TIC

Lineamientos Relación con Proveedores de Tecnologías de la Información y las Comunicaciones

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Lineamientos Relación con Proveedores de Tecnologías de la Información y las Comunicaciones Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Tabla de contenido

Listado de Tablas

Lineamientos Relación con Proveedores de Tecnologías de la Información y las Comunicaciones

Las entidades estatales del orden nacional y territorial deben establecer relaciones con proveedores para adquirir productos y servicios. Cuando estas adquisiciones están vinculadas a la gestión de la seguridad digital, es común que los proveedores tengan acceso directo o indirecto a los sistemas de información y a los datos institucionales, o que suministren componentes (software, hardware, procesos o personal) que intervienen en el procesamiento de dicha información.

Asimismo, durante el control o seguimiento de los procesos de producción y entrega, las entidades pueden acceder física o lógicamente a información de los proveedores. Esta interacción bilateral implica que ambas partes pueden representar riesgos mutuos en materia de seguridad digital.

Por ello, estos riesgos deben ser identificados, evaluados y gestionados adecuadamente mediante la implementación de controles proporcionales a la criticidad de la información tratada. Este anexo ofrece una guía con los aspectos clave para tener en cuenta en las relaciones contractuales con proveedores de productos y servicios de seguridad digital.

Los riesgos se acentúan cuando el proveedor carece de una adecuada gestión de seguridad de la información, particularmente en el caso de proveedores TIC que:

- Desarrollan aplicaciones o administran sistemas que tratan datos institucionales.

- Prestan servicios de infraestructura tecnológica que almacenan o procesan información crítica.

- Tienen conocimiento de elementos sensibles como configuraciones, vulnerabilidades, logs, direccionamiento interno, entre otros, asociados a procesos misionales de la entidad.

Ante este escenario, es indispensable que la entidad:

- Identifique claramente la información a la que pueden acceder los proveedores.

- Determine las operaciones autorizadas sobre dicha información.

- Establezca los controles necesarios para protegerla, incluyendo cláusulas contractuales como acuerdos de confidencialidad, sanciones por incumplimientos e indemnizaciones por negligencia comprobada.

En paralelo, el proveedor debe asumir responsabilidades específicas, tales como:

- Cumplir con los requisitos en materia de seguridad de la información y protección de datos personales.

- Notificar de manera inmediata cualquier incidente o brecha de seguridad que afecte los activos de información de la entidad.

- Colaborar activamente en la gestión, mitigación y análisis de los incidentes que involucren los activos de información gestionados.

Cuando se prevea la transferencia o acceso a la información fuera del país, la entidad debe gestionar los riesgos transfronterizos, asegurando que tanto proveedores nacionales como internacionales cumplan con las normas vigentes en seguridad digital y protección de datos.

La entidad debe tener plena conciencia de que la responsabilidad legal y contractual sobre la información permanece en todo momento bajo su control, incluso cuando un proveedor la administre. Por lo tanto, debe verificar que los controles aplicados por terceros estén alineados con su plan de tratamiento de riesgos, incluyendo los escenarios de cambio de proveedor o interoperabilidad entre tecnologías de distintos fabricantes.

Estas disposiciones deben estar documentadas en el plan de tratamiento de riesgos y reflejarse explícitamente en los acuerdos contractuales, garantizando así la trazabilidad y la responsabilidad compartida en la gestión de la seguridad de la información.

1. Planificación de las relaciones con Proveedores.

Para gestionar adecuadamente la seguridad de la información en las relaciones con proveedores, las entidades establecer un plan de relación que documente la decisión adoptada por el nivel directivo de iniciar la contratación de un producto o servicio relacionado con activos de información, así como las consideraciones de seguridad de la información relacionadas con esta contratación.

Lineamiento:	Establecer un plan de relación con proveedores que documente la decisión adoptada por el nivel directivo de iniciar la contratación de un producto o servicio relacionado con activos de información, así como las consideraciones de seguridad de la información relacionadas con esta contratación incluyendo la evaluación de seguridad de los proveedores y la gestión de riesgos asociados a servicios o sistemas de terceros.
Propósito:	Gestionar con éxito la seguridad de la información dentro del proceso de planeación de la relación con los proveedores de productos o servicios de seguridad de la información.

Entradas recomendadas	Salidas
• Decisión de adquisición de un producto o servicio relacionado con activos de información documentando necesidades, expectativas y motivos del proceso de adquisición. • Alcance previsto del producto o servicio que se prevé adquirir. • Si es aplicable: o Documentación existente de gestión de relaciones con proveedores, como planes y acuerdos de relaciones con proveedores.	I) Plan de evaluación y tratamiento de riesgos de seguridad de la información asociados al producto o servicio que se contrate; II) Decisión de gestión documentada que indica la aprobación del plan de evaluación y tratamiento de riesgos de seguridad de la información y que se puede iniciar la adquisición del producto o servicio; III) La decisión de no adquirir un producto o servicio también deberá documentarse con la información de las razones de seguridad que han inducido esta decisión. IV) Plan de relación con proveedores. V) Cuando aplique: análisis de impacto si se presenta un cambio en el acuerdo inicial que afecte la continuidad de negocio.

Actividades a realizar por parte de la entidad contratante:

Identificar y evaluar los riesgos de seguridad de la información que acompañan la posible adquisición del producto o servicio con base en el MSPI y en la estrategia de relación con proveedores.

- Las entidades deberán garantizar que esta evaluación de riesgos de seguridad de la información:

1) Es proporcional a la criticidad del producto o servicio que se planea adquirir.

2) Tiene en cuenta los requisitos legales y regulatorios aplicables a el producto o servicio que se planea adquirir para garantizar que se hayan obtenido los permisos y licencias formales antes de iniciar la relación con el proveedor.

3) En particular al adquirir productos de nube que durante su operación puedan resultar en tratamiento o transferencia de datos personales resulta fundamental planear dónde se

almacenarán los datos, el tipo de almacenamiento y la región geográfica de ese almacenamiento.

4) Se debe tener cuidado y considerar los posibles impactos en la seguridad de la información del producto o servicio que se adquirirá con respecto a los riesgos de seguridad de la información asociados con las relaciones existentes con los proveedores, particularmente si existe una alta dependencia de los proveedores. Para disminuir la complejidad y facilitar los procesos de gestión de Seguridad Digital se recomienda adoptar buenas prácticas en materia de consolidación de proveedores.

- Identificar el nivel aceptable de riesgos en la relación con el potencial proveedor;

- Identificar y evaluar opciones para el tratamiento de los riesgos identificados y evaluados;

- Definir e implementar un plan de tratamiento de riesgos de seguridad de la información para que los riesgos identificados y evaluados sean mitigados al nivel de riesgo aceptable;

  NOTA: No se debe proceder con la adquisición de los bienes o servicios cuando los riesgos de seguridad de la información identificados no puedan reducirse a un nivel aceptable de riesgos.

- Asesorar a la entidad sobre el plan de evaluación y tratamiento de riesgos de seguridad de la información como insumo para el proceso de negociación de la relación con proveedores;

- Definir un plan de relación con proveedores del producto o servicio que se prevé adquirir. En particular, el plan de relación con proveedores deberá contener lo siguiente:

  1) Especificaciones del producto o servicio que se prevé contratar, en particular su alcance, audiencia, tipo y naturaleza;

  2) Activos, tales como servidores, bases de datos, aplicaciones, infraestructura de red, que tengan relevancia para la seguridad de la información en el uso del producto o servicio, y sus propietarios asociados;

  3) Entradas de clasificación de información de la entidad, la clasificación de información del proveedor y otros controles de seguridad de la información;

  4) Los requisitos legales y regulatorios aplicables a la entidad, y las áreas de leyes y reglamentos que vinculan al proveedor potencial que deben revisarse durante el proceso de selección de proveedores, a saber:

  I) Control de exportaciones;

  II) Legislación de protección de datos personales y leyes laborales; en particular las previstas en la Ley 1581 de 2012, la CIRCULAR EXTERNA 10 de 2001 -Circular única Superintendencia de Industria y Comercio -SIC, y demás normatividad aplicable.

III) propiedad intelectual de terceros; y

IV) Otros requisitos legales y reglamentarios, como leyes fiscales, responsabilidad por productos defectuosos, facultades de investigación.

Si se requieren autorizaciones o licencias de autoridades internas o externas para el cumplimiento legal y reglamentario, estas deberán obtenerse antes de celebrar cualquier acuerdo de relación de proveedor con el proveedor.

5) Roles y responsabilidades de seguridad de la información asignados dentro de la entidad y específicos del producto o servicio que se puede adquirir;

6) Información de la entidad que se puede compartir con posibles proveedores del producto o servicio.

NOTA: La información del adquirente debe tener un propietario designado, responsable de su difusión y de garantizar que las reglas de manejo relacionadas se apliquen correctamente.

7) Requisitos mínimos de seguridad de la información que se acordarán con el proveedor seleccionado para la adquisición del producto o servicio. Estos requisitos deben resultar directamente del plan de evaluación y tratamiento de riesgos de seguridad de la información y del marco de requisitos de seguridad de la información definido en la estrategia de relación con el proveedor.
Estos requisitos también deben definirse considerando la criticidad del producto o servicio que se puede adquirir y lo siguiente:

- Clasificación de la información hecha por la entidad;

- Los requisitos de seguridad de la información definidos en los planes de relación con proveedores existentes y acuerdos.

- Realizar un proceso de articulación del entorno de red que contemple los elementos físicos, virtuales y en la nube y la interacción entre ellos.

2. Selección de proveedores.

Para gestionar con éxito la seguridad de la información dentro del proceso de selección de proveedores, las entidades deben establecer los controles de seguridad de la información específicos para cada producto o servicio de seguridad digital a adquirir de acuerdo con la criticidad de la información que van a tratar y así seleccionar un proveedor que brinde la seguridad de la información requerida.

Lineamiento:	Planificar la selección de los proveedores de productos o servicios de seguridad de la información.
Propósito:	Gestionar con éxito la seguridad de la información dentro del proceso de selección de proveedores de productos o servicios de seguridad de la información**.**

Entradas recomendadas	Salidas
• Criterios de seguridad para la selección de proveedores existentes para otros productos y servicios. • Acuerdos de confidencialidad existentes para otros productos o servicios. • Identificación de la información y los activos de información de la entidad a la que tendrá acceso: el proveedor, las herramientas y sistemas de información del proveedor.	VI) Nuevos criterios de seguridad para la selección de proveedores específicos para los productos o servicios a adquirir. VII) Acuerdos de confidencialidad específicos para los productos o servicios a adquirir. VIII) Permisos que tendrá el proveedor sobre la información y los activos identificados. IX) Análisis de riesgos de seguridad de la información incluyendo los riesgos asociados a posibles migraciones de datos entre diferentes proveedores y la interoperabilidad entre herramientas y servicios de diferentes fabricantes. X) Resultados de la evaluación del cumplimiento de los requisitos de seguridad de la información de los proveedores. XI) Plan de evaluación y tratamiento de riesgos de seguridad de la información asociados al producto o servicio que será suministrado este plan debe ser realizado por parte del proveedor seleccionado.

Actividades a realizar por parte de la entidad contratante:

Definir e implementar criterios de selección de proveedores que contenga especificaciones del producto o servicio que se puede contratar y en el marco de criterios de selección de proveedores definido; Los criterios de selección de proveedores cubrirán lo siguiente:

- Aceptación por parte del proveedor de los requisitos de seguridad de la información definidos en el pliego de condiciones;

- La madurez en seguridad de la información del proveedor podrá demostrarse mediante certificación ISO/IEC 27001:2022 o, en su defecto, a través de documentación técnica que evidencie controles implementados, tales como planes de continuidad, recuperación, gestión de incidentes y políticas internas. Esta flexibilidad busca asegurar condiciones mínimas de seguridad sin afectar la pluralidad de oferentes en procesos de contratación.

- Los términos bajo los cuales el proveedor permite ser auditado por la entidad o por un tercero autorizado para verificar el cumplimiento de los requisitos de seguridad de la información definidos;

- Aceptación transitoria cuando el producto o servicio a contratar haya sido previamente explotado o fabricado por la entidad o por otro proveedor;

- Aceptación de terminación para mantener la seguridad de la información en caso de terminación del contrato de relación con el proveedor;

- Gestión de la capacidad del proveedor para suministrar el producto o servicio que pueda contratar,

- Fortaleza financiera del proveedor que puede suministrar el producto o servicio; y la ubicación del proveedor y desde donde se suministrará el producto o servicio. Se debe tener especial cuidado para identificar esta ubicación con el fin de:

    - Identificar cualquier riesgo legal y regulatorio potencial causado por la diferencia en las leyes y regulaciones entre la entidad y el proveedor. NOTA: Es necesario realizar investigaciones relacionadas con la legislación extranjera en el caso de contratación interjurisdiccional.

    - Garantizar que las obligaciones legales y reglamentarias que se aplican al proveedor no puede afectar negativamente el acuerdo de relación con el proveedor en términos de seguridad de la información.

    - Evaluar las amenazas ambientales, como las tasas de criminalidad locales o los problemas geopolíticos, y sus impactos potenciales.

  NOTA: Los criterios de selección de proveedores existentes definidos para otros productos o servicios adquiridos también se pueden utilizar al definir e implementar los criterios de selección de proveedores del producto o servicio que se puede suministrar.

Preparar un acuerdo de confidencialidad para ser firmado por el proveedor para proteger los activos de la entidad, como información y sistemas de información. transmitidos durante el proceso de selección de proveedores. NOTA: Si corresponde, este acuerdo de confidencialidad debe ser firmado por la entidad y el proveedor potencial antes de cualquier intercambio de información que se relacione con el producto o servicio que se pueda contratar.

NOTA: Los acuerdos de confidencialidad existentes deben utilizarse como soporte para la elaboración del acuerdo de confidencialidad del producto o servicio que se vaya a adquirir.

Preparar y proporcionar un documento de licitación, al proveedor potencial; El documento debe contener información suficiente para que el proveedor pueda preparar su propuesta con fundamento. En particular, el pliego de condiciones deberá contener lo siguiente:

1) Especificaciones (p. ej., alcance, audiencia, tipo y naturaleza) del producto o servicio a adquirir;

2) Requisitos de seguridad de la información que el proveedor deberá seguir mientras suministre el producto o servicio;

3) Niveles de servicio o indicadores clave de desempeño a seguir durante el suministro del producto o servicio; Las posibles sanciones que puede imponer la entidad en caso de incumplimiento de los requisitos de seguridad de la información.

NOTA: En la medida de lo posible, el pliego de condiciones solo debe contener contenido público o desclasificado. Dicho documento solo debe contener la información necesaria para permitir que el proveedor responda justifica mente.

La información altamente sensible nunca debe incluirse en un documento de licitación en ninguna circunstancia.

Se deben recopilar los documentos de respuesta que han sido transmitidos por proveedores potenciales en respuesta al documento de licitación y estos deben ser evaluados con base a los criterios de selección de proveedores.

e) Seleccionar un proveedor basado en la evaluación de estos documentos de respuesta.

NOTA: Las entidades deben propender por seleccionar a los proveedores que proporcionan una mayor transparencia en toda la cadena de suministro de productos o servicios y garantías de que los requisitos de seguridad de la información de la entidad se cumplirán de acuerdo con lo definido en el pliego de condiciones.

3. Negociación de Acuerdos con Proveedores.

Con el objetivo de mantener la Seguridad de la información durante la negociación de los acuerdos con proveedores las entidades deberán mantener la seguridad de la información durante el período de ejecución de la relación con el proveedor de acuerdo con el contrato con el proveedor y considerando en particular lo siguiente: I) Evaluar el impacto del cambio

en el suministro del producto o servicio cuando haya sido previamente operado o fabricado por la entidad o por un proveedor diferente; II) Capacitar al personal involucrado en los requisitos de seguridad de la información definidos en el contrato con el proveedor; III) Gestionar cambios e incidentes que puedan tener impactos en la seguridad de la información en el suministro del producto o servicio; IV) Supervisar y asegurar el cumplimiento de las disposiciones de seguridad de la información definidas en el contrato con el proveedor.

Lineamiento:	Gestionar la seguridad de la información en el proceso en el proceso de negociación de acuerdos con proveedores.
Propósito:	Gestionar con éxito la seguridad de la información dentro del proceso de negociación de la relación con los proveedores de productos o servicios de seguridad de la información.

Entradas recomendadas	Salidas
• Decisión sobre quién llevará a cabo las actividades de supervisión del proveedor; • Resultados anteriores de las actividades de seguimiento y cumplimiento de los proveedores.	XII) Evaluación de riesgos de seguridad de la información e informes de auditoría relacionados con las actividades de supervisión y ejecución del cumplimiento. Cuando aplique: XIII) Evaluación de riesgos de seguridad de la información relacionada con cambios que no están cubiertos por el procedimiento de gestión de cambios de seguridad de la información; XIV) Informe de ejecución del plan de migración; XV) Historial de cambios de seguridad de la información e informes asociados; XVI) Historial de incidentes de seguridad de la información e informes asociados; XVII) Acuerdo de relación con proveedores actualizado; XVIII) Lista de acciones correctivas que se han acordado y el estado actual (por ejemplo, abierto, retirado o implementado).

Actividades a realizar por parte de la entidad contratante:

- Asegurarse de que la otra parte haya recibido el documento de relación con el proveedor y de que comprenda completamente los aspectos de seguridad de la información contenidos en el mismo;

- Exigir al proveedor el cumplimiento de las políticas de seguridad y privacidad de la información y de continuidad del negocio de la entidad, para el tratamiento de la información y los activos a los que tenga acceso.

- Operar la transición del producto o servicio de acuerdo con el plan de transición acordado y notificar a la otra parte de manera oportuna en caso de que ocurran eventos inesperados durante esta actividad;

- Gestionar los cambios e incidentes de seguridad de la información de acuerdo con los procedimientos acordados;

- Solicitar la autorización para poder realizar auditorías al proveedor, con el fin de verificar el cumplimiento a las Políticas de Seguridad de la Información.

- Capacitar periódicamente al personal que pueda estar involucrado en la ejecución del plan de terminación;

- Gestionar otros cambios, como los que no estén amparados por el procedimiento de gestión de cambios de seguridad de la información y que puedan impactar en el suministro del producto o servicio contratado, cuando sean notificados por la otra parte:

    - Cambio en el negocio, la misión o el entorno de la organización;

    - Cambio relacionado con la solidez financiera de la organización;

    - Cambio de propiedad de la organización, o creación de joint ventures;

    - cambio de ubicación desde donde se adquiere o suministra el producto o servicio;

    - Cambio en el nivel de seguridad de la información de la organización, como el logro o la pérdida de una certificación ISO/IEC 27001:2022;

    - Cambio en la capacidad de soportar las capacidades requeridas de continuidad del negocio; y

    - Cambio en los requisitos legales, regulatorios y contractuales aplicables a la organización.

- Asegurarse de que las actividades de monitoreo y supervisión cumplan con el plan asociado y el proceso de manejo de acciones correctivas. En caso de que ocurran cambios en los riesgos de seguridad de la información o de no conformidades de auditoría, la entidad con el apoyo del proveedor deberá:

    identificar y evaluar los impactos en la seguridad de la información resultantes de estos cambios o auditar las no conformidades;

Determinar si se deben reconsiderar los aspectos de seguridad de la información definidos en el contrato con el proveedor;

Determinar qué acciones correctivas se deben implementar dentro de una escala de tiempo definida y acordada para recuperar un nivel aceptable de seguridad de la información dentro del alcance del producto o servicio adquirido;

- Acordar con el proveedor:
    - Los cambios por realizar en los aspectos de seguridad de la información definidos en el contrato con el proveedor;
    - Medidas correctivas aplicables
- Aprobar el contrato con el proveedor.

4. Gestión de relaciones con proveedores.

Con el objetivo de mantener la seguridad de la información es necesario contar con una apropiada gestión de los proveedores, para ello debe ser considerado lo establecido en la Política de seguridad de la información en las relaciones con los proveedores y así mitigar los riesgos asociados con el acceso del proveedor a los activos de la organización y mantener el relacionamiento acorde a lo establecido en los Acuerdos de Nivel de Servicio determinados.

Lineamiento:	Mantener la seguridad de la información durante el período de ejecución de la relación con el proveedor.
Propósito:	Gestionar con éxito la seguridad de la información durante la relación con el proveedor de productos o servicios de seguridad de la información**.**

Entradas recomendadas	Salidas
• Documento firmado que incluya cláusulas de cumplimiento al proveedor sobre las disposiciones de seguridad de la información, protocolos de migración, procedimientos de capacitación y plan de transición definidas por la organización, el cual debe mantener la reserva según los protocolos y normatividad existente.	XIX) Informes periódicos de los servicios o productos que evidencie el cumplimiento de los indicadores establecidos. XX) Evidencias de reuniones periódicas de seguimiento acorde a lo establecido en las cláusulas y según requerimiento del supervisor del contrato. XXI) Resultados de revisiones técnicas, administrativas o

	auditorias de cumplimiento en búsqueda de acciones de mejora o verificación del cumplimiento requerido

Actividades a realizar por parte de la entidad contratante:

Establecer las actividades que deben ser tenidas en cuenta por la entidad contratante, para la gestión de la prestación de los servicios o productos contratados, verificación de las responsabilidades y controles aplicables para dar alcance al objeto contractual, por lo cual se recomienda:

a) Asegurar que los documentos y pólizas estén se encuentren vigentes durante el periodo de ejecución, en caso de prorrogas estar atentos a las actualizaciones contractuales que den a lugar.

b) Realizar revisiones periódicas a los documentos, planes y procedimientos entregados por el proveedor, sobre los cuales basan la operación, para determinar la funcionalidad y/o necesidad de actualización o mejoras que permita ajustarse al proceso y políticas existentes de la entidad.

c) Evaluación de riesgos de seguridad de la información de forma periódica en acuerdo con el con el proveedor, para determinar posibles nuevas amenazas o vulnerabilidades en los productos o servicios contratados, los cuales como resultado deberán ser gestionados por el proveedor del servicio de acuerdo con los ANS establecidos en el contrato.

d) Adoptar los procedimientos del proveedor según corresponda, a los procesos existentes en la entidad, para así alinear las estrategias de continuidad del negocio entre las partes.

e) Verificar la ejecución del plan de capacitación y realizar las mediciones sobre la efectividad y nivel de apropiación de los conocimientos de los asistentes.

f) Ejecutar pruebas de verificación sobre los planes de continuidad del servicio, recuperación y gestión de incidentes.

g) Contar con un plan de gestión de cambios que permita tener control y trazabilidad de las acciones realizadas por el proveedor.

h) Establecer un plan terminación que incluya entre documentación para la transición, métodos de intercambio de datos, reglas o registros (si aplica), que permita un proceso transparente en el caso que no sea posible o adecuada la continuidad con el proveedor.

i) Contar con la bitácora de eventos relevantes que se presenten durante el desarrollo del contrato, ya que serán determinantes en la generación de los procesos de lecciones aprendidas al finalizar el relacionamiento con el proveedor.

j) Contar con un repositorio único en el cual se cuente con la información de la ejecución contractual tales como registros, documentos, procedimientos, manuales, listados y en general todos aquellos que sean considerados como elementos de valor o evidencias durante la ejecución contractual.

k) Realizar un monitoreo de las actividades y acciones de los servicios en la nube

5. Proceso de terminación de la relación con el proveedor.

La finalidad en todos los casos es proteger la confidencialidad, integridad y disponibilidad de la información, por ello, dar por terminado el relacionamiento contractual debe ser transparente y preciso para la organización, evitando traumatismo y materialización de eventos adversos en el proceso durante el cierre y entrega a un nuevo proveedor o a la entidad, para todos los casos, es imperante que el servicio o producto siempre este funcional según corresponda, para así evitar impactos operacionales, legales o económicos.

Es preciso tener presente los tiempos, documentos y elementos requeridos para el cierre, con base en lo establecido en los términos contractuales y la normatividad vigente.

Lineamiento:	Planificar el cierre contractual con los proveedores de productos o servicios de seguridad de la información.
Propósito:	Gestionar con éxito y de manera segura la terminación de la relación con el proveedor de productos o servicios de seguridad de la información garantizando la continuidad de la operación.

Entradas recomendadas	Salidas
• Contar con un plan de migración o de terminación avalado y probado para la entrega de los productos o servicios de seguridad de la información a la entidad o al proveedor entrante. • Documento con la evaluación de los riesgos existentes en los procesos de entrega o migración de los servicios o productos de seguridad de la información.	XXII) Acta de finalización del contrato avalada y firmada por el supervisor, en el cual certifica el cierre de la relación contractual. XXIII) Informe de lecciones aprendidas durante el tiempo del servicio y en el cierre del contrato.

• Activación del plan de continuidad del negocio, verificación de controles existentes y respaldo de información o dispositivos según corresponda.	

Actividades a realizar por parte de la entidad contratante:

Establecer las actividades a realizar para la finalización contractual con el proveedor de productos o servicios de seguridad de la información, para ello, es importante establecer y contar con un plan de terminación que contemple diversas actividades con el objetivo de mantener la continuidad en la operación para ello es necesario:

a) Describir las actividades y procedimientos generales para tener en cuenta durante el cierre y posterior a la finalización del servicio sin que se incurran en costos adicionales para las partes.

b) Establecer un comité técnico entre las partes, el cual tendrá como función coordinar las actividades de cierre de los servicios contratados acorde al plan de finalización.

c) Contar con la previa evaluación de riesgos y cronograma de ejecución correspondiente para la terminación contractual teniendo en cuenta los eventos adversos que pueden presentarse, la forma de mitigarlos y las desviaciones que puedan reflejarse en el cronograma por la materialización de las amenazas.

Nota: en caso tal que el servicio deba ser entregado de un proveedor a otro, debe ser conformado un comité técnico el cual estará compuesto por las partes incluyendo personal del proveedor saliente y entrante.

d) Durante el proceso de entrega, el proveedor deberá relacionar documentación técnica, bitácoras de procedimientos, registros actualizados, y en general toda la información que sea parte integral y de relevancia sobre las labores adelantadas durante la ejecución contractual.

Nota: de acuerdo con el servicio deberán ser requeridos en la entrega como mínimo:

- Documentación técnica del diseño y de la operación.
- Archivos de Imágenes de máquinas virtuales.
- Archivos de bases de datos.
- Archivos de bases de datos de administración de configuraciones (CMDB).
- Archivos que se encuentren dispuestos en los servicios de almacenamiento contratado.

- Toda aquella documentación sobre topologías o estructuras físicas o lógicas.

e) Solicitar apoyo al proveedor o al comité técnico durante el proceso de cierre contractual para la coordinación de los despliegues técnicos, y operativos que sean necesarios para verificar, probar, trasladar y ejecutar la entrega o migración de los productos o servicios de seguridad de la información.

Nota: La entidad compradora generará un acta que contenga la relación de los procedimientos realizados, documentación de configuraciones, parámetros y procedimientos sobre los servicios o productos de seguridad de la información entregados por el proveedor.

f) Solicitar certificación al proveedor la cual indicara la eliminación total y segura de los datos almacenados con herramientas especializadas que no permitan la recuperación o reúso.

g) Acta de finalización del proceso contractual avalada y firmada por el supervisor, en el cual certifica el cierre del proceso contractual.

h) Verificar el cambio de credenciales de acceso, eliminación de usuarios y cierre de conexiones remotas al proveedor saliente.

6. Lineamientos adicionales a considerar

A continuación, se detallan los siguientes lineamientos a considerar:

Lineamiento Sugerido	Acciones Claves
- Los contratos con proveedores deberán contemplar cláusulas específicas sobre la gestión de amenazas (control A.5.7) y seguridad en la nube (A.5.23), incluyendo requerimientos sobre evaluación de amenazas emergentes, responsabilidad compartida, trazabilidad, cifrado y protección de datos en servicios cloud.	- Incluir cláusulas contractuales que exijan al proveedor identificar, reportar y mitigar amenazas relevantes. - Solicitar evidencias de controles en la nube: cifrado, gestión de accesos, respaldo, monitoreo. - Establecer acuerdos de nivel de servicio (SLA) específicos en seguridad.
- La entidad debe identificar y evaluar los riesgos asociados a sus proveedores críticos, considerando elementos como la cadena de suministro, el manejo de información	- Elaborar una matriz de riesgos de proveedores: criticidad del servicio, sensibilidad de los datos, dependencia tecnológica.

sensible, y la continuidad del servicio. Se deben establecer mecanismos de evaluación inicial y periódica del cumplimiento en seguridad.	- Clasificar a los proveedores según su nivel de riesgo. - Establecer revisiones de cumplimiento en seguridad al menos una vez al año.
- Se deberán establecer protocolos de reporte y coordinación con proveedores frente a incidentes de seguridad, incluyendo tiempos de notificación, medidas de contención y responsabilidad en la remediación. Estas condiciones deberán estar formalizadas en los contratos.	- Definir en contrato el tiempo de notificación de incidentes por parte del proveedor (ej. 4 horas). - Acordar el procedimiento conjunto para análisis, contención y remediación. - Documentar responsabilidades compartidas para incidentes multientidad.
- En la contratación de servicios en la nube, se deberá considerar la ubicación geográfica del proveedor y del almacenamiento de datos, verificando que las condiciones contractuales y técnicas cumplan con las leyes nacionales y estándares de protección de datos. Se debe definir claramente el modelo de responsabilidad compartida.	- Identificar la ubicación física de los centros de datos donde se almacenan los datos institucionales. - Verificar cumplimiento de leyes colombianas (protección de datos, soberanía). - Establecer el modelo de responsabilidad compartida entre entidad y proveedor (p. ej., gestión de accesos: proveedor, contenido: entidad).
- Para activos de información compartidos o administrados por terceros, se deberán establecer lineamientos específicos que aseguren su identificación, clasificación, control de acceso, trazabilidad y eliminación segura. Estos lineamientos deberán aplicarse desde la etapa de contratación.	- Identificar activos tercerizados en el inventario (p. ej., bases de datos alojadas en proveedores). - Establecer controles de acceso, monitoreo y eliminación segura de información tercerizada. - Exigir reportes periódicos del estado de estos activos.
- La gestión de la seguridad de la información en relación con los proveedores debe abordarse de forma integral, incluyendo requisitos contractuales, evaluación de riesgos, participación en la gestión de incidentes, cumplimiento normativo y medidas técnicas específicas según el tipo de servicio prestado o el acceso a activos de información.	- Incorporar requisitos de seguridad en los términos de referencia, evaluaciones y contratos. - Incluir a los proveedores en pruebas de continuidad del negocio y simulacros de ciberseguridad. - Asegurar trazabilidad de accesos de proveedores a sistemas internos.

Tabla 1 Lineamientos a considerar