TABLA DE CONTENIDO

1. INTRODUCCIÓN.

La gestión de riesgos de Seguridad y privacidad de la Información, de los servicios le permite al Hospital San Vicente de Paúl de Santa Rosa de Cabal Risaralda, realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones y en la prevención de la materialización de estos. La administración de riesgos de seguridad y privacidad de la información se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la Empresa.

2. DEFINICIONES.

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Amenaza:** 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).
- **Vulnerabilidad:** Falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Control 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.
- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de exactitud y completitud.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

3. OBJETIVOS.

Establecer el marco de acción para el tratamiento integral de los riesgos de seguridad y privacidad de la información, sobre los activos de tecnología que soportan los servicios digitales del Hospital San Vicente de Paúl de Santa Rosa de Cabal Risaralda, definiendo acciones para aportar al tratamiento de estos, de acuerdo al contexto de la Empresa, las

capacidades y recursos disponibles, para fortalecer la confianza de los ciudadanos, grupos de valor y demás partes interesadas.

4. ALCANCE.

La gestión de riesgos de Seguridad y Privacidad de la información, aplica e integra los procesos de la entidad, a través de la implementación de buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

5. PROPOSITO DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO.

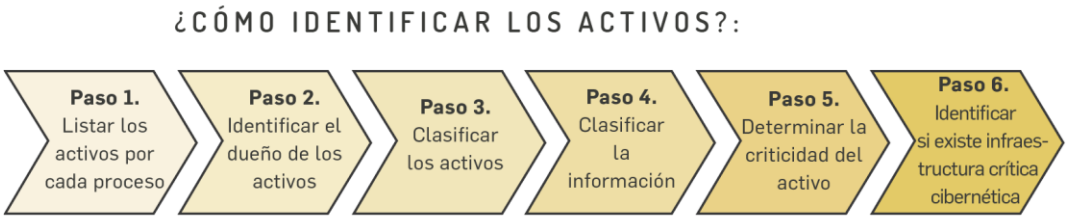
Fortalecer la implementación y desarrollo de la Política de administración del Riesgo a través del adecuado tratamiento de los riesgos que garanticen el cumplimiento de la misión y objetivos de la institución, generando una cultura de conocimiento y manejo de los riesgos involucrando y comprometiendo a todos los servidores de la E.S.E. Hospital San Vicente de Paúl de Santa Rosa de Cabal en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos, que prevengan la ocurrencia de eventos adversos, dentro de los cuales se identifican los siguientes: tecnológicos, financieros, de la misma manera para proteger la seguridad del paciente y los recursos humanos, de la E.S.E. Hospital San Vicente de Paúl de Santa Rosa de Cabal, resguardándolos contra la materialización de los riesgos.

6. METOLOGÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La implementación de esta metodología se realiza con el objetivo de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron dando cumplimiento a la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5 de diciembre de 2020, así:

Identificación de los activos de seguridad 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: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5

Establecimiento del contexto:

Las posibles causas de los riesgos se establecen a partir del análisis del contexto una vez realizado el análisis podemos identificar los riesgos.

Identificación del riesgo:

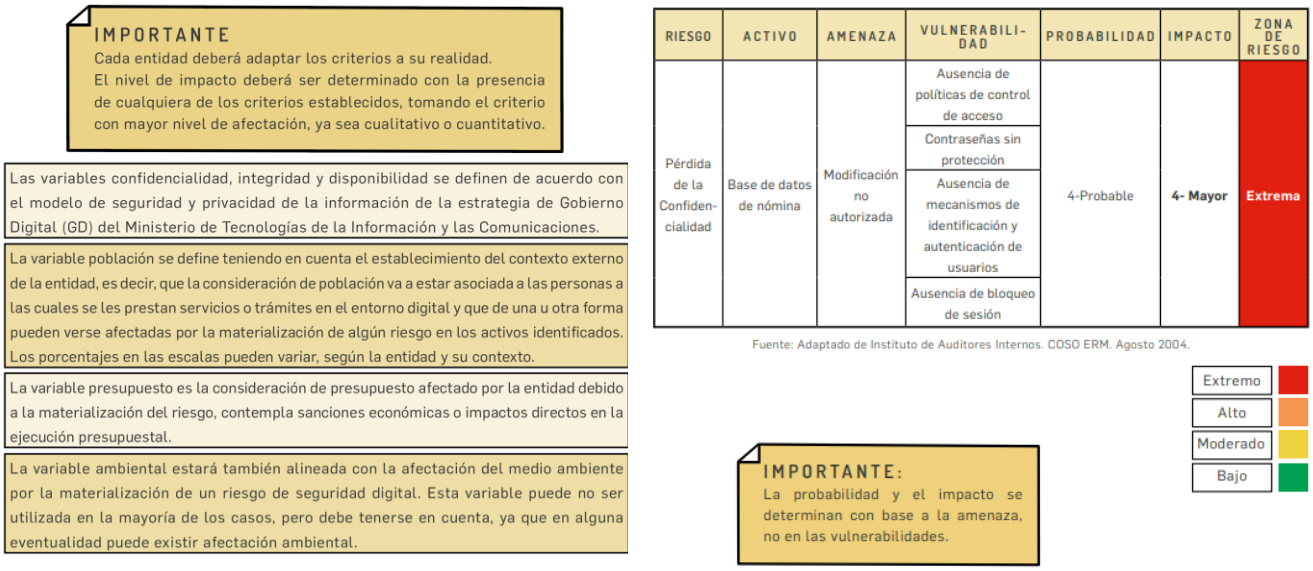
Para la identificación de riesgos de Seguridad y Privacidad de la Información de los Servicios del Hospital San Vicente de Paúl de Santa Rosa de Cabal Risaralda, se debe tener en cuenta diferentes aspectos como infraestructura física, áreas de trabajo, entorno y ambiente en general, para lo cual se hace indispensable que cada uno de los procesos tenga identificado los activos de información y reconocer las situaciones potenciales que causarían daño al Hospital poniendo en riesgo el logro de los objetivos establecidos.

Para la identificación se pueden abarcar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes involucradas.

Valoración del Riesgo:

La valoración de los riesgos de Seguridad y Privacidad de la Información de los Servicios del Hospital San Vicente de Paúl de Santa Rosa de Cabal Risaralda se realizará acorde a la metodología Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5 de diciembre de 2020, emitida por el Departamento Administrativo de la Función Pública,
Se analiza el contexto, se identifican los riesgos y se realiza el análisis de la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus vulnerabilidades e identificando los controles para mitigarlas.

Valoración del riesgo en seguridad de la información:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5

Controles asociados a la seguridad y privacidad de la información:

Una vez identificado el nivel del riesgo inherente y asociado vulnerabilidades, se establecen los controles para mitigarlos, a estos controles se le identifican las variables a evaluar para el adecuado diseño de como son: responsable, periodicidad, propósito, cómo se realiza la actividad de control, observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute de manera consistente, de tal forma que pueda mitigar el riesgo. Esta valoración se realiza de acuerdo con las tablas y metodología establecida Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5 de diciembre de 2020.

Definición y aprobación de mapas de riesgos y planes de tratamiento:

Una vez concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de Seguridad y Privacidad de la Información del Hospital, En el Comité de Gestión y Desempeño Institucional, los líderes de los procesos presentan para aprobación los mapas de riesgos. De igual forma en esta acta se aprobarán los planes de tratamiento con las actividades requeridas que permitan mitigar aquellos riesgos cuyo nivel residual este en zona Moderada, Alta o Extrema.

Materialización:

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información. Así mismo se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos. En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en la matriz.

Oportunidad de Mejora

La gestión de los riesgos analizará e identificará las oportunidades. La cual deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

7. RECURSOS.

RECURSOS	VARIABLE
Humanos	Jefe Planeación y Sistemas de Información. Técnico Administrativo Sistemas. Ingeniero de Sistemas. Personal de mantenimiento. Personal de soporte de sistemas de información. Técnico en sistemas. Tecnólogo en sistemas.
Técnicos	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital Herramienta para la gestión de riesgos (Matriz de Riesgos Institucional)
Logísticos	Disposición de recursos para ejecutar: Procedimiento de inducción y reinducción, Plan institucional de capacitaciones, gestión de los riesgos identificados.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías

Fuente, Plan de tratamiento riesgos SPI – MINTIC – 2021.

8. PRESUPUESTO.

El presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información de los servicios identificados en la entidad, se establece por el líder del proceso asociado al riesgo identificado, quien es el responsable del seguimiento y de la implementación de los controles y la inclusión de los recursos en el presupuesto institucional.

9. MEDICIÓN.

La medición se realiza con un indicador orientado a determinar el porcentaje de ejecución de los controles definidos para mitigar los riesgos identificados en los sistemas de gestión de la entidad, se realizará seguimiento a los riesgos por parte del responsable de planeación y del proceso, con periodicidad anual y semestral.

10. EJEMPLOS DE AMENAZAS Y VULNERABILIDADES FRENTE A LOS ACTIVOS DE INFORMACIÓN.

Fuente: Guía de gestión de riesgos. (Guía No 7). MINTIC.

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión y congelamiento.
	Ausencia de un eficiente control de cambios en la configuración.	Error en el uso.
	Susceptibilidad a las variaciones de voltaje.	Pérdida del suministro de energía.
	Almacenamiento sin protección.	Hurtos medios o documentos.
	Falta de cuidado en la disposición final.	
	Copia no controlada.	
SOFTWARE	Ausencia o insuficiencia de pruebas de software.	Abuso de los derechos.
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo.	
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.	
	Ausencias de pistas de auditoría.	
	Asignación errada de los derechos de acceso.	
	Software ampliamente distribuido.	Corrupción de datos.
	En términos de tiempo utilización de datos errados en los programas de aplicación.	
	Interfaz de usuario compleja.	Error en el uso.
	Ausencia de documentación.	
	Configuración incorrecta de parámetros.	

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
	Fechas incorrectas.	
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario.	Falsificación de derechos.
	Tablas de contraseñas sin protección.	
	Gestión deficiente de las contraseñas.	
	Habilitación de servicios innecesarios.	Procesamiento ilegal de datos.
	Software nuevo o inmaduro.	Mal funcionamiento del software.
	Especificaciones incompletas o no claras para los desarrolladores.	
	Ausencia de control de cambios eficaz.	
	Descarga y uso no controlado de software.	Manipulación con software.
	Ausencia de copias de respaldo.	
	Ausencia de protección física de la edificación, puertas y ventanas.	Hurto de medios o documentos.
	Fallas en la producción de informes de gestión.	Uso no autorizado del equipo.

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
	Ausencia de procedimiento formal para el registro y retiro de usuarios.	Abuso de los derechos.
	Ausencia de proceso formal para la revisión de los derechos de acceso.	
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad).	
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información.	
	Ausencia de auditorías.	
	Ausencia de procedimientos de identificación y valoración de riesgos.	
	Ausencia de reportes de fallas en los registros de administradores y operadores.	
	Respuesta inadecuada de mantenimiento del servicio.	

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
ORGANIZACIÓN	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de procedimientos de control de cambios.	
	Ausencia de procedimiento formal para la documentación del MSPI.	Corrupción de datos.
	Ausencia de procedimiento formal para la supervisión del registro del MSPI.	
	Ausencia de procedimiento formal para la autorización de la información disponible al público.	Datos provenientes de fuentes no confiables.
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información.	Negación de acciones.
	Ausencia de planes de continuidad.	Falla del equipo.
	Ausencia de políticas sobre el uso de correo electrónico.	Error en el uso.
	Ausencia de procedimientos para introducción del software en los sistemas operativos.	
	Ausencia de registros en bitácoras.	
	Ausencia de procedimientos para el manejo de información clasificada.	
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos.	
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información.	Hurto de equipo.
	Ausencia de política formal sobre la utilización de computadores portátiles.	
	Ausencia de control de los activos que se encuentran fuera de las instalaciones.	
	Ausencia de política sobre limpieza de escritorio y pantalla.	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información.	

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad.	
	Ausencia de revisiones regulares por parte de la gerencia.	Uso no autorizado de equipo.
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad.	
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado.
RED	Ausencia de pruebas de envío o recepción de mensajes.	Negación de acciones.
	Líneas de comunicación sin protección.	Escucha encubierta.
	Tráfico sensible sin protección.	
	Conexión deficiente de los cables.	Fallas del equipo de telecomunicaciones.
	Punto único de fallas.	
	Ausencia de identificación y autentificación de emisor y receptor.	Falsificación de derechos.
	Arquitectura insegura de la red.	Espionaje remoto.
	Transferencia de contraseñas en claro.	
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento).	Saturación del sistema de información.
	Conexiones de red pública sin protección.	Uso no autorizado del equipo.
PERSONAL	Ausencia del personal	Incumplimiento en la disponibilidad del personal.
	Procedimientos inadecuados de contratación.	Destrucción de equipos y medios.
	Entrenamiento insuficiente en seguridad.	Error en el uso.
	Uso incorrecto de software y hardware.	
	Falta de conciencia acerca de la seguridad.	
	Ausencia de mecanismos de monitoreo.	Procesamiento ilegal de los datos.
	Trabajo no supervisado del personal externo o de limpieza.	Hurto de medios o documentos.

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.	Uso no autorizado del equipo.
LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.	
	Red energética inestable.	Falla en la red eléctrica.
	Ubicación en área susceptible de inundación.	Falla en la infraestructura física.
	Ausencia de protección física de la edificación (Puertas y ventanas).	

NOTAS DE CAMBIO

Versión	Fecha de Actualización	Descripción del cambio
1	28-01-2022	Elaboración del Documento
2	27-01-2023	Actualización de la información de acuerdo a los cambios

CONTROL DE EMISIÓN		
Elaboró / Actualizó		Revisó / Aprobó
Nombre	Carolina Ramírez Naranjo	Javier de Jesús Cadenas Pérez
Cargo	Jefe Oficina Planeación y Sistemas de Información	Gerente
Firma		
Fecha	27-01-2023	27-01-2023