MANUAL DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE

SECRETARÍA DISTRITAL DE CULTURA, RECREACIÓN Y DEPORTE

2022

Contenido

Índice de tablas

Índice de ilustraciones

1. INTRODUCCIÓN

El presente documento hace parte de la estrategia y actividades para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI de MinTIC, en el cual se prevé la identificación, valoración y tratamiento de los riesgos de Seguridad de la Información, en concordancia con las directrices para la administración de riesgos, definida por el Departamento Administrativo de la Función Pública (DAFP), en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.

2. OBJETIVO

Establecer la metodología que oriente a los responsables de los activos de información en la identificación, valoración y tratamiento de los riesgos de Seguridad de la Información de la Secretaría Distrital de Cultura, Recreación y Deporte en adelante identificada con la sigla SCRD, cuya finalidad es la protección de los activos y fortalecer la toma de decisiones, respecto al adecuado tratamiento de los riesgos de Seguridad de la Información.

3. OBJETIVOS ESPECÍFICOS

- Identificar, analizar y valorar los riesgos de Seguridad de la Información de los activos de información de las dependencias de la SCRD.
- Identificar las amenazas e impacto de Seguridad de la Información a las cuales están expuestos los activos de información.
- Identificar e implementar los controles necesarios para el tratamiento de los riesgos de Seguridad de la Información.
- Definir y socializar, los instrumentos para la identificación, valoración y tratamiento de los riesgos de Seguridad de la Información.

4. ALCANCE

La metodología para la identificación, valoración y tratamiento de los riesgos de Seguridad de la Información, aplica a todas las dependencias y procesos de la SCRD, quienes deben aplicarla para realizar las actividades correspondientes al tratamiento de riesgos de Seguridad de la Información.

5. NORMATIVIDAD Y DOCUMENTOS ASOCIADOS

Se tendrán como línea base para la identificación, clasificación y valoración del inventario de activos de información las siguientes normas y/o Leyes:

- **Ley 1266 de 2008:** por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **Ley 1581 de 2012:** por la cual se dictan disposiciones generales para la protección de datos personales.

- **Decreto 1377 de 2013**: por el cual se reglamenta parcialmente la Ley 1581 de 2012. Que mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1, tiene por objeto "(.. .) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

- **Ley 1712 de 2014:** por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- **Decreto 103 de 2015**: por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Que para facilitar la implementación y cumplimiento de la Ley 1712 de 2014 se hace necesaria su reglamentación en los temas relacionados con la gestión de la información pública en cuanto a: su adecuada publicación y divulgación, la recepción y respuesta a solicitudes de acceso a ésta, su adecuada clasificación y reserva, la elaboración de los instrumentos de gestión de información, así como el seguimiento de la misma.

- **Decreto 1081 de 2015:** por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República, compiló el decreto 2641 de 2012, reglamentario de los artículos 73 y 76 de la ley 1474 de 2011, mediante el cual se estableció como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano, la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano".

- **Decreto 1083 de 2015:** por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública, entre otros aspectos establece que, se deben tomar medidas para administrar los riesgos en la entidad pública (Artículo 2.2.21.5.4).

- **Decreto 1078 de 2015:** por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- **Decreto 648 de 2017:** por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública, y en su Artículo 2.2.21.1.6 literal g., establece dentro de las funciones del Comité Institucional de Coordinación de Control Interno que se debe someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.

- **Decreto 1008 de 2018:** 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.

- **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5:** establece los lineamientos que deben ser utilizados por los responsables de la gestión y tratamiento de riesgos en las entidades públicas.

- **Norma NTC ISO/IEC 27001:2013:** es el referente internacional a la hora de implementar el Sistema de Gestión de Seguridad de la Información, emite lineamientos y directrices para que las organizaciones aseguren la confidencialidad, integridad y disponibilidad de la información.

6. DEFINICIONES

A continuación, se relacionan una serie de conceptos necesarios para la comprensión de la metodología,

- **Activo de información:** un activo de información es, cualquier elemento que contenga, genere, adquiera, gestione y/o procese información, que tiene valor para uno o más procesos de la organización en razón a qué aporta al cumplimiento de su objetivo y por lo cual debe protegerse[1]. En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital[2].

[1] Adaptado de ISO IEC 27000.

[2] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.

- **Apetito de riesgo**: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar[3].

- **Capacidad de riesgo**: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad[4].

- **Causa**: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo[5].

- **Causa Inmediata**: circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo[6].

- **Causa Raíz**: causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo[7].

- **Confidencialidad:** es la propiedad que determina que la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados[8].

- **Consecuencia**: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas[9].

- **Control**: medida que permite reducir o mitigar un riesgo[10].

- **Disponibilidad:** es la propiedad de acceso y utilización de la información por parte de los individuos, entidades o procesos autorizados cuando lo requieran[11].

- **Factores de Riesgo**: Son las fuentes generadoras de riesgos[12].

- **Integridad:** es la propiedad que garantiza la exactitud y completitud de la información[13].

- **Impacto**: las consecuencias que puede ocasionar a la organización la materialización del riesgo[14].

- **Nivel de riesgo**: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad

[3] Ibidem.
[4] Ibidem.
[5] Ibidem.
[6] Ibidem.
[7] Ibidem.
[8] Adaptado de ISO IEC 27000.
[9] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.
[10] Ibidem.
[11] Adaptado de ISO IEC 27000.
[12] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.
[13] Adaptado de ISO IEC 27000.
[14] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.

* Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto[15].

- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año[16].

- **Propietario de la Información:** cargo, proceso, o dependencia que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso[17].

- **Riesgo**: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos[18].

- **Riesgo Inherente**: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad[19].

- **Riesgo Residual**: el resultado de aplicar la efectividad de los controles al riesgo inherente[20].

- **Riesgo de Seguridad de la Información**: 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. (ISO/IEC 27000) [21].

- **Tolerancia del riesgo**: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad[22].

- **Vulnerabilidad**: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas[23].

[15] Ibidem.
[16] Ibidem.
[17] Adaptado de la Guía de Gestión de Activos - MINTIC.
[18] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.
[19] Ibidem.
[20] Ibidem.
[21] Ibidem.
[22] Ibidem.
[23] Ibidem.

7. ROLES Y RESPONSABILIDADES:

Los siguientes roles son los responsables y tienen participación directa en la correcta implementación y ejecución de la metodología para la identificación, valoración y tratamiento de los riesgos de Seguridad de la Información de la SCRD.

Rol	Responsable	Responsabilidades
ALTA DIRECCIÓN (LÍNEA ESTRATÉGICA)	Comité Institucional de coordinación de Control Interno	Verificar los riesgos de Seguridad de la Información.
TODAS LAS DEPENDENCIAS Y PROCESOS (PRIMERA LÍNEA DE DEFENSA)	Líderes de Proceso. Responsables de la Información.	- Identificar y tratar sus riesgos de Seguridad de la Información. - Designar personal de planta o contratistas, para la identificación y tratamiento de riesgos de Seguridad de la Información, teniendo en cuenta que deben ser idóneos en el tema. - Aprobar y realizar el tratamiento de los riesgos de Seguridad de la Información de su competencia.
OFICINA ASESORA DE PLANEACIÓN (SEGUNDA LÍNEA DE DEFENSA)	Jefe Oficina Asesora de Planeación.	-Gestionar el versionamiento y publicación en la Cultunet del documento manual identificación, valoración y tratamiento de los riesgos de Seguridad de la Información. - Articular y acompañar la concertación de mesas de trabajo con cada uno de los "responsables" designados por cada dependencia para la identificación, valoración y tratamiento de riesgos de Seguridad de la Información. - Realizar el monitoreo a los riesgos de Seguridad de la Información y al plan de acción, acorde con la información suministrada por los líderes de procesos
OFICINA DE TECNOLOGÍAS DE INFORMACIÓN	Jefe Oficina de Tecnologías de la Información Equipo Seguridad de la Información.	Definir, revisar y/o actualizar el manual de gestión de riesgos de Seguridad de la Información. Apoyar a la OAP y las dependencias en el seguimiento, identificación, valoración y tratamiento de los riesgos de Seguridad de la Información.

Tabla 1. Responsables
Fuente: Elaboración propia Seguridad de la Información.

NOTA: La definición, revisión, actualización, modificación, anulación, control de cambios y gestión para aprobación, es responsabilidad del Equipo de Seguridad de la Información de la Oficina de Tecnologías de la Información de la SCRD.

8. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Secretaría Distrital de Cultura, Recreación y Deporte definió y aprobó la política **DES-POL-01 POLÍTICA DE ADMINISTRACIÓN DE RIESGOS**, en la cual se definen los lineamientos institucionales para la gestión de riesgos en la Entidad, se contemplan los riesgos asociados a Gestión, Corrupción y Seguridad de la Información.

9. METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta las indicaciones de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5, se debe determinar el contexto de la organización como parte inicial de la identificación de los riesgos, posteriormente se realiza la valoración del riesgo y se determinan las acciones necesarias para disminuir el riesgo a un nivel aceptable y continua con el tratamiento de los riesgos.

La aceptación del riesgo debe asegurar que los riesgos residuales sean aceptados explícitamente por el equipo directivo de la entidad. Esto es especialmente importante dado el caso en el que la implementación de los controles se omita o deba posponerse, por ejemplo, por temas presupuestales o de capacidades de la Entidad[24].

En la siguiente tabla se presentan las actividades propias de la gestión de riesgos de Seguridad de la Información, de acuerdo con las diferentes fases que define el Modelo de Seguridad y Privacidad de la Información – MSPI.

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Ilustración 1Etapas de la Gestión del Riesgo a lo Largo del MSPI
Fuente: Guía N°7 – Gestión de Riesgos de MinTIC.

10. IDENTIFICACIÓN DE RIESGOS

Para realizar la gestión de riesgos asociados a seguridad de la información, es necesario que los responsables designados por cada dependencia conozcan el objetivo de su respectiva área, de igual forma, se debe tener disponible el inventario de activos de información de su competencia, este insumo se obtiene como resultado de las actividades del manual GOT-MN-02 “Manual para la identificación y clasificación de activos de información” con lo cual se puede proceder a realizar las actividades correspondientes a la identificación, valoración y tratamiento de riesgos de Seguridad de la Información y de esta manera propender por implementar las acciones necesarias para cumplir con el respectivo tratamiento y el nivel adecuado de protección.

10.1 Riesgos de Seguridad de la Información

A continuación, se definen los riesgos de Seguridad de la Información, las vulnerabilidades y amenazas en concordancia con los lineamientos del Anexo lineamientos para la Gestión de Riesgos de Seguridad Digital en

[24] Guía N°7 – Gestión de Riesgos. MinTIC.

Entidades Públicas de MINTIC, que incluye el identificador tanto para seguridad como para privacidad de la información, los cuales son la línea base en el diligenciamiento del mapa riesgos.

Para la identificación del riesgo se debe realizar frente a los activos de información que tengan un nivel de criticidad ALTO, a estos activos se les realizará el respectivo proceso de gestión de riesgos.

En seguridad de la información se definen 3 riesgos que son:

1. Posibilidad de pérdida de confidencialidad
2. Posibilidad de pérdida de integridad
3. Posibilidad de pérdida de disponibilidad

En Datos Personales se definen 4 riesgos que son:

1. Posibilidad de pérdida de confidencialidad, divulgación no autorizada o uso mal intencionado de la información de datos personales
2. Posibilidad de pérdida de integridad, alteración o sustracción de Información de datos personales
3. Posibilidad de afectación de la disponibilidad de la plataforma tecnológica que gestiona datos personales
4. Posibilidad de sanciones por incumplimiento de las directrices normativas frente a datos personales

Los riesgos de seguridad de la información y de datos personales, se basan en la afectación de alguno de los tres principios de seguridad de la información, Integridad, Confidencialidad o Disponibilidad de los activos de información identificados y valorados en cada proceso y/o dependencia de la SCRD.

10.2 Vulnerabilidades

Son las debilidades identificadas y que pueden ser explotadas por una amenaza, la tecnología, los activos de información, las personas y/o la infraestructura con la que se realiza el procesamiento de la información pueden ser aprovechadas por las amenazas, afectando la confidencialidad, integridad y/o disponibilidad de la información. La Tabla 2. Vulnerabilidades, presenta un listado de causas identificadas por la SCRD, que sirven como guía para la identificación del riesgo, es de aclarar que la vulnerabilidad se debe redactar citando el contexto y los detalles que la sustenten de forma clara y precisa.

Es fundamental entender que las vulnerabilidades están sobre los activos de hardware, software, personas e infraestructura física que contienen o manejan la información y esto debe quedar claramente diferenciado, por eso al describir una vulnerabilidad se debe especificar si esta radica sobre el hardware, el software, las personas o la infraestructura física. Se proponen a modo de guía para la formulación las siguientes:

VULNERABILIDADES		
TIPO	**ID**	**ÍTEM**
1. Personas	**1.1**	Ausencia de personal idóneo.
	1.2	Ausencia o carencia de conocimientos y habilidades en informática.
	1.3	Desconocimiento de los lineamientos de Seguridad de la Información.
	1.4	Ausencia de reporte de incidentes de Seguridad de la Información.
	1.5	Debilidad frente a la gestión y uso de herramientas de seguridad informática.
	1.6	Falta de conciencia en Seguridad de la Información.
	1.7	Desconocimiento de las políticas para el buen uso de los servicios tecnológicos (Red, Correo, Internet, Sistemas de Información, otros).

VULNERABILIDADES		
TIPO	**ID**	**ÍTEM**
	1.8	Personal inconforme.
	1.9	Desconocimiento del marco legal y regulatorio de seguridad de la información.
	1.10	Desconocimiento de los controles de seguridad informática aplicados a la información de su responsabilidad.
	1.11	Desconocimiento del marco legal y regulatorio de la protección de los datos personales.
	1.12	Falta de conciencia en Protección de Datos Personales
	1.13	Dualidad de tareas en los funcionarios y contratistas
2. Infraestructura Tecnológica	**2.1**	Insuficiencia o mal funcionamiento de controles de acceso físico a las instalaciones de la entidad.
	2.2	Falta de monitoreo para el control de acceso físico a las edificaciones y recintos.
	2.3	Falta de mantenimiento a la infraestructura de: cableado, racks, aire acondicionado, sistemas de detección de incendios, UPS y planta eléctrica.
	2.4	Ubicación en un área susceptible de inundación o deterioro físico y locativo.
	2.5	Ausencia de protección contra la humedad, polvo y suciedad.
	2.6	Ausencia de controles antisísmicos.
	2.7	Ausencia o deficiencia en los controles para detección y/o prevención de incendios.
	2.8	Almacenamiento de documentos impresos sin medidas de protección.
	2.9	Errores humanos.
	2.10	Error en la manipulación de la Infraestructura Tecnológica.
	2.11	Fallas Técnicas de Hardware
3. Sistemas de Información/Servicios informáticos/Información	**3.1**	Ausencia de mantenimientos preventivos y correctivos.
	3.2	Mala identificación de los requisitos técnicos y funcionales.
	3.3	Asignación inadecuada de privilegios de acceso.
	3.4	Ausencia de parchado de los componentes tecnológicos
	3.5	Ausencia de mecanismos de identificación y autenticación de usuario.
	3.6	Inadecuada segregación de funciones, roles y perfiles de usuario.
	3.7	Ausencia de un proceso formal para la revisión periódica de los permisos de acceso de los usuarios.
	3.8	Ausencia de documentación actualizada de los Sistemas de Información.
	3.9	Imposibilidad de actualización de los Sistemas de Información por integración con otros.
	3.10	Falta de control en el cumplimiento de actualización de software.
	3.11	Ausencia o insuficiencia de pruebas de software.

VULNERABILIDADES		
TIPO	**ID**	**ÍTEM**
	3.12	Uso de software desactualizado o que no cumple con los requerimientos de los usuarios.
	3.13	Configuraciones por defecto.
	3.14	Los ambientes de pruebas, desarrollo y producción no se encuentran separados.
	3.15	Incapacidad del sistema para atender un alto volumen de conexiones.
	3.16	Permitir la ejecución de sesiones simultáneas del mismo usuario en el sistema de información o servicio.
	3.17	Uso de código con vulnerabilidades, para la protección de la información.
	3.18	Versión desactualizada de software y medios de almacenamiento para las Copias de Respaldo.
	3.19	Ausencia de Backup y pruebas de restauración.
	3.20	Ausencia de documentación de los puertos que utilizan los Sistemas de Información o Servicios.
	3.21	Errores humanos
	3.22	Ausencia de control para "terminar sesión" luego de un tiempo determinado de inactividad.
	3.23	No activación de registros de logs
	3.24	Habilitación de servicios de red innecesarios.
	3.25	Ausencia de pruebas de vulnerabilidad periódicas.
	3.26	Ausencia de líneas base para la instalación de los componentes tecnológicos.
4. Datos personales	**4.1**	Ausencia o carencia de personal que se encargue de la implementación de los temas relacionados con protección de los datos personales.
	4.2	Ausencia de personal de respaldo para los roles y responsabilidades en protección de datos personales.
	4.3	Ausencia de una política de protección de datos personales.
	4.4	Ausencia de procedimientos para la recolección de datos personales.
	4.5	Falta de conocimiento del personal en el debido tratamiento de los datos personales descritos en la finalidad del tratamiento.
	4.6	Ausencia de evidencia de la autorización para recolección y tratamiento de datos personales.
	4.7	Ausencia o debilidades en la parte contractual para la transmisión y/o transferencia de datos personales.
	4.8	Ausencia de lineamientos para el tratamiento de datos personales.

VULNERABILIDADES		
TIPO	**ID**	**ÍTEM**
	4.9	Ausencia de procedimientos para la eliminación de los datos personales cuando ya no se requieran.
	4.10	Carencia de procedimientos y/o herramientas para la solicitud de rectificaciones, cancelaciones y demás relacionadas con los datos personales.
	4.11	Dificultar o imposibilitar el ejercicio de los derechos de los titulares de los datos personales.
	4.12	Utilizar los datos personales para finalidades diferentes a las especificadas.
	4.13	Falta de controles de acceso frente a información de datos personales en temas reservados.
	4.14	Intereses a favor de un tercero o perfil inadecuado de los servidores públicos que intervienen en el proceso
	4.15	Intrusión informática y manipulación, modificación, eliminación, robo o cifrado de la información.
	4.16	Fallas en la plataforma tecnológica para control y validación de los campos que registran información de datos personales.
5. Hardware	**5.1**	Ausencia de mantenimientos preventivos.
	5.2	Mantenimiento insuficiente o inoportuno de los componentes de hardware.
	5.3	Falta o fallas de sincronización de reloj del servidor.
	5.4	Debilidades en la seguridad física de la red de datos.
	5.5	Arquitectura de red de datos que no cumple los requerimientos de seguridad de la información.
	5.6	Ausencia de control sobre dispositivos móviles.
	5.7	Ausencia o deficiencia en los procedimientos de monitoreo a los recursos de procesamiento de información.
	5.8	Ausencia de pruebas de vulnerabilidad.
	5.9	Ausencia de Planes de Continuidad o Planes de Recuperación de Desastres (DRP).
	5.10	Ausencia de Pruebas de los Planes de Continuidad y/o los Planes de Recuperación de Desastres (DRP).
	5.11	Ausencia de sistemas redundantes (Alta disponibilidad).
	5.12	Único proveedor de Internet.
	5.13	Ausencia o insuficiencia de ANS (Acuerdos de niveles de servicio).
	5.14	Susceptibilidad a las variaciones de voltaje.
	5.15	Ausencia de copias de respaldo del firmware de los dispositivos de comunicaciones, seguridad, servidores y otros que aplique.
	5.16	Falta de pruebas de verificación de las copias de respaldo.
	5.17	Ausencia de almacenamiento externo de las copias de respaldo.
	5.18	Obsolescencia de medios de respaldo de información.
	5.19	Obsolescencia tecnológica.

Tabla 2 Vulnerabilidades
Fuente: Adaptado del Anexo 4, lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas

10.3 Amenazas

Es la circunstancia o evento que puede causar un daño o impacto negativo cuando explota la vulnerabilidad afectando la confidencialidad, integridad o disponibilidad de la información de la SCRD, quiere decir esto, que la amenaza explota las vulnerabilidades identificadas de la información, el hardware, el software, los servicios, las personas, las bases de datos personales y/o la infraestructura tecnológica.

Cuando se analice el evento es necesario determinar si este tiene origen en las personas, los equipos, activos o es de tipo natural. Si tiene origen en las personas se debe determinar si el evento es de tipo intencional o accidental. El mayor nivel de detalle provisto facilita el análisis del riesgo correspondiente.

En la Tabla 3. Amenazas, se presenta listado guía de amenazas identificadas por la SCRD, las cuales son la base para formular las que se requieran.

AMENAZAS		
TIPO	**ID**	**AMENAZAS**
1. Personas	**1.1**	Sobrecarga laboral.
	1.2	Ingeniería social.
	1.3	Coacción.
	1.4	Sabotaje.
	1.5	Errores humanos en el cumplimiento de las labores.
	1.6	Acciones fraudulentas.
	1.7	Entrega indebida de la información.
	1.8	Modificación indebida de la información.
2. Infraestructura Física	**2.1**	Contaminación, polvo, corrosión.
	2.2	Niveles de temperatura o humedad por fuera de los rangos aceptables.
	2.3	Fallas de electricidad.
	2.4	Señales de interferencia.
	2.5	Daño en instalaciones físicas.
	2.6	Fallas en el aire acondicionado.
	2.7	Fallas en las UPS.
	2.8	Fallas en la planta eléctrica.
	2.9	Desastres naturales.
	2.10	Incendio.
	2.11	Inundación.
	2.12	Asonada/Conmoción civil/Terrorismo.
	2.13	Desastre accidental.
3. Sistemas de Información/Servicios informáticos/Información	**3.1**	Ataque informático para acceder a información clasificada o reservada.
	3.2	Ataque informático para modificar datos.
	3.3	Ingeniería social.
	3.4	Interceptación de información.
	3.5	Cifrado no autorizado de la información por malware o acción mal intencionada.

AMENAZAS		
TIPO	**ID**	**AMENAZAS**
	3.6	Corrupción de los datos por fallas en el software.
	3.7	Suplantación de usuarios.
	3.8	Abuso de privilegios.
	3.9	Elevación de privilegios.
	3.10	Exposición de información clasificada o reservada por errores de configuración.
	3.11	Malware.
	3.12	Denegación de servicios.
4. Hardware	**4.1**	Fallas en los componentes de hardware.
	4.2	Falla de medios de respaldo y recuperación.
	4.3	Fallas en el aire acondicionado.
	4.4	Uso de equipos no autorizados como piñas, videocámaras, y grabadoras entre otros.
	4.5	Hurto de equipos, medios magnéticos o documentos.
	4.6	Fallas en el suministro de energía eléctrica.
	4.7	Acceso a información clasificada o reservada dese componentes tecnológicos reciclados o desechados.
5. Datos Personales	**5.1**	No facilitar o generar mecanismos de acceso a la información en materia de datos personales a los titulares.
	5.2	Tratar datos personales inadecuados y excesivos para la finalidad del tratamiento.
	5.3	Tratar datos personales con una finalidad distinta para la cual fueron recolectados.
	5.4	No disponer de una estructura organizativa, procesos y recursos para la adecuada gestión de los datos personales en la SDCR.
	5.5	Almacenar los datos personales, por tiempos superiores a los necesarios, según su finalidad de tratamiento.
	5.6	Realizar transferencias internacionales de datos personales a países que no ofrezcan un nivel de protección adecuado.
	5.7	No tramitar o dificultar el ejercicio de los derechos de los interesados.
	5.8	Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma.
	5.9	Seleccionar o mantener una relación con un encargado de tratamiento sin disponer de las garantías adecuadas.
	5.10	No disponer de una estructura organizativa, procesos y recursos para una adecuada gestión datos personales en la SCRD.
	5.11	Violaciones de la confidencialidad de los datos personales por parte de los funcionarios, contratistas o proveedores externos de la SCRD.
	5.12	Información no actualizada o incorrecta (Registros duplicados con información inconsistente o con campos de datos incorrectos).
	5.13	Acceso a información, servicios, aplicaciones o dispositivos de forma no autorizada, por personas no autorizadas.
	5.14	Manipulación o modificación no autorizada de la información de datos personales.

AMENAZAS		
TIPO	**ID**	**AMENAZAS**
	5.15	Deficiencias en los protocolos de recolección, almacenamiento, uso, circulación o supresión de los datos personales en formato físico
	5.16	Desordenes de carácter social que atenten contra activos que contienen información personal.

Tabla 3 Amenazas

Fuente: Adaptado del Anexo 4, lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas

NOTA: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control[25].

[25] Tomado de Anexo 4, lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas.

11. EFECTOS O CONSECUENCIAS

Son los efectos ocasionados por la materialización de un riesgo de seguridad de la información y que afecta los objetivos o procesos de la Entidad causando consecuencias para la Entidad, los cuales pueden ser de tipo económico y reputacional. A continuación, se presenta una propuesta de consecuencias a modo de guía para adaptarlas a las necesidades.

CONSECUENCIAS		
TIPO	**ID**	**ÍTEM**
1. Consecuencias Riesgos de Seguridad de la Información	**1.1**	Indisponibilidad de servicios y sistemas de información, afectando a usuarios internos y externos. Afectación a toda la entidad.
	1.2	Imposibilidad o dificultad para toma de decisión, debido a información inexacta o desactualizada.
	1.3	Retraso en procesos.
	1.4	Indisponibilidad de los servicios de TICs.
	1.5	Violación a las políticas de seguridad.
	1.6	Quejas, reclamos frente a la prestación de servicios.
	1.7	Retrasos en las actividades de los funcionarios y/o contratistas.
	1.8	Pérdida de credibilidad en las herramientas informáticas de la SCRD.
	1.9	Sanciones legales y disciplinarias.
	1.10	Afectación de la Imagen de la Entidad.
	1.11	Deterioro o debilitamiento de los soportes documentales.
	1.12	Pérdida parcial o total de información de la Entidad.
	1.13	Sanciones disciplinarias, penales o fiscales, demandas o acciones judiciales en contra de la Entidad.
	1.14	Posibles hallazgos de auditorías internas y/o externas.
	1.15	La pérdida de información o filtración puede generar riesgos a la seguridad de la información institucional.
	1.16	Vulneración de derechos de personas naturales o jurídicas o afectación de intereses públicos.
	1.17	Dificultades en el acceso a la información, por parte de la ciudadanía y partes interesadas.
	1.18	Inoportunidad en la entrega de información.
	1.19	Se pueden presentar casos de corrupción.
	1.20	La pérdida de información o filtración puede generar riesgos a la seguridad y privacidad de la información de datos personales.

CONSECUENCIAS		
TIPO	**ID**	**ÍTEM**
	1.21	Vulneración de derechos de personas naturales.
	1.22	Incumplimiento del tiempo de respuesta que tienen las PQRS que reciben las dependencias.
	1.23	Dificultades en el acceso a la información, por parte de los titulares de datos personales.
2. Consecuencias Riesgos de Datos Personales	**2.1**	Hallazgos y/o sanciones por entes de control internos y externos.
	2.2	Incumplimiento de las estrategias, objetivos, procedimientos y programas.
	2.3	Pérdida de credibilidad e imagen de la Entidad.
	2.4	Pérdidas económicas y/o sobrecostos por inoperatividad en los procesos.
	2.5	Sanciones disciplinarias internas en la organización.
	2.6	Pérdida de la información.
	2.7	Incumplimiento en la normatividad legal vigente.
	2.8	Recolección de Información no veraz ni utilizable.
	2.9	Afectación física de los activos de la información.

Tabla 4 Amenazas
Fuente: Adaptado del Anexo 4, lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas

12. VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En esta fase se establece la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de identificar la zona de riesgo inherente, en otras palabras, es el riesgo antes de aplicar controles.

12.1 Probabilidad

Para determinar la probabilidad, se tiene en cuenta la exposición del proceso o la actividad al riesgo que se está analizando, es decir, es el número de veces que se pasa por el punto de riesgo durante un año, como se muestra en la siguiente tabla.

ANÁLISIS DE PROBABILIDAD

Valor Inherente	Probabilidad Inherente	Frecuencia
Muy Baja	20%	La actividad que conlleva el riesgo se ejecuta como máximo 5 veces al año.
Baja	40%	La actividad que conlleva el riesgo se ejecuta de 6 a 25 veces por año.
Media	60%	La actividad que conlleva el riesgo se ejecuta de 26 a 150 veces por año.

Valor Inherente	Probabilidad Inherente	Frecuencia
Alta	80%	La actividad que conlleva el riesgo se ejecuta de 151 a 300 veces por año.
Muy Alta	100%	La actividad que conlleva el riesgo se ejecuta más de 301 veces por año.

Tabla 5 Análisis de Probabilidad
Fuente: Adaptado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5

12.2 Impacto

Para determinar el impacto referente a afectaciones económicas y/o reputacionales, los cuales contemplan afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio como lo señala la guía del DAFP, en este sentido se tienen los siguientes criterios para definir los niveles de impacto.

ANÁLISIS DE IMPACTO

Valor Inherente	Impacto Inherente	Afectación económica	Afectación reputacional
Muy Baja	20%	Pérdida económica hasta 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Baja	40%	Pérdida económica de 11 hasta 20 SMLV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, a nivel interno, de directivos y/o de proveedores.
Media	60%	Pérdida económica de 20 hasta 100 SMLV	Afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Alta	80%	Pérdida económica de 100 hasta 500 SMLV	Afecta la imagen de la entidad con efecto publicitario sostenido a nivel Sectorial.
Muy Alta	100%	Pérdida económica superior a 500 SMLMV	Afecta la imagen de la entidad a nivel nacional, con efecto publicitarios a nivel Distrital.

Tabla 6 Análisis de Impacto
Fuente: Adaptado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5

12.3 Evaluación del riesgo

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se obtiene el resultado del riesgo inherente o inicial, es decir antes de aplicar controles, y se identifica el nivel de severidad del riesgo, que puede quedar ubicado en alguna de las 4 zonas (Extremo, Alto, Moderado, Bajo), para lo cual se tiene como referencia la siguiente matriz de calor.

MATRIZ DE CALOR						
PROBABILIDAD	Muy alta 100%					
	Alta 80%					
	Media 60%					
	Baja 40%					
	Muy baja 20%					
IMPACTO		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Tabla 7 Análisis de Impacto

Fuente: Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5

Es importante tener en cuenta las siguientes premisas:

- La fuente de información de los controles, son los Líderes de procesos, dependencia o funcionarios, quienes tienen el criterio experto, en concordancia con el objetivo de su proceso o dependencia.
- Los responsables de implementar y realizar seguimiento a la efectividad de los controles son los Líderes de proceso con el apoyo de su equipo de trabajo.

13. TRATAMIENTO DE LOS RIESGOS

Una vez identificados y valorados los riesgos, se debe definir el tratamiento para cada uno de ellos teniendo en cuenta los criterios definidos en la Política de Administración del Riesgo adoptada por la SCRD. Estas decisiones que se toman de acuerdo al nivel de riesgo pueden ser **Aceptar, Reducir o Evitar**.

Así mismo, se definen **niveles de aceptación del riesgo**, con el fin de determinar el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad, partiendo del "**Apetito**" que es el nivel de riesgo que se puede aceptar en relación con sus objetivos, el marco legal y se define por las diferentes clasificaciones de riesgos, así mismo, se establece el valor máximo de desviación y la "**Tolerancia**" Tope máximo admisible del nivel de riesgo con respecto al apetito determinado, para lo cual para los riesgos de seguridad, se define[26]:

Riesgo	Nivel de Aceptación	Zona de Riesgo Inherente	Gestión del Riesgo	Seguimiento Primera y Segunda línea de defensa (OAP)
SEGURIDAD DE LA INFORMACIÓN		BAJA	Se deben mantener los controles existentes	Se realiza seguimiento a los controles con periodicidad SEMESTRAL y se registran sus avances en el instrumento destinado.
	APETITO	MODERADA		
	TOLERANCIA	ALTA	Se deben establecer nuevos controles o fortalecer los existentes que permitan reducir el riesgo.	
		EXTREMA		

[26] POLÍTICA DE ADMINISTRACIÓN DE RIESGOS - SCRD

Tabla 8 Niveles de aceptación del riesgo
Fuente: Tomado de POLÍTICA DE ADMINISTRACIÓN DE RIESGOS - SCRD

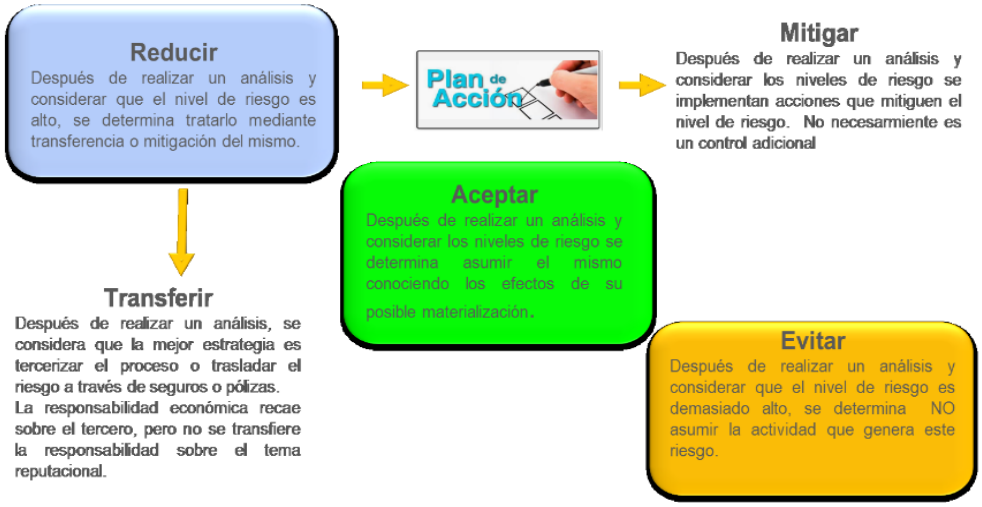

Ilustración 2 Estrategias para combatir el riesgo
Fuente: Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.

Es importante resaltar que cuando se decide reducir el riesgo es necesario definir un plan de acción o tratamiento, donde se incluya entre otros, el responsable, la fecha en la que se implementará el control y la fecha de seguimiento a este[27].

14. CONTROLES ASOCIADOS

De acuerdo a las directrices de la Guía de Administración del Riesgo del DAPF, para el tratamiento de los riesgos, es necesario aplicar como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, cuando estos se ajusten al respectivo análisis de los riesgos que se han identificado los controles también se encuentran identificados en la Guía No. 8 del Modelo de Seguridad y Privacidad de la Información – MSPI. El listado completo de los controles puede ser consultado y tomado como referencia de la siguiente URL: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

El seguimiento a la implementación de los controles, se realiza mediante el plan de tratamiento de riesgos, en este punto se indica el control aplicado, el respectivo soporte, el responsable y el tiempo de implementación y finaliza con un indicador de eficacia ya definido en la Guía del DAFP.

14.1 Indicadores

1. **EFICACIA**:
   Índice de cumplimiento de actividades = (# de actividades cumplidas / # de actividades programadas) x 100[28].

[27] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5
[28] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5

15. DOCUMENTOS ASOCIADOS

NOMBRE	CODIGO	FISICO	MAGNÉTICO	APLICATIVO
Matriz de riesgos de seguridad de la información[29]	DES-MN-04-FR-01	X	X	

,

16. CONTROL DE CAMBIOS

Nota: A partir de la aprobación del mapa de procesos versión 09, se reinicia el versionamiento documental esto quiere decir que inicia en versión 1, teniendo en cuenta el rediseño institucional y la nueva codificación, buscando la simplificación de documentos

No.	CAMBIOS REALIZADOS
1	Solicitud inicial. Ver formato "Solicitud de elaboración, modificación o eliminación de documentos" Fecha: 18/08/2022 Radicado ORFEO 20221700314823

17. RESPONSABLES DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

ELABORÓ	REVISÓ OAP	REVISÓ	APROBÓ
NOMBRE: Andrés Cadena	NOMBRE: Ruth Yanina Bermúdez Alejandra Trujillo Díaz	NOMBRE: Patricia Rodríguez Jairo León Wilmar Valencia Gustavo Nieto	NOMBRE: Juan Manuel Vargas Ayala (E) Liliana Morales
CARGO: Contratista Oficina de Tecnologías de la Información	CARGO: Profesional Universitario Oficina Asesora de Planeación Contratista Oficina Asesora de Planeación	CARGO: Contratistas Oficina de Tecnologías de la Información	CARGO: Jefe Oficina Asesora de Planeación Jefe Oficina de Tecnologías de la Información
FIRMA: Electrónica	FIRMA: Electrónica	FIRMA: Electrónica	FIRMA: Electrónica

[29] Tomada de MINTIC – Máxima Velocidad 2022