UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

GESTION DE SEGURIDAD DE LA INFORMACION EN RELACION CON LOS PROVEEDORES

OFICINA ASESORA DE TECNOLOGÍAS E INFORMACIÓN

4 de noviembre de 2024

Contenido

1. INTRODUCCION

En un entorno empresarial altamente interconectado y digitalizado, la seguridad de la información se ha convertido en un pilar fundamental para garantizar la integridad, confidencialidad y disponibilidad de los datos sensibles. La colaboración con proveedores es una práctica común en las organizaciones, lo que implica compartir información crítica y confidencial. Por tanto, es imperativo establecer medidas de seguridad robustas para proteger estos datos y mitigar posibles riesgos como daño reputacional, interrupción de las operaciones, violaciones en la privacidad de los datos personales o multas o sanciones que deriven en pérdidas económicas en la cadena de suministro. En esta propuesta de gestión de seguridad de la información, se abordará de manera integral cómo fortalecer y controlar la seguridad de los datos en la relación con los proveedores, asegurando que se cumplan los estándares de seguridad necesarios para preservar la confianza, la continuidad operativa y la reputación de nuestra organización.

2. OBJETIVO GENERAL

Definir una propuesta de gestión de la seguridad de la Información para las relaciones con los proveedores, con el fin de disminuir el impacto que pueda generarse sobre la confidencialidad, integridad y disponibilidad de la información compartida con los proveedores, asegurando el cumplimiento de las políticas y procedimientos de seguridad de la información de la Universidad Distrital.

3. OBJETIVOS ESPECIFICOS

- Exigir el cumplimiento por parte de los proveedores, de los requisitos de seguridad de la información definidos por la Universidad Distrital mediante los compromisos establecidos en los acuerdos y contratos.
- Establecer mecanismos de control con los proveedores, asegurando que la información y los servicios provistos por estos, cumplan con las políticas y procedimientos de seguridad de la información definidas por la Universidad Distrital
- Dar los criterios, orientaciones y/o recomendaciones a utilizar al interior de la Universidad Distrital asegurando el manejo adecuado de los activos de información por parte de los proveedores.

4. ALCANCE

Esta propuesta se aplica a todos los proveedores que, en el curso de sus servicios, tienen acceso, manejan o procesan información de la Universidad Distrital. Esto incluye proveedores de servicios tecnológicos, consultores, contratistas, proveedores de hardware y software, así como proveedores de servicios en la nube. De igual forma, aplica a las dependencias y funcionarios relacionados con los procesos y/o servicios con proveedores.

5. CONTEXTO

En el entorno empresarial actual, la colaboración con proveedores externos es una práctica común y necesaria para el éxito y la competitividad de las organizaciones. Esta colaboración introduce riesgos de seguridad de la información que deben gestionarse cuidadosamente. Los proveedores, que pueden tener acceso a datos sensibles, sistemas críticos y procesos esenciales, se convierten en puntos vulnerables si no se implementan las medidas adecuadas de seguridad.

La relación con los proveedores puede exponer a la organización a diversos tipos de riesgos de seguridad de la información, tales como accesos no autorizados, pérdida de datos, incumplimiento de normativas, y ataques cibernéticos. Estos riesgos pueden surgir por varios factores, como la falta de controles de seguridad en los proveedores, la insuficiente capacitación de su personal o la inadecuada gestión de incidentes de seguridad.

El propósito de esta propuesta es que una vez implementada se mitiguen los riesgos de seguridad de la información asociados con la relación con proveedores, proporcionando una comprensión profunda de los posibles puntos de vulnerabilidad y las amenazas que pueden afectar la integridad, confidencialidad y disponibilidad de la información.

6. PLANIFICACIÓN

En esta sección, es necesario determinar una estrategia metodológica que facilite el establecimiento de políticas, objetivos, procesos y procedimientos relevantes. Esto ayudará a la Universidad Distrital Francisco José de Caldas a preparar adecuadamente las TIC para garantizar la seguridad de la información en la relación con los proveedores.

6.1. Metas de preparación de las TIC para la Gestión de seguridad de la información en la relación con los proveedores

De acuerdo con el “Plan Indicativo 2022-2025”, se plantean las siguientes metas de preparación de las TIC para la seguridad de la información en la relación con los proveedores, alineado con:

- “Eje transformador 1. Fortalecimiento curricular y aseguramiento de la calidad” y el lineamiento “Implementación de estrategias que permitan contar con información institucional confiable y pertinente que redunden en reportes de información con criterios de calidad.”
- “Eje transformador 2. Modernización institucional” y los lineamientos “Conformación e implementación de una Unidad con carácter directivo que coordine y lidere los procesos relacionados con TIC en la U. Distrital” y “Fortalecimiento del Sistema Integrado de Gestión de la Universidad, SIGUD y su marco de referencia el Modelo Integrado de Planeación y Gestión, MIPG, de tal manera que se consolide como una herramienta integrada para la gestión institucional.”
- “Eje transformador 4. Talento Humano y Bienestar” y el lineamiento “Integrar la gestión de información que garantice la adecuada caracterización con transparencia de la información y las acciones realizadas para los diversos apoyos brindados a la comunidad universitaria.”

- “Eje transformador 5. Transformación digital” y el lineamiento “Implementación de una estrategia de transformación digital en la Universidad Distrital que este fundamentada en las tecnologías disruptivas para brindar servicios de alto valor además de emprendimientos digitales.”

Estas son consignadas en la política general de seguridad de la información en su apartado de relación con los proveedores:

- La universidad establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.
- Antes de iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesaria durante y después del contrato.

6.2. Conformación del Equipo de trabajo y Plan de trabajo

Para establecer los mecanismos de control de seguridad de la información en las diferentes etapas de la relación con los proveedores sobre la información a la que tengan acceso y/o a la que sea requerida para la prestación de sus servicios, la Oficina Asesora de Tecnologías e Información (OATI) debe conformar un equipo de personas y definir un Plan de trabajo que contemple al menos las etapas, actividades y actores con sus responsabilidades según se detallan más adelante.

El equipo del proyecto responsable de la implementación de la propuesta de gestión de seguridad de la información en la relación con los proveedores debe estar conformado por:

- La Oficina Asesora Jurídica
- La Oficina de Contratación
- La Oficina Asesora de Tecnologías e Información (OATI)
- La Oficina de Control Interno
- Oficina Asesora de Planeación

Los responsables de las áreas contratantes se encargarán de verificar que los proveedores cumplan con los requisitos de seguridad establecidos con el apoyo de la OATI y los responsables de cada área de la Universidad Distrital garantizarán que la información compartida con los proveedores sea la mínima necesaria y esté clasificada.

Las responsabilidades especificas son:

- La Oficina Jurídica, que debe ser la encargada de la adecuación de los procesos contractuales que regulen la relación con los proveedores.
- La Oficina de Contratación, quienes revisaran el cumplimiento de las políticas y los procesos de contratación definidos para la institución.

- La Oficina Asesora de Tecnologías e Información, que definirá los requerimientos mínimos de seguridad de la información y evaluará los controles definidos en el proveedor que presta el servicio.
- La Oficina de Control Interno para definir los criterios para validar el cumplimiento continuo de los proveedores con los requisitos de seguridad de la información, con el fin de identificar y abordar posibles desviaciones o riesgos.
- La Oficina de Planeación, que incluirá las modificaciones en los respectivos formatos para exigir a los proveedores el cumplimiento de los requisitos de seguridad de la información.

Responsable: OATI

6.3. Cronograma de implementación

Las actividades que deben incluirse en el cronograma del Plan de trabajo para la implementación de la propuesta de gestión de seguridad de la información en la relación con los proveedores, incluyendo los responsables son:

ACTIVIDADES	RESPONSABLE	MES	RECURSOS
Definición del equipo del proyecto	OATI	1	Sujeto a disponibilidad de recursos
Definición de Cronograma	Equipo del Proyecto	1	Sujeto a disponibilidad de recursos
Asignación de presupuesto	OATI	2	Sujeto a disponibilidad de recursos
Definición de los Requisitos de seguridad de la información	OATI	2	Sujeto a disponibilidad de recursos
Definición de criterios de selección	OATI	3	Sujeto a disponibilidad de recursos
Definición de metodología de análisis de riesgos	OATI	3	Sujeto a disponibilidad de recursos
Identificación de requisitos legales y regulatorios	Oficina Jurídica	4	Sujeto a disponibilidad de recursos
Definición de roles y responsabilidades	Equipo del Proyecto	4	Sujeto a disponibilidad de recursos
Identificación de requisitos mínimos de seguridad de la información	OATI	5	Sujeto a disponibilidad de recursos

Mejora o definición de cláusulas contractuales	Oficina Jurídica	5	Sujeto a disponibilidad de recursos
Modificación de procedimiento de cambios	OATI	6	Sujeto a disponibilidad de recursos
Modificación de procedimiento de incidentes	OATI	6	Sujeto a disponibilidad de recursos
Definición de procedimiento de monitoreo	OATI	7	Sujeto a disponibilidad de recursos
Definición de Plan de Terminación	OATI	7	Sujeto a disponibilidad de recursos
Definición de Estrategia de concientización	OATI	8	Sujeto a disponibilidad de recursos
Definición de Auditoria en proveedores	Oficina de Control Interno	8	Sujeto a disponibilidad de recursos
Definición de procedimiento de mejora continua	OATI	9	Sujeto a disponibilidad de recursos
Definición de métricas de desempeño	OATI	10	Sujeto a disponibilidad de recursos
Modificación de Formatos	Equipo del Proyecto	11	Sujeto a disponibilidad de recursos
Definición procedimiento de Seguridad de la información en la relación con los proveedores	OATI	12	Sujeto a disponibilidad de recursos

Responsable: Equipo del Proyecto

6.4. Recursos y Presupuesto

En el documento ficha MGA están definidas las partidas presupuestales para la actividad de implementación del modelo gestión de seguridad y privacidad de la información en relación con los proveedores, en el cual se detallan las siguientes actividades:

- lmplementación del modelo de seguridad y privacidad de la información en relación con los proveedores
- Evaluación del cumplimiento de los proveedores del modelo de seguridad y privacidad de la información.
- Ejecutar, revisar e institucionalizar el informe de la implementación del modelo de gestión de seguridad y privacidad de la información en relación con los proveedores

Responsable: OATI

6.5. Definir los requisitos de seguridad de la información que se desea contratar

La Universidad Distrital Francisco José de Caldas debe definir una única vez los aspectos relacionados a la seguridad de la información y calidad del servicio, incluyendo aspectos como cumplimiento normativo, desarrollo de software, conectividad, equipos, control de cambios, auditoria, control de acceso, plazos incumplimientos, disponibilidad y continuidad.

La aplicación de estos requisitos de seguridad de la información (**Ver Anexo 1. Requerimientos de Seguridad de la Información para proveedores)** debe ser revisada de acuerdo al servicio que prestará el proveedor.

Responsable: OATI

6.6. Definir los criterios de selección de proveedores

Los criterios de selección de proveedores, de acuerdo con los requisitos de seguridad de la información deberán incluir lo siguiente:

- Aceptación por parte del proveedor de los requisitos de seguridad de la información definidos en el pliego de condiciones
- Madurez del proveedor en seguridad de la información. Esta madurez se puede definir solicitando al proveedor que tenga una certificación ISO/IEC 27001 o que proporcione documentación de seguridad de la información, como continuidad del servicio documentada y probada, planes para garantizar su capacidad para admitir activaciones simultáneas por parte de diferentes clientes de planes de recuperación y gestión de incidentes. Si no existe una certificación ISO 27001 por parte del proveedor, es necesario validar la madurez del proveedor en temas de seguridad de la información mediante un monitoreo de implementación de controles asociados a seguridad de la información.
- Los términos bajo los cuales el proveedor permite ser auditado por la Universidad Distrital Francisco José de Caldas (**Ver Anexo 1. Requerimientos de Seguridad de la Información para proveedores)** o por un tercero autorizado para verificar el cumplimiento de los requisitos de seguridad de la información definidos
- Acuerdo de confidencialidad para ser firmado por el proveedor para proteger la información transmitida durante el proceso de selección de proveedores.
- Aceptación por parte del proveedor de salvaguardar la confidencialidad, integridad y disponibilidad de los datos personales a los cuales tiene acceso dentro del servicio contratado, así como cumplir todas las exigencias sobre datos personales establecidas por la Superintendencia de Industria y Comercio.
- Los resultados de la evaluación de riesgos de seguridad de la información efectuada al proveedor

Responsable: OATI

6.7. Definir o aplicar metodología existente para identificar y evaluar los riesgos

Aplicando el Manual de Gestión de Riesgos de la Universidad Distrital Francisco José de Caldas se debe garantizar que esta evaluación de riesgos de seguridad de la información:

- Es proporcional a la criticidad del producto o servicio que se planea adquirir;
- 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.
- Identifica el nivel aceptable de riesgos en la relación con el potencial proveedor;
- Identifica y evalúa opciones para el tratamiento de los riesgos identificados y evaluados;

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.

Responsable: OATI

6.8. Requerimientos legales y regulatorios

Identificación e inclusión de los requisitos legales y regulatorios aplicables a la Universidad Distrital Francisco José de Caldas, y las áreas de leyes y reglamentos que vinculan al proveedor potencial que deben revisarse durante el proceso de selección de proveedores, a saber:

- 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.
- Propiedad intelectual de terceros; y
- Otros requisitos legales y reglamentarios, como leyes fiscales, responsabilidad por productos defectuosos, facultades de investigación.

Responsable: Oficina Asesora Jurídica

6.9. Requisitos mínimos de seguridad de la información

La OATI debe definir los requisitos mínimos de seguridad de la información basados en el documento **Anexo 2, e**l cual servirá para evaluar la madurez del proveedor frente a seguridad de la información y que, en conjunto con la aplicación de la metodología de riesgo, permitirá establecer los controles necesarios a implementar en el proveedor.

Responsable: OATI y Supervisor del contrato

6.10. Definición o mejoramiento de las cláusulas contractuales

La oficina Jurídica debe revisar las cláusulas referentes al cumplimiento de los requisitos de seguridad de la información en la relación con los proveedores, incluyendo clausulas referentes a confidencialidad de la información, protección de datos personales, requerimientos de seguridad de la información, riesgos y continuidad del proveedor y la definición de las posibles sanciones que puede imponer la Universidad Distrital Francisco José de Caldas en caso de incumplimiento de los requisitos de seguridad de la información. (**Ver Anexo 3. Clausulas Proveedores)**

Responsable: Oficina Asesora Jurídica

6.11. Definición de la metodología de cambios

Acordar y definir con el proveedor la metodología para el manejo los cambios en el contrato con el proveedor y basados en el análisis de riesgo efectuado y las medidas correctivas aplicables.

Estos cambios pueden generarse por:

- 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;
- Cambio en la capacidad de soportar las capacidades requeridas de continuidad del negocio;
- Cambio en los requisitos legales, regulatorios y contractuales aplicables a la organización.
- Cambios en los aspectos de seguridad de la información
- Cambios necesarios por identificación de no conformidades generados por revisiones de auditoria

Responsable: OATI

6.12. Definir o actualizar el procedimiento de Incidentes de Seguridad

Exigir al proveedor la definición de un procedimiento de gestión de incidentes que incluya:

- Notificación de Incidentes: Procedimientos para la notificación y gestión de incidentes de seguridad de la información por parte de los proveedores.
- Respuesta y Recuperación: Planes de respuesta y recuperación ante incidentes que involucren a proveedores.
- Si el proveedor no cuenta con el procedimiento de gestión de incidentes, puede aplicar el definido por la Universidad Distrital Francisco José de Caldas
- Acordar con el proveedor el reporte inmediato de cualquier incidente de seguridad de la información en el contrato con el proveedor.

Responsable: OATI

6.13. Definir un procedimiento de monitoreo y revisión de la calidad del servicio para los proveedores

Definir un procedimiento de monitoreo para validar la implementación y efectividad de los controles de seguridad de la información, teniendo en cuenta los aspectos establecidos en los contratos. Este procedimiento de monitoreo debe incluir entre otras cosas lo siguiente:

- 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 Universidad Distrital Francisco José de Caldas.
- Evaluación de riesgos de seguridad de la información de forma periódica en acuerdo 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
- Validación de las estrategias de continuidad del negocio, pruebas de verificación sobre los planes de continuidad del servicio, recuperación y gestión de incidentes.
- Verificación de la ejecución del plan de capacitación y realizar las mediciones sobre la efectividad y nivel de apropiación de los conocimientos de los asistentes.
- Revisión del plan de gestión de cambios que permite tener control y trazabilidad de las acciones realizadas por el proveedor
- Realización de un monitoreo de las actividades y acciones de los servicios en la nube

Responsable: OATI

6.14. Establecer un Plan de Terminación

Este debe contemplar diversas actividades con el objetivo de mantener la continuidad en la operación, para ello es necesario que incluya:

- Descripción de 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.
- Establecimiento entre las partes, de quien coordinará las actividades de cierre de los servicios contratados según el plan de finalización.
- 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.
- Listado de 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, 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.
- Solicitud de apoyo al proveedor 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.
- Solicitud de 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.

- Acta de finalización del proceso contractual avalada y firmada por el supervisor, en el cual certifica el cierre del proceso contractual.
- Verificación del cambio de credenciales de acceso, eliminación de usuarios y cierre de conexiones remotas al proveedor saliente.

Responsable: OATI

6.15. Transferencia de conocimiento y sensibilización

Establecer estrategias de transferencia de conocimiento y sensibilización sobre seguridad de la información para los proveedores, asegurando que comprendan sus responsabilidades y los estándares de seguridad requeridos.

Responsable: OATI

6.16. Auditorías de Cumplimiento

Incorporar auditorías periódicas para verificar el cumplimiento continuo de los proveedores con los requisitos de seguridad de la información, con el fin de identificar y abordar posibles desviaciones o riesgos.

Los objetivos de la auditoria deben ser:

- Evaluar de forma objetiva si se han implementado los controles adecuados para mitigar los riesgos informáticos.
- Probar el cumplimiento de las regulaciones por parte de terceros.
- En caso de incumplimientos, brindarles la oportunidad de ser partícipes de la solución.
- Emitir recomendaciones y mejores prácticas con el fin de mejorar su desempeño.

Los aspectos que deben ser tenidos en cuenta son:

- Políticas y procedimientos de seguridad en términos de desarrollo de código (aplicativos y sistemas)
- El estado actual de las redes de comunicación.
- El cumplimiento de las normas vigentes como es el caso de la ISO 27001 que tiene como objetivo velar por el mejoramiento constante de la seguridad de la información en las organizaciones.
- La capacitación del personal a cargo del uso de la tecnología.
- Detectar oportunidades de mejora.
- Las vulnerabilidades informáticas.
- La protección de datos y resguardo de la información.
- Supervisar los acuerdos de nivel de servicio (SLA).

Responsable: Oficina de Control Interno

6.17. Revisión y Mejora Continua

Incorporar un ciclo de revisión y mejora continua en el plan de relación con proveedores, permitiendo ajustes y actualizaciones basados en lecciones aprendidas, cambios en el entorno de amenazas y requisitos regulatorios.

Cuando se identifique una oportunidad de mejora se deberá:

- Reaccionar al hallazgo, y, según sea el caso se deberán adoptar las medidas necesarias para controlar y corregir, además de hacer frente a todas las consecuencias.
- Es necesario evaluar la necesidad de adoptar medidas para eliminar las causas de no conformidad con el fin de que no vuelva a ocurrir o que no se produzcan en otros lugares. Esto se puede conseguir mediante la revisión del hallazgo, estableciendo las causas de dicha no conformidad y determinando si existen incumplimientos similares o si puede ocurrir de forma potencial.
- Poner en práctica las medidas oportunas.
- Revisar la eficiencia de las medidas correctoras llevadas a cabo.
- Realizar los cambios necesarios, si es el caso.

Responsable: OATI

6.18. Definición de Métricas de Desempeño

Incluir métricas cuantificables para evaluar el cumplimiento de los proveedores con los requisitos de seguridad de la información definidos en los contratos.

Las métricas deben incluir:

- % de (Numero de riesgos tratados / Numero de riesgo identificados) * 100
- Número de incidentes presentados en el proveedor a fecha de corte
- % de (Numero de cambios a la plataforma tecnológica que soporta el servicio / Numero de cambios presentados en el proveedor) * 100
- % de (número de empleados del proveedor capacitados en seguridad de la información / Número total de empleados del proveedor) * 100
- Numero de hallazgos identificados en las auditorías realizadas

Responsable: OATI

6.19. Modificación de Políticas y procedimientos

Los siguientes políticas o procedimientos de Control de cambios, incidentes, monitoreo, mejora continua, auditoria de proveedores, plan de terminación y gestión de riesgos deben ser definidos o modificados para incluir los diferentes requisitos mencionados anteriormente.

6.20. Modificación de Formatos

Los siguientes formatos deben ser modificados para incluir los diferentes requisitos:

- GC-PR-003-FR-008 Estudios y documentos previos solicitud de adquisición de bienes y servicios.
- En este formato se puede incluir definir requerimientos que se desea contratar en el capítulo Definición de la necesidad (objeto del contrato)
- En este formato se puede incluir efectuar análisis de riesgos en el capítulo evaluación posible riesgos
- En este formato se puede incluir validar el cumplimiento requisitos de seguridad de la información en el capítulo requisitos para evaluar y comparar propuestas.
- En este capítulo se puede incluir calificar al proveedor por cumplimiento de requisitos de seguridad de la información en el capítulo cumplimiento requisitos de seguridad de la información en el capítulo requisitos para evaluar y comparar propuestas
- En este formato se puede incluir madurez en seguridad información en el capítulo de documentos técnicos (certificación en seguridad de la información)
  En este formato se puede incluir aplicar criterios de selección proveedores en el capítulo Requisitos para evaluar y comparar propuesta.
  GC-PR-003-FR-012 Cumplido a satisfacción por parte de la dependencia. En este formato se puede incluir el Plan de terminación (incluyendo todo lo de la propuesta)
- GC-PR-006-FR-028 Evaluación y revaluación de proveedores. En este formato se puede incluir el Plan de terminación (incluyendo todo lo de la propuesta)

Responsable: OATI y Oficina Asesora de Planeación

7. EJECUCIÓN

Cada vez que se vaya a contratar un proveedor que tenga acceso a información sensible o crítica de la Universidad Distrital, se deben adelantar las siguientes actividades:

7.1. ANTES DE LA CONTRATACION

- Definir los requisitos que se desea contratar
- Efectuar análisis de riesgo al posible proveedor
- Identificar los requisitos legales y regulatorios
- Aplicar los criterios de selección de proveedores.
- Validar el cumplimiento de los requisitos mínimos de seguridad de la información en el proveedor
- Calificar el proveedor frente al cumplimiento de los requisitos de seguridad

7.2. DURANTE LA EJECUCION DEL CONTRATO

- Implementar los programas de capacitación y sensibilización en seguridad de la información en el proveedor
- Aplicar la metodología de cambios (si aplica)
- Aplicar el procedimiento de incidentes de seguridad (si aplica)
- Aplicar el procedimiento de monitoreo y revisión de la calidad del servicio para los proveedores

- Realizar auditorías de cumplimiento
- Efectuar revisión y mejora continúa resultado de la relación con el proveedor
- Evaluar las métricas de desempeño

7.3. FINALIZACION DEL CONTRATO

Aplicar el Plan de terminación

ANEXO 1. REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION PARA PROVEEDORES

Este documento se refiere exclusivamente a lineamientos y estándares de seguridad generales, que deberán adoptarse según las particularidades del servicio prestado a la Universidad Distrital Francisco José de Caldas. Dado que EL CONTRATISTA es el único y directo responsable de la operación y aseguramiento de toda su infraestructura, deberá ser consciente y convenientemente actualizado de los riesgos y amenazas de seguridad que puedan surgir; en este sentido deberá contar con políticas y procedimientos complementarios a los lineamientos y estándares aquí establecidos, que le aseguren el establecimiento y mantenimiento de niveles óptimos de seguridad.

Por lo anterior, EL CONTRATISTA se compromete a cumplir a cabalidad este anexo en la ejecución del contrato u orden de compra del que hace parte integral.

CUMPLIMIENTO NORMATIVO O REGULATORIO.

- EL CONTRATISTA deberá contar con políticas, procedimientos, estándares y/o metodologías de seguridad de la información, riesgos y continuidad del negocio, debidamente documentadas, implementadas, monitoreadas y auditables.
- EL CONTRATISTA deberá contar con líneas base de seguridad o plantillas de hardening sobre los sistemas operativos, elementos de red, bases de datos, aplicaciones y cualquier dispositivo (desktop, laptop y/o equipos móviles) que sea utilizado para la prestación del servicio contratado por la Universidad Distrital Francisco José de Caldas.
- EL CONTRATISTA deberá contar con políticas, estándares y procedimientos definidos y auditables de control de acceso y manejo de perfiles sobre los sistemas o elementos de red que soporten el servicio contratado.
- EL CONTRATISTA deberá contar con políticas, procedimientos y controles sobre los cambios que se realicen sobre cualquier infraestructura (software, hardware y middleware) que soporte el servicio contratado.
- EL CONTRATISTA declara conocer y se obliga a cumplir las normas ISO 27001 que le apliquen de acuerdo con los procesos y servicios desarrollados para la Universidad Distrital Francisco José de Caldas.

- El CONTRATISTA tendrá cláusula de confidencialidad firmada con Universidad Distrital Francisco José de Caldas.
- EL CONTRATISTA se obliga a dar cumplimiento a los lineamientos establecidos por las leyes 1266 de 2008 y 1581 de 2012, así como sus decretos y circulares reglamentarios.
- EL CONTRATISTA deberá exigir cláusula de confidencialidad a sus empleados y colaboradores.
- EL CONTRATISTA deberá implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.
- EL CONTRATISTA deberá adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.
- EL CONTRATISTA deberá realizar periódicamente campañas de sensibilización en seguridad de la información.
- Es responsabilidad de EL CONTRATISTA validar los antecedentes del personal asignado a la prestación del servicio con la Universidad Distrital Francisco José de Caldas, deberá corroborar que no ha sido sancionado por problemas de confidencialidad de información o fallas profesionales.
- EL CONTRATISTA deberá establecer cláusula en el contrato del empleado que permita tomar acciones correctivas frente a la divulgación de información sensible posterior a la finalización del contrato.
- EL CONTRATISTA deberá solicitar las autorizaciones de los titulares para realizar la consulta de base de datos en centrales de riesgo, así como para la recolección, almacenamiento y tratamiento de datos personales.
- El CONTRATISTA implementará los controles que le permitan conservar y proteger la información suministrada por la Universidad Distrital Francisco José de Caldas, para la ejecución de los servicios contratados, impidiendo su deterioro, pérdida, alteración, uso no autorizado o fraudulento.
- EL CONTRATISTA deberá atender los requerimientos que sean realizados por la Superintendencia de Industria y Comercio sobre los titulares que hayan sido consultados.
- EL CONTRATISTA deberá dar buen uso de los tokens entregados para el acceso a los sistemas designados por la Universidad Distrital Francisco José de Caldas, cumpliendo con los controles necesarios para asegurar la confidencialidad de los datos que entregan estos dispositivos.

DESARROLLO DE SOFTWARE

EL CONTRATISTA debe contar con una metodología para cumplir el ciclo de desarrollo seguro de software la cual puede ser auditada por la Universidad Distrital Francisco José de Caldas, siempre y cuando el objeto del contrato sea el desarrollo de software y/o aplicaciones, para ello debe contemplar:

- Establecer requisitos de seguridad y privacidad
- Realizar evaluaciones de riesgos de seguridad y privacidad.
- Establecer requisitos de diseño.
- Análisis / Reducción de vectores de ataque
- Modelamiento de amenazas
- Utilizar herramientas aprobadas

- Desactivar funciones inseguras
- Realizar análisis estático
- Realizar análisis dinámico
- Pruebas de fuzzing (introducción deliberada de datos malformados o aleatorios)
- Revisión de vectores de ataque
- Crear un plan de respuesta a incidentes
- Realizar la revisión final de seguridad
- Certificar software para puesta en producción
- Ejecutar un plan de respuesta a incidentes y corrección de vulnerabilidades identificadas en el Sistema de información.

CONECTIVIDAD EXTERNA CON LA RED DE LA UNIVERSIDAD DISTRITAL

El CONTRATISTA debe contar con conexiones cifradas para garantizar la confidencialidad e integridad de la información que es intercambiada con la Universidad Distrital Francisco José de Caldas.

EL CONTRATISTA deberá cumplir con las siguientes condiciones técnicas:

- Interfaces físicas: Compatibilidad en los tipos de interfaz y verificación de las conexiones.
- Última milla: Disponibilidad controlada.
- Ubicación y espacio: Reservar la ubicación y el espacio de los elementos, garantizar el control de temperatura / condiciones ambientales (humedad, temperatura, disipación térmica, ruido, ventilación, etc.)
- Control de acceso: Procedimientos implementados de control de acceso físico y lógico sobre los equipos que soportan el servicio.
- Aislamiento de manera lógica: Aislar virtualmente el tráfico con los otros segmentos de red conectados en el mismo dispositivo o dominio.
- Servicios de NAT (Network Address Traslation): Deberán ser conciliados entre las partes para el correcto funcionamiento de las aplicaciones y la correcta asignación de direcciones IP.
- Servicios de PAT (Port Address Traslation): Los servicios PAT están restringidos y no deben ser configurados.
- Documentación del servicio: Ingeniera de detalle de la red que soportara los servicios. Seguridad perimetral: Contar con firewall y mecanismos de conexión cifrada de extremo a extremo.
- EL CONTRATISTA deberá asegurar de extremo a extremo los canales de comunicación y garantizar que los mismos no sean susceptibles de ser manipulados o conocidos por personal ajeno a la prestación del servicio.
- Los dispositivos de red de EL CONTRATISTA que se involucren en la conectividad deberán estar protegidos y asegurados.
- EL CONTRATISTA deberá contar con controles perimetrales que garanticen la confidencialidad, disponibilidad e integridad de la información de la Universidad Distrital Francisco José de Caldas.
- EL CONTRATISTA no hará uso de protocolos o servicios de comunicación inseguros (no cifrados) y deberá deshabilitar, de cualquier dispositivo de red, aquellos servicios que no sean necesarios o utilizados.

- Todos los servidores o estaciones involucradas con actividades del servicio prestado a la Universidad Distrital Francisco José de Caldas que se ubiquen en la red de EL CONTRATISTA deberán estar convenientemente aislados en una zona independiente. Estos servidores no deberán ubicarse lógicamente en zonas expuestas a tráfico proveniente de internet (por ejemplo, la zona DMZ) ni tampoco convivir con servidores de EL CONTRATISTA que no estén relacionados con la operación del servicio prestado a la Universidad Distrital Francisco José de Caldas.
- EL CONTRATISTA deberá contar con estándares de direccionamiento para redes privadas.
- EL CONTRATISTA deberá realizar análisis periódicos de vulnerabilidades técnicas sobre los dispositivos de red involucrados en la prestación del servicio, y cerrará cualquier brecha de seguridad identificada por esta actividad. La Universidad Distrital Francisco José de Caldas en cualquier momento, podrá desarrollar dichos ejercicios, previa coordinación y validación con EL CONTRATISTA.
- EL CONTRATISTA deberá contar con mecanismos que permitan realizar la trazabilidad punta a punta de cualquier evento de operación o seguridad que se genere durante la prestación del servicio.
- EL CONTRATISTA deberá contar con planes de continuidad que garanticen la prestación del servicio, incluyendo: infraestructura tecnológica, sistemas de información, canales de comunicación, recurso humano y su correspondiente escala de comunicaciones para manejar eventos disruptivos.

EQUIPOS DE CONTRATISTA EN EJECUCIÓN DEL CONTRATO.

EL CONTRATISTA se obliga a que todos los equipos de trabajo que utilice en la ejecución del contrato:

- Contarán con sistemas de antivirus, antispyware y/o antimalware licenciados, legalmente adquiridos y vigentes.
- Contarán con sistemas operativos, bases de datos y herramientas de ofimática soportadas por el fabricante.
- Contarán con su propio dominio de correo electrónico; está prohibido el uso de correo de dominio público.
- Contarán con procedimientos claramente definidos y de ejecución periódica para implementación de actualizaciones de seguridad (parches) en las plataformas.
- Contarán con repositorios lógicos y/o físicos de información internos y con controles de acceso claramente definidos para garantizar que no será expuesta información confidencial de la Universidad Distrital Francisco José de Caldas.
- Los equipos de funcionabilidad portable deberán está debidamente cifrado, así mismo, el contratista deberá contar con un repositorio de credenciales.
- Los usuarios asignados por el contratista deberán estar basado en el menor privilegio requerido para el correcto desempeño de sus funciones.
- El contratista deberá prohibir la conexión o instalación no autorizada de cualquier clase de dispositivo de comunicaciones o software que modifique o revise la topología de la red de la organización.
- El CONTRATISTA deberá garantizar un borrado seguro de la información propiedad de la

Universidad Distrital Francisco José de Caldas en los siguientes casos: A) Finalice el contrato, B) el usuario responsable sea retirado de proyecto con la Universidad Distrital Francisco José de Caldas o es retirado de la compañía, C) Renovación de tecnología o tecnología obsoleta, D) Información histórica no requerida por el proyecto. Y deberá notificar oportunamente a la Universidad Distrital Francisco José de Caldas solicitando la debida autorización.

- EL CONTRATISTA deberá realizar mantenimiento preventivo a los equipos que asegure su disponibilidad y su integridad.
- El software utilizado por EL CONTRATISTA para prestar el servicio a la Universidad Distrital Francisco José de Caldas debe ser usado dentro de los términos y condiciones establecidos en su licenciamiento, lo cual incluye las restricciones de uso establecidas en las licencias de software libre. Lo anterior aplica indiferentemente si el software se instala en algún equipo del CONTRATISTA o es accedido por el mismo en la plataforma de un tercero en modalidad software como servicio. Cualquier condición de licenciamiento que brinde al fabricante o representante del software o de la plataforma, a cambio del uso de la herramienta, algún tipo de derecho sobre la información que la Universidad Distrital Francisco José de Caldas comparte con el proveedor, de inmediato hace no viable el uso de dicho software.
- El CONTRATISTA será responsable frente a los incidentes que se puedan generar por la instalación incontrolada de Software, cuya consecuencia sea fuga, perdidas de integridad y/ o genere indisponibilidad de la información propiedad de la Universidad Distrital Francisco José de Caldas, así como por la violación de los derechos de propiedad intelectual en la que lleguen a incurrir.

EQUIPOS DE CONTRATISTA EN LA RED DE LA UNIVERSIDAD DISTRITAL

EL CONTRATISTA se obliga a que todos los equipos de trabajo que utilice en la ejecución del contrato estarán sujetos al cumplimiento de los siguientes lineamientos y estándares:

- Cumplir con las políticas, procedimientos y estándares de seguridad de la Universidad Distrital Francisco José de Caldas.
- Estar registrados en el dominio o dominios de la Universidad Distrital Francisco José de Caldas.
- Contar con un usuario y contraseña el cual es personal e intransferible.
- Contar con sistemas de antivirus, antispyware y/o antimalware debidamente licenciados y legalmente adquiridos. Si la Universidad Distrital Francisco José de Caldas lo considera conveniente se podrá instalar el antivirus corporativo en las estaciones de EL CONTRATISTA durante la ejecución del contrato.
- El CONTRATISTA deberá informar oportunamente a la Universidad Distrital Francisco José de Caldas cuando un colaborador suyo haya dejado de prestar sus servicios.
- Ningún colaborador del CONTRATISTA deberá retirar información de la Universidad Distrital Francisco José de Caldas de sus instalaciones sin la autorización previa y escrita de un representante de la Universidad Distrital Francisco José de Caldas.
- Los equipos deberán tener única y exclusivamente el software autorizado por la Universidad Distrital Francisco José de Caldas.
- Antes de finalizar el contrato, el CONTRATISTA debe garantizar o permitir un borrado seguro de la información propiedad de la Universidad Distrital Francisco José de Caldas.

- EL CONTRATISTA entiende y acepta que no está permitido el uso de medios removibles o unidades de almacenamiento externas que no sean proporcionados por la Universidad Distrital Francisco José de Caldas.
- Permitir la instalación de software proveído por la Universidad Distrital Francisco José de Caldas.

CONTROL DE CAMBIOS Y AUDITORIAS DE SEGURIDAD

EL CONTRATISTA estará en la obligación de comunicar oportunamente a la Universidad Distrital Francisco José de Caldas cualquier cambio a la infraestructura (software, hardware y middleware) que soporte el servicio contratado y pueda afectar directa o indirectamente el nivel de seguridad establecido. Igualmente, EL CONTRATISTA estará sujeto a auditorías por parte de la Universidad Distrital Francisco José de Caldas, que se acordarán para verificar el cumplimiento de los requerimientos de seguridad y realizar las observaciones y recomendaciones del caso.

EL CONTRATISTA deberá estar dispuesto en cuanto a la atención y respuesta de las auditorías realizadas por Seguridad de la Información.

CONTROL DE ACCESO

- Al recibir un usuario y una contraseña, EL CONTRATISTA acepta las condiciones de la Universidad Distrital Francisco José de Caldas y se compromete a usar adecuadamente y mantener la confidencialidad que ella otorga. En ninguna circunstancia, EL CONTRATISTA está autorizado a compartir sus usuarios y claves. Es responsabilidad del CONTRATISTA transmitir a las personas a su cargo el carácter confidencial, privado e intransferible de los usuarios y contraseñas que la Universidad Distrital Francisco José de Caldas otorga a cada uno. El mismo sentido compartir cualquier usuario o contraseña será un incumplimiento grave. De detectarse y comprobarse esta conducta, la Universidad Distrital Francisco José de Caldas, tomará todas las acciones disciplinarias, penalizaciones o sanciones definidas contractualmente a las que haya lugar.
- Participar activamente en el proceso de certificación y depuración de cuentas de usuarios, confirmando la existencia de sus usuarios y reportando irregularidades detectadas.
- Ser el responsable por el buen uso de los accesos otorgados a plataformas de la Universidad Distrital Francisco José de Caldas.
- Informar de manera inmediata a la Universidad Distrital Francisco José de Caldas cualquier incidente de seguridad presentado con los accesos otorgados por la Universidad Distrital Francisco José de Caldas.
- Informar de manera inmediata a la Universidad Distrital Francisco José de Caldas, las bajas o cambios con relación a privilegios de acceso debido a retiros, trasferencias y/o cambios de funciones o actividades.

PLAZO DE IMPLEMENTACION DE OBLIGACIONES POR PARTE DEL CONTRATISTA

EL CONTRATISTA contará con un plazo máximo de 2 meses contados a partir de la firma del contrato u otro si para dar cumplimiento a los lineamientos establecidos en el presente anexo.

EL CONTRATISTA dispondrá de un plazo máximo de 2 meses para corregir las vulnerabilidades que se identifiquen posterior a la ejecución de escaneo y/o ethical hacking solicitados por la Universidad Distrital Francisco José de Caldas.

INCUMPLIMIENTO

Cuando al CONTRATISTA incumpla cualquiera de las obligaciones establecidas en el anexo, la Universidad Distrital Francisco José de Caldas podrá imponer multas equivalentes al uno por ciento (1%) del valor del contrato por cada día de retraso en el cumplimiento de sus obligaciones.

18. ANEXO 2. REQUISITOS MINIMOS DE SEGURIDAD DE LA INFORMACON QUE SE ACORDARAN CON EL PROVEEDOR

De acuerdo con los resultados del análisis de riesgo efectuado en el proveedor se deberán implementar los controles de los siguientes temas:

- Política de seguridad
- Diagrama de red
- Concientización, educación y formación en seguridad de la información
- Controles de accesos físico
- Gestión de cambios
- Segregación de tareas
- Registros de auditoría
- Política de control de acceso
- Política de escritorio y pantalla limpios
- Políticas sobre el uso de servicios en red
- Protección de datos de prueba del sistema
- Control de vulnerabilidades técnicas
- Gestión de incidentes de seguridad de la información.
- Continuidad del negocio y evaluación de riesgos
- Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio
- Seguridad en dispositivos
- Seguridad perimetral
- Borrado seguro de información
- Gestión de riesgos
- Cláusula de confidencialidad
- Política de protección de datos personales
- Actualización de parches.
- Hardening
- Ciclo de vida desarrollo de sistemas

19. ANEXO 3. CLAUSULAS PROVEEORES

Las siguientes cláusulas referentes al cumplimiento de los requisitos de seguridad de la información en la relación con los proveedores, deben ser incluidas:

CLAUSULA XX. PROTECCIÓN DE DATOS PERSONALES

EL PROVEEDOR entiende y acepta que si en la ejecución de sus servicios para con la Universidad Distrital Francisco José de Caldas tiene acceso a cualquier Base de Datos Personales en la cual la Universidad Distrital Francisco José de Caldas ostente la calidad de Responsable del tratamiento, por ese hecho inmediatamente adquiere EL PROVEEDOR la calidad de Encargado del Tratamiento de conformidad con el alcance del artículo 25 del Decreto 1377 del 27 de junio de 2013 y cualquier norma que lo modifique, adicione y complemente. De acuerdo con lo anteriormente expuesto, además de las previsiones legales contenidas en la norma citada, se obliga a aplicar las Políticas de Tratamiento de la información que XXXXX publicarán en la página web.

CLAUSULA XX. REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

EL PROVEEDOR se obliga para con la Universidad Distrital Francisco José de Caldas, a cumplir con el Anexo "Requerimientos de Seguridad de la Información para proveedores", el cual se anexa al presente Contrato y hace parte integral de mismo. El mencionado anexo le es aplicable por razón de las actividades que desempeña en ejecución del presente Contrato o servicio, y en consecuencia, será responsable por las acciones u omisiones, suyas o de sus dependientes sean estos empleados directos o terceros proveedores suyos, que incumplan con lo establecido en el mencionado anexo.

El incumplimiento de las obligaciones establecidas en el anexo mencionado en el inciso anterior dará lugar a que la Universidad Distrital Francisco José de Caldas, pueda exigir las medidas correctivas que resulten procedentes a costo de EL PROVEEDOR y/o dar por terminado el Contrato sin que haya lugar al pago de indemnización alguna a su favor y sin necesidad de requerimiento previo o judicial alguno.

La Universidad Distrital Francisco José de Caldas podrá imponer al PROVEEDOR cuando incumpla cualquiera de las obligaciones establecidas en el Anexo, multas equivalentes al uno por ciento (1%) del valor del Contrato por cada día de retraso en el cumplimiento de sus obligaciones.

CLAUSULA XX. AUDITORIAS Y MONITOREO DE SEGURIDAD DE LA INFORMACION

EL PROVEEDOR estará sujeto a auditorías o monitoreos por parte de la Universidad Distrital Francisco José de Caldas, que serán acordadas con el ánimo de verificar el cumplimiento de los requerimientos de seguridad y realizar las observaciones y recomendaciones del caso, para asegurar el cumplimiento de los controles de seguridad, los cuales serán adoptados por el PROVEEDOR en el plazo señalado por la Universidad Distrital Francisco José de Caldas.

20. ANEXO 4. FORMATOS

Documento GC-PR-006-FR-028

ESTUDIOS Y DOCUMENTOS PREVIOS – SOLICITUD DE ADQUISICIÓN DE BIENES Y SERVICIOS

Dependencia Solicitante:	(Señalar el nombre completo de la dependencia solicitante de la cual surge la necesidad)
Rubro:	(Indique el rubro a afectar)
Fecha:	(Indique la fecha)
Funcionario responsable del proceso en la dependencia:	(Indique el funcionario responsable del proceso en la dependencia)

1. **DEFINICIÓN DE LA NECESIDAD (OBJETO DEL CONTRATO)**

(Indicar el objeto del contrato que se requiere)

(Indicar los requerimientos de Seguridad de la Información)

2. **JUSTIFICACIÓN DEL PROCESO DE SELECCIÓN**

(Indicar la justificación del proceso de selección)

3. **RAZONES DE CONVENIENCIA Y OPORTUNIDAD (marque X si el contrato está vigente)**

Objeto	Contrato Vigente		Oportunidad		
	Sí	No	Fecha de Inicio	Fecha Final	Plazo Max. de Inicio Nuevo Contrato
(Describir el objeto, señalar si el contrato está vigente e indicar las fechas)					

4. **EVALUACIÓN DE LOS POSIBLES RIESGOS (La tipología de los riesgos que podrían ser)**

4.1. **Riesgos previsibles con cargo al oferente ganador:**

(Indicar los riesgos previsibles con cargo al oferente ganador)

4.2. **Riesgos imprevisibles:**

(Indicar los riesgos imprevisibles)

4.3. **Riesgos previsibles a cargo de la Universidad Distrital Francisco José de Caldas:**

(Indicar los riesgos previsibles a cargo de la Universidad Distrital Francisco José de Caldas)

4.4. **Riesgos de Seguridad de la Información**

(Indicar los riesgos de Seguridad de la Información identificados por la Universidad Distrital Francisco José de Caldas)

4.5. **Otros riesgos que se consideran:**

(Indicar los otros riesgos que se consideran)

5. **JUSTIFICACIÓN DEL VALOR DEL CONTRATO - ANÁLISIS DEL MERCADO Y DEL SECTOR:**

Para las contrataciones se deberá adjuntar como mínimo tres cotizaciones para el estudio del mercado, lo anterior se hace con el fin de realizar un comparativo de los precios en el mercado y determinar el contratista basados en el menor precio que cumpla con lo requerido por la universidad.

Nota: Para el caso de la **CONTRATACIÓN DE BIENES Y SERVICIOS DE CARACTERÍSTICAS TÉCNICAS UNIFORMES Y DE COMÚN UTILIZACIÓN** Articulo No. 16 del Acuerdo No.03 de 2015: *Para la adquisición de este tipo de bienes y servicios, en cuantías*

que superen los Cien (100) Salarios Mínimos Legales Mensuales Vigentes, el Ordenador del Gasto deberá acudir a cualquiera de los siguientes mecanismos dispuestos en la ley 1150 de 2007, reglamentada por el Decreto 151 O de 2013: Acuerdo Marco de Precios, Bolsa de Productos o Subasta inversa.

I. ANALISIS DE LA OFERTA

Para este análisis se deberá quien vende en el mercado los bienes y/o servicios que se van a adquirir. Identificando las principales características como tamaño, ubicación, comportamiento financiero.

En el estudio de la oferta, la Entidad Estatal debe contestar, entre otras, las siguientes preguntas:

¿Quién vende? Se debe identificar los proveedores en el mercado del bien, obra o servicio, así como sus principales características como tamaño empresarial, ubicación, esquemas de producción y comportamiento financiero.

En este análisis se debe incluir como mínimo tres cotizaciones para determinar cómo, a qué precio y en qué condiciones técnicas se está ofreciendo el bien y/o servicio en el mercado, las cuales se deberán anexar al estudio y relacionar en el siguiente cuadro:

TABLA 2: DE ANÁLISIS DEL MERCADO – OFERTA

	Nombre de la empresa cotizante	**Condiciones ofrecidas**	**Objeto**	**Valor Ofrecido**
1				
2				
3				
			VALOR PROMEDIO	

Frente a esto, no se trata solo de comparar ofertas, sino de mirar las condiciones usuales en las que el mercado contrata ese tipo de bien o servicio, de manera que se justifiquen las exigencias que se hagan al contratista en cuanto a requisitos habilitantes, mínimos técnicos y se le pague algo coherente con el valor que tengan esos bienes o servicios en el mercado.

II. ANÁLISIS DE LA DEMANDA

Para este análisis se requiere preguntarse lo siguiente:

¿Cómo la Universidad ha adquirido en vigencias anteriores el bien y/o servicio?

El análisis debe incluir el precio, objeto, plazo y forma de pago como se ha adquirido con anterioridad el mismo bien y/o servicio, su comportamiento histórico y las perspectivas de cambios sobre estos. La información que se recolecte deberá ser adjuntada al estudio y consignada en el siguiente cuadro:

TABLA 3: DE ANÁLISIS DEL MERCADO – DEMANDA – HISTORICO DE LA ENTIDAD

	Año	No. Contrato	Objeto	Plazo de Ejecución	Valor	Requisitos mínimos exigidos contratista
1						
2						
3						

¿Cómo adquieren otras Entidades y/o las empresas privadas este bien, obra o servicio?

Con esto se busca examinar y tomar las mejor prácticas usadas por otras entidades y/o empresas privadas para la adquisición de este bien y/o servicio. La información que se recolecte deberá ser adjuntada al estudio y consignada en el siguiente cuadro:

TABLA 4: DE ANÁLISIS DEL MERCADO – DEMANDA – OTRAS ENTIDADES Y/O EMPRESAS

	Año	No. Contrato	Objeto	Plazo de Ejecución	Valor	Entidad y/o empresa	Buenas practicas a tomar
1							
2							
3							

III. CONDICIONES GENERALES DEL SECTOR

En este punto se debe analizar los siguientes aspectos generales y otros que considere necesarios para el estudio, así:

A qué sector económico pertenece, que tipo de empresas participan en ese sector, materias primas necesarias para la producción y la variación de sus precios y la dinámica de importaciones, exportaciones que aplican cuando haya lugar.

Condiciones técnicas del bien y/o servicio, cambios tecnológicos, especificaciones de calidad, soportes técnicos, condiciones de entrega y tiempos.

Regulación aplicable al contrato de mercado, de precios, ambientales, tributarias y de cualquier otro tipo, así como las modificaciones recientes a tales regulaciones y el impacto en su aplicación. También debe estudiar si en el sector hay Normas Técnicas Colombianas, acuerdos o normas internacionales aplicables y autoridades regulatorias o de vigilancia.

6. **PRESUPUESTO OFICIAL ESTIMADO**

6.1. **Valor total estimado según estudio de mercado:** (Indique el valor total estimado según estudio de mercado)

6.2. **Valor establecido en el Plan Anual de Adquisiciones:** (Indique el valor establecido en el Plan Anual de Adquisiciones)

7. **MARCO LEGAL**

7.1. **Norma(s) General(es):**

(Ingrese aquí la(s) norma(s) general(es))

7.2. **Norma(s) Específica(s):**

(Ingrese aquí la(s) norma(s) específica(s))

8. **TIPO DE CONTRATO**

8.1. **El contrato a celebrar con el oferente ganador del proceso de selección será de:** (Ingrese aquí de qué será el contrato a celebrar con el oferente ganador del proceso de selección)

9. **SUPERVISOR DEL CONTRATO**

El supervisor del contrato será:	(Indique el nombre del supervisor del contrato)
Cargo:	(Indique el cargo del supervisor del contrato)
Teléfono	(Indique el teléfono del supervisor del contrato)
Correo electrónico:	(Indique el correo electrónico del supervisor del contrato)
Contacto:	(Indique el contacto del supervisor del contrato)
Teléfono del contacto:	(Indique el teléfono del contacto del supervisor del contrato)
Correo electrónico del contacto:	(Indique el correo electrónico del contacto del supervisor del contrato)

10. **TIPOS DE OFERTAS (marque con X en "Selección" las ofertas que podrían ser):**

Tipo	Descripción	Selección
Totales	Propuestas totales, en las que se involucran todos los elementos a contratar y se evidencia con un solo precio ofertado (incluido IVA)	

Parciales	En las que se involucran algunos elementos de la totalidad requerida y se admite que los oferentes puedan ofertar solo algunos elementos con una oferta de precio parcial (el IVA se puede discriminar o incluir en el precio ofertado). Recuerde que si se aceptan las ofertas parciales, se pueden efectuar adjudicaciones parciales.	
Por Soluciones Integrales	Debe involucrar la totalidad de los elementos que se necesitan y se incluyen en ella	
Por precios unitarios	La adjudicación seria parcial dado que se adjudicaría cada uno de los ítems solicitados, a los oferentes que realicen la mejor oferta que normalmente es el menor precio	
Otra	Descríbala:	

11. **PLAZO DEL CONTRATO:**

El tiempo para realizar la actividad contratada:	Meses		Días	
El tiempo para liquidar el contrato:	Meses		Días	
TOTAL	Meses		Días	

12. **VALOR Y FORMA DE PAGO (marque con X en "Selección" la forma de pago del contrato)**

Forma de Pago del Contrato	Selección
Total , contra entrega de los bienes o servicios contratados	
Parcial, a medida que el proveedor entregue los bienes y servicios contratados	
Con anticipo económico	

12.1. **Reglamento para su desembolso y manejo :**

(Fijar en los Términos de Referencia un reglamento para su desembolso y manejo)

Nota: el anticipo puede ser utilizado según el caso específico y se puede combinar con la forma de pago.

13. **GARANTÍAS Y AMPAROS EXIGIBLES (marque con X en "Selección" las garantís y amparos exigibles)**

Garantías y Amparos Exigibles	Selección
Póliza de Cumplimiento	
Póliza de Calidad	

Pago de Salarios y Prestaciones Sociales	
Responsabilidad Civil frente a terceros	

13.1. **Justificación de las garantías y amparos exigibles:**

(Indicar la justificación de las garantías y amparos exigibles)

14. **REQUISITOS PARA EVALUAR Y COMPARAR PROPUESTAS (marque con X en "Selección" los requisitos para evaluar y comparar propuestas y exponga con el profesional a cargo del proceso)**

Aspectos a Evaluar	Calificación	Selección
Estudio Jurídico	Admisible / No admisible	
Estudio Financiero	Admisible / No admisible	
Estudio Técnico	Admisible / No admisible	
Con puntaje por experiencia general	Puntaje	
Con puntaje por experiencia especifica	Puntaje	
Con puntaje por mayor tiempo de garantía ofrecida	Puntaje	
Precio	A menor precio por ítem (con o sin intervalo de aceptación)	
Precio	A menor precio total (todos los ítems) con o sin intervalo de aceptación	
Precio	A menor precio por solución integral (con o sin intervalo de aceptación)	
Precio	Con utilización de media geométrica (adjudicación al que esté más cerca de la media geométrica)	
Precio	Con utilización de media aritmética (adjudicación al que esté más cerca de la media geométrica)	
Seguridad de la Información	Puntaje (número de riesgos de seguridad de la información identificados, clasificados por tipo de riesgo)	
Seguridad de la Información	Puntaje (% de cumplimiento de los requisitos de Seguridad de la Información)	
Otras formas de evaluar	Señale cuales:	

15. **DOCUMENTOS TÉCNICOS PROPUESTOS**

Certificaciones Contractuales (marque con X en "Selección" la forma propuesta)		Selección
Tipo de experiencia a solicitar	General	

	Específica	
Número máximo de certificaciones a solicitar para experiencia general:		
Número máximo de certificaciones a solicitar para experiencia especifica:		

Capacidad de Contratación		**Valor**
K de contratación general mínimo requerido para el proceso de selección:	SMMLV	
K de contratación residual mínimo requerido para el proceso de selección:	SMMLV	

Seguridad de la Información	**Selección**
Documento Nivel de Madurez en Seguridad de la Información (Certificado)	

Marcas (marque con X en "Selección" la marca)	**Selección**
Por razones de compatibilidad de bienes y servicios anteriormente comprados para evitar malos funcionamientos	
Por razones de hacer efectiva una garantía, se deba contratar con la marca inicialmente adquirida	
Se presenta la posibilidad de obtener un producto que tenga iguales características técnicas en marcas diferentes. En este caso se deben relacionar un mínimo de marcas con características similares	
Otras Razones. Establezca:	

Nota: si no tiene alguna de las anteriores, no señale.

16. **LISTADO DE GENERAL DE ELEMENTOS REQUERIDOS –FICHA TÉCNICA–**

Nombre del Elemento	**Unidad de Medida**	**Cantidad**	**Especificación técnica y Actividades a realizar**	**Valor Unitario**	**IVA**	**Valor Total IVA incluido**

Nota: La valores deberán ajustarse de acuerdo a la necesidad a contratar.

17. **OTROS**

(Incluya cualquier otro aspecto que a criterio de la dependencia que requiere el proceso, deba ser incluido y tenido en cuenta en el proceso de selección del bien o servicio solicitado.)

(nombre y firma del jefe de la dependencia solicitante)

	NOMBRE	CARGO	FIRMA	FECHA
Responsable de la elaboración técnica				
Responsable de la elaboración jurídica				
Revisó				
Aprobó				

Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales y/o técnicas aplicables y vigentes, y por tanto bajo nuestra responsabilidad, lo presentamos para la firma.

Nota: Resolución No. 262 de 2015 Artículo 9. Los estudios previos estarán a cargo del Jefe de la Dependencia en donde se haya identificado la necesidad, quien luego lo remitirá al ordenador del gasto para su aprobación y solicitud de Certificado de Disponibilidad Presupuestal.

Documento GC-PR-006-FR-008

ESTUDIOS Y DOCUMENTOS PREVIOS – SOLICITUD DE ADQUISICIÓN DE BIENES Y SERVICIOS

Dependencia Solicitante:	(Señalar el nombre completo de la dependencia solicitante de la cual surge la necesidad)
Rubro:	(Indique el rubro a afectar)
Fecha:	(Indique la fecha)
Funcionario responsable del proceso en la dependencia:	(Indique el funcionario responsable del proceso en la dependencia)

1. **DEFINICIÓN DE LA NECESIDAD (OBJETO DEL CONTRATO)**

(Indicar el objeto del contrato que se requiere)

(Indicar los requerimientos de Seguridad de la Información)

2. **JUSTIFICACIÓN DEL PROCESO DE SELECCIÓN**

(Indicar la justificación del proceso de selección)

3. **RAZONES DE CONVENIENCIA Y OPORTUNIDAD (marque X si el contrato está vigente)**

Objeto	Contrato Vigente	Oportunidad

	Sí	No	Fecha de Inicio	Fecha Final	Plazo Max. de Inicio Nuevo Contrato
(Describir el objeto, señalar si el contrato está vigente e indicar las fechas)					

4. **EVALUACIÓN DE LOS POSIBLES RIESGOS (La tipología de los riesgos que podrían ser)**

4.1. **Riesgos previsibles con cargo al oferente ganador:**

(Indicar los riesgos previsibles con cargo al oferente ganador)

4.2. **Riesgos imprevisibles:**

(Indicar los riesgos imprevisibles)

4.3. **Riesgos previsibles a cargo de la Universidad Distrital Francisco José de Caldas:**

(Indicar los riesgos previsibles a cargo de la Universidad Distrital Francisco José de Caldas)

4.4. **Riesgos de Seguridad de la Información**

(Indicar los riesgos de Seguridad de la Información identificados por la Universidad Distrital Francisco José de Caldas)

4.5. **Otros riesgos que se consideran:**

(Indicar los otros riesgos que se consideran)

5. **JUSTIFICACIÓN DEL VALOR DEL CONTRATO - ANÁLISIS DEL MERCADO Y DEL SECTOR:**

Para las contrataciones se deberá adjuntar como mínimo tres cotizaciones para el estudio del mercado, lo anterior se hace con el fin de realizar un comparativo de los precios en el mercado y determinar el contratista basados en el menor precio que cumpla con lo requerido por la universidad.

Nota: Para el caso de la **CONTRATACIÓN DE BIENES Y SERVICIOS DE CARACTERÍSTICAS TÉCNICAS UNIFORMES Y DE COMÚN UTILIZACIÓN** Articulo No. 16 del Acuerdo No.03 de 2015: *Para la adquisición de este tipo de bienes y servicios, en cuantías que superen los Cien (100) Salarios Mínimos Legales Mensuales Vigentes, el Ordenador del Gasto deberá acudir a cualquiera de los siguientes mecanismos dispuestos en la ley 1150 de 2007, reglamentada por el Decreto 151 O de 2013: Acuerdo Marco de Precios, Bolsa de Productos o Subasta inversa.*

I. ANALISIS DE LA OFERTA

Para este análisis se deberá quien vende en el mercado los bienes y/o servicios que se van a adquirir. Identificando las principales características como tamaño, ubicación, comportamiento financiero.

En el estudio de la oferta, la Entidad Estatal debe contestar, entre otras, las siguientes preguntas:

¿Quién vende? Se debe identificar los proveedores en el mercado del bien, obra o servicio, así como sus principales características como tamaño empresarial, ubicación, esquemas de producción y comportamiento financiero.

En este análisis se debe incluir como mínimo tres cotizaciones para determinar cómo, a qué precio y en qué condiciones técnicas se está ofreciendo el bien y/o servicio en el mercado, las cuales se deberán anexar al estudio y relacionar en el siguiente cuadro:

TABLA 2: DE ANÁLISIS DEL MERCADO – OFERTA

	Nombre de la empresa cotizante	Condiciones ofrecidas	Objeto	Valor Ofrecido
1				
2				
3				
			VALOR PROMEDIO	

Frente a esto, no se trata solo de comparar ofertas, sino de mirar las condiciones usuales en las que el mercado contrata ese tipo de bien o servicio, de manera que se justifiquen las exigencias que se hagan al contratista en cuanto a requisitos habilitantes, mínimos técnicos y se le pague algo coherente con el valor que tengan esos bienes o servicios en el mercado.

II. ANÁLISIS DE LA DEMANDA

Para este análisis se requiere preguntarse lo siguiente:

¿Cómo la Universidad ha adquirido en vigencias anteriores el bien y/o servicio?

El análisis debe incluir el precio, objeto, plazo y forma de pago como se ha adquirido con anterioridad el mismo bien y/o servicio, su comportamiento histórico y las perspectivas de cambios sobre estos. La información que se recolecte deberá ser adjuntada al estudio y consignada en el siguiente cuadro:

TABLA 3: DE ANÁLISIS DEL MERCADO – DEMANDA – HISTORICO DE LA ENTIDAD

	Año	No. Contrato	Objeto	Plazo de Ejecución	Valor	Requisitos mínimos exigidos contratista
1						

2						
3						

¿Cómo adquieren otras Entidades y/o las empresas privadas este bien, obra o servicio?

Control de Cambios			
Versión	Descripción y justificación	Responsable	Fecha
1	Creación del documento.	CPS Oficina Asesora de Tecnologías e Información	4/11/2024

Responsabilidades		
	NOMBRE	**CARGO**
CREACIÓN	Oscar Sanabria	CPS OATI
REVISÓ	Sebastián Vanegas	CPS OATI
APROBÓ	Alejandro Paolo Daza Corredor	Jefe OATI