PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ENERO 2021

Dirección: Av el Dorado, Calle 26 No 69-76 Torre 1 Piso 9
Código Postal: 111071
PBX: 3169001
Página WEB: www.sdmujer.gov.co
Presente su petición, queja, reclamo o sugerencia al correo electrónico:
Servicioalaciudadania@sdmujer.gov.co

1. INTRODUCCIÓN

En el marco de la administración y gestión de los riesgos, la **Secretaria Distrital de la Mujer - SDMUJER** está trabajando en establecer una política de gestión frente a los temas relacionados con la Seguridad y Privacidad de la Información.

La información de la SDMUJER es fundamental para el cumplimiento de los objetivos misionales y su relación con las ciudadanas, por lo tanto es prioridad el manejo y cuidado de la misma, para evitar la posibilidad de la alteración, mal uso, pérdida y/o filtración, por lo tanto, es necesario definir el Plan de Tratamiento de Riesgos de Información que permita la identificación, análisis, valoración y tratamiento de riesgos relacionados con la seguridad de la información institucional ya sea física o digital, en cada uno de sus procesos, con el fin de garantizar la seguridad en términos de integridad, confiabilidad y disponibilidad.

2. OBJETIVO

Establecer el tratamiento de los riesgo Riesgos de Seguridad de Información como una guía metodológica para la SDMUJER que permita a los lideres o liderezas del proceso gestionar y administrar el riesgo para prevenir su materialización y asegurar la información y los recursos tecnologicos, mediante la identificación, análisis, valoración de riesgos y el establecimiento de acciones de tratamiento dirigidos a prevenir la ocurrencia o minimizar el impacto de los riesgos de seguridad y privacidad de la información.

3. ALCANCE

El plan de tratamiento de riesgos de seguridad de la información será aplicado en la SDMUJER de acuerdo con los lineamientos y metodología de identificación, calificación, seguimiento, monitoreo, y evaluación del riesgo, establecido para el control y mejoramiento continuo. Teniendo en cuenta aspectos como: el manejo de documentos en medio físico, el proceso de almacenaje y recuperación, los sistemas de información con los que cuenta la Entidad, los sistemas externos a los que esté obligada a reportar información, la forma de almacenamiento de los datos digitales y los modelos de respaldo de información.

4. METODOLOGÍA DE GESTIÓN INTEGRADA DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

De acuerdo con el Manual de Gestión del Riesgo del Departamento Administrativo de la Función pública y la Norma ISO 31000, se establecen tres pilares o principios de la Seguridad de la Información: Confencialidad, Integridad y Disponibilidad.

El proceso para la gestión del riesgo debe estar adaptado a los procesos de la Entidad y comprende las siguientes actividades que se presentan en la siguiete ilustración. Proceso para la gestión del riesgo de la norma ISO 31000.

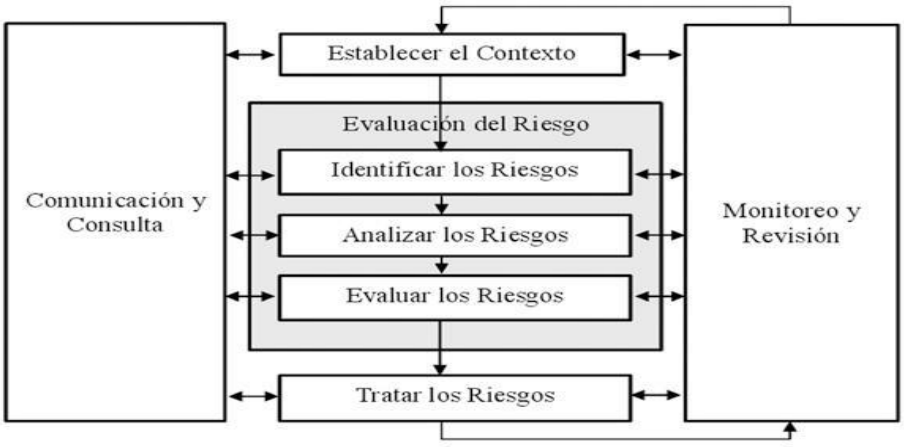

Ilustración I. Proceso para la gestión de riesgos

- **Comunicación y consulta:** Las partes involucradas tanto a nivel interno de la Entidad como externo deben tener una comunicación eficaz durante todas las etapas del proceso de gestión del riesgo y tener definidos los medios de comunicación, con el fin de garantizar que los responsables del proceso y las partes involucradas entiendan las bases sobre las cuales se toman decisiones (Icontec, 2011).

- **Establecer el Contexto** Se procede a identificar las características de los factores internos y externo que influyen sobre la gestión del riesgo, esto se analizará a partir

del uso del método DOFA – Fortalezas, Oportunidades, debilidades y Amenazas. El punto de partida de la identificación de riesgos es realizar una identificación y clasificación de activos de información de los procesos.

- **Valoración del Riesgo:** La definición de este término de acuerdo a la Norma ISO 31000, "valoración del riesgo es el proceso total de la identificación del riesgo, análisis del riesgo y evaluación del riesgo"

- **Identificación de los Riesgos** "El propósito de la identificación del riesgo es la identificación de lo que puede ocurrir o las situaciones que puedan presentarse que afecten el logro de los objetivos del sistema o de la Entidad". Comprende la identificación de las causas, consecuencias, fuentes generadoras de riesgo que puedan afectar el cumplimiento de los objetivos planteados para los procesos.

- **Análisis de los Riesgos** "El análisis de riesgos implica la consideración de las causas y las fuentes de riesgo, sus consecuencias (impacto) y la probabilidad en que estas consecuencias puedan ocurrir"

- **Evaluación de los Riesgos** La Norma ISO 31000 estable que la evaluación de la gestión del riesgo debe realizarse con base en los resultados del análisis de riesgos. La finalidad de la evaluación del riesgo es ayudar a la toma de decisiones, determinando los riesgos a tratar. La evaluación del riesgo es la comparación de los niveles de riesgo estimados con los criterios de evaluación y los criterios de aceptación del riesgo.

- **Tratamiento de Riesgos:** "El tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica" (Icontec, 2011).

- **Monitoreo y Revisión:** Como parte del proceso de gestión del riesgo, los riesgos y los controles deberían ser monitoreados y revisados regularmente para comprobar que:

    - La hipótesis acerca de los riesgos sigue siendo válidas
    - La hipótesis en la que está basada la valoración del riesgo, incluyendo el contexto interior y exterior, siguen siendo válidas.
    - Se van cumpliendo los resultados esperados

- La técnica de valoración del riesgo se aplica correctamente
- Los tratamientos del riesgo son efectivos

5. IDENTIFICACIÓN Y CLASIFICACIÓN DE UN RIESGO DE SEGURIDAD DIGITAL

Seguido de este plan de tratamiento de los riesgos de seguridad de la información, la Sdmujer desarrollará una guia metodologica que contemple los lineamientos de Función Pública, donde establecera los moderadores, lideres y liderezas del proceso, estableciendo a la Oficina Asesora de Planeación como moderardor metodologico para los ejerciciso de identificación analisis y seguimiento de los riesgos con el apoyo del aréa de tecnologia para los riesgos realcionados con seguridad de la información; definiendo así, los responsables de la aplicación adecuada y oportuna del presente plan de tratamiento.

RESPONSABLE DE SEGURIDAD DIGITAL
Definir el procedimiento para la Identificación y Valoración de Activos.
Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Este documento apoya al lider y responsable de la información o delegado para la etapa de identificación y clasificación del riesgo cuando se trata de un “Riesgo Seguridad Digital”, alineado con el Instructivo para la Gestión del Riesgo (E-IN-005) – Pasos 4 y 5, en donde es necesario tener en cuenta que estos riesgos serán tratados en sus etapas iniciales y finales de acuerdo al mencionado instructivo y para los activos de información que en el Registro de Activos de Información de la SDP (RAI) (A-LE- 283) hayan sido clasificados como de criticidad “Alta” por sus responsables, según la valoración dada a su confidencialidad, integridad y disponibilidad, razón por la cual se consideraría que existe un riesgo de la información en alguno de éstos tres pilares.

5.1 Definición de recursos para la Gestión de riesgos de seguridad digital

La entidad pública debe disponer de los recursos suficientes para el desarrollo de la gestión de riesgos de seguridad digital, (capital, tiempo, personal, procesos, sistemas y tecnologías), con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos de seguridad digital.

La línea estratégica o alta dirección debe asignar entre otros, recursos tales como:

- Personal capacitado e idóneo para la gestión del riesgo de seguridad digital.
- Recursos económicos para la implementación de controles de mitigación de riesgos
- Recursos para los aspectos de mejora continua, monitoreo y auditorías.

5.2 Identificación de activos de seguridad digital

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.

Es necesario que la entidad pública identifique los activos y documente un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (FrontOffice), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado.

La identificación y activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública.

La siguiente tabla presenta una propuesta de tipología de activos con el fin de hacer la clasificación mencionada.

Tipo de activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Ilustración II. Clasificación de Activos

5.3 Criticidad de los Activos

La criticidad de los activos de información fue valorada de acuerdo a la Guía para la Gestión y Clasificación de Activos de Información de Min TIC, referenciada en el Anexo 4 para Riesgos de Seguridad Digital, midiéndose por los tres pilares de la seguridad de la información “CONFIDENCIALIDAD”, “INTEGRIDAD”, “DISPONIBILIDAD” de la siguiente manera:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Ilustración III. Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información

Tras la valoración del activo de información por cada uno de los tres pilares en el Formato Registro De Activos De Información (RAI) (A-FO-209) se clasifica el Activo en el nivel de criticidad “ALTA”, “MEDIA” ó “BAJA”), de acuerdo a las condiciones de la Guía para la Gestión y Clasificación de Activos de Información de MinTIC de la siguiente manera:

El resultado de esta valoración se refleja finalmente en el documento SIG Registro de Activos de Información (RAI) (A-LE-283), a partir del cual se seleccionan para tratamiento de riesgos, todos los activos de información clasificados con nivel de criticidad “ALTA”

De acuerdo con lo lineamientos para la Gestión del Riesgo de seguridad digital en las Entidades Públicas, se deberá especificar la amenaza de acuerdo a la siguiente tabla de referencia:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Ilustración IV. Niveles de Clasificacion de la Información

5.4 Identificar y analizar los riesgos inherentes de seguridad digital

Para el tratamiento de riesgos se seleccionan todos los activos de información clasificados con nivel de criticidad "ALTA y se debe especificar la amenaza de acuerdo a la siguiente tabla de referencia:

Tipo	Amenaza
Daño físico	Fuego
	Agua
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua
	Fallas en el suministro de aire acondicionado
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida
	Espionaje remoto
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
Compromiso de las funciones	Error en el uso o abuso de derechos
	Falsificación de derechos

Fuente: ISO/IEC 27005:2009

Ilustración V. Tipos de riesgo y Amenazas

Tras el registro de una amenaza, se deberán especificar las vulnerabilidades, de acuerdo a la siguiente tabla de referencia:

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalacione
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas con uso aceptable de activos, control de cambios, valoración de riesgos, escritorio pantalla limpia entre otros)

Ilustración VI. Vulnerabilidades

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.

A continuación, se presentan ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Ilustración VII. Amenazas y Vulnerabilidades

Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la SDMUJER debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.

Adicionalmente, se debe identificar el responsable del riesgo, es decir, “quien tiene que rendir cuentas sobre el riesgo o quien tiene la autoridad para gestionar el riesgo” .

La identificación de riesgos, amenazas y vulnerabilidades puede ser realizada a través de diferentes metodologías. Como ejemplo, se citan las siguientes:

- Lluvia de ideas: Mediante esta opción se busca animar a los participantes a que indiquen qué situaciones adversas asociadas al manejo de la información digital y los activos de información se pueden presentar o casos ocurridos que los participantes conozcan que se hayan dado en la SDMUJER o en el sector. Deben existir un orden de la sesión, un líder y personas que ayuden con la captura de las memorias.

- Juicio de expertos: A través de este esquema se reúnen las personas con mayor conocimiento sobre la materia de análisis e indican cuáles aspectos negativos o riesgos de seguridad digital se pueden presentar. Para emplear esta técnica, se requiere disponer de una agenda con un orden de temas, establecer reglas claras y contar con la participación de un orientador o moderador, así como personas que tomen notas de los principales conceptos expuestos. Al finalizar, se retoman los principales riesgos identificados y se procede a hacer una valoración

- Análisis de escenarios: en este esquema también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que pueden llegar a presentarse: explosión de un pozo, sobrecarga de un nodo, pérdida de control de una unidad operada remotamente; y con base en estas posibilidades, se determina qué puede llegar a suceder, desde la perspectiva digital, a los activos de información y las consecuencias de la afectación.

- Otras técnicas que pueden ser empleadas son: entrevistas estructuradas, encuestas o listas de chequeo.

Posterior a la identificación de los riesgos de seguridad digital con sus respectivas amenazas y vulnerabilidades enunciadas en este documento, se deberá continuar con el Paso 3. Valoración del Riesgo, de la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" del DAFP.

5.5 Identificación y evaluación de los controles existentes

Como lo indica la Guía de DAFP, arriba mencionada, una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes para evitar trabajo o costos innecesarios.

Nota: Para determinar si existen uno o varios controles asociados a los riesgos inherentes identificados se puede consultar el Anexo A de la Norma ISO/IEC 27001:2013 como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad digital que están enunciados en dicho anexo.

5.6 Tratamiento de los riesgos de seguridad digital

Una vez se han identificado los riesgos, la SDMUJER debe definir el tratamiento para cada uno de los riesgos analizados y evaluados. Este es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, puede tener en cuenta las opciones

planteadas en la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" del DAFP:

- **Evitar**
- **Aceptar**
- **Compartir**
- **Mitigar el riesgo**

5.7 Monitoreo y revisión

La SDMUJER debe hacer un 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: una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la SDMUJER debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, 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 de los controles propuestos, de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad pública. Así mismo, también deberán tenerse en cuenta los incidentes de seguridad digital que hayan afectado a la entidad y también las métricas o indicadores definidos para hacer seguimiento a 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 Institucional de Coordinación de Control Interno) y las partes interesadas.

6. SEGUIMIENTO Y CONTROL

El seguimiento y monitoreo a la ejecución de las actividades establecidas para el planes/proyectos del Plan de Tratamiento de Riesgos Seguridad y Privacidad de la Información, se realizará a través del MIPG, se determinará la periodicidad en Cronograma de Seguimiento a los Planes definidos en el Decreto 612 de 2018.

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN	RESPONSABLE
1	20/01/2021	Aprobación del Plan Tratamiento de riesgos de Seguridad y Privacidad de la Información	María Carolina Ardila Garzón Oficina Asesora de Planeación