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

TABLA DE CONTENIDO

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

CORPORACION HOSPITAL SAN JUAN DE DIOS – UNIREMINGTON, SANTA ROSA DE OSOS

Es muy importante que la Alcaldía de Santa Rosa de Osos o las entidades que cuenten con un plan de tratamiento de riesgos para minimizar perdidas y maximizar oportunidades. Por este motivo, se ha visto la necesidad de desarrollar un análisis de gestión de riesgo de seguridad de la información aplicado en La Alcaldía Municipal de Santa Rosa de Osos.

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procesos referentes a la seguridad de la información y recursos, todos los servidores públicos, están en cumplimiento de sus funciones expuestos a riesgos que puedan hacer fracasar una gestión; por tal razón es necesario tomar medidas para identificar las causas y consecuencias de la materialización de dichos riegos.

1. OBJETIVOS Y ALCANCE

4.1 Objetivo General

Especificar la metodología de gestión de riesgos de seguridad y privacidad de la información contemplando: Identificación de activos de información, amenazas, vulnerabilidades, riesgos y controles, los niveles aceptables y tratamiento de riesgo en

la Alcaldía de Santa Rosa de Osos teniendo en cuenta los lineamientos descritos en Modelo de seguridad de la información.

Realizar un análisis y valoración de los riesgos de seguridad de la información en cuanto al impacto y la probabilidad de ocurrencia para la Alcaldía de Santa Rosa de Osos Identifica las medidas de protección y remediación que contribuyan al correcto tratamiento de los riesgos a través de una adecuada selección y relación de controles informados en el Anexo A de la Norma Técnica Colombiana NTCISO/IEC 27001:2013 y los cuales ayuden al cumplimiento de los objetivos de cada Proceso y Procedimiento evaluado.

4.3 Alcance

La Guía Metodológica de Análisis de Riesgos de Seguridad y Privacidad de la Información provee los mecanismos necesarios para identificar, analizar, evaluar y tratar de manera adecuada los riesgos asociados a los activos de información de la Alcaldía de Entrerríos.

1. MARCO ESTRATÉGICO

2.1 Misión

Somos una institución prestadora de servicios de salud de baja complejidad y mediana complejidad, con énfasis en el modelo de Atención Primaria en Salud (AP), comprometidos, con criterios de calidad, seguridad, formación en salud del talento humano, eficiencia y humanización, buscando la satisfacción de los clientes internos y externos.

2.2 Visión

Para el 2027, seremos una institución referente en el norte antioqueño de baja y mediana complejidad, que presta servicios de salud con altos estándares de calidad,

centrada en el modelo de Atención Primaria en Salud (APS) que satisfaga las expectativas de nuestros usuarios y familias.

2.3 Mapa de Procesos

Ilustración 1. Mapa de Procesos Adoptado por la Administración Municipal de Santa Rosa de Osos en la vigencia 2025.

2.4 Valores Institucionales

a la institucionalidad.

• Respeto: Reconoceremos en cada una de mis actuaciones, el valor a la diferencia y dignidad de cada uno de los usuarios internos y externos con los que interactuamos diariamente.

• Comportamiento ético: Cumpliremos nuestros deberes con transparencia, coherencia y rectitud, fundamentado en la verdad y favoreciendo el interés general.

• Responsabilidad social en lo público y lo privado: Nos caracterizaremos por el cumplimiento de las obligaciones, orientando y valorando nuestras actuaciones y consecuencias de nuestros actos en el desempeño de las funciones.

Compromiso: Velaremos por el cuidado integral de la salud de las personas para el mejoramiento del bienestar y calidad de vida, con responsabilidad y lealtad, poniendo el mayor esfuerzo para lograr un servicio satisfaga y supere las expectativas de los clientes.

• Equidad: Nos caracterizaremos por promover la igualdad, sin ningún tipo de discriminación por creencias, sexo, raza, cultura, generando ambientes de confiabilidad y seguridad, todos los usuarios.

• Respeto a la diversidad: Habilidad profundamente interpersonal, definida como el entendimiento de que las personas participan paritariamente en un mundo ético común, en virtud de su condición humana, al tiempo que se reconoce la singularidad y diferencias de cada individuo.

• Solidaridad: Nos comprometemos a trabajar en equipo respetando y ayudando, coligados por una meta en común, logrando con ello una total cooperación en proyectos o metas en común

• Valoración del espacio ambiental: Favoreceremos la sostenibilidad, apoyando los sistemas de gestión ambiental del hospital, mejorando el logro de estándares superiores de huella ambiental y atención en salud.

2.5 Objetivos Estratégicos Plan de Desarrollo Municipal -Santa Rosa de Osos Seguro 2024-2027

Trabajo en equipo: La institución propenderá con su personal, en el fortalecimiento del trabajo participativo como metodología para el cumplimiento de sus objetivos y metas. • Humanización en el Servicio: Actuaremos amable y cálidamente con los usuarios y familia, transmitiendo empatía y actuando diligente y oportunamente, reconociendo y satisfaciendo las necesidades de los usuarios.

1. ÁMBITO DE APLICACIÓN

La presente Guía aplica para el plan de tratamiento de riesgo de seguridad y privacidad de la información.

2. REQUISITOS DE CALIDAD APLICABLE

Está Guía da cumplimiento a los lineamientos establecidos Gestión de Riesgos del Modelo de Seguridad y Privacidad de la Información en la entidad.

3. DEFINICIONES

A continuación, se definen los términos Basados en la Norma ISO 27001. (ISO/IEC 27000) Para una mejor comprensión de la presente Guía Metodológica, se toman como referencia los términos y definiciones establecidos en la Norma NTC-ISO/IEC 27000, Norma NTC-ISO/IEC 27005, Norma NTC-ISO/IEC 31000 y la Guía # 7

Gestión de Riesgos del Modelo de Seguridad y Privacidad de la Información.

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

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

potencial de un incidente no deseado, que puede provocar dañosa un sistema o a la organización.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinarel nivel de riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

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

Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de lasmisiones y funciones.

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 informaciónpor debajo del nivel de riesgo asumido.

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

Evento de seguridad de la información: Presencia identificada de una condiciónde 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: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el 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 exclusionesde controles del anexo A de la norma técnica NTC-ISO/IEC 27001:2013.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuandolo requiera una entidad autorizada. La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesariospara su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante los clientes.

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

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 amenazarla seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud. La información de la Superintendencia Nacional de Salud debe ser 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 empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas económicas.

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 misma.

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.

Responsable de Seguridad Informática: Los adscritos a la Secretaría General y de Gobiernoen el área TIC's, serán los encargados de realizar el seguimiento y monitoreo al sistema de Gestión de la Seguridad de la información (SGSI) cuando este implementado.

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 ejecuciónde 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 organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utilizauna organización para establecer una política y unos 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 la 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.

1. VALORACIÓN DE RIESGOS EN EL CONTEXTO DE LA ALCALDÍA DE ENTRERRÍOS A LOS ACTIVOS DE INFORMACIÓN

1.1. Contexto de la alcaldía de Entrerríos

La Alcaldía de Entrerríos se fortalece como una entidad territorial administrativa garantizará la prestación de los servicios públicos que determina la ley, así como la construcción de las obras necesarias con calidad para el progreso del municipio; promover el desarrollo integral para mejorar la calidad de vida de la comunidad, administrar los recursos del estado con transparencia, eficiencia y eficacia, con el desarrollo de planes, programas y proyectos encaminados al mejoramiento social, cultural, al ordenamiento y desarrollo de su territorio.

1.2. Contexto Interno

Servicios:

Protección a la información, protección al usuario y participación ciudadana.

1.3. Contexto de Seguridad y Privacidad de la Información

La información de La Alcaldía de Entrerríos, debe ser es decisiva para el desarrollode su proceso, su correcto desempeño dentro de la política y su relación con el ciudadano, es por ello que debe ser protegida de cualquier posibilidad de salida deeventos de riesgo de seguridad de la información y que pudiese parecer un impactoindeseado generando una consecuencia negativa para el normal progreso de las actividades de la entidad.

2.RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2.1. Definición del Riesgo

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 la alcaldía.

De acuerdo con lo anterior y en el marco de la Política Nacional de Seguridad Digital,la estrategia de administración de riesgos para el flujo de la información en los procesos busca diseñar una metodología ligera enfocada en la identificación, gestión y tratamiento de los Riesgos de Seguridad y Privacidad de la Información.

Figura 1 Riesgos de Seguridad y Privacidad de la Información

3.1. Riesgos de Seguridad Digital

Riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico.

1.1. Privacidad

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

1.2. Incidente de Seguridad de la Información

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 Lasactividades y vulnerar la seguridad”; por consiguiente, se representarían en Riesgosde Seguridad y Privacidad de la Información.

Los factores de riesgos que se encuentran identificados dentro de la entidad estánlos siguientes:

Factor de Riesgo	Descripción
Personas	Personal de la organización que se encuentra relacionado con la realización del proceso de forma directa o indirecta.
Procesos	Contexto relacionado entre sí de actividades y tareas necesarias para llevar a cabo el proceso.
Tecnología	Conjunto de herramientas tecnológicas que intervienen de manera directa o indirecta en la ejecución del proceso.
Infraestructura	Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el proceso.
Factores Externos	Situaciones generadas por agentes externos, las cuales no son controlables por la entidad y que afectan de manera directa o indirecta el proceso.

2.ANÁLISIS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA

a. Se identifican los activos de información, con el objetivo de valorarlos e identificar los riesgos de seguridad y privacidad de la información asociada alos factores.

gestión de valoración del activo, se consideran los siguientes aspectos:

ACTIVOS	DESCRIPCIÓN
Activos Esenciales	Datos importantes o vitales para la Administración de la Entidad: Aquellos que son esenciales, imprescindibles para la continuidad de la entidad; es decir que su carencia o daño afectaría directamente a la entidad, permitiría reconstruir las misiones críticas o que sustancian la naturaleza legal de la organización o de sus usuarios. Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012). Datos Clasificados o Calificados: Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
Datos / Información	Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. Ejemplo: Copias de Respaldo, Datos de Configuración, Contraseñas, Datos de Control de Acceso, Registros de Actividad, Código Fuente.

Hardware / Infraestructura	Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Equipos de Respaldo, Periféricos, Dispositivos Biométricos, Impresoras, Escáneres, Equipos Soporte de la Red, IP interconectados con tecnología Grandstream, IP y 4 NVR para los registros y administración, Lector de huellas biométrico IP para control
	de acceso, arquitectura Ethernet Router Board Mikrotic _CCR 1009-7G-1C-1S+PC.
Software / Aplicaciones Informáticas	Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. Ejemplo: Estándar, Navegador, Servidor, Correo Electrónico, Servidor de Correo Electrónico, Sistemas de Gestión de Bases de Datos, Software ARIES, Ofimática, Antivirus, Sistema Operativo, Backup o Respaldo.
Servicios	Funciones que permiten suplir una necesidad de los usuarios (del servicio). Ejemplo: Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, Gestión de Identidades (altas y bajas de usuarios del sistema)
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Contratistas, Proveedores.

Soportes de Información	Dispositivos físicos electrónicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo. Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red, Memorias USB, CDROM, DVD, Cinta Magnética, Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso.
Redes de Comunicaciones	Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro. Ejemplo: Red Telefónica, Red Inalámbrica.
Equipos Auxiliares	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos. Ejemplo: Fuentes de alimentación, generadores eléctricos, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, paneles solares, fibra óptica.
Instalaciones	Lugares donde residen los sistemas de información y comunicaciones.

Se establecen los niveles de riesgos teniendo una clasificación propia para de la alcaldía de Entrerríos.

Dimensión del Riesgo de seguridad y Privacidad de la Información	Acción Requerida
Riesgo Extremo	Evadir 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. Compartir o transferir el riesgo mediante la ejecución de pólizas.

Riesgo Alto	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.
Riesgo Moderado	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor. Compartir el riesgo.
Riesgo Bajo	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones defectivas y preventivas.

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

Con base en el resultado del análisis de riesgos de seguridad y privacidad de la información, se proponen acciones de mejora los cuales pueden estar en marcha por medio de planes de acción o de tratamiento con la finalidad de que la información siempre conserve las Características de confidencialidad, integridad y disponibilidad de esta, desarrollándose como un proceso de seleccionar e implementar medidas para modificar el nivel de riesgo.

La formulación de actividades de tratamiento de riesgos de seguridad de la información y su aplicación de acuerdo con la valoración del riesgo inherente documentado.

1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

La alcaldía de Entrerríos “evaluará el plan de tratamiento de riegos de seguridad y privacidad de la información”, por medio de un monitoreo esencial para revisar quelas acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando verificaciones al menos una vez al año o cuando sea necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo enla aplicación de las acciones de tratamiento.

El monitoreo anual o en el momento que se determine, debe estar a cargo de los responsables de los procesos, el jefe de Control Interno y la coordinación TIC, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo de seguridad y privacidad de la información.

CONTROL DE CAMBIOS:

NÚMERO DE VERSIÓN	TIPO DE MODIFICACIÓN	FECHA DE APROBACIÓN	ELABORADOR
01	Creación de documento	28 Enero 2025	Doria Ledy Rúfeles Toro

REVISIÓN Y APROBACIÓN DE LOS DOCUMENTOS:

PROYECTADO POR:	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Carlos Andrés Pérez Lopera	Doria Ledy Rúfeles Toro	Carlos Andrés Pérez Lopera Juan Esteban Lopera Julieth Stephane Gil Salazar	Doria Ledy Rúfeles Toro
Subdirector Científico y Asistencial.	Director general	Subdirector administrativo y financiero. Subdirector Científico y Asistencial. Asesora de calidad	Director general