PLAN DE TRATAMIENTO DE RIESGO DE LA INFORMACIÓN

EMPRESA SOCIAL DEL ESTADO HOSPITAL

SAN VICENTE DE RAMIRIQUI

SANDRA VIVIANA SAMPAYO DIAZ

GERENTE

CONTENIDO

INTRODUCCIÓN

La Empresa Social del Estado Hospital San Vicente de Ramiriquí en cumplimiento de los fines esenciales del estado enunciados en el artículo segundo de la Constitución Política de Colombia " servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la constitución, facilitar la participación de todos en las decisiones que los afecten en la vida económica, política, administrativa y cultural de la Nación, defender a independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigilancia de un orden justo"

La E.S.E Hospital san Vicente de Ramiriquí en cumplimiento de la prestación de los servicios y desarrollo de las actividades en la gestión de los procesos estratégicos, misional de apoyo y evaluación continuamente se está procesando, gestionando, almacenando, custodiando, transfiriendo e intercambiando información.

De acuerdo con lo mencionado anteriormente, dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información (en adelante MSPI), un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Por otra parte, Teniendo en cuenta que el contexto organizacional de esta guía y del MSPI en sí, son las entidades del Estado, la metodología en la cual se basa la presente guía es la "Guía de Riesgos" del DAFP1, buscando que haya una integración a lo que se ha desarrollado dentro de la Entidad para otros modelos de Gestión, y de este modo aprovechar el trabajo adelantado en la identificación de Riesgos para ser complementados con los Riesgos de Seguridad.

Por lo anteriormente expuesto la entidad implementa el plan de tratamiento de riesgo de la información de acuerdo a los lineamientos del Departamento Administrativo de la función pública con la estrategia del Modelo integrado de planeación y Gestión MIPG y el ministerio de tecnologías e información.

1.JUSTIFICACIÓN

En la actualidad y de acuerdo con la expedición del Decreto 2573 de 2014 contenida en el Decreto Único Reglamentario 1078 de 2015 del sector de Tecnologías de la información y las Comunicaciones; la Empresa Social del Estado Hospital San Vicente de Ramiriquí trabaja la implementación del Sistema de Gestión de Seguridad de la Información SGSI, siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información mediante la adecuada gestión del riesgo, la aplicación de la normatividad vigente y la implementación de mejores prácticas relacionadas con seguridad de la información.

El modelo de SGSI de la Empresa Social del Estado Hospital San Vicente de Ramiriquí se adoptará de acuerdo al ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), el cual asegura que el SGSI esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar el SGSI.

2. MARCO NORMATIVO

Para el desarrollo el plan de tratamiento de riesgo de la información de la Empresa Social del Estado Hospital San Vicente de Ramiriquí, se toma como referencia las normas que lo reglamentan:

Constitución Política de Colombia1991 - Artículo 15 "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar".

"Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye "El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles" entre otras disposiciones.

Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos

Decreto 2573 de 2014 "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".

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

Decreto 1078 de 2015 contempló en el artículo 2.2.9.1.2.2, los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad de un Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI, de un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información

Decreto 612 de abril 4 de 2018 "por *el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado*"

3. MARCO CONCEPTUAL

Activo de información: Los activos son los recursos del Sistema de Seguridad de la Información ISO 27001, necesarios para que la empresa funciones y consiga los objetivos que se ha propuesto la alta dirección.

Administración del Riesgo: es el proceso de análisis de todos los riesgos a los cuales está expuesta la institución.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización. Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Análisis de Riesgos: es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Confidencialidad: Atributo de la información almacenada en un sistema por el cual, por tratarse de datos privados o sensibles, puede causar perjuicios si es accedida o publicada sin autorización.

Consecuencia: Resultado de un evento que afecta los objetivos. Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada. Control: Medida que modifica el riesgo.

Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad

Disponibilidad: la certeza que un sistema de información sea accesible por los usuarios autorizados cada vez que sea necesario o que esté programado o predefinido.

Evaluación de riesgos: 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.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Integridad: Propiedad de la información relativa a su exactitud y completitud

Impacto: son las consecuencias que genera un riesgo una vez se materialice.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión. Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgos de seguridad digital: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

MSPI: Modelo de Seguridad y privacidad.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Desarrollar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, de acuerdo con lo establecido en el Modelo de Privacidad y Seguridad de la Información, con el propósito de adoptar medidas y acciones encaminadas a reducir y eliminar riesgos relacionada con la infraestructura de tecnologías de la Información de la Empresa Social del Estado Hospital San Vicente de Ramiriquí.

4.2 OBJETIVOS ESPECÍFICOS

Establecer los principales lineamientos de seguridad y privacidad de la información enmarcados dentro de la estrategia del gobierno en línea.

Promover las prácticas de seguridad y privacidad de la información en la entidad.

Aplicar las metodologías del Departamento Administrativo de la Función Pública DAFP e ISO respectivamente en seguridad y riesgo de la información en la E.S.E Hospital San Vicente de Ramiriquí

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que el MINTIC

Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en la Entidad.

5. ALCANCE

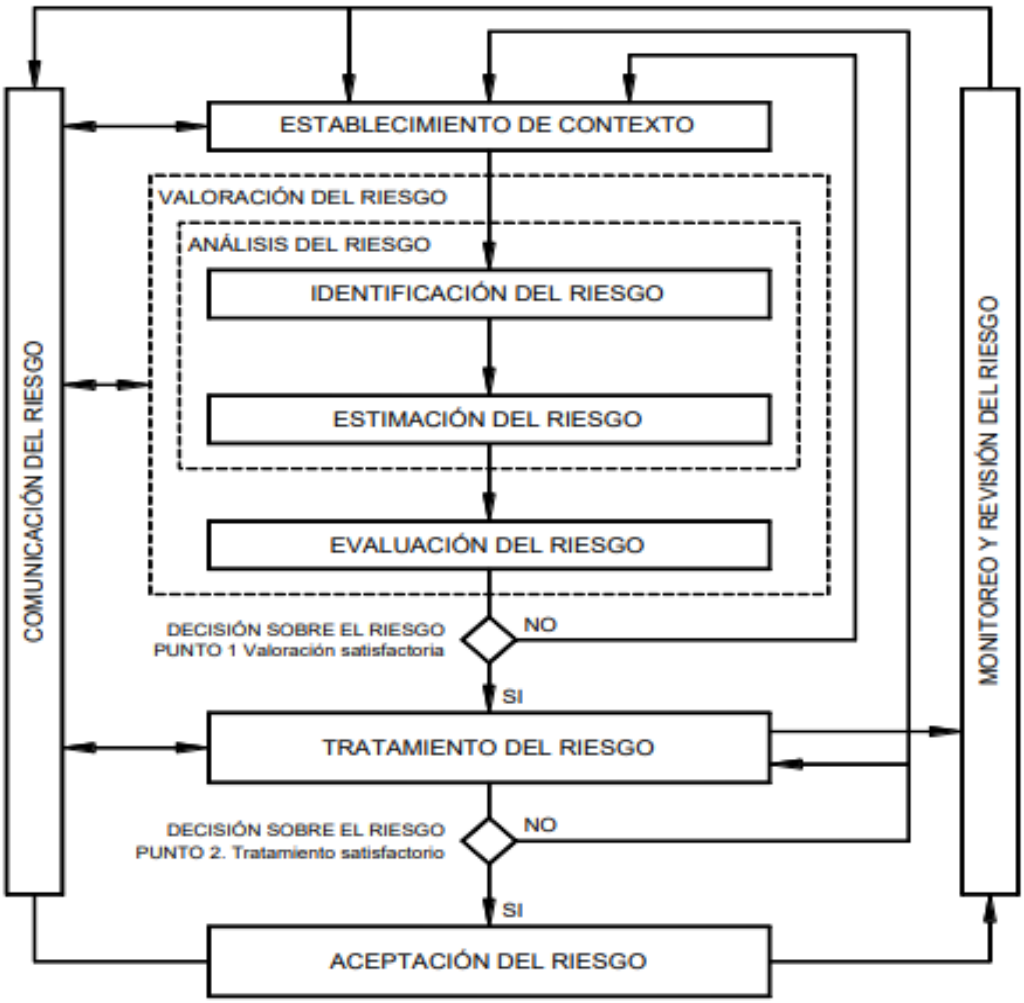
El plan de tratamiento de riesgo de seguridad y privacidad de la información contempla los requisitos, lineamientos y acciones establecidas para ser aplicados de forma permanente a los procesos estratégicos, misionales, de apoyo y evaluación, por lo cual deberán ser conocidos y cumplidos por todos los funcionarios vinculados a la entidad (de planta, contratistas y terceros) que accedan a los activos de información, sistemas de información e instalaciones físicas de la entidad

6. RECURSOS

La Empresa Social del Estado Hospital San Vicente de Ramiriquí en el marco de la gestión de riesgos de seguridad y privacidad de la información, Seguridad Digital, dispone de los siguientes recursos

RECURSO	VARIABLE
Humanos	La entidad a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua
Técnicos	Guía de Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - octubre de 2018 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI).
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos para los controles producto de la gestión de riesgos

7. PROCESO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



Fuente:https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

El proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento de este. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración.

El contesto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministrada información suficiente para determinar de manera eficaz las acciones que se necesitan para modifica los riesgos a un nivel aceptable entonces la labor está determinada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riesgo con un contexto revisado ejemplo los criterios de evaluación del riesgo los criterios para aceptar el riesgo o los criterios de impacto.

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la entidad. Esto es especialmente importante en una situación en la que la implementación de los controles se omite o se pospone, por ejemplo, por costos. La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI.

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

8. CONTEXTO ESTRATÉGICO

El contexto estratégico se tiene en cuenta en el proyecto del MSPI desde el inicio, sobre todo en el momento de definir el objetivo y el alcance del proyecto, así como la política de Seguridad de la Entidad, esto debido a que es necesario tener claro el entorno en el cual se desarrollará el proyecto, precisando cuál será el contexto en el que se desenvolverá, qué procesos involucrará, cual es el flujo de dicho o dichos procesos, y de ésta forma identificar sus objetivos y finalmente, de allí obtener los riesgos de Seguridad asociados.

De igual forma el personal asignado para el desarrollo del MSPI tiene como ventaja, el contexto estratégico avanzado para los modelos de Gestión establecidos en la Entidad, analizando los flujos de procesos ya identificados, para aportar su visión desde el MSPI. Sin embargo cabe mencionar que la guía señala las siguientes estrategias a través de las cuales se puede hacer ese levantamiento del contexto Estratégico

1. Inventario de Eventos

2. Talleres de Trabajo

3. Análisis de Flujo de Procesos

Es esencial determinar el propósito de la gestión del riego en la seguridad de la información ya que esto afecta al proceso total y, en particular, al establecimiento del contexto. Este propósito puede ser:

Dar soporte al modelo de seguridad de la información al interior de la entidad.

- Conformidad legal y evidencias de la debida diligencia.
- Preparación de un BCP.
- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.

El resultado de la especificación del contexto estratégico es la especificación del criterio básicos alcance, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

CRITERIOS BASICOS

Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diferentes enfoques, pero debe ser adecuado y que contenga criterios como: criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo:

CRITERIOS DE EVALUACIÓN DEL RIESGO

Se recomienda desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la institución teniendo en cuenta los siguientes aspectos:

- El valor estratégico del proceso de información para la entidad
- La criticidad de los activos de información involucrados en el proceso
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la entidad.

CRITERIOS DE IMPACTO

Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información del proceso
- Brechas en la seguridad de la información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- Operaciones deterioradas

- Perdida del negocio y del valor financiero
- Alteración de planes y fechas limites
- Daños para la reputación
- Incumplimiento de los requisitos legales

CRITERIOS DE ACEPTACIÓN DEL RIESGO

Es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas La organización debería definir sus propias escalas para los niveles de aceptación del riesgo. Durante el desarrollo, se deberían considerar los siguientes aspectos:

- Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas.
- Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado.
- Los diferentes criterios de aceptación del riesgo pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos si esto se especifica como un requisito contractual.
- Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga el riesgo y se podrían considerar los siguientes elementos:

- Criterios de negocio.
- Aspectos legales y reglamentarios.
- Operaciones.

- Tecnologías.
- Finanzas.
- Factores sociales y humanitarios

9. ALCANDE Y LÍMITES PARA LA GESTION DE RIESGOS EN SEGURIDAD DE LA INFORMACION

Es importante que la entidad defina el alcance y los límites y el alcance para de esta manera garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo. Al definir el alcance y los límites la entidad debería considerar la siguiente información

- Objetivos estratégicos de negocio, políticas y estrategias de la organización
- Procesos del negocio
- Funciones y estructura de la organización
- Los requisitos legales, reglamentarios y contractuales aplicables a la organización
- La política de seguridad de la información de la organización
- El enfoque global de la organización hacia la gestión del riesgo
- Activos de información
- Ubicación de la organización y sus características geográficas
- Restricciones que afectan a la organización
- Expectativas de las partes interesadas
- Entorno sociocultural
- Interfaces (Ej. Intercambio de información con otras entidades)

10. CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, cronograma propuesto para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Entidad y descripción general de las tareas principales.

ACTIVIDAD	RESPONSABLE	FECHA PROGRAMADA
Identificación de riesgos en cada uno de los procesos de la entidad	Auxiliar Administrativo	Mayo de 2022
Identificación de las amenazas	Auxiliar Administrativo	Julio de 2022
Identificación de vulnerabilidades	Auxiliar Administrativo	Agosto de 2022
Valoración de controles	Auxiliar Administrativo	Septiembre de 2022

11.BIBLIOGRAFIA

Guía de gestión de riesgos. Seguridad y privacidad de la información MINTIC Guía No 7

https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos

VALIDACIÓN DEL DOCUEMENTO		
ELABORO	**REVISO**	**APROBÓ**
FIRMA: **NOMBRE: JENNY BUITRAGO** **CARGO: ASESOR**	**FIRMA:** **NOMBRE: COMITE** **CARGO: GESTION Y DESEMPEÑO**	**FIRMA:** **NOMBRE: COMITE** **CARGO: GESTIÓN Y DEEMPEÑO**
CONTROL DE CAMBIOS		
CAMBIO REALIZADO	**FECHA DE CAMBIO**	**VERSIÓN**
Elaboración de documento	25 de enero de 2022	01