UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

OFICINA ASESORA DE TECNOLOGÍAS E INFORMACIÓN

4 de noviembre de 2024

Contenido

Índice de tablas

Índice de Figuras

1. INTRODUCCIÓN

La gestión de riesgos de seguridad digital establece procesos, procedimientos y actividades encaminados a lograr un equilibrio entre la prestación de servicios y los riesgos asociados a los activos de información que dan apoyo y soporte en el desarrollo de la misionalidad de la Universidad Distrital Francisco José de Caldas. Esto implica la implementación de medidas que requieren tiempo, esfuerzo y recursos para abordar los riesgos, así como para controlar y gestionar la ocurrencia de eventos o incidentes, mitigando así los impactos adversos que podrían afectar a la universidad.

2. OBJETIVO GENERAL

Establecer un marco de gestión de riesgos de seguridad digital con el que se mitiguen las vulnerabilidades y amenazas asociados a los activos de información de la Universidad Distrital Francisco José de Caldas, para reducir la calificación de los riesgos residuales a un nivel bajo y su nivel de tolerancia sea aceptable con relación a los atributos de disponibilidad, integridad y confidencialidad de la información de la Universidad Distrital Francisco José de Caldas.

3. OBJETIVOS ESPECIFICOS

- Evaluar y analizar los riesgos de seguridad digital relacionados a los activos de información para facilitar el desarrollo de la misionalidad de la Universidad Distrital Francisco José de Caldas.
- Estandarizar el proceso de gestión de riesgos de seguridad digital en la Universidad Distrital Francisco José de Caldas.
- Generar mecanismos para que la Universidad Distrital Francisco José de Caldas pueda establecer los elementos para identificar, analizar, valorar y tratar los riesgos, amenazas y vulnerabilidades del entorno digital.
- Proponer estrategias para la ejecución de planes de acción para mitigar los riesgos generados en el entorno digital.
- Determinar los mecanismos para el seguimiento de los riesgos asociados a la seguridad digital.

4. ALCANCE

El alcance del plan de gestión de riesgos de seguridad digital inicia con la definición del contexto estratégico al que está expuesta la Universidad Distrital Francisco José de Caldas cubriendo los

procesos misionales, estratégicos, apoyo y control concluyendo con el plan de acción con el que se realizará el tratamiento, monitoreo y revisión de los riesgos de seguridad digital identificados.

5. DEFINICIONES

Para la adecuada gestión de riesgos de seguridad digital es necesario manejar con propiedad los siguientes términos:

- Activo: [Según ISO 27000]: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- Amenaza: [Según ISO 27000]: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- Análisis del riesgo: [NTC ISO 31000:2011]: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- Apetito de riesgo: Es el nivel máximo de riesgo que la Universidad Distrital Francisco José de Caldas está dispuesta a asumir.
- Consecuencia: [NTC ISO 31000:2011]: Resultado o impacto de un evento que afecta a los objetivos.
- Controles: [Según ISO 27000]: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control se usa como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- CSIRT: Equipo de Respuesta a Incidentes de Seguridad Informática
- Criterios del riesgo: [Según NTC ISO 31000:2011]: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.
- Evaluación del riesgo: [Según NTC ISO 31000:2011]: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- Identificación del riesgo: [Según NTC ISO 31000:2011]: Proceso para encontrar, reconocer y describir el riesgo.
- Impacto: [Según ISO 27000]: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
- Inventario de activos: [Según ISO 27000.ES]: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.
- Nivel de riesgo: [Según NTC ISO 31000:2011]: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad.
- Perfil del riesgo: [Según NTC ISO 31000:2011]: Descripción de cualquier conjunto de riesgos.
- Política: [Según ISO/IEC 27000:2016]: Intenciones y dirección de una organización como las expresa formalmente su alta dirección.

- Política: para la gestión del riesgo [Según NTC ISO 31000:2011]: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
- Reducción del riesgo: [Según NTC ISO 31000:2011]: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo.
- Riesgo: [Según ISO 27000]: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- Riesgo Residual: [Según ISO 27000]: El riesgo que permanece tras el tratamiento del riesgo.
- Vulnerabilidad: [Según ISO 27000]: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6. FASE DE PLANEACION DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

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 implementación del Modelo de gestión de riesgos de seguridad digital.

6.1. Metas de preparación de las TIC para la protección de los datos personales

De acuerdo con el "Plan Indicativo 2022-2025", se plantean las siguientes metas de preparación de las TIC para la implementación del Modelo de gestión de riesgos de seguridad digital, 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 conduzcan a 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 el Manual de Gestión de riesgos de la siguiente manera:

- Definir el Marco de Referencia para la Administración del Riesgo aplicable a la Universidad Distrital, en los Ejes de Calidad, Seguridad de la Información, Gestión Ambiental, Gestión de la Seguridad y Salud en el Trabajo y Corrupción.
- Armonizar la Administración del Riesgo con las Dimensiones, Políticas y Procesos que componen el Sistema Integrado de Gestión.
- Promover medidas encaminadas a gestionar los Riesgos propios de las actividades desarrolladas en la Universidad, a través del diseño y ejecución de Controles, de acuerdo con la metodología establecida.

La Universidad Distrital Francisco José de Caldas siguiendo los lineamientos del Gobierno Nacional según la Ley de transparencia 1712 de 2014, la Estrategia Gobierno en Línea y la Política de Gobierno Digital establece un plan de gestión de riesgos de seguridad digital que identifica las amenazas, vulnerabilidades, impacto y nivel asociados a los activos de información.

En la gestión de riesgos de seguridad digital resulta importante lograr una aceptación de los riesgos con base en las posibles consecuencias de afectación, estableciendo una estrategia de mitigación adecuada que logre un entendimiento y aceptación del riesgo residual así como de los recursos empleados en relación costo-beneficio con el fin de emplear medidas para salvaguardar, proteger y custodiar la información de las aplicaciones, servicios tecnológicos, bases de datos, redes de comunicaciones, equipos de cómputo y documentos físicos garantizando la disponibilidad, confidencialidad e integridad de la información.

La fase de planificación es el punto de partida para llevar a cabo el proceso de la gestión de riesgos de seguridad digital. Se considera una fase esencial donde se identifica el contexto de la Universidad Distrital Francisco José de Caldas, los criterios de impacto y probabilidad, y el apetito de riesgo, entre otros parámetros necesarios para manejar de buena forma los riesgos de seguridad digital.

Por lo tanto, resulta indispensable definir actividades que de manera articulada permitan implementar medidas de control que coadyuven a la prevención, contención y mitigación de amenazas a las que se encuentran expuestos los activos de información de la Universidad Distrital Francisco José de Caldas por medio de una metodología descrita a continuación.

6.2. Contexto externo

El 17 de octubre el Congreso de la República decretó la Ley 1581 de 2012que establece un derecho fundamental de las personas para conocer, actualizar y rectificar información personal recogida en las diferentes bases de datos o archivos de entidades públicas o privadas, por lo que toda información personal de los distintos medios o dispositivos de almacenamiento de la Universidad Distrital Francisco José de Caldas debe contemplar medidas de protección de dicha información para que no se afecte la integridad y buen nombre de las personas.

El 6 de marzo de 2014 el Congreso de la República estableció la Ley 1712, que creó la ley de transparencia y el derecho de acceso a la información pública nacional, lo que convierte en un derecho constitucional para las personas acceder a la información pública que les permita realizar estudios estadísticos, científicos o estar informados. La Universidad Distrital Francisco José de Caldas se compromete a identificar y clasificar toda información creada, almacenada, administrada y publicada, permitiendo así cumplir lo establecido en esta ley.

Por su parte, el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC el 14 de Junio de 2018 estableció el decreto 1008 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" que por medio del uso de tecnologías de la información y las comunicaciones permita lograr una mejor competitividad, proactividad e innovación en la ciudadanía y el Estado, por lo que la Universidad Distrital Francisco José de Caldas desempeña un papel importante con la implementación de recursos tecnológicos que le permita alcanzar los propósitos que dispone esta ley, gestionando los riesgos y amenazas que traigan consigo la implementación de nuevas tecnologías de la información o avances tecnológicos.

6.3. Contexto interno.

La Universidad Distrital Francisco José de Caldas es una institución autónoma de educación superior, de carácter público, constituida esencialmente por procesos y relaciones que generan estudiantes y profesores identificados en la búsqueda libre del saber.

Su misión se concreta en la calificación de egresados con capacidad de actuar como protagonistas del cambio social y de sí mismos, en la formación del espíritu científico aplicado a la indagación, interpretación y modificación de la realidad, en la contribución a forjar ciudadanos idóneos para promover el progreso de la sociedad.

6.4. Misión

La Universidad Distrital Francisco José de Caldas es un espacio social y una organización institucional, ente autónomo del orden distrital, que tiene entre sus finalidades la formación de profesionales especializados y de ciudadanos activos; la producción y reproducción del conocimiento científico, además de la innovación tecnológica y la creación artística. Impulsa el diálogo de saberes y promueve una pedagogía, capaz de animar la reflexión y la curiosidad de los estudiantes; además, fomenta un espíritu crítico en la búsqueda de verdades abiertas; en la promoción de la ciencia y la creación; asimismo, de la ciudadanía y la democracia; y alienta la deliberación, fundada en la argumentación y en el diálogo razonado.

6.5. Visión

Para el 2030 la Universidad Distrital Francisco José de Caldas será reconocida, nacional e internacionalmente, como una institución de alta calidad en la formación de ciudadanos responsables y profesionales del mejor nivel, en la producción de conocimiento científico, artístico y de innovación tecnológica; propósitos que desplegará en los campos de la docencia, la investigación y la extensión.

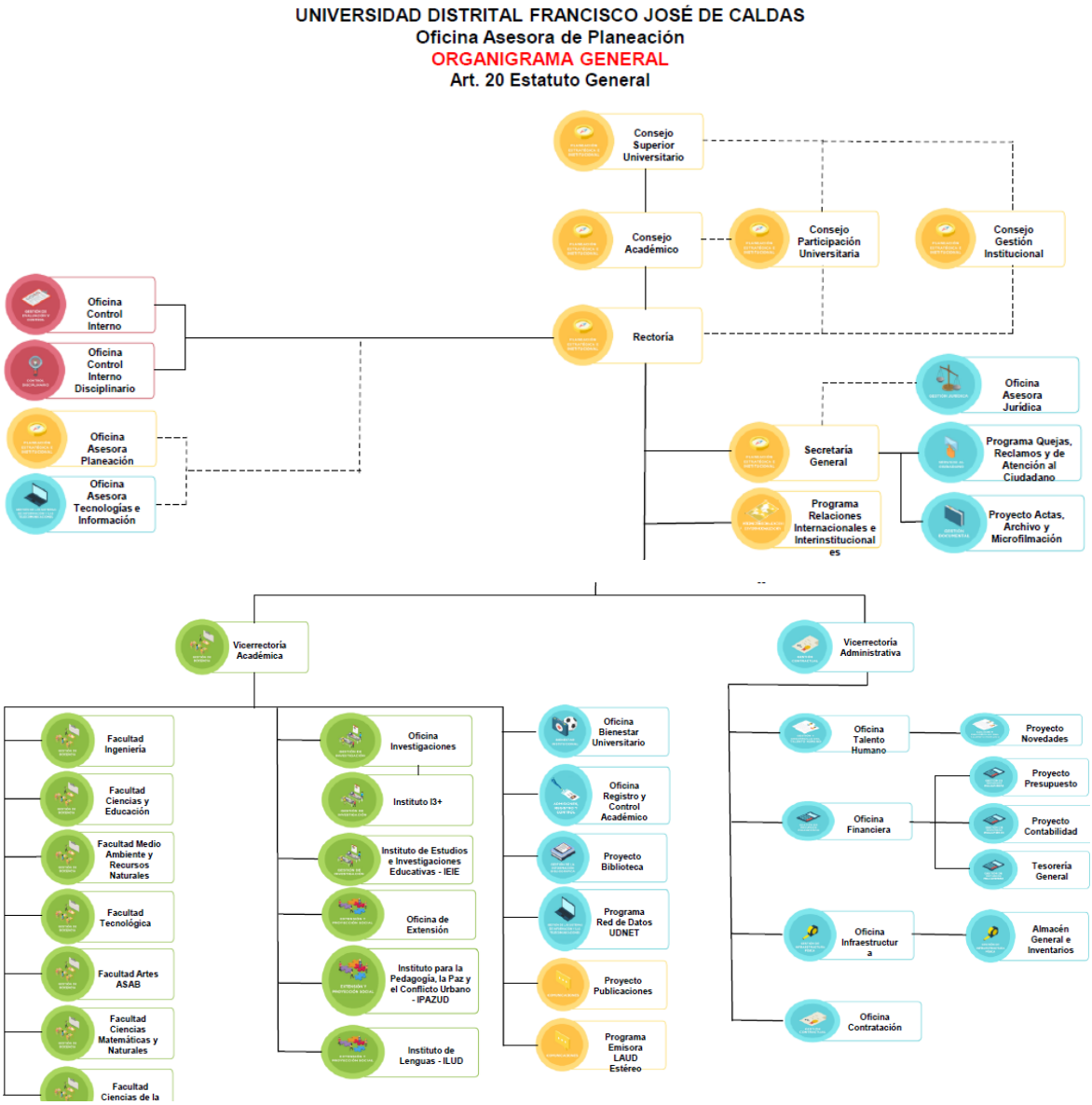
6.6. Objetivos

- Como institución de servicio público, impartir educación superior en las modalidades tecnológica, universitaria y avanzada o de posgrado, como medio eficaz para la realización plena del ciudadano colombiano, con el fin de configurar una sociedad más justa, equilibrada y autónoma, enmarcada dignamente en la comunidad internacional.
- Ampliar las oportunidades de acceso a la educación superior, para que los colombianos y particularmente los egresados de los colegios oficiales del Distrito, que cumplan los requisitos, puedan ingresar a ella y beneficiarse de sus programas.
- Contribuir a que la Universidad sea factor de desarrollo espiritual y material del Distrito Capital de Bogotá.
- En síntesis, la visión de futuro para la Universidad Distrital Francisco José de Caldas es la de una institución de educación superior reconocida por la excelencia en la investigación, en la formación y en el servicio al grupo social, en el contexto de una cultura institucional basada en la eficiencia, la transparencia y la coherencia.
- La Universidad Distrital ha definido como objetivos estratégicos:
- Formar ciudadanos, profesionales, investigadores, creadores e innovadores, íntegros con pensamiento crítico y cultura democrática, en contextos diferenciados inter y multiculturales para la transformación de la sociedad.
- Establecer un diseño curricular dinámico y flexible que promueva el pluralismo y consolide una comunidad universitaria crítica-transformadora y en armonía ambiental.
- Integrar las funciones universitarias mediante la investigación, creación, innovación para ampliar el conocimiento como bien público y solucionar problemas urbano-regionales y sociales.
- Garantizar, gestionar y proveer las condiciones institucionales para el cumplimiento de las funciones universitarias y el bienestar de su comunidad.
- Consolidar y fortalecer la democracia participativa, la gobernanza y la gobernabilidad para la cohesión de la comunidad universitaria.

6.7. Estructura de la Universidad Distrital

El Organigrama General de la Universidad Distrital Francisco José de Caldas se puede observar en la Figura 1. Organigrama, que se encuentra a continuación:

Figura 1. Organigrama



Fuente: http://planeacion.udistrital.edu.co:8080/sigud/organizacion - 2023

El organigrama está constituido por:

- Consejo superior universitario, Consejo académico, Rectoría, Consejo de participación ciudadana y Consejo de gestión institucional.
- De la Rectoría dependen las oficinas de Control Interno, Control Interno Disciplinario, Oficina Asesora de Planeación, Oficina Asesora de Tecnologías e información.
- De igual forma existen las Vicerrectorías Académica de la cual dependen las Facultades de Ingeniería, Ciencias y Educación, Ambiente y Recursos naturales, Tecnológica, Artes ASAB, Ciencias Matemáticas y Naturales y Ciencias de la Salud.
- De la Vicerrectoría Administrativa dependen la oficina de Talento Humano, Financiera, Infraestructura y Contratación

6.8. Procesos

La Universidad Distrital cuenta con veintidós (22) procesos detallados en la Tabla 1. Procesos, los cuales dan cubrimiento a la estrategia, la misionalidad, el apoyo y la evaluación:

Tabla 1. Procesos

Procesos Misionales	Gestión de Docencia
	Gestión de Investigación
	Extensión y Proyección Social
Procesos Estratégicos	Planeación Estratégica e Institucional
	Gestión Integrada
	Currículo y Calidad
	Comunicaciones
	Interinstitucionalización e Internacionalización
Procesos de Apoyo	Admisiones, Registro y Control
	Bienestar Institucional
	Gestión de la Información Bibliográfica
	Gestión de Laboratorios
	Servicio al Ciudadano
	Gestión de los Sistemas de Información y las Comunicaciones
	Gestión y Desarrollo del Talento Humano
	Gestión Documental
	Gestión de Infraestructura Física
	Gestión de Recursos Financieros
	Gestión Contractual
	Gestión Jurídica
Procesos de Control	Evaluación y Control
	Control Disciplinario

6.9. Recursos económicos

Los recursos económicos para la implementación del Modelo de riesgos de seguridad de la información se establecerán en una ficha MGA donde se definirá las partidas presupuestales.

6.10. Organización Seguridad de la Información

Respecto a la organización de la seguridad de la información, la Universidad Distrital ha venido trabajando en la implementación del SGSI para establecer un marco de confianza en el ejercicio de sus deberes con el Estado, la sociedad y las empresas del sector, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con su misión y visión. Así las cosas, en aras de cumplir con este compromiso, las directrices, normas y buenas prácticas en la materia, la Universidad Distrital está adoptando el Sistema de Gestión de Seguridad de la Información -SGSI, la Política General de Seguridad y Privacidad de la Información, el Manual de Políticas Específicas de Seguridad y Privacidad de la Información y, la Política de Protección de Datos Personales, entre otros instrumentos.

Las tareas están orientadas a los esfuerzos en la actualización de la identificación y clasificación del inventario de activos de información, así como de la evaluación de riesgos de seguridad de la información / seguridad digital por proceso.

El proceso actual de Gestión de los Sistemas de Información y las Telecomunicaciones se encarga de garantizar la seguridad de la información, contando con facilitadores en cada proceso que sirven de contacto y a quienes se les brinda el acompañamiento necesario. El objetivo principal es gestionar los sistemas y las telecomunicaciones para asegurar el acceso, adquisición, disponibilidad, confiabilidad, confidencialidad y seguridad de los activos de información, utilizando la infraestructura y las soluciones informáticas dentro del marco de la normativa vigente aplicable. Todo esto se realiza en apoyo a los procesos misionales de la Universidad, con el fin de satisfacer las necesidades de la comunidad universitaria.

La Universidad Distrital cuenta con un equipo técnico cuyo objetivo es gestionar los Sistemas de Información y las Telecomunicaciones para asegurar el acceso, adquisición, disponibilidad, confiabilidad, confidencialidad y seguridad de los activos de información a través de la infraestructura y las soluciones Informáticas en el marco de la normatividad vigente aplicable, como apoyo a los Procesos Misionales de la Universidad para satisfacer las necesidades de la comunidad universitaria.

La Universidad Distrital Francisco José de Caldas cuenta con un Comité de Transformación Digital que sigue los estándares establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones para la incorporación y uso de tecnologías emergentes y disruptivas. El principal objetivo de este comité es aprovechar estas tecnologías para formar ciudadanos competitivos, proactivos e innovadores, lo que permitirá a la Universidad contribuir al desarrollo social, mejorar la gobernanza, garantizar derechos, satisfacer necesidades, ofrecer servicios de calidad y mejorar las condiciones de vida de la sociedad.

6.11. Sistema Integrado de Gestión

EL Sistema Integrado de Gestión de la Universidad Distrital Francisco José de Caldas - SIGUD es el conjunto de políticas, normas, procesos, recursos, información e instancias, cuyo objeto es garantizar un desempeño institucional articulado y armónico, para el cumplimiento de la misión de la Universidad Distrital, así como la consecución de resultados para la satisfacción de la Comunidad Universitaria y los Grupos de Valor.

6.12. Manual de funciones

En el MANUAL ESPECÍFICO DE FUNCIONES PARA LOS CARGOS EN LA PLANTA GLOBAL DE PERSONAL ADMINISTRATIVO DE LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS (2023, https://sgral.udistrital.edu.co/xdata/rec/res_2024-001.pdf), se definen las responsabilidades a Nivel directivo, Nivel asesor, Nivel profesional, Nivel técnico y Nivel asistencial

6.13. Política de Gestión de riesgos

El modelo de Gestión de riesgos de seguridad digital - MGRSD está integrado en el documento Manual de Gestión de Riesgos definido para la Universidad Distrital Francisco José de Caldas, específicamente en su capítulo de Riesgos de Seguridad y privacidad de la información, detallando la gestión de riesgos desde la identificación de los activos de información hasta la definición de planes de tratamiento de riesgo.

6.14. Roles y responsabilidades

La gestión de riesgos de seguridad digital es una responsabilidad que debe ser apropiada por las dependencias, funcionarios y/o contratistas al interior de la Universidad Distrital Francisco José de Caldas. Estas responsabilidades se incluyeron dentro del Rol de Oficial de Seguridad de la Información.

La Universidad Distrital Francisco José de Caldas asigno las responsabilidades de fomentar la implementación de la Política de Gobierno Digital al Oficial de Seguridad de la Información, sin embargo, en el documento de la Estrategia de Seguridad Digital se detallan las siguientes responsabilidades:

- Rectoría: Proveer la dirección estratégica y garantizar los recursos necesarios para la implementación y mantenimiento de la estrategia de seguridad digital.
- Oficina Asesora de Tecnologías e Información: Coordinar la implementación de la estrategia de seguridad digital, la implementación de la estrategia de seguridad, gestionar riesgos e incidentes, y supervisar los controles y el monitoreo de seguridad.
- Control interno: Conducir auditorías y evaluaciones de la seguridad digital.
- Usuarios Finales: Adherirse a políticas de seguridad, reportar incidentes y participar en formación continua.

7. FASE DE EJECUCIÓN DEL MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL (MGRSD)

En esta fase se desarrollan un conjunto de actividades que permiten la implementación del MGRSD, ante lo cual la Universidad Distrital Francisco José de Caldas, adoptó los lineamientos de Gestión de Riesgos para riesgos de seguridad digital que se encuentran definidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022, la cual se detalla a continuación:

7.1. Identificación de los activos de información

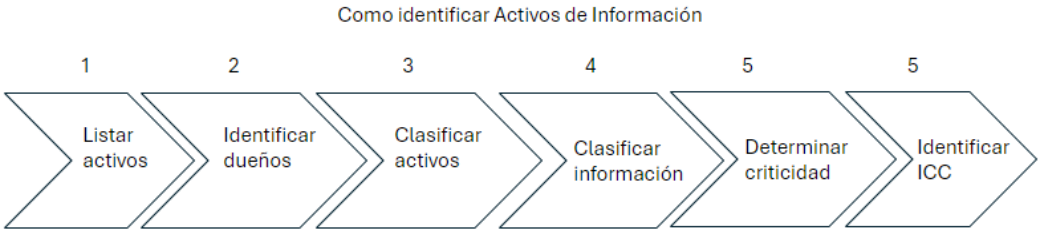
Definiendo Activos de Información a todos aquellos recursos de valor para una organización que generan, procesan, almacenan o transmiten información. Es necesario abarcar lo siguiente:

- Funciones de la Organización,
- Información y Datos,
- Recursos físicos (equipamiento, edificios),
- Recursos Humanos,
- Recursos de Software,
- Servicios, etc.
- Aplicaciones de la organización
- Servicios web
- Redes
- Información física o digital
- Tecnologías de información TI
- Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital

La identificación de los activos de información permite a la Universidad Distrital Francisco José de Caldas reconocer cuáles son los recursos más valiosos para su operación, tales como bases de datos, archivos, servidores web y aplicaciones clave. Estos activos son esenciales para que la Universidad pueda ofrecer sus servicios de manera eficiente y segura. Al identificarlos, se garantiza que los recursos críticos reciban la protección adecuada, asegurando la continuidad y calidad de los servicios ofrecidos a la comunidad universitaria.

Para identificar los activos de información se deben llevar a cabo las actividades descritas en la Figura 2. Como identificar activos de información:

Figura 2. Como identificar activos de Información



Fuente: Reconstrucción de imagen de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022

Asociado al concepto de Activo está el rol de Propietario de Información, quién es responsable de clasificar al Activo de Información de acuerdo con su grado de criticidad y de definir qué usuarios podrán acceder al mismo.

Este paso debe realizarse de acuerdo con la GSIT-GUI-002, Guía para la Identificación de Activos de Información y con la herramienta GSIT-GUI-002-FR-017, Formato de Inventario y Clasificación de Activos de Información.

7.2. Identificación del riesgo

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Manual de gestión de riesgo de la Universidad Distrital Francisco José de Caldas donde se encuentran las siguientes tablas necesarias para este análisis:

- Tabla de amenazas comunes
- Tabla de amenazas dirigida por el hombre
- Tabla de vulnerabilidades comunes

7.3. Identificación de amenazas

Una amenaza tiene el potencial de causar daños a los activos de información, incluyendo datos, información, procesos y sistemas, lo que puede afectar a la Universidad Distrital Francisco José de Caldas. Estas amenazas pueden ser de origen natural o humano, y pueden manifestarse de manera accidental o deliberada. Por ello, es recomendable identificar todos los posibles orígenes de las amenazas, tanto las accidentales como las deliberadas, para implementar medidas efectivas de mitigación y protección.

En la Tabla 2. Amenazas, se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas: Deliberadas (D), fortuito (F) o ambientales (A).

Tabla 2. Amenazas

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E

	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Compromiso de la información	D
	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

Fuente: Reconstrucción de imagen de ANEXO 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS

Es necesario tener particular atención a las amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros, dado estas pueden generar riesgos internos como externos afectando la confidencialidad, integridad y disponibilidad de la información. Estas se desglosan específicamente en la Tabla 3. Fuentes de amenazas humanas:

Tabla 3. Fuentes de amenazas humanas

Fuente de Amenaza	**Motivación**	**Acciones Amenazantes**
Pirata	Reto Ego	Piratería

informático, intruso ilegal	Rebelión Estatus Dinero	Ingeniería Social Intrusión, accesos forzados al sistema *Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	Crimen por computador Acto fraudulento Soborno de la información Suplantación de identidad Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	Bomba/Terrorismo Guerra de la información Ataques contra el sistema DDoS Penetración en el sistema Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Ventaja política Explotación económica Hurto de información Intrusión en privacidad personal Ingeniería social Penetración en el sistema Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	Asalto a un empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingreso de datos falsos o corruptos Interceptación Código malicioso Venta de información personal Errores en el sistema Intrusión al sistema Sabotaje del sistema Acceso no autorizado al sistema.

Fuente: Reconstrucción de imagen de ANEXO 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS

7.4. Identificación de vulnerabilidades

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de

amenazas comunes, la lista de inventario de activos y el listado de controles existentes.

Los siguientes son ejemplos de vulnerabilidad es (ver Tabla 4. Ejemplo de vulnerabilidades):

- La falta de mantenimiento de las instalaciones.
- La falta de Capacitación al Personal.
- La falta de manuales de procedimientos.
- La inexistencia de respaldos de información y equipamiento redundante.
- La falta de políticas de acceso a los sistemas informáticos.
- La divulgación o utilización de contraseñas inseguras.
- La transmisión de información por medios inseguros.
- Los errores de programación en las aplicaciones.
- La falta de mobiliario de oficina con llave.
- El acceso irrestricto al lugar de trabajo.
- La eliminación insegura de la información.

Tabla 4. Ejemplo de vulnerabilidades

Tipo de activo	**Ejemplos de vulnerabilidades**
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento
	Ausencia de esquemas de reemplazo periódico
	Susceptibilidad a la humedad, el polvo y la suciedad
	Sensibilidad a la radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final.
	Copia no controlada.
	Ausencia o insuficiencia de pruebas de software
	Defectos bien conocidos en el software
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Ausencias de pistas de auditoria

SOFTWARE	Defectos bien conocidos en el software
	Asignación errada de los derechos de acceso
	Software ampliamente distribuido
	En términos de tiempo utilización de datos errados en los programas de aplicación
	Interfaz de usuario compleja
	Ausencia de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
INFORMACION	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario
	Tablas de contraseñas sin protección
	Gestión deficiente de las contraseñas
	Habilitación de servicios innecesarios
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores
	Ausencia de control de cambios eficaz
	Descarga y uso no controlado de software
	Ausencia de copias de respaldo
	Ausencia de protección física de la edificación, puertas y ventanas
	Fallas en la producción de informes de gestión
RED	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables
	Punto único de fallas
	Ausencia de identificación y autentificación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)

	Conexiones de red pública sin protección

Fuente: ANEXO 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS

7.5. Identificación de consecuencias

Para la identificación de las consecuencias es necesario tener:

- Lista de activos de Información y su relación con cada proceso de la Universidad Distrital Francisco José de Caldas.
- Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

Nota: Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, entre otros.

Para esta actividad hay que identificar los daños o consecuencias para la Universidad Distrital que podrían causarse por un escenario de incidente. Un escenario de incidente se define como la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades relacionadas a un activo.

A continuación, se relacionan los factores a considerar para determinar el nivel de impacto actual:

- Disponibilidad:

¿El incidente está afectando la disponibilidad de los sistemas y servicios?

¿Hay interrupciones en la operación normal?

- Integridad:

¿Se ha comprometido la integridad de los datos o sistemas?

¿Se han alterado o manipulado de alguna manera?

- Confidencialidad:

¿Se ha violado la confidencialidad de la información sensible?

¿Se han accedido o filtrado datos confidenciales?

- Alcance:

¿El incidente está afectando solo a un sistema o a múltiples sistemas y/o redes?

¿Está impactando a un departamento o a toda la organización?

- Consecuencias:

¿Qué daños se producen por el incidente?

¿Hay pérdida de datos, pérdida financiera, interrupción del negocio u otras consecuencias

significativas?

7.6. Valoración del riesgo

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, para lo cual se asociarán las tablas de probabilidad e impacto, como se detalla a continuación:

7.7. Probabilidad

La probabilidad se entiende como la posibilidad de ocurrencia del riesgo.

Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Bajo este esquema, se elimina la subjetividad que a menudo afecta este tipo de análisis, permitiendo determinar con claridad la frecuencia con la que se lleva a cabo una actividad. En lugar de basarse en posibles eventos ocurridos en el pasado, se establece un enfoque más objetivo. De esta manera, si nunca se han presentado incidentes, los riesgos tienden a clasificarse en niveles bajos, lo que no refleja la realidad de la gestión de la Universidad Distrital Francisco José de Caldas. Este enfoque permite una evaluación más precisa de los riesgos, asegurando que se tomen las medidas adecuadas para proteger los activos de la Universidad Distrital.

Para este análisis la siguiente Tabla 5. Probabilidad de ocurrencia del riesgo:

Tabla 5. Probabilidad de ocurrencia del riesgo

Nivel	Frecuencia de la actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces al año	20%
Baja	La actividad que conlleva el riesgo se ejecuta como máximo 3 a 24 veces al año	40%
Media	La actividad que conlleva el riesgo se ejecuta como máximo 24 a 500 veces al año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022

7.8. Impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado

Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

Los criterios para definir el nivel de impacto se detallan en la Tabla 6. Impacto de ocurrencia del riesgo:

Tabla 6. Impacto de ocurrencia del riesgo

Nivel	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores
Moderado 60%	Entre 50 y 100 SMLMV	EL riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022

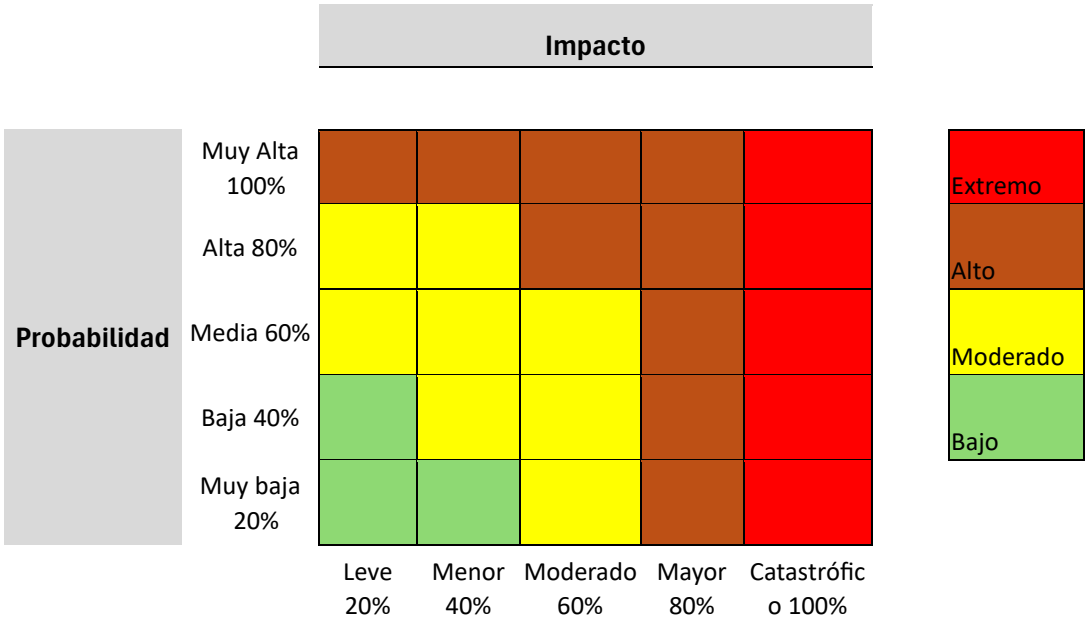
7.9. Nivel de severidad del riesgo

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

Análisis preliminar (riesgo inherente): se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto.

Las 4 zonas de severidad en la matriz de calor, se detalla en la Tabla 7. Matriz de calor de riesgos.

Tabla 7. Matriz de Calor de riesgos



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022

7.10. Controles asociados a la seguridad de la información

La Universidad Distrital Francisco José de Caldas mitigara/tratara los riesgos de seguridad de la información empleando al menos los controles del anexo A de la ISO/IEC 27001:2022, siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración

Para esta etapa se debe especificar el tipo de control definidos de la siguiente manera:

- Control preventivo: Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.
- Control detectivo: Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles detectan el riesgo fiscal, pero generan reprocesos.
- Control correctivo: Control accionado en la salida de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo) y después de que se materializa el riesgo fiscal. Estos controles tienen costos implícitos

Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, detallados en Tabla 8. Evaluación de controles

Tabla 8. Evaluación de controles

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos	15%
		Correctivo	Dado que permite reducir el impacto de materialización del riesgo, tiene un costo en su implementación	10%
	Implementación	Automático	Son actividades de procedimiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso	0%
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	0%

Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo	0%
	Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	0%
Evidencia	Con registro	El control deja un registro que permite evidenciar la ejecución del control	0%
	Sin registro	El control no deja registro de la ejecución del control	0%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022

Adicionalmente, se realizará una evaluación a la efectividad de cada control para validar que el impacto de riesgo se logró minimizar alcanzando niveles deseados de aceptación del riesgo. Por lo tanto, resulta indispensable registrar esta información en la Matriz Integral de Riesgo en donde se realiza seguimiento y revisión a la efectividad de los controles implementados y de esta manera determinar acciones sobre el riesgo residual

La aplicación de Controles permite reducir el impacto y probabilidad del Riesgo en cuestión, de esta manera genera un desplazamiento en la zona de Riesgo Inherente, de acuerdo con los criterios establecidos en la Tabla 9. Desplazamiento de probabilidad del riesgo:

Tabla 9. Desplazamiento de probabilidad e impacto del riesgo

Solidez del conjunto de controles	Controles disminuir la probabilidad	Controles reducen el impacto	# de columnas que se desplaza la probabilidad	# de columnas que se desplaza el impacto
Fuerte	directamente	directamente	2	2
Fuerte	directamente	indirectamente	2	1
Fuerte	directamente	no disminuye	2	0
Fuerte	no disminuye	directamente	0	2
Moderado	directamente	directamente	1	1
Moderado	directamente	indirectamente	1	0
Moderado	directamente	no disminuye	1	0
Moderado	no disminuye	directamente	0	1

Fuente: Guía para la Administración del Riesgo Departamento Administrativo de la Función Pública (DAFP).

Nivel de riesgo (riesgo residual): Es el resultado de aplicar la efectividad de los controles al riesgo inherente.

7.11. Tratamiento de los riesgos de seguridad digital

Es la respuesta establecida por los Líderes y Gestores de Procesos, para la mitigación de los diferentes Riesgos. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo,

los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la Universidad Distrital Francisco José de Caldas, la probabilidad e impacto de éste y la relación costo-beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá volver a analizar y revisar dicho tratamiento. El tratamiento o respuesta dada al riesgo, se enmarca como esta descrito en la Tabla 10. Tratamiento de riesgo.

Tabla 10. Tratamiento de riesgo

Medida de tratamiento	Descripción
Aceptar el Riesgo	No se adopta ninguna medida que afecte la probabilidad o el impacto del Riesgo. Aplica para los Riesgos cuya zona residual sea baja, y para aquellos casos en los que el Riesgo Residual se ubique en otra zona (moderada, alta o extrema) y no se les puedan aplicar Controles.
Reducir el Riesgo	Se adoptan medidas para reducir la probabilidad o el impacto del Riesgo, o ambos; por lo general conlleva a la implementación de nuevos Controles.
Evitar el Riesgo	Se abandonan las actividades que dan lugar al Riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.
Compartir el Riesgo	Se reduce la probabilidad o el impacto del Riesgo transfiriendo o compartiendo una parte de éste. Esta medida debe implementarse cuando la Universidad Distrital no tenga la capacidad para gestionarlo de manera adecuada y lo comparte con una parte interesada competente para gestionarlo con mayor eficacia. Los dos principales métodos de compartir o transferir parte del Riesgos son a través de seguros y tercerización.

Fuente: Manual de Gestión de riesgo Universidad Distrital

7.12. Planes de Tratamiento de riesgos de seguridad digital e indicadores para la gestión del riesgo

La Universidad Distrital Francisco José de Caldas debe definir los planes que debe seguir para priorizar los tratamientos de acuerdo con el impacto del riesgo residual, teniendo en cuenta lo siguientes planes de acción:

- Acción inmediata: considerar el plan de tratamiento de riesgo a muy corto plazo, es decir, el nivel de riesgo de seguridad digital puede afectar considerablemente factores sociales, económicos, ambientales; además de la confidencialidad, integridad y disponibilidad de la información.
- Decisión normal: considerar el plan de tratamiento a mediano plazo, es decir, el nivel de riesgo de seguridad digital no puede afectar de forma inmediata factores sociales, económicos, ambientales; además de la confidencialidad, integridad y disponibilidad de

la información, pero se requiere gestionar el riesgo, ejecutando controles o fortaleciendo los ya existentes, de tal forma que no se desplacen a niveles superiores.

- Mantener nivel: considerar a mediano o largo plazo en el plan de tratamiento la posibilidad de convivir con el nivel de riesgo de seguridad digital monitoreando la efectividad de los controles o en su defecto, pensar en alternativas de mitigación e implementar controles complementarios o transferir a un tercero el riesgo de seguridad de la información.
- Evaluar aceptación: considerar permanentemente el nivel de monitoreo de la efectividad de los controles sobre los riesgos de seguridad digital y mantener intactos en el tiempo los niveles de impacto y probabilidad.

El plan de tratamiento se convierte en una herramienta de ruta crítica sobre la cual se definen responsables, recursos y tiempos para lograr el propósito definido como parte de la gestión de riesgo de seguridad digital.

La Universidad Distrital Francisco José de Caldas debe hacer un seguimiento al plan de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Documentar los resultados de los planes de acción que ponga en marcha.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.

8. FASE DE IMPLEMENTACION

Esta fase se centra en la implementación de los planes de tratamiento de riesgos definidos en la fase anterior, en esencia es seguir la ruta crítica definida y llevar a cabo todo lo planeado en la fase de planeación

Aquí la línea estratégica de la Universidad Distrital Francisco José de Caldas debe cumplir con el compromiso de brindar los recursos necesarios para iniciar el tratamiento de los riesgos.

El Oficial de Seguridad de la Información responsable de seguridad digital supervisará y acompañará el proceso de implementación de los planes de tratamiento, verificando que los responsables (Primer línea de defensa y la Oficina Asesora de Tecnologías e Información) ejecuten las tareas en los tiempos pactados y que los recursos se ejecuten según lo planeado.

9. FASE DE MONITOREO Y REVISIÓN

La Universidad Distrital Francisco José de Caldas a través de las líneas de defensa (ver Tabla 11. Líneas de defensa) hace seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

Nota: cuando el plan de tratamiento se ejecute en las fechas y con las disposiciones de recursos previstas, la Universidad Distrital Francisco José de Caldas debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (si se desplazó de una zona mayor a una menor en el mapa de calor) y compararlo con el último nivel de riesgo residual.

En esta fase se deben evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y los controles propuestos, según el Manual de Administración de Riesgos de la Universidad Distrital Francisco José de Caldas. También se considerarán los incidentes de seguridad digital que hayan afectado a la Universidad Distrital Francisco José de Caldas y las métricas o indicadores definidos para seguir las medidas de seguridad implementadas. Todo lo anterior contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la línea estratégica (Alta dirección y Comité Coordinador de Control Interno) y las partes interesadas.

Tabla 11. Líneas de Defensa

Línea de defensa	Conformación	Descripción de su rol y responsabilidades
Línea Estratégica	Alta Dirección Comité Coordinador de Control Interno	Define el marco general para la gestión del Riesgo y el Control y supervisa su cumplimiento.
Primera Línea	Líderes y Gestores de Procesos Supervisores e Interventores	Desarrolla e implementa los procesos de Control y gestión de Riesgos, a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.
Segunda Línea	Jefe Oficina Asesora de Planeación y Control Coordinadores de Subsistemas	Soporta y guía la línea estratégica y la primera línea de defensa en la gestión adecuada de los Riesgos que puede afectar el cumplimiento de los objetivos institucionales y sus Procesos.
Tercera Línea	Jefe Oficina Asesora de Control Interno	Provee aseguramiento a través de su rol de evaluación independiente y objetiva, sobre la efectividad del Sistema de Gestión de Riesgos, validando que las

		demás líneas cumplan con sus responsabilidades.

Fuente: Manual de Gestión de riesgo Universidad Distrital

9.1. Registro y reporte de incidentes de seguridad digital

La Universidad Distrital Francisco José de Caldas registra y gestiona los incidentes de seguridad digital de acuerdo con el procedimiento de Gestión de incidentes de seguridad GSIT-PR-004, que se hayan materializado, para analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar, lo que garantiza que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

9.2. Reporte de la gestión del riesgo de seguridad digital al interior de la Universidad Distrital Francisco José de Caldas

El responsable de seguridad digital debe generar un informe periódicamente a la línea estratégica (Alta Dirección y Comité Coordinador de Control Interno) y a las partes interesadas que contenga la siguiente información:

- Matriz Integral de Riesgos que contiene: Matriz de los riesgos identificados de seguridad digital, reporte de criticidad/impacto de la Universidad Distrital, plan de tratamiento de riesgos, cantidad de riesgos por fuera de la tolerancia del riesgo identificado de acuerdo con la periodicidad de evaluación realizada
- Reporte de evolución de riesgos y modificación del apetito de riesgo
- Impacto económico que puede presentarse frente a la materialización del riesgo
- Listado de Activos críticos e ICC

Este reporte debe presentarse:

- Cuando ocurra un cambio organizacional o de los procesos de la Universidad Distrital Francisco José de Caldas que generen un impacto en las operaciones o que pueda afectar los riesgos ya identificados anteriormente. En cuyo caso realizar una nueva evaluación de los riesgos y reportar los resultados.
- Cuando se incluya un proceso dentro de la gestión de riesgos de seguridad digital de la Universidad Distrital Francisco José de Caldas, ante lo que se debe evaluar riesgos y reportar los resultados.

9.3. Reporte de la gestión del riesgo de seguridad digital a autoridades o entidades especiales

Una vez La Universidad Distrital Francisco José de Caldas obtenga los resultados de la gestión de riesgos de seguridad digital, se debe consolidar información (previamente obtenida con la aplicación

del modelo) con el fin de reportarla a futuro a las autoridades o instancias encargadas del tema y que el gobierno defina.

La finalidad del reporte de esta información es que el Gobierno Nacional pueda identificar posibles oportunidades para la generación de política pública, generación de capacidades o asignación de recursos que permita ayudar a la mejora de la seguridad digital.

La Universidad Distrital Francisco José de Caldas consolidara la siguiente información puntual para poder llevar a cabo el reporte respectivo:

- Riesgos con nivel crítico
- Amenazas críticas
- Vulnerabilidades críticas
- Tipos de Activos afectados por los riesgos críticos (incluyendo servicios digitales o que delimitan con internet)
- Planes de tratamiento propuestos para la mitigación y si han sido ejecutados
- Servicios digitales críticos en la Universidad Distrital Francisco José de Caldas (Servicios o trámites para los ciudadanos o sistemas de información críticos para la Universidad Distrital Francisco José de Caldas).
- Esta información pretende permitir la construcción de un panorama de riesgos de seguridad digital de todo el país, para tomar decisiones estratégicas para la construcción de políticas públicas, generación de capacidades o planes de acción según la información analizada.
- Las infraestructuras críticas cibernéticas -ICC- que hayan sido identificadas deben reportarse a las autoridades o instancias encargadas del tema en el Gobierno nacional.

Nota: Es importante indicar que los reportes de riesgos de seguridad digital a las entidades de gobierno no implicarían o significarían el traslado de la responsabilidad sobre los riesgos o su tratamiento.

9.4. Auditorías internas y externas

Le corresponde a la Oficina Asesora de Control Interno (tercera línea de defensa), cuya responsabilidad es proveer aseguramiento a través de su rol de evaluación independiente y objetiva, sobre la efectividad del Sistema de Gestión de Riesgos, validando que las demás líneas cumplan con sus responsabilidades, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo de seguridad digital en la Universidad Distrital Francisco José de Caldas, catalogándola como una unidad auditable más dentro de su Universo de Auditoría, conforme al Plan Anual de Auditoría aprobado por el Comité Coordinador de Control Interno de la Universidad Distrital Francisco José de Caldas.

9.5. Medición del desempeño

La Universidad Distrital Francisco José de Caldas debe utilizar medidas de desempeño para la gestión de los riesgos de seguridad digital, las cuales reflejan el cumplimiento de los objetivos propuestos y son evaluadas periódicamente alineadas con la revisión por la línea estratégica.

Para lograr la medición del desempeño se deben llevar a cabo las siguientes actividades de revisión:

- De la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de del Modelo de Gestión de Riesgo de Seguridad Digital.
- De la evaluación de los riesgos desarrollada en la Universidad Distrital, donde a su vez se validen los niveles aceptables de riesgo y el riesgo residual después de la aplicación de controles y medidas administrativas.

Para realizar la medición del desempeño solicitar:

- Objetivos del Modelo de Gestión de Riesgos de Seguridad Digital.
- Informes de auditoría anteriores.
- Informes de incidentes de seguridad y medidas implementadas.
- Informes de planes de mejoramiento ejecutados.
- Indicadores definidos del MSPI.

Las siguientes son las actividades generales que soportan la etapa de evaluación del desempeño del Modelo de Gestión de Riesgos de Seguridad Digital:

- Identificar los objetivos del Modelo de Gestión de Riesgos de Seguridad Digital
- Recolección de resultados de auditorías de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
- Recolección y Consolidación de indicadores de cumplimiento definidos para el MSPI.
- Evaluar indicadores frente a las metas de cumplimiento definidas y compararlos con los resultados identificados previamente.
- Graficar los indicadores.
- Analizar causas de las desviaciones.
- Preparar informes de efectividad para la alta dirección

Los indicadores serán los siguientes:

- Riesgos tratados

Numero de riesgos con definición de controles / Número total de riesgos identificados

- Riesgos materializados

Numero de riesgo materializados / Número total de riesgos identificados

- Numero de hallazgos

Numero de hallazgos identificados mediante las Auditorias

- Riesgos críticos

Numero de riesgos críticos identificados / número total de riesgos identificados.

- Cumplimiento de Planes de tratamiento

Planes de tratamiento cumplidos / Número total de plan de tratamiento definidos

10. FASE DE MEJORAMIENTO CONTINUO DE LA GESTIÓN RIESGO DE SEGURIDAD DIGITAL

La Universidad Distrital Francisco José de Caldas debe garantizar la mejora continua de la gestión de riesgos de seguridad digital, para mitigar el impacto de hallazgos, falencias o incidentes de seguridad digital y actuar para controlarlos y prevenirlos. Además, de revisar las consecuencias de la no conformidad que se materializó.

Definir las acciones para mejorar continuamente la gestión de riesgos de seguridad digital de la siguiente forma:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la Universidad Distrital Francisco José de Caldas o de los servicios que presta al ciudadano.
- Adicionalmente, llevar un registro documentado del tratamiento realizado al hallazgo, incluyendo las acciones realizadas, las fechas en que se realizaron y los responsables de su ejecución.

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