CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA ACTUALIZACIÓN
2	23/01/2020	9. Actividades a Realizar en Tratamiento del Riesgo
3	12/01/2021	8.Valoración del Riesgo. 9. Actividades a Realizar en Tratamiento del Riesgo
4	20/01/2022	Revisión y actualización general del documento
5	11/01/2023	5. Descripción del Plan 9. Referencias bibliográficas

Elaboró: Técnico Administrativo Sistemas	**Actualizó:** Yeinson Javier Cárdenas V.	**Revisó**: Comité de Gestión y Desempeño MIPG	**Aprobó**: Comité de Gestión y Desempeño MIPG
Cargo:	**Cargo:** Técnico Administrativo Sistemas	**Cargo:** Comité de Gestión y Desempeño MIPG	**Cargo:** Comité de Gestión y Desempeño MIPG
Fecha:28/01/2019	**Fecha**:03/01/2023	**Fecha**: 10/01/2023	**Fecha**: 11/01/2023

CONTENIDO

INTRODUCCION

La norma ISO 27005:2011 es un estándar internacional diseñado para la gestión del riesgo en la seguridad de la información dentro de un sistema de gestión de seguridad de la información. Contiene procedimientos y directrices, que permiten establecer los riesgos que enfrenta una organización y poder mitigarlos de la mejor manera. Se realiza la identificación, el análisis, la evaluación de los riesgos, las políticas y controles que permiten reaccionar ante una posible materialización del riesgo a través de él plan de tratamiento de riesgos.

La necesidad de crear un plan de seguridad y tratamiento de riesgos enfocados a la información es de vital importancia, hoy día uno de los activos más importantes en toda institución es la información, y es por ello por lo que se deben tener barreras de seguridad y controles en la administración y tratamiento de esta.

1. OBJETIVO GENERAL

Desarrollar el plan de tratamiento de riesgo seguridad y privacidad de la información, que permita minimizar la pérdida total o parcial de la información en el Hospital San Juan Bautista E.S.E.

1.1. OBJETIVOS ESPECIFICOS

- Identificar la ubicación y propietarios de los activos de información a través del inventario de activos.
- Establecer la categoría y valoración los activos de información.
- Proyectar el mapa de riesgos informáticos del Hospital san Juan Bautista E.S.E, a través de la matriz de riesgo instrumento MINTIC articles-176927_recurso_1.xlsx.
- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

El plan de tratamiento de riesgo y seguridad de la información aplica a todos los procesos que desarrollan, procesan e interactúan con los activos de información en la E.S.E., esencialmente los más críticos identificados y clasificados a través de la matriz de riesgo instrumento MINTIC articles-176927_recurso_1.xlsx y establecidos en el mapa de riesgo basado en la Política de Administración del Riesgo Institucional.

3. TERMINOS Y DEFINICIONES

Los términos y definiciones aplicables para la identificación de riesgos de Seguridad de la Información se basan en la Norma NTC-ISO/IEC 27000, Norma NTC-ISO/IEC 27005, Norma NTC-ISO/IEC 31000, Guía GTC 137 (ISO Guía 73:2009 - Vocabulario de Gestión de Riesgos), GTC ISO 27035:

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto.

Activo: Cualquier cosa que tiene valor para la organización. La norma ISO/IEC 27000, define los siguientes tipos de activos:

- información;
- software, como programas informáticos;
- físico, como computadores;
- servicios;
- personas, y sus calificaciones, habilidades y experiencia; e
- intangibles, como reputación e imagen

Activo de información: Conocimiento o información que tiene valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo con base en su probabilidad e impacto de ocurrencia.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de Seguridad de la Información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. También se puede definir como una medida que modifica el riesgo.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de la Seguridad de la Información (SGSI) de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de la norma técnica NTC-ISO/IEC 27001:2013.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona/entidad autorizada. La información debe estar en el momento y en el formato que se requiera, al igual que los recursos necesarios para su uso. La no disponibilidad de la

información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante los usuarios de la E.S.E.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de Seguridad de la Información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión de incidentes de Seguridad de la Información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros, como pérdida de reputación o implicaciones legales.

Inventario de Activos: 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.

Incidente de seguridad de la información: Un evento o serie de eventos de Seguridad de la Información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud. La información de la E.S.E. debe ser con calidad, clara y completa, y solo podrá ser modificada por el personal expresamente autorizado para ello. La falta de integridad de la información puede exponer a la Entidad a toma de decisiones incorrectas, lo cual puede tener impacto reputacional, financiero y/o legal.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de Seguridad de la Información inaceptables e implantar los controles necesarios para proteger la información.

Probabilidad: Medida para estimar la ocurrencia del riesgo.

Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Recursos de tratamiento de la información: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

Riesgo: 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.

Riesgo inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Selección de controles: Proceso de elección de las salvaguardas que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Sistema de Gestión de la Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizacional, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer la política y los objetivos de Seguridad de la Información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

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

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4. MARCO NORMATIVO

- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública.
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública.
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales.
- Ley 594 de 2000 - Ley General de Archivos.
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática.
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.

- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

- Decreto 2364 de 2012 - Firma electrónica.

- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos.

- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales.

- Ley 527 de 1999 - Ley de Comercio Electrónico.

- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos trámites innecesarios existentes en la Administración Pública.

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Ley Estatutaria 1581 de 2012 - Protección de datos personales.

- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información.

5. METODOLOGIA DE PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

Para lograr determinar una metodología de identificación, análisis y valoración del riesgo en la E.S.E. se toma como base la guía para la administración del riesgo del DAFP, determinado de esta manera las clases de riesgo, administración, seguimiento y control.

De acuerdo con la implementación de la gestión del riesgo se puede obtener:

- Aumento en la oportunidad de alcance de logros institucionales.
- Garantía en la seguridad, confidencialidad y disponibilidad de la información.
- Mejoramiento en la prestación de los servicios en los contextos Interno y externos.
- Aplicación de los controles del SGSI.
- Prevención de los incidentes de acuerdo con las lecciones aprendidas.
- Mejoramiento en la disponibilidad de los servicios de tecnología de la información.
- Cumplimiento de la normatividad vigente.
- Cumplimiento de los requerimientos realizados por los entes de control.

5.1. PROCESO PARA LA ADMINISTRACION DEL RIESGO

Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública.

5.1.1. CONTEXTO ESTRATEGICO ORGANIZACIONAL.

5.1.1.1. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO INSTITUCIONAL

Objetivos de la Política de Administración del Riesgo Institucional

- Unificar los lineamientos en los aspectos comunes de las metodologías para la administración de todo tipo de riesgos y fortalecer el enfoque preventivo con el fin de facilitar a las entidades, la identificación y tratamiento de cada uno de ellos.

- Ofrecer herramientas para identificar, analizar, evaluar los riesgos y determinar roles y responsabilidades de cada uno de los servidores del hospital (esquema de las líneas de defensa) en los riesgos de gestión.

- Suministrar lineamientos basados en una adecuada gestión del riesgo y control a los mismos, que permitan a la alta dirección de las entidades tener una seguridad razonable en el logro de sus objetivos.

5.1.1.2. ALCANCE

La política de riesgos es aplicable a todos los procesos, proyectos, de la ESE y a las acciones ejecutadas por los servidores durante el ejercicio de sus funciones, con el fin de garantizar el conocimiento y control de los riesgos del Hospital.

5.1.1.3. IDENTIFICACION Y CLASES DE RIESGOS

Según el DAFP El riesgo está vinculado con todo el que hacer, y no solo se debe tener en cuenta el riesgo de carácter económico, entre las clases de riesgo que pueden presentarse están:

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Para llevar a cabo la implementación del plan de tratamiento de seguridad y privacidad de la información se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, que a su vez se están, basados en los lineamientos, y decretos del DAFP.

De acuerdo con lo anterior se definen las fases de implementación del plan de tratamiento de riesgos y seguridad de la información:

Para iniciar la etapa de diagnóstico es necesario identificar a los líderes del proceso sobre el cual se vaya a realizar el análisis de riesgos, quienes son definidos por los responsables de la información con base en la oficina o dependencia productora, y a su vez son los responsables del tratamiento de los riesgos de seguridad identificados.

Una vez identificados, los líderes de procesos con el acompañamiento del área de Gestión de Sistemas Informáticos, se realiza la identificación de riesgos de Seguridad de la Información, los cuales quedan registrados en el formato Matriz de Análisis de Riesgos de Seguridad y Privacidad de la Información instrumento MINTIC • Proyectar el mapa de riesgos informáticos del Hospital san Juan Bautista E.S.E, a través de la matriz de riesgo instrumento MINTIC articles-176927_recurso_1.xlsx, El formato contiene las siguientes secciones:

1. Información del proceso
2. Identificación del riesgo
3. Análisis del riesgo
4. Evaluación de controles
5. Plan de acción de los riesgos

5.1.1.4. CARACTERIZACIÓN DE LOS PROCESOS.

Contiene la descripción del proceso y demás herramientas de enlace que son fundamentales para su desarrollo y ejecución.

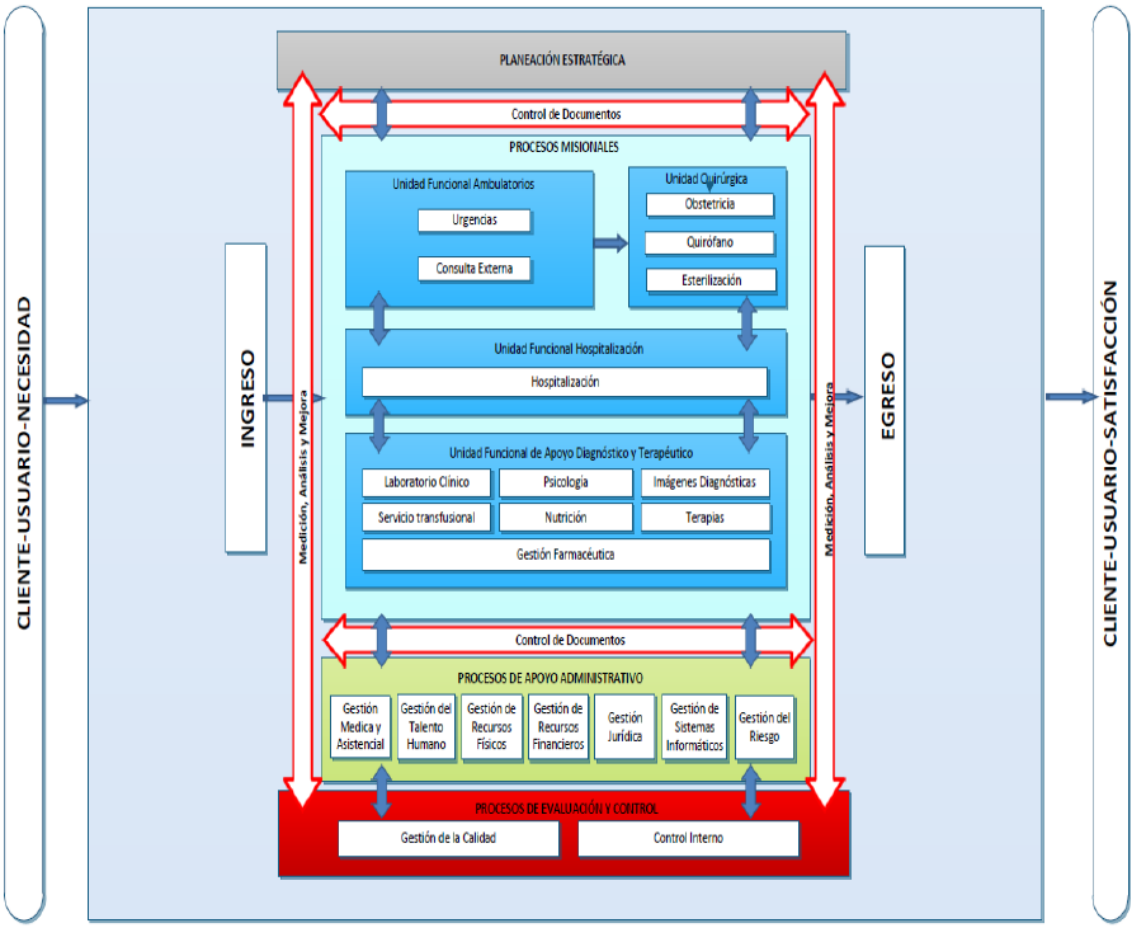
MACROPROCESO: Son los procesos que soportan la estructura Institucional, y se encuentran identificados los Procesos Estratégicos, Procesos Misionales, Procesos de Apoyo y Procesos de Evaluación y Control. Según la Función Pública, cada tipo de proceso se define de la siguiente manera:

- **Estratégicos:** Tienen como tarea primordial el establecer las políticas y estrategias, fijación de objetivos, comunicación y disposición de recursos necesarios, facilitan el seguimiento y la mejora.

- **Misionales:** Cadena de valor que permite obtener el resultado previsto por la entidad en el cumplimiento del objeto social o razón de ser.

- **Apoyo:** Proveen los recursos necesarios para el desarrollo de los procesos estratégicos, misionales y de evaluación.

- **Evaluación:** Necesarios para medir y recopilar datos para el análisis del desempeño y la mejora de la eficacia y la eficiencia de la entidad.



Mapa de proceso Institucional

El área de tecnologías de la información se encuentra definido dentro del macroproceso de Apoyo, proceso Gestión de Sistemas Informáticos, su estrategia de TI, es la de apoyar el proceso de diseño, implementación y evolución de la Arquitectura de TI en las E.S.E, para lograr que esté alineada con los objetivos y estrategias institucionales definidas en el plan de desarrollo y de gestión de la alta dirección, contando con un contexto estratégico y un enfoque actual, los cuales son descritos a continuación:

Contexto Estratégico: La tecnología de la información es una función que apoya la misión institucional, proporcionando herramientas e infraestructura que facilitan la colaboración asistencial, la gestión financiera, contable, administrativa, la planificación, el seguimiento y la evaluación; la gestión basada en resultados y el intercambio de conocimientos.

Enfoque actual: La tecnología de la información en el área de Gestión de Sistemas Informáticos del Hospital San Juan Bautista E.S.E, se centra actualmente en las funciones y servicios de apoyo de todos los procesos institucionales, como:

- Los sistemas para la administración de los servicios misionales (administración de la historia clínica y odontológica de los servicios de PyD, primer y segundo nivel, apoyo terapéutico y de diagnóstico, cirugía, farmacia, referencia y contra referencia); Servicios generales de apoyo administrativo (facturación, control de citas, administración de cuentas).

- Los sistemas para la administración de los servicios generales financieros (contabilidad, inventarios, compras, cuentas por pagar, cuentas por cobrar, tesorería, presupuesto y otros.

- Administración de los servicios de las telecomunicaciones y red institucional (cableado estructurado, medios de transmisión de información guiados y no guiados, correo electrónico, teléfonos, internet, configuración lógica), la infraestructura (servidores, puertas de enlace y PAC's. otros).

- Administración de recursos de hardware y software ofimáticos que permiten la automatización de procesos misionales y administrativos como computadores, impresoras, teléfonos, paquetes de software ofimáticos de licencias de uso comercial y libre, mensajería instantánea, plataformas web y de hosting entre otros.

Bajo el enfoque actual y las funciones de apoyo que desarrolla el área de TI, a continuación se describe la definición del riesgo.

5.1.2. IDENTIFICACION DE RIESGO EN TI

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la “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”. De igual manera, el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información del Hospital San Juan Bautista E.S.E.

De acuerdo con lo anterior, la política de tratamiento de datos personales Institucional y nacional, el hospital San Juan Bautista ESE, identifica los siguientes riesgos al momento de aplicar los procesos misionales, de apoyo, administrativos y financieros.

5.1.2.1. Riesgos de Ciberseguridad

Riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dada su naturaleza dinámica incluye también aspectos relacionados con el entorno físico. Estos riesgos tienen una relación directa con los principios de la Seguridad de la Información y se clasifican teniendo en cuenta los siguientes grupos:

Pérdida de la Confidencialidad: Pérdida de la propiedad de la información que impide su divulgación a individuos, entidades o procesos no autorizados.

Pérdida de la Integridad: Pérdida de la propiedad de contar con información exacta y completa, o que pudo haber sido sin ser manipulada o alterada por personas o procesos no autorizados.

Pérdida de la Disponibilidad: Pérdida de la cualidad o condición de la información de encontrarse a disposición de quienes requieran acceder a ella, ya sean personas, procesos o aplicaciones.

5.1.2.2. Riesgos de Seguridad y Privacidad de la Información

Riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.

De acuerdo con lo descrito en la norma GTC-ISO/IEC 27035, un incidente de seguridad de la información está definido como *"Evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y vulnerar la seguridad"*; por consiguiente, se representarían en Riesgos de Seguridad y Privacidad de la Información, como lo es el riesgo de tener un uso no adecuado de la información personal, lo que repercute en una violación de los derechos constitucionales.

5.1.3. ANALISIS DEL RIESGO

Una vez identificados los riesgos que posiblemente afectan la continuidad de los procesos o generen un incidente o una amenaza creada por una vulnerabilidad ya sea a través de un fallo de la ciberseguridad o falta a la seguridad de la informática.

Estos riesgos serán identificados, registrados, tipificados, clasificados y aplicando la valoración, a través de la matriz de riesgo instrumento MINTIC articles-176927_recurso_1.xlsx.

5.1.4. VALORACION DEL RIESGO

5.1.4.1. CRITERIOS PARA LA VALORACIÓN DE RIESGOS

Para la valoración de riesgos se toman como base dos variables: la **probabilidad** de ocurrencia del riesgo y su **impacto** en caso de que se materialice.

5.1.4.1.1. PROBABILIDAD DE OCURRENCIA

Se define la probabilidad de ocurrencia para cada riesgo teniendo en cuenta los siguientes criterios de valoración:

PROBABILIDAD		
NIVEL	**FRECUENCIA**	**PROBABILIDAD**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año - Riesgo cuya probabilidad de materializarse es mínima (Improbable).	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año - Riesgo que puede presentarse de manera eventual (Raro).	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año - Riesgo que se presenta de forma casual o accidental (Posible).	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año - Riesgo que puede materializarse de manera habitual (Probable).	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año - Riesgo cuya materialización es recurrente (Casi seguro).	100%

Tabla 2. Valoración de la Probabilidad de Ocurrencia

5.1.4.1.2. IMPACTO

La valoración del impacto que puede ocasionar a la E.S.E. la materialización de los Riesgos de Seguridad y Privacidad de la Información se representa con la descripción de los siguientes niveles:

IMPACTO		
NIVEL	**AFECTACIÓN ECONÓMICA**	**REPUTACIONAL**
Leve	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor	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
Moderado	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor	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.
Catastrófico	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Tabla 3. Valoración del Impacto

Esta valoración se realiza sobre en los principios de la Seguridad de la Información:

Confidencialidad: Mide el impacto que tendría para la pérdida de confidencialidad sobre los activos de información, es decir, que sean conocidos por personas no autorizadas.

Integridad: Mide el impacto que tendría la pérdida de integridad, es decir, si la exactitud y estado completo de los activos de información o sus métodos de procesamiento fueran alterados.

Disponibilidad: Mide el impacto que tendría la pérdida de disponibilidad, es decir, si los usuarios autorizados no tuvieran acceso a los activos de información en el momento que lo requieran.

5.1.4.2. VALORACIÓN DE LOS RIESGOS

Con base en la probabilidad y la valoración del impacto de cada riesgo, se establecen los niveles de riesgos (tanto los inherentes como los residuales luego de aplicar los controles identificados) teniendo una clasificación propia para la E.S.E:

Dimensión del Riesgo de Seguridad y Privacidad de la Información	Valor Asignado	Acción Requerida
Riesgo Extremo	**Mayor que 80% y menor o igual 100%**	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad, reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa o compartir y/o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Alto	**Mayor que 60% y menor o igual 80%**	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado o compartir y/o transferir el riesgo.
Riesgo Moderado	**Mayor que 40% y menor o igual 60%**	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor o compartir el riesgo.
Riesgo Bajo	**Mayor que 20% y menor o igual 40%**	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones de detección y preventivas.
Riesgo muy Bajo	**Menor o igual a 20%**	Reducir el riesgo, prevenir con actividades propias del proceso y por medio de acciones de detección y preventivas.

Tabla 4. Dimensión de Riesgos

De igual forma, se distribuyen los riesgos (inherentes y residuales) en las zonas de riesgo de acuerdo con el siguiente Mapa de Calor:

MATRIZ DE CALOR (NIVELES DE SEVERIDAD DEL RIESGO)

PROBABILIDAD						
	Muy Alta 100%	ALTO	ALTO	ALTO	ALTO	EXTREMO
	Alta 80%	MODERADO	MODERADO	ALTO	ALTO	EXTREMO
	Media 60%	MODERADO	MODERADO	MODERADO	ALTO	EXTREMO
	Baja 40%	BAJO	MODERADO	MODERADO	ALTO	EXTREMO
	Muy Baja 20%	BAJO	BAJO	MODERADO	ALTO	EXTREMO
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
		IMPACTO				

Tabla 5. Mapa de Calor para la Representación de los niveles de Riesgo por Zonas

Las acciones requeridas según la zona de riesgo identificada se indican en la siguiente tabla:

Zona de Riesgo Baja	Transferir el Riesgo: Riesgos para los cuales se determina que el nivel de exposición es bajo y por lo tanto permiten eliminar el riesgo por medio de la transferencia.
Zona de Riesgo Aceptable	**Aceptar el Riesgo:** Riesgos para los cuales se determina que el nivel de exposición es adecuado y por lo tanto se acepta.
Zona de Riesgo Moderado	**Mitigar o Evitar el Riesgo:** Riesgos para los cuales se requiere fortalecer los controles existentes y/o agregar nuevos controles.
Zona de Riesgo Importante	**Mitigar o Evitar el Riesgo:** Implementación de controles adicionales como parte del fortalecimiento de los actuales o como resultado de haberlo compartido o transferido.
Zona de Riesgo Inaceptable	**Evitar el Riesgo:** Se requiere de acciones inmediatas que permitan reducir la probabilidad y el impacto de materialización.

5.1.5. POLITICA ADMINISTRACION DEL RIESGO

Las políticas de administración del riesgo estarán guiadas por el trabajo realizado de identificación, análisis, tipificación y clasificación en cada una de las áreas o servicios,

complementando los resultados y procedimientos del MSPI, específicamente en los temas de la definición de la declaración de aplicabilidad (SOA).

Durante a vigencia se llevará a cabo el ejercicio por cada una de las áreas o servicios a través de los lideres de proceso quienes son los responsables del proceso por ende responsables del riesgo.

6. ACTIVIDADES PARA REALIZAR EN TRATAMIENTO DEL RIESGO

Nombre	Descripción	Calculo	Meta	Frec. Medición
Actualización de activos de información	Hace referencia a los activos de información y su clasificación de acuerdo con TI, electrónicos, .de hardware, software, etc.	Número de Activos de Información Clasificados / Número de Activos de Información Identificados	80%	Semestral
Definición de la Política de Administración del Riesgo de TI.	Hace referencia al tratamiento del riesgo una vez es materializado.	Número de riesgos Clasificados en matriz/ Número de riesgos Identificados	80%	Semestral

7. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

El monitoreo anual o en el momento que se determine, debe estar a cargo de los responsables de los procesos con el apoyo de la oficina de Control Interno y el área de Gestión de Sistemas Informáticos, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo de los riesgos de Seguridad y Privacidad de la Información.

8. DOCUMENTOS RELACIONADOS

CÓDIGO	TITULO
PE-PE-MIPG-PL6	Plan Estratégico de Tecnologías de la Información - PETI
PE-PE-MIPG-PL8	Plan de Seguridad y Privacidad de la Información
articles-176927_recurso_1	Matriz de riesgo instrumento MINTIC
Articles-5482 MINTIC	Instrumento Evaluación MSPI MINTIC
PA-GSI-ARI-M1 (V1)	Manual Políticas de Seguridad y Privacidad