EMPRESA SOCIAL DEL ESTADO

PASTO SALUD E.S.E

NIT.900091143-9

GUIA PARA LA ADMINISTRACION DEL RIESGO PARA LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VERSIÓN 6.0

SAN JUAN DE PASTO
2021

GUIA PARA LA ADMINISTRACION DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
PASTO SALUD E.S.E.

ELABORÓ

WILLIAM MONTENEGRO GUEVARA
PROFESIONAL UNIVERSITARIO, OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS

SAN JUAN DE PASTO
2021

TABLA DE CONTENIDO

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9

SOLICITUD DE CREACIÓN, MODIFICACION Ó ELIMINACION DE DOCUMENTOS Y REGISTROS

VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
7.0	GESTION DE SISTEMAS DE INFORMACION	GSI-MDR	225

PROCESO: GESTION DE SISTEMAS DE INFORMACION

TIPO DE DOCUMENTO	MANUAL	PLAN	PROCEDIMIENTO	INSTRUCTIVO	GUIA	PROTOCOLO	ESQUEMA	FORMATO	OTRO
					X				

NOMBRE DEL DOCUMENTO: METODOLOGIA GESTION DEL RIESGO PARA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION — **CODIGO**

FECHA: 27/07/2021

CREACIÓN	X	MODIFICACIÓN		ELIMINACIÓN	

CAUSAS DE (Creación, Modificación o eliminación): Creación de la guía metodológica para la gestión del riesgo de seguridad y privacidad de la información. Como recomendación realizada por la guía de gestión del riesgo de seguridad de la información del MINITIC y la guia de las Dirección y Gestión de Desempeño Institucional

DESCRIPCION DE LAS MEJORAS

SECCIÓN MODIFICADA AL DOCUMENTO

	NOMBRE Y CARGO DE QUIEN ELABORÓ	NOMBRE Y CARGO DE QUIEN REVISÓ (Líder de proceso o jefe inmediato de acuerdo a la estructura organizacional de la empresa)	ACEPTADO	SI	X	NO
	WILLIAM MONTENEGRO GUEVARA PROFESIONAL UNIVERSITARIO OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS	HARVEY VALLEJO NARVAEZ JEFE OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS	GERENTE			
FIRMA		FIRMA	ANA BELEN ARTEAGA TORRES			

EL PRESENTE FORMATO ES IDENTICO AL ORIGINAL APROBADO. LAS MODIFICACIONES AL FORMATO NO SON VÁLIDAS SIN APROBACIÓN (FIRMAS EN FORMATO ORIGINAL). OFICINA ASESORA DE PLANEACION FECHA DE CREACION Y/O ACTUALIZACION: 25-06-2020

VIGILADO Supersalud

CONTROL DE CAMBIOS

E: Elaboración del documento
M: Modificación del documento
X: Eliminación del documento

Versión	CONTROL DE CAMBIOS	INFORMACIÓN DE CAMBIOS					Acto Administrativo de Adopción
		E	M	X	Actividades o Justificación del cambio	Elaboró / Actualizó	
6.0	Elaboración del documento guía para la administración del riesgo de seguridad de la información.	X			**Justificación** Dar cumplimiento a los lineamientos técnicos para la gestión del riesgo emitidos por el departamento de la función pública y el marco del modelo de seguridad y privacidad de la información del ministerio de las TICS.	William Montenegro Guevara. Profesional Universitario Asesora de Comunicaciones y Sistemas	Formato 225 de creación, modificación o eliminación de documentos y registros del 27de julio de 2021

INTRODUCCIÓN

Pasto Salud E.S.E genera en el día a día información en todas sus sedes la cual es importante para el correcto desempeño y cumplimiento de los objetivos organizacionales en cada uno de los procesos, de esta manera la seguridad y privacidad de la información se convierten en un factor esencial que asociados a los atributos de confidencialidad, Integridad y disponibilidad de la información permiten evitar el mal uso, pérdida y alteración, lo que puede significar cambios en el normal desarrollo en la prestación de servicios de salud. Por lo anterior, dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información –MSPI-, un tema fundamental, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. De esta manera la Empresa Social del Estado Pasto Salud E.S.E adopta la metodología “Guía de Riesgos” del Departamento Administrativo de la Función Púbica e integra los lineamientos para la gestión del riesgo de seguridad digital en entidades públicas y se establece una herramienta metodológica propia para la gestión del riesgo de seguridad de la información. De esta manera la gestión de riesgos se adopta como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo generando resultados que permitan minimizar pérdidas, maximizar rendimientos y cuidar de la seguridad de los grupos de interés.[1]

[1] Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Hospital General de Medellín 2019

1. JUSTIFICACIÓN

Se requiere dar cumplimiento a los lineamientos técnicos para la gestión del riesgo emitidos por el departamento de la función pública y el marco del modelo de seguridad y privacidad de la información del ministerio de las TICS. De tal manera que la metodología implementada sea de fácil aplicación para el responsable y su equipo de trabajo

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer lineamientos para la Implementación de la guía de gestión del riesgo de seguridad de la información fundamentada en la metodología del Departamento Administrativo de la Función Pública y los lineamientos técnicos del Ministerio de las TICS

2.2 OBJETIVOS ESPECÍFICOS

- Revisar la metodología de la administración de la función pública.
- Adoptar los lineamientos técnicos de seguridad de la información del Minitic.
- Adaptar el instrumento para la administración del riesgo de seguridad de la información.

2.3 ALCANCE

La elaboración de esta metodología aplica únicamente para la seguridad de todos los activos de la información que hayan sido priorizados y que forman parte del proceso de Gestión de Sistemas de Información.

3. MARCO LEGAL

- **Ley 1712 de 2014:** Ley de transparencia y de acceso al derecho a la información pública
- **Ley 1581 de 2001:** Ley de la protección de los datos (Habeas data)
- **NTC ISO/IECE 27005:2009:** Catálogo de amenazas y vulnerabilidades
- **Ley 87 de 1993:** Por la cual se establece normas para el ejercicio del control interno en la entidades y organismos del Estado y se dictan otras disposiciones, articulo 2 literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Artículo 2 literal f). Definir y aplicar medidas que se presenten en la organización y que puedan afectar el logro de los objetivos
- **Decreto 2145 de 1999:** Por el cual se dictan normas sobre el sistema Nacional de Control Interno de las entidades y organismos de la administración pública del orden Nacional y Territorial y de dictan otras disposiciones, modificado parcialmente por el Decreto 2593 del 2000.
- **Decreto 1537 de 2001:** Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado. ARTICULO 4. ADMINISTRACION DE RIESGOS. Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas.
- **Decreto 943 de 2014:** Por el cual se actualiza el Modelo Estándar de Control Interno (MECI)
- **Decreto 648 de 2017**: Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentaria Único del Sector de la Función Pública en cuanto al régimen de ingreso, administración de personal, situaciones administrativas y retiro de los empleados públicos.
  Se establecen los Roles de la Oficina de Control Interno: liderazgo estratégico; **enfoque hacia la prevención, evaluación de la gestión del riesgo,** evaluación y seguimiento, relación con entes externos de control.
- **Decreto 1499 de 2017:** Por medio del cual se modifica el Decreto 1083 de 2015, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
  Se establece la actualización del MECI, se efectué a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG, **Dimensión de Control Interno.**
- **Acuerdo No. 22 de 23 diciembre de 2020:** Mediante el cual se aprobó el Plan de Desarrollo Institucional para el periodo 2021-2024. En el cual se incluye la Política de Gestión del Riesgo
- **ISO 9001:2015**: La norma ISO 9001:2015 será el estándar internacional de carácter certificable que regule los sistemas de gestión de la calidad.

4. GLOSARIO

- Activo Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854:2016, pág.56)
- Activo cibernético En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Amenaza Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO 2700:2016).
- Amenaza cibernética Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).
- Análisis del riesgo Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011)
- Ataque cibernético Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia).
- Ciberseguridad Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. (CONPES 3854, pág. 87).
- Control Medida que modifica al riesgo. (NTC ISO 31000:2011), medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- Evaluación del control Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces. (NTC ISO 31000:2011).
- Evaluación del riesgo Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables. (NTC ISO 31000:2011).
- Evitar el riesgo Decisión de no involucrarse o de retirarse de una situación de riesgo. (NTC ISO 31000:2011).
- Frecuencia Medición del número de ocurrencias por unidad de tiempo. (NTC ISO 31000:2011).
- Identificación del riesgo Proceso para encontrar, reconocer y describir el riesgo. (NTC ISO 31000:2011).
- Incidente de seguridad de la información Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016)
- Inventario de activos Sigla en inglés: Assets inventory. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.)

dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos (ISO 27000.ES).

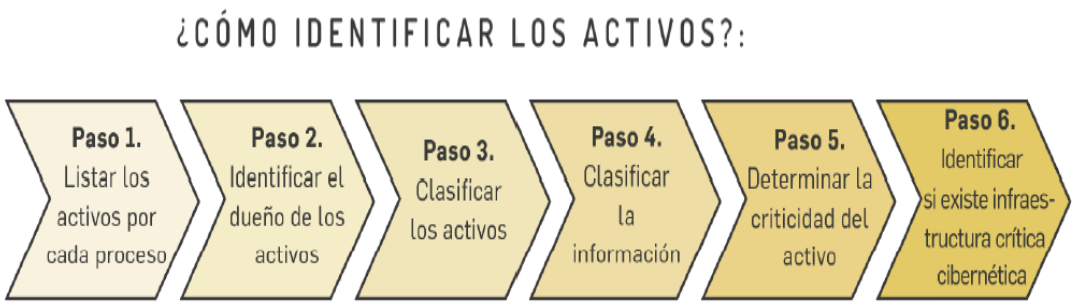
- Nivel de riesgo Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad. (NTC ISO 31000:2011).
- Probabilidad Oportunidad de que algo suceda. (NTC ISO 31000:2011).
- Propietario del riesgo Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. (ISO GUIA 73:2009).
- Riesgo Efecto de la incertidumbre sobre los objetivos. (NTC ISO 31000:2011).
- Riesgo inherente Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. (NTC ISO 31000:2011).
- Riesgo residual Remanente después del tratamiento del riesgo. (NTC ISO 31000:2011). Seguridad de la información Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27001:2016).
- Seguridad digital Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854, pág. 29).
- Tratamiento del riesgo Proceso para modificar el riesgo. (ISO/IEC Guía 73:2009). Valoración del riesgo Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo. (ISO GUÍA 73:2009). 30 vulnerabilidad Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).[2]

[2] Modelo Nacional de Gestión de Riesgos de Seguridad Digital

5. DESARROLLO DE LA METODOLOGIA DE GESTION DEL RIESGO PARA LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1 IDENTIFICAR LOS ACTIVOS DE LA INFORMACIÓN

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

Para esta identificación se tiene en cuenta la matriz de registro de activos de la información, índice de información clasificada y reservada y esquema de publicación de la información, se deben tener en cuenta la ley 1712 de 2014 y la ley 1581 de 2012.

- Paso 1. Se listan los activos, indicando el nombre y descripción breve de cada uno.
- Paso 2. Para cada uno de los activos se identifican el dueño del activo
- Paso 3. Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red, Instalaciones y Talento Humano.
- Paso 4. Se Realiza la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos.
- Paso 5. Valoración del Activo: En este paso se evalúa la criticidad (Alta, Media, Baja) para valorar los activos con respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso. (Tomado de Guía de Gestión de Activos del Modelo de Seguridad y Privacidad de la Información)[3]

Realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación:

3 Guía de Gestión de Activos del Modelo de Seguridad y Privacidad de la Información

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

Tabla 1. Criterios de Clasificación

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.

Tabla 2. Niveles de Clasificación

Fuente: Guía gestión de riesgos de seguridad y privacidad de la información Minitic

5.2 IDENTIFICACIÓN DEL RIESGO

La identificación del riesgo se hace con base en causas identificadas para los procesos dichas causas pueden ser internas o externas. En este momento se establece cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Una vez clasificados se debe tener en cuenta como en estos activos se podría vulnerar alguno de los pilares de la seguridad de la información y para ello se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital

- Perdida de Integridad
- Pérdida de la confidencialidad
- Perdida de disponibilidad de la información[4]

[4] Guía de Gestión de Activos del Modelo de Seguridad y Privacidad de la Información

Para cada riesgo se asocia el grupo de activos de la información y conjuntamente se analiza las posibles amenazas y vulnerabilidades y consecuencias que podrían causar su materialización.

Riesgo	Tipo de activo	Activo	Amenaza	Vulnerabilidad	Consecuencia	Valoración del Activo

Fuente: Adoptado de la metodología de administración del riesgo de la Función Pública

5.3 ANALISIS Y EVALUACION DEL RIESGO

En esta etapa, se deben establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO ABSOLUTO - INHERENTE), en su peor escenario posible, en términos de probabilidad y consecuencia o impacto.

5.3.1 Determinar la probabilidad

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de Frecuencia o Posibilidad.

Posibilidad: Se analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que se dé.

Frecuencia: Se analizan el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.

5.3.2 Criterios de medición de probabilidad

Calificación del riesgo, en la cual se realiza una estimación, de cuál podría ser la probabilidad de ocurrencia del riesgo y el impacto que traería éste, en caso de materializarse.

Tabla 1: Criterios para definir la probabilidad

PROBABILIDAD			
	POSIBILIDAD	**FRECUENCIA DE OCURRENCIA**	**PROBABILIDAD**
Muy Baja	El evento puede ocurrir solo en circunstancias excepcionales (poco	No se ha presentado en los últimos 5 años	20%
Baja	Insignificante posibilidad de que el evento ocurra	Al menos de una vez en los últimos 5 años	40%
Media	Alguna posibilidad de que el evento ocurra	Al menos 1 vez en los últimos 2 años	60%
Alta	Posiblemente ocurra varias veces	Al menos 1 vez en el último año.	80%
Muy Alta	Se espera que el evento ocurra la mayoría de veces	Más de 1 vez al año	100%

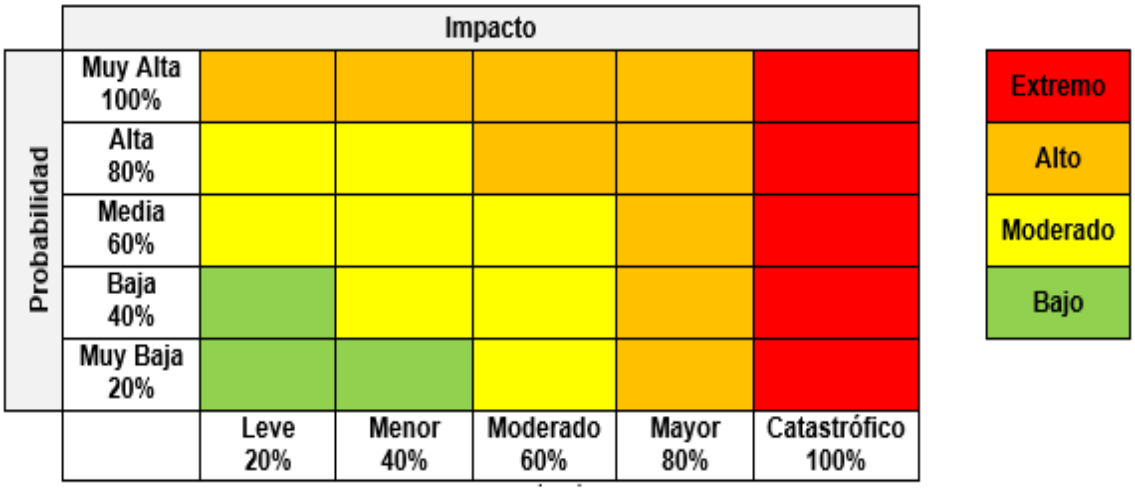
Tabla 2: Criterios para definir el nivel de impacto

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

	IMPACTO
Leve 20%	Si el hecho llegara a presentarse, tendría consecuencias o efectos **mínimos** sobre la entidad.
Menor-40%	Si el hecho llegara a presentarse, tendría **bajo** impacto o efecto sobre la entidad.
Moderado 60%	Si el hecho llegara a presentarse, tendría **medianas** consecuencias o efectos sobre la entidad.
Mayor 80%	Si el hecho llegara a presentarse, tendría **altas** consecuencias o efectos sobre la entidad.
Catastrófico 100%	Si el hecho llegara a presentarse, tendría **desastrosas** consecuencias o efectos sobre la entidad.

Fuente: Adoptado de la metodología de administración del riesgo de la Función Pública

Matriz de Calor niveles de severidad



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas del departamento de la administración pública.

Para la anterior evaluación se debe tener en cuenta las siguientes tablas y matriz de calor.

Descripción del Riesgo	Probabilidad de Ocurrencia (inherente)	Impacto Inherente	Nivel de Riesgo

Fuente: Adoptado de la metodología de administración del riesgo de la Función Pública

5.4 ANÁLISIS Y EVALUACIÓN DE RIESGOS CON CONTROLES

Se busca confrontar los resultados del análisis del riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final. (Riesgo residual).

5.4.1 Valoración de controles:

En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su que hacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

5.4.2 Estructura para la descripción del control:

Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- Responsable de ejecutar el control: Se identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

5.4.3 Tipos de controles y ejecución:

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- 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.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

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

Por cada escenario de riesgo se determinan los controles, se analizan los atributos para el diseño del control, se identifican con el peso asociados a cada uno de ellos, 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.

Controles y sus Características				Peso
Control No:	Tipo	Preventivo		25%
		Detectivo		15%
		Correctivo		10%
	Implementación	Automático		25%
		Manual		15%
	Documentación	Documentado		
		Sin Documentar		
	Frecuencia	Continua		
		Aleatoria		
	Evidencia	Con Registro		
		Sin Registro		

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas del departamento de la administración pública.

5.5 NIVEL DE 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.

Para lo anterior se tiene en cuenta la siguiente tabla.

Nivel de riesgo (riesgo residual)				
Datos relacionados con la probabilidad		**Datos valoración de controles**		**Cálculos requeridos**
Probabilidad inherente				
Valor probabilidad para aplicar control No:1		Valoración control No:1		
Valor probabilidad para aplicar control No: n		Valoración control No: n		
Probabilidad residual				
Datos relacionados con impacto		**Datos valoración de controles**		**Cálculos requeridos**
Impacto inherente				
Valor Impacto para aplicar control No: 1		Valoración control No:3		
Valor Impacto para aplicar control No: n		Valoración control No:		
Impacto residual				

Zona de Riesgo final (con controles)		
Probabilidad con controles	**Impacto con controles**	**Zona de Riesgo final**

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas del departamento de la administración pública.

5.6 TRATAMIENTO

Para el plan de tratamiento de riesgos se lo realizará de acuerdo a la metodología para gestión del riesgo administrativo versión 8.0

BIBLIOGRAFÍA

- Guía 7 Gestión de riegos. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

- Guía 8 controles de seguridad y privacidad de la información. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

- Guía para la administración del riesgo y el diseño de controles en entidades públicas del departamento de la administración pública.

- Guía para la gestión y clasificación de los activos de la información

- Anexo 4 Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas

- Modelo Nacional de Gestión del Riesgo de seguridad digital Gobierno de Colombia

Fin del documento.

ELABORADO POR:

WILLIAM MONTENEGRO GUEVAR
Profesional Universitario

REVISADO POR:

ARVEY VALLEJO NARVAEZ
Jefe Oficina Asesora de Comunicaciones y Sistemas

APROBADO POR:

ANA BELÉN ARTEAGA TORRES
Gerente