UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

GESTIÓN DE PROVEEDORES DE TI

BOGOTÁ D.C. JUNIO 2023

USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

TABLA DE CONTENIDO

1. PROCESO

Gestión de Tecnologías de la Información.

2. OBJETIVO

Llevar a cabo una adecuada gestión de proveedores de los diferentes productos y/o servicios que se adquieren para la gestión de la seguridad digital que se encuentran vinculados con el procesamiento de la información institucional, con el fin de salvaguardar la integridad, confidencialidad y disponibilidad de los activos de información a los que en cumplimiento de sus obligaciones tienen acceso.

3. ALCANCE

Esta guía inicia con la selección de proveedores y finaliza con la terminación de la gestión del proveedor. A través de estos lineamientos se da cumplimiento a lo establecido en la Resolución 746 de 2022, expedida por MINTIC y su anexo “Relación con proveedores de seguridad digital”.

4. DEFINICIONES

- **ACTIVOS DE INFORMACIÓN:** elementos que tienen valor para la organización identificadas por cada proceso, tienen niveles de criticidad respecto a su confidencialidad, disponibilidad e integridad, y cada jefe de área o jefe de oficina es el responsable del activo. Para la USPEC, los activos se clasifican en información, hardware, software, servicios, componentes de red, instalaciones y personas.

- **ANS:** Acuerdos de Niveles de Servicio.

- **AMENAZAS:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

- **VULNERABILIDADES:** representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. DISPOSICIONES GENERALES

Las solicitudes de adquisición de bienes y/o servicios relacionados con gestión de información y seguridad digital deben ser analizadas por la Oficina de Tecnología – OTEC y remitidas a través del correo g.tecnologia@uspec.gov.co

Es necesario para la Entidad llevar a cabo un análisis de las necesidades en materia de adquisición de bienes y/o servicios en pro del mejoramiento de la infraestructura tecnológica y la seguridad digital de la Entidad, en tal sentido se hace necesario contar con un comité que lleve a cabo la validación de aspectos técnicos con el fin de determinar la viabilidad de las necesidades generadas por cada una de las dependencias de la USPEC. Por tal razón se crea el comité técnico de la OTEC, a continuación, se detalla su conformación y sus responsabilidades:

a. El Comité Técnico de la OTEC, está conformado por:

- Jefe Oficina de Tecnología.
- Coordinador del Grupo de Comunicaciones.

- Administradores de la plataforma tecnológica.
- Delegado Sistema de Gestión de Seguridad de Información.
- Responsable del bien o servicio.
- En caso que la solicitud proceda de otra dependencia diferente a la OTEC, es necesario contar con la participación del Director o Jefe o su delegado.

Nota: es potestad del comité convocar al personal que se considere relevante en las sesiones del mismo.
Los análisis y decisiones que se tomen al interior del comité deben quedar registradas en acta de reunión, incluyendo las consideraciones de seguridad que se deban tener en cuenta para posibles contrataciones.

b. Responsabilidades del Comité Técnico:

- Analizar la viabilidad del bien o servicio que se pretende adquirir, evaluando aspectos de seguridad digital y demás requisitos técnicos relacionados con el mismo.
- Analizar los posibles riesgos de seguridad de información a que puede estar expuesta la información institucional ante la posible adquisición del bien o servicio, identificando la viabilidad de su mitigación.
- Documentar las decisiones generadas al interior del comité indicando las razones de seguridad que han inducido a esta decisión, incluidas aquellas de no adquirir un determinado producto o servicio.

Una vez se tome la decisión de iniciar el proceso de contratación se debe dejar claros los riesgos de seguridad de información que el producto o servicio puede conllevar y su respectivo plan de tratamiento.

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.

Todas las gestiones de adquisición de bienes y/o servicios deben estar incluidas en el plan anual de adquisiciones.

6. CONTENIDO

6.1 SELECCIÓN DE PROVEEDORES

Esta fase se lleva a cabo a través de un estudio de mercado, la definición de la ficha técnica y el estudio previo, según los lineamientos establecidos por la Dirección de Gestión Contractual y debe intervenir el Comité Técnico de la OTEC.

En la ficha técnica debe incluirse elementos de seguridad de información para tener en cuenta al momento de cotizar. A continuación, se presentan los requisitos a tener en cuenta en la definición de estudios previos de aquellos productos o servicios que implican el acceso o gestión sobre los activos de información institucional:

a. Se requiere incluir el análisis de riesgos de seguridad de información vinculados al producto o servicio que se pretende adquirir y así mismo, definir las actividades de tratamiento, estás últimas deben ser verificadas durante la ejecución del contrato. Entre los elementos a tener en cuenta en el análisis de riesgos de seguridad de información, se encuentran:

- Activos de información que serán accedidos por el contratista.

- Requisitos legales y regulatorios aplicables al producto o servicio, evaluando que al momento de la contratación cuente con los permisos y licencias necesarias para la ejecución del contrato.

b. Es necesario definir la documentación requerida para llevar a cabo la transición del producto o servicio, métodos de intercambio de datos, reglas o registros (si aplica) que permitan gestionar la información de manera oportuna a la terminación de la relación contractual.

c. Todos los cambios del producto o servicio se deben realizar conforme a lo establecido en el procedimiento de Control de Cambios TI-PR-013 adoptado por la USPEC, con el fin de tener la trazabilidad de las acciones realizadas por el contratista.

d. El proveedor debe generar la apropiación de conocimiento por parte del personal de la Entidad involucrado en la gestión y operación del bien o servicio.

e. De forma periódica tanto el proveedor como la USPEC realizarán evaluación de riesgos de seguridad con el fin de determinar amenazas y /o vulnerabilidades que puedan afectar los productos o servicios, como resultado, se debe llevar a cabo la gestión por parte del proveedor para su mitigación de acuerdo con los ANS definidos en el contrato y según los lineamientos establecidos por la Entidad para la gestión de vulnerabilidades. Estos ANS no aplican para los contratos de compra venta.

Nota: en el caso de Colombia Compra Eficiente, se tomará como referencia los requisitos contenidos en los diferentes Acuerdo Marco de Precios o Instrumento de Agregación de Demanda.

6.2 NEGOCIACIÓN DE ACUERDOS CON PROVEEDORES

- Gestionar los cambios e incidentes de seguridad de la información de acuerdo con los procedimientos definidos por la Entidad.

- En caso que se presenten cambios en los riesgos de seguridad de la información o de los hallazgos de auditoría, la Entidad con el apoyo del proveedor debe:

  a. Identificar y evaluar los impactos en la seguridad de la información resultantes de estos cambios o auditar las no conformidades.

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

  c. 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.

6.3 GESTIÓN DE RELACIONES CON PROVEEDORES

En los análisis técnicos de riesgos de seguridad de información gestionados por la OTEC, se deben incluir los productos o servicios que se consideren pertinentes con el fin identificar, clasificar, priorizar y resolver las vulnerabilidades o debilidades detectadas sobre los mismos, que hacen parte del contrato que se está ejecutando.

Por parte de la supervisión del contrato se debe contar con una bitácora para el registro de eventos relevantes que comprometan la seguridad de la información y que se presenten durante el desarrollo del contrato, ya que serán determinantes en la generación de los procesos de lecciones aprendidas al finalizar la relación contractual.

La supervisión del contrato debe 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.

6.4 TERMINACIÓN DE LA RELACIÓN CON EL PROVEEDOR

A continuación, se presentan las actividades mínimas que se deben establecer para la finalización contractual con el proveedor del producto o servicio de seguridad de la información, con el fin de mantener la continuidad de la operación:

- El proveedor debe 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. según el producto o servicio deben ser requeridos en la entrega como mínimo:

  a. Documentación técnica del diseño y de la operación.
  b. Documentación de configuraciones y parámetros requeridos para operar adecuadamente el producto o servicio de seguridad de información.
  c. Archivos de imágenes de máquinas virtuales.
  d. Archivos de bases de datos.
  e. Archivos de bases de datos de administración de configuraciones (CMDB).
  f. Archivos que se encuentren dispuestos en los servicios de almacenamiento contratado.
  g. Toda aquella documentación sobre topologías o estructuras físicas o lógicas.

Adicionalmente, en la adquisición de sistemas de información se debe tener en cuenta la documentación relacionada en el procedimiento Ciclo de Vida del Software TI-PR-011.

- Solicitar apoyo al proveedor o al Comité Técnico de la OTEC 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.

- Cuando sea necesario el proveedor debe certificar la eliminación total y segura de los datos almacenados con herramientas especializadas que no permitan la recuperación o reúso.

- La dependencia contratante debe verificar el cambio de credenciales de acceso, eliminación de usuarios y cierre de conexiones remotas al proveedor saliente.

- Se debe generar un acta de finalización del contrato, firmada por su supervisor y los supervisores de apoyo, a través de la cual se certifique el cierre de la relación contractual y las lecciones aprendidas.

Nota: estas recomendaciones deben quedar definidas en los pliegos de condiciones de los procesos de adquisición de bienes y servicios de TI que realice la Entidad.

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
01	29/06/2023	Todos	Se crea el documento.

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Nombre: Mayra Alexandra Agudelo Carvajal	Nombre: Camilo Alejandro Romero González	Nombre: Imelda Muñoz Mancipe
Cargo: Profesional Especializado	Cargo: Coordinador Grupo Comunicaciones	Cargo: Jefe Oficina de Tecnología
Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología
	Nombre: Álvaro Camargo Barbosa	
	Cargo: Analista de Sistemas	
	Dependencia: Oficina de Tecnología	
	Nombre: Ricardo Díaz Rodríguez	
	Cargo: Profesional Universitario	
	Dependencia: Oficina de Tecnología	