TABLA DE CONTENIDO

1. INTRODUCCION.

Teniendo en cuenta que un Riesgo es la probabilidad de que se produzca un evento, cuyas consecuencias negativas impiden el normal desarrollo de los procesos y actividades que terminan afectando el objetivo misional de la entidad, se hace necesario establecer una metodología adecuada que permita identificar, evaluar, tratar y hacer seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos de la información de la entidad.
En este documento se describe la metodología de gestión del riesgo, tomando como base los lineamientos de MinTIC y guía de tratamiento de riesgos emitida por el DAFP.

2. OBJETIVO.

Gestionar de manera oportuna el riesgo bajo una metodología acorde a la normatividad vigente, los lineamientos emitidos por las entidades del orden nacional que apliquen para las entidades de naturaleza pública.
Todo esto con el objetivo de lograr minimizar la materialización de riesgos que afecten el cumplimiento de los objetivos misionales de la entidad.

3. ALCANCE.

La Metodología para Identificar evaluar, tratar y hacer seguimiento a los riesgos de seguridad de la información, es de aplicabilidad en todos los procesos de la entidad.

4. DEFINICIONES.

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).

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.

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

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.

Control: Medida que permite reducir o mitigar un riesgo.

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.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

Integridad: Propiedad de exactitud y completitud.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Activo de información: Cualquier cosa que genere valor para la entidad.
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.

5. NORMATIVIDAD.

- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 DAFP.
- Ley 1581 de 2012, Protección de datos personales
- Ley 1712 de 2014, Ley de Transparencia y del derecho de acceso a la información pública Nacional
- Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Decreto 1499 de 2017, Por medio del cual se modifica el Decreto *1083* de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- ISO/IEC 27005:2009, Gestión de riesgos de seguridad de información.

6. ROLES Y RESPONSABILIDADES.

Los roles y responsabilidades definidos en torno a la identificación, evaluación, tratamiento y seguimiento a los riesgos de seguridad de la información, se encuentra a cargo de la Secretaría TIC, quien se encargará del registro de información en la matriz su actualización y la gestión de los riesgos identificados.

7. METODOLOGÍA PARA LA IDENTIFICACIÓN DE RIESGOS, AMENAZAS Y VULNERABILIDADES

La metodología empleada será la de “Análisis de escenarios”, en donde el personal de la secretaría TIC determina situaciones potenciales que han sucedido o pueden llegar a presentarse, 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.
Lo anterior utilizando las guías e instrumentos dispuestos por el DAFP Y la norma ISO/IEC 27005:2009 Gestión de riesgos de seguridad de información.

7.1. DEFINICIÓN DE LA MATRIZ DE IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:

Con base a la normatividad aplicable, se elabora la matriz que contendrá los riesgos de seguridad y privacidad de la información de la entidad, que contiene la siguiente información que se deberá registrar para cada uno de los riesgos identificados:

A. Activo de la Información: Tipo de activos sobre los cuales se hace la identificación de riesgos. No se definirán riesgos por activo, teniendo en cuenta que pueden generarse un sinnúmero de Riesgos, lo que haría que la gestión y seguimiento se conviertan en algo muy complejo para la entidad. Se agruparán por tipos de activos de iguales características y nivel criticidad.

B. Identificación del Riesgo:

- **No.:** Número único que identifica el riesgo.
- **Descripción del riesgo**: Descripción detalla del riesgo identificado.
- **Riesgo u Oportunidad**: Riesgo que puede ser negativo o positivo, en el caso de ser positivo, tenderemos a interpretarlo como una oportunidad, ya que nos facilitará el camino para obtener un resultado satisfactorio.

- **Posibles causas:** Describir la(s) posible(s) causa(s) que generan el riesgo.
- **Clasificación del riesgo**: Muestra las clases de riesgos que se pueden presentar.

CLASIFICACIÓN DEL RIESGO	
Estratégicos	Son aquellos que se asocian con toda posibilidad de que suceda algo relacionado con el cumplimiento de los objetivos estratégicos y la misión institucional, la sostenibilidad y subsistencia de la entidad en el corto, mediano y largo plazo.
Imagen	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la entidad, tiene que ver con conocimiento de prácticas corruptas, manejo desacertado de los medios de comunicación, insatisfacción ciudadana por el mal servicio, incumplimiento de planes, programas y proyectos.
Operativo	Son aquellos relacionados con la parte operativa y técnica de la entidad que provienen de la operación cotidiana y específica de cada proceso. Dentro de ellos se pueden encontrar deficiencias en los flujos de información y comunicación, cifras, así como desarticulación entre procesos, debilidades en infraestructura, dotación y talento humano, lo cual conduce a ineficiencias, corrupción e incumplimiento de los objetivos institucionales.
Financiero	Son los relacionados con la Gestión Financiera de la entidad, los cuales pueden estar relacionados con transferencias, ejecución presupuestal, pagos, tesorería, ineficiencias en el manejo de bienes, pérdidas económicas.
Cumplimiento	Son todos los relacionados con la capacidad de la entidad para cumplir con los requisitos, acá están inmersos los requisitos regulativos, legales, contractuales, políticas internas, solicitudes de información, ética, calidad, entre otros.
Tecnología	Son los relacionados con la capacidad de la entidad, para que la tecnología disponible y proyectada satisfaga las necesidades actuales, futuras y de soporte de la entidad. Esto tiene que ver con Software (compatibilidad, configuración), Hardware (capacidades, desempeños, obsolescencia), Sistemas (Diseños, especificidades, complejidad)
Conocimiento	Son aquellos que se relacionan con el daño generado por la pérdida de conocimiento e información vital para el desarrollo de las actividades de la entidad. En esta clasificación se encuentran los riesgos en los activos y la seguridad de la información.
Ambientales y de Seguridad y Salud En El Trabajo	Son aquellos generados por la exposición a factores internos y externos que afectan el medio ambiente de la entidad (la contaminación, ambientes poco saludables, malos hábitos) inherentes a las actividades que desarrolla en cada proceso.

- **Origen del riesgo:** son los factores internos y externos que puedan afectar a la organización

Externo: son todos aquellos que provienen del entorno de la Entidad y que influyen o condicionan su operativa pudiendo convertirse en amenazas para su desarrollo, ej.: riesgo del país, localización, fuerza mayor.

Interno: son todos aquellos que dependen de la gestión dentro de la Entidad y de las distintas dependencias que la componen, ej. Instalaciones obsoletas, falta de liquidez.

- **Posibles Consecuencias:** todas las posibles consecuencias que genera el riesgo si se llega a materializar.

C. Valoración del riesgo de seguridad y privacidad de la información:

Para la valoración del riesgo es necesario establecer los criterios para el análisis de probabilidad e impacto del riesgo identificado y su respectivo nivel de severidad.

- **Probabilidad:**

Esta se entiende como la posibilidad de ocurrencia del riesgo y se mide teniendo en cuenta la frecuencia con la que el evento se ha presentado a través del tiempo en la entidad y su nivel va de 1 a 5.

Teniendo en cuenta lo anterior se determinan los criterios para definir el nivel de probabilidad:

TABLA DE PROBABILIDAD			
NIVEL	DESCRIPTOR	DESCRIPCIÓN (FACTIBILIDAD)	FRECUENCIA
1	RARO	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años.
2	IMPROBABLE	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
3	POSIBLE	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
4	PROBABLE	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
5	CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

- **Impacto:**

El impacto se mide de acuerdo al grado de afectación hacia la entidad que puede tener la materialización del riesgo.

Teniendo en cuenta lo anterior se determinan los criterios para definir el nivel de impacto.

TABLA DE IMPACTO			
TIPO	NIVEL	DESCRIPTOR	DESCRIPCIÓN En caso que el riesgo se materialice el impacto u afectación sería.....
CONFIDENCIALIDAD EN LA INFORMACIÓN	1	INSIGNIFICANTE	Se afecta a una persona en particular.
	2	MENOR	Se afecta a un grupo de trabajo interno del proceso.
	3	MODERADO	Se afecta a todo el proceso.
	4	MAYOR	La afectación se da a nivel Organizacional
	5	CATASTRÓFICO	La afectación se da a nivel estratégico.
CREDIBILIDAD O IMAGEN	1	INSIGNIFICANTE	Se afecta al grupo de funcionarios y contratistas del proceso.
	2	MENOR	Se afecta a todos los funcionarios y contratistas de la entidad.
	3	MODERADO	Se afecta a los usuarios de la Sede Central de la entidad.
	4	MAYOR	Se afecta a los usuarios de las Direcciones Territoriales.
	5	CATASTRÓFICO	Se afecta a los usuarios de la empresa
LEGAL	1	INSIGNIFICANTE	Se producen multas para la entidad.
	2	MENOR	Se producen demandas para la entidad.
	3	MODERADO	Se producen investigaciones disciplinarias.
	4	MAYOR	Se producen investigaciones fiscales.
	5	CATASTRÓFICO	Se producen intervenciones y o sanciones para la entidad.
OPERATIVO	1	INSIGNIFICANTE	Se tendrían que realizar ajustes a una actividad concreta del proceso.
	2	MENOR	Se tendrían que realizar ajustes en los procedimientos del proceso.
	3	MODERADO	Se tendrían que realizar ajustes en la interacción de procesos.
	4	MAYOR	Se presentarían intermitencias o dificultades en la operación del proceso
	5	CATASTRÓFICO	Se presentaría paro o no en la operación del proceso.

- **Valoración del riesgo:**

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se determina la zona de riesgo.

Para esto se definen 4 zonas de severidad en la matriz de calor

VALORACIÓN DEL RIESGO	Min	Max
RIESGO BAJO	1	4
RIESGO MEDIO	5	9
RIESGO ALTO	10	15
RIESGO MUY ALTO	16	25

Quedando la matriz de calor de la siguiente manera

VALORACIÓN DEL RIESGO					
	IMPACTO				
PROBABILIDAD	INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
RARO (1)	1	2	3	4	5
IMPROBABLE (2)	2	4	6	8	10
POSIBLE (3)	3	6	9	12	16
PROBABLE (4)	4	8	12	16	20
CASI SEGURO (5)	5	10	16	20	25

D. Identificación de controles existentes: un control se define como la medida que permite reducir el riesgo.

Una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes, los cuales se deben identificar por cada riesgo.

Una vez identificado el control se debe determinar el tipo de control y como se ejecuta.

Tipo de Control:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. estos controles tienen costos implícitos.

Modo de ejecución:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

Evaluación de los controles: para evaluar los controles se deben tener en cuenta los atributos de eficiencia y los informativos.

Cabe aclarar que los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Los controles Correctivos atacan el Impacto y los controles Preventivos y Detectivos atacan la probabilidad.

Para evaluar los controles se toma como base la tabla suministrada por el Dafp la cual asigna un peso a cada tipo de control con base a sus atributos.

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 permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento 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%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

E. Riesgo Residual: es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Formula:
Resultado Probabilidad * Peso Control preventivo= Vr. resultante luego de aplicación 1er control
Resultado Probabilidad – Resultado Probabilidad = Valor probabilidad para aplicar 2o control

Valor probabilidad para aplicar 2o control * Valoración control 2 detectivo = Vr. Resultante luego de aplicar 2o control
Valor probabilidad para aplicar 2o control – resultado luego de aplicar 2º control = riesgo residual

Ejemplo:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual	25,2 %			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente.

F. TRATAMIENTO:

Con base al nivel de Severidad del riesgo se puede tomar la decisión para el tratamiento del riesgo.

TRATAMIENTO DEL RIESGO		
NIVEL DEL RIESGO	**TRATAMIENTO**	**SEGUIMIENTO**
RIESGO BAJO	Aceptar riesgo	Cada 3 meses
RIESGO MEDIO	Mitigar riesgo o Aceptar riesgo (de acuerdo al análsis de este)	Cada 3 meses
RIESGO ALTO	Mitigar, evitar, Transferir o aceptar riesgo	Cada 3 meses
RIESGO MUY ALTO	Evitar, Transferir, Mitigar o aceptar riesgo	Cada mes

- **Evitar el Riesgo:** si los riesgos son muy altos o los costos de los controles superan los beneficios, la decisión es evitar el riesgo mediante el retiro de la actividad o cambiando sus condiciones.
- **Mitigar o Reducir el Riesgo:** Tener en cuenta costos, tiempos de implementación de controles, aspectos técnicos y el retorno de inversión con respecto a la reducción del riesgo. Si se decide **reducir el riesgo** mediante la selección de controles que permitan disminuir la probabilidad o el impacto del riesgo, se deberá tener en cuenta los controles basados en la norma ISO/IEC 27001:2013 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad de la información, sin embargo, se puede implementar nuevos controles de seguridad que no estén incluidos dentro del Anexo, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

- **Aceptación o retención del Riesgo:** analizar:
  - La materialización del riesgo es menos costosa que la implementación de controles
  - El nivel del riesgo satisface los criterios para su aceptación
  - No es necesario implementar controles

- **Transferir el Riesgo:** Al transferir el riesgo a un tercero le damos la responsabilidad para su administración, pero hay que tener en cuenta que el impacto si se materializa el riesgo se atribuirá a fallas en la organización por parte de los afectados.

  La Transferencia se hará por medio de: Seguros, Garantías y Contratos

G. Plan de Tratamiento de Riesgos

- **Acciones o Tareas:** describir planes de acción, actividades o tareas propuestos para evitar, reducir, transferir, asumir o compartir los riesgos.

- **Control del anexo A y de la norma ISO 27001:** identificar qué control de la norma se debe aplicar para el tratamiento del riesgo.

H. Responsable: es quien tiene que responder sobre el riesgo o quien tiene la autoridad para gestionar el riesgo.

I. Seguimiento al riesgo

- **Trimestral:** Para los riesgos Bajo, Medio y Alto se hace seguimiento al riesgo trimestralmente.

- **Mensual:** Para los riesgos Muy Altos se hace seguimiento al riesgo Mensualmente

- **Indicadores**: se deben generar indicadores para medir la gestión realizada en cuanto a la eficacia y la efectividad de los planes de tratamiento implementados.

  - **Indicador de eficacia:** que indique el cumplimiento de las actividades para la gestión del riesgo

  - **Indicador de efectividad**: para cada riesgo o la suma de todos los riesgos de seguridad (pérdida de confidencialidad, de integridad, de disponibilidad).

7.2. IDENTIFICACIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORAMACIÓN:

Para dar inicio con la identificación de riesgos, se conforma desde la Secretaría TIC un equipo que se encargará de identificar los riesgos con los propietarios y custodios de la información identificados en la matriz de activos de la información de la entidad, registrando la información en la matriz generada con los campos mencionados en el punto 7.1.

Con base a la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas” emitida por el DAFP Versión 6., para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad y privacidad de la información:

• Pérdida de la confidencialidad
• Pérdida de la integridad

• Pérdida de la disponibilidad

Con el fin de facilitar la identificación de vulnerabilidades y amenazas la Norma ISO 27005, gestión de riesgos de seguridad de información nos presenta los posibles escenarios de riesgo, facilitándonos listados ejemplo donde podemos encontrar las Amenazas, Vulnerabilidades y su relación.

7.2.1 Identificación de Amenazas:

Amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos:

• Deliberadas (D), fortuitas (F) o ambientales (A).

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F

Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Fuente: ISO/IEC27005:2009

- Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	• Reto • Ego • Rebelión • Estatus • Dinero	• Piratería • 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,	• Curiosidad • Ego • Inteligencia • Ganancia monetaria	• Asalto a un empleado • Chantaje

negligentes, deshonestos o despedidos)	• Venganza • Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• 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: ISO/IEC27005:2009

7.2.2. Identificación de vulnerabilidades:

Se puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

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 instalaciones
	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 como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: ISO/IEC27005:2009

7.2.3 Relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas:

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.

TIPOS	VULNERABILIDADES	AMENAZAS QUE EXPLOTAN LAS VULNERABILIDADES
Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del servidor y equipos de computo
	Instalación fallida de los medios de almacenamiento	Error en el uso
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo. Corrosión, congelamiento
	Ausencia de un eficiente control de cambios	Error en el uso

	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Almacenamiento sin protección	Hurto de medios
	Falta de cuidado en la disposición final	Hurto de medios
	Copia no controlada	Hurto de medios
Software	Ausencia o insuficiencia de pruebas de software	Abuso de derechos
	Defectos bien conocidos en el software	Abuso de derechos
	Ausencia de Terminación de la sesión cuando se abandona la estación de trabajo	Abuso de derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de derechos
	Ausencia de auditoría	Abuso de derechos
	Asignación errada de los derechos de acceso	Abuso de derechos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Ausencia de identificación y autenticación de emisor y receptor	Falsificación de derechos

	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia de personal	Incumplimiento en la disponibilidad del personal
	procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios, Destrucción o daño de equipos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipos o medios
	Red energética inestable	Pérdida del suministro de energía
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de derechos
	Ausencia de disposiciones con respecto a la seguridad de la información en los contratos con los clientes y/o terceras partes	Abuso de derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia en los mismos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información

	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registro en las bitácoras (logs) de administrador y operador	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia en las disposiciones con respecto a la seguridad de la información en los contratos con los empleados	Procesamiento ilegal de datos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información.	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de políticas sobre limpieza de escritorio y pantalla limpia	Hurto de medios
	ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado

Fuente: ISO/IEC27005:2009

7.2.4 Identificación del riesgo inherente de seguridad de la información:

Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales se deben identificar, valorar y posteriormente tratar, dependiendo del nivel del riesgo.

7.2.5 Identificación del dueño del riesgo:

El dueño del riesgo es quien tiene que responder sobre el riesgo o quien tiene la autoridad para gestionar el riesgo.

7.3. VALORACIÓN DEL RIESGO:

Para la valoración del riesgo es necesario establecer los criterios para el análisis de probabilidad e impacto del riesgo identificado y su respectivo nivel de severidad.

7.3.1. Análisis de riesgos: en este punto se establece la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

7.3.2 Determinar la probabilidad: esta se entiende como la posibilidad de ocurrencia del riesgo.

Para determinar la probabilidad de ocurrencia se asocia la exposición al riesgo del proceso sobre el cual 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.

Como referente, se toma la tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
*Tecnología (incluye disponibilidad de aplicativos), ***Nota:** En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez.	Diaria	Muy alta

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Con base a la tabla anterior se determinan los criterios para definir el nivel de probabilidad.

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

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

7.3.3 Determinar el impacto: Para definir el impacto se tienen en cuenta las variables económicas (afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal) y reputacionales (afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio,

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

Teniendo en cuenta lo anterior se determinan los criterios para definir el nivel de impacto.

Nivel	Afectación Económica	Afectación Reputacional
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
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.
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.
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

7.3.4. Evaluación de riesgos: a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se determina la zona de riesgo inicial (Riesgo Inherente).

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

Para esto se definen 4 zonas de severidad en la matriz de calor

BAJO	MODERADO	ALTO	EXTREMO

Quedando la matriz de calor de la siguiente manera

PROBABILIDAD	IMPACTO				
	Leve	Menor	Moderado	Mayor	Catastrófico
Muy Baja	Bajo	Bajo	Moderado	Alto	Extremo
Baja	Bajo	Moderado	Moderado	Alto	Extremo

Media	Moderado	Moderado	Moderado	Alto	Extremo
Alta	Moderado	Moderado	Alto	Alto	Extremo
Muy Alta	Alto	Alto	Alto	Alto	Extremo

7.3.5 Identificación de controles existentes: un control se define como la medida que permite reducir el riesgo.

Una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes, los cuales se deben identificar por cada riesgo.

Una vez identificado el control se debe determinar el tipo de control y como se ejecuta.

Tipo de Control:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. estos controles tienen costos implícitos.

Modo de ejecución:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

7.3.6 Evaluación de los controles: para evaluar los controles se deben tener en cuenta los atributos de eficiencia y los informativos.

Cabe aclarar que los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Los controles Correctivos atacan el Impacto y los controles Preventivos y Detectivos atacan la probabilidad.

Para evaluar los controles se toma como base la tabla suministrada por el Dafp la cual asigna un peso a cada tipo de control con base a sus atributos.

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 permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento 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.	-
		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.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

7.3.7 Riesgo residual: es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Formula:

Resultado Probabilidad * Peso Control preventivo= Vr. resultante luego de aplicación 1er control
Resultado Probabilidad – Resultado Probabilidad = Valor probabilidad para aplicar 2o control

Valor probabilidad para aplicar 2o control * Valoración control 2 detectivo = Vr. Resultante luego de aplicar 2o control
Valor probabilidad para aplicar 2o control – resultado luego de aplicar 2º control = riesgo residual

Ejemplo:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual	25,2 %			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente.

7.4. TRATAMIENTO DEL RIESGO:

Con base al nivel de Severidad del riesgo se puede tomar la decisión para el tratamiento del riesgo.

BAJO	Aceptar riesgo
MODERADO	Mitigar riesgo o Aceptar riesgo (de acuerdo al análisis de éste)
ALTO	Mitigar, evitar, Transferir o aceptar riesgo
EXTREMO	Evitar, Transferir, Mitigar o aceptar riesgo

- **Evitar el Riesgo:** si los riesgos son muy altos o los costos de los controles superan los beneficios, la decisión es evitar el riesgo mediante el retiro de la actividad o cambiando sus condiciones.

- **Mitigar o Reducir el Riesgo:** Tener en cuenta costos, tiempos de implementación de controles, aspectos técnicos y el retorno de inversión con respecto a la reducción del

riesgo. Si se decide **reducir el riesgo** mediante la selección de controles que permitan disminuir la probabilidad o el impacto del riesgo, se deberá tener en cuenta los**. CONTROLES** basados en la norma ISO/IEC 27001:2013 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad de la información, sin embargo, se puede implementar nuevos controles de seguridad que no estén incluidos dentro del Anexo, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

- **Aceptación o retención del Riesgo:** analizar:
  - La materialización del riesgo es menos costosa que la implementación de controles
  - El nivel del riesgo satisface los criterios para su aceptación
  - No es necesario implementar controles

- **Transferir el Riesgo:** Al transferir el riesgo a un tercero le damos la responsabilidad para su administración, pero hay que tener en cuenta que el impacto si se materializa el riesgo se atribuirá a fallas en la organización por parte de los afectados.

  La Transferencia se hará por medio de: Seguros, Garantías y Contratos

7.5. PLAN DE TRATAMIENTO DE RIESGOS E INDICADORES PARA SU GESTIÓN:

Se debe definir las actividades a ejecutar para tratar los riesgos y cada trimestre registrar el avance de cumplimiento, complementariamente a esto se deben definir como mínimo 2 indicadores por proceso de la siguiente manera:

- 1 indicador de eficacia que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad de la información en cada PROCESO de la entidad.

- 1 indicador de efectividad para cada riesgo o la suma de todos los riesgos de seguridad de la información (pérdida de confidencialidad, de integridad, de disponibilidad).

8. BIBLIOGRAFIA

“Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas” emitida por el DAFP.
Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas.

9. DOCUMENTOS Y REGISTROS RELACIONADOS.

N/A.

10. ANEXOS.

N/A.

11. CONTROL DE CAMBIOS.

Versión	Fecha de versión	Descripción del cambio	Responsable
01	23/08/2023	Creación del Documento	Secretario TIC, Innovación y Gobierno Abierto

12. RESPONSABLE.

El responsable de este documento es el Secretario TIC, Innovación y Gobierno Abierto, quien debe revisarlo, y si es necesario actualizarlo.

13. REVISIÓN, VALIDACIÓN Y APROBACIÓN.

Revisión:	Aprobación:	Verificación:
Nombre: Raúl Alejandro Ortiz Navarro	Nombre: Comité Institucional de Gestión y Desempeño	Nombre: Nixon Ortega Bravo
Cargo: Secretario TIC, Innovación y Gobierno Abierto	Cargo: Comité Institucional de Gestión y Desempeño	Cargo: Profesional Universitario 219 grado 04