistema de control de acceso: definir los motivos para los derechos de acceso de terceros, procesos permitidos de inicio de sesión y claves, proceso de autorización para acceso y asignación de privilegios a usuarios determinados, obligación de llevar un registro de todos los usuarios y sus derechos de acceso, procesos para eliminar derechos de acceso.
24. Una cláusula que especifique claramente que todos los derechos de acceso no autorizados explícitamente están prohibidos.
25. El derecho para supervisar y anular cualquier actividad relacionada con los activos de la organización.
26. Controles para garantizar la continuidad de negocio de acuerdo con las prioridades de la organización: qué servicios deben ser recuperados dentro de qué plazos.
27. Responsabilidad por daño en caso de incumplimiento de relaciones contractuales, incluyendo responsabilidad patrimonial en caso de violación de confidencialidad de la información o en caso de no prestación de servicio.
28. Responsabilidad del proveedor para almacenar datos en conformidad con las regulaciones.
29. Condiciones para prórroga o cancelación del contrato.
30. El idioma del contrato y de la comunicación futura entre la organización y los proveedores o socios.

4.1 Roles y Responsabilidades

- Consejo de Administración
- Proveedores de servicios de TI
- Líder de tecnología.
- Analista de Logística.
- Comité de Seguridad de la Información.
- Área Jurídica.
- Oficial de Cumplimento y Protección de datos.

Cargo	Responsabilidades
Consejo de Administración	• Revisión y Aprobación de la política. • Asignación de recursos requeridos para el cumplimiento de la política.

Cargo	Responsabilidades
Líder de Tecnología - Analista de Logistica.	• Ejecución de la política • Garantizar la adecuada ejecución de los recursos para el cumplimiento de la política • Gestión de proveedores. • Establecimiento de contactos con entidades de gobierno para la gestión de incidentes de seguridad de la información en aspectos de la gestión de seguridad de la información en las relaciones con Proveedores. • Establecimiento de contactos con entidades especializadas en seguridad de la Información para recibir asesoría en buenas prácticas de seguridad en aspectos de la gestión de seguridad de la información en las relaciones con Proveedores • Evaluar el cumplimiento de los acuerdos con proveedores.
Comité de Seguridad de la Información	• Evaluación de riesgos de seguridad de la información relacionados con la gestión de seguridad de la información en las relaciones con Proveedores. • Postulación y recomendación de controles para la gestión de seguridad de la información en las relaciones con Proveedores. • Selección de controles óptimos para la gestión de seguridad de la información en las relaciones con Proveedores. • Evaluación de los controles implementados. • Documentación de los riesgos de seguridad de la información en las relaciones con Proveedores. • Comunicación de los riesgos identificados y los planes de tratamientos recomendados. • Planeación, ejecución, seguimiento y mejora continua del programa de comunicación de la política a los colaboradores, asociados y proveedores de sistemas de información. • Actualizar los documentos relacionados con esta política. • Establecer, implementar, hacer seguimiento a los planes correctivos, preventivos y de mejora.

Cargo	Responsabilidades
Líder de Tecnología	• Revisión del cumplimiento técnico de los servicios implementados por proveedores. • Revisión periódica del cumplimiento de los ANS de los servicios provistos por proveedores. • Evaluación e implementación de tecnologías que permitan monitorear los servicios provistos por proveedores. • Ejecución de pruebas de seguridad para validar la correcta ejecución de los controles de seguridad implementados por los proveedores para la prestación el servicio contratado
Comité de Seguridad de la Información.	• Planear, ejecutar, evaluar y mejorar un programa de concientización y capacitación en la gestión de seguridad en la gestión de seguridad de la información en las relaciones con Proveedores a los nuevos empleados y reforzar los conocimientos en los empleados existentes. • Planear, ejecutar, evaluar y mejorar un programa de comunicación con asociados, proveedores y empleados en la gestión de seguridad de la información en las relaciones con Proveedores.
Área Jurídica	Validar de manera completa el contrato previo a la firma del mismo, determinar que cláusulas deben incorporarse y revisar la terminología de la relación contractual.
Oficial de Cumplimiento	Análisis y revisión en listas de control del proveedor y representante legal, antes de establecer la relación contractual.

4.2 Revisión y Actualización

Esta política estará sometida a una permanente revisión mínimo una vez al año y a su actualización siempre que se produzcan cambios en el contexto de la Cooperativa, los sistemas de información, el sistema de tratamiento, la organización, las relaciones contractuales con proveedores, que puedan afectar a las medidas de seguridad implementadas. Así mismo, las políticas deben adaptarse en todo momento a la normativa legal en materia de seguridad, los requisitos de calidad y seguridad de la información de la circular externa n 036 y demás leyes o reglamentaciones aplicables.

4.3 Nivel de Cumplimiento

Todas las personas y proveedores cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100 % de la política.

4.4 Incumplimiento de la Política

En caso de violación de la política, ya sea de forma intencional o por negligencia, Coopetraban tomará las acciones disciplinarias y legales correspondientes

5. Proceso de la Gestión de la Seguridad en las relaciones con Proveedores.

Planeación de la Gestión de las Relaciones con los Proveedores	•Definición y aprobación de Políticas, procesos, procedimientos y controles. •Gestión de Riesgos.
Proceso de Compra de Productos y /o Servicios con Proveedores	•Elaboración de requisitos del producto y servicio y especificaciones de seguridad, Cotización y compra de Productos y Servicios, elaboración de contratos, Polizas de cumplimiento,acuerdos de confidencialidad, establecimiento de ans.
Ejecución de los servicios contratados con Proveedores	•Prestación del servicio contratado, o la entrega del producto comprado •Recepción del Producto contratado con Proveedores •Validación del cumplimiento del servicio entregado •Gestión de solicitudes dentro del alcance del servicio contratado
Finalización de los contratos y Servicios con Proveedores	•Consideraciones que se deben cumplir luego de finalizado el contrato, o la entrega del sevicio o producto comprado. •Evaluación del servicio o producto.
Monitoreo de los Contratos, acuerdos y Servicios con Proveedores	•Medición de los ANS e indicadores del Servicio. •Monitoreo del cumplimiento de los ANS acordados de los servicios contratados.
Auditoria de a los Servicios Críticos Contratados	•Ejecución del programa de Audioria anual a los servicios contratados •Elaboración del informe de las auditorias realizadas •Comunicación de los resultados de las auditorias •Elaboración de un Plan de acción de acuerdo a los resultados de la auditoria
Mejora continua de la Gestión de las Relaciones con Proveedores	•Plan, ejecución y monitoreo de las Acciones correctivas, preventivas y de mejora continua para mejorar la seguridad de la información en la gestión de relaciones con proveedores.

5.1 Criterios para la Evaluación de Proveedores

La descripción del proceso de evaluación está registrado en el procedimiento de Compras.

5.2 Documentos Relacionados

- Procedimiento de Compras
- Manual SARLAFT
- Manual de Seguridad de la Información

5.3 Registros

- Registro de los servicios críticos prestados por proveedores.
- Registro de proveedores.
- Registros de requisitos que deben cumplir los proveedores y los servicios por estos ofrecidos.
- Registros de la evidencia de que el proveedor comprende y está de acuerdo con las políticas de seguridad de la información de Coopetraban.
- Inventario de servicios de TIC activos y sus correspondientes documentos: contratos, acuerdos, especificaciones funcionales, ANS (acuerdos de niveles de servicio) y requisitos de seguridad.
- Registros de análisis y valoración de riesgos de servicios prestados por proveedores.
- Registros de monitoreo de los servicios prestados por proveedores
- Registros de evaluaciones realizadas a Proveedores.
- Registros de acciones correcticas, preventivas y de mejora para la prestación de un servicio por un proveedor.
- Políticas de controles de acceso desde las redes de proveedores documentadas e implementadas.
- Evidencia de Monitoreo de tráfico entre las redes propias y las redes de proveedores.
- Registro de las tecnologías de canales usadas para la comunicación con Proveedores.

- Registro de las tecnologías de encripción usadas para asegurar las comunicaciones con Proveedores.
- Registro de las tecnologías de encripción usadas para asegurar las comunicaciones entre las aplicaciones, bases de datos con Proveedores.

(Original Firmado)

Comité de Seguridad de la Información