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

GESTIÓN INTEGRAL DE LA INFORMACIÓN

CODIGO
VERSIÓN
ENERO 2022

HOSPITAL UNIVERSITARIO DE SANTANDER
EMPRESA SOCIAL DEL ESTADO

1.

2. OBJETIVO

Estructurar las acciones a seguir que permitan identificar, medir, controlar, y monitorear, comunicar y mitigar la materialización de los riesgos de seguridad y Privacidad de la Información.

3. ALCANCE

Este documento inicia con la identificación de los riesgos de información por parte de los procesos y/o servicios de la institución y finaliza con la ejecución del plan de tratamiento de riesgos.

4. APLICABLE A

Este documento es aplicable a todos los procesos estratégicos, misionales, de apoyo y evaluación de la E.S.E. Hospital Universitario de Santander.

5. RESPONSABLE

Profesional Universitario Sistemas

6. DEFINICIONES

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

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.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Análisis de brechas: es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.

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.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

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. En una definición más simple, es una medida que modifica el riesgo.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).

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

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.

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.

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. (ISO/IEC 27000).

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

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Información: Conjunto de datos que tienen un significado.

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

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.

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.

Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Probabilidad: Posibilidad de que una amenaza se materialice.

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. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación.

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

Procedimiento: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

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

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

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. (ISO/IEC 27000).

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

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

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

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

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.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

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

Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

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: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

7. MARCO NORMATIVO

- **Decreto 612 de 2018**: Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado.

- **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.

- **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.

- **Norma Técnica Colombiana - NTC ISO 27001.** Norma internacional de sistemas de gestión de seguridad y confidencialidad de la información.
- **Resolución 355 de Agosto de 2018 ESE HUS**. Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión MIPG, se reglamentan las disposiciones relativas al sistema institucional de control interno y se dictan nuevas disposiciones.

- **Resolución 427 de Septiembre de 2018** que modifica la Resolución 358 del 3 de Agosto de 2018 ESE HUS. Por medio del cual se aprueban las políticas institucionales de la ese hospital universitario de Santander y se dictan nuevas disposiciones.

8. CONDICIONES GENERALES

- La E.S.E. Hospital Universitario de Santander a través de la política de gestión integral del riesgo es responsable de definir el nivel de riesgo que es aceptable y crea una estructura de control de riesgo para mantener los riesgos dentro de los limites apropiados, garantizando recursos humanos, financieros y logísticos a fin de favorecer la gestión del riesgo.

- Este plan de tratamiento de riesgo pretende hacer un análisis de riesgo, con la documentación, diseño de recomendaciones, procedimiento y controles de seguridad dentro del contexto de acceso a la información tanto interna como externa.

- No existe un número máximo o mínimo de riesgos a identificar, la E.S.E. Hospital Universitario de Santander identificará los riesgos que amenacen el cumplimiento de los objetivos de los procesos, sistemas de gestión, estándares, grupos de estándares y/o ejes trazadores de acreditación trazados, por lo que el ejercicio de identificación se debe realizar de la manera más objetiva posible.

- La E.S.E Hospital Universitario de Santander analizará y tomará decisiones estratégicas con las cuales podrá gestionar efectivamente los riesgos, las cuales contemplan:

  Aceptar el riesgo, pero tomando algunas acciones para disminuir su probabilidad de ocurrencia o su magnitud de impacto.

  Transferir el riesgo a un tercero u organización.

  Eliminar el riesgo por el retiro o cesación del desarrollo o ejecución de la actividad o función causante de éste.

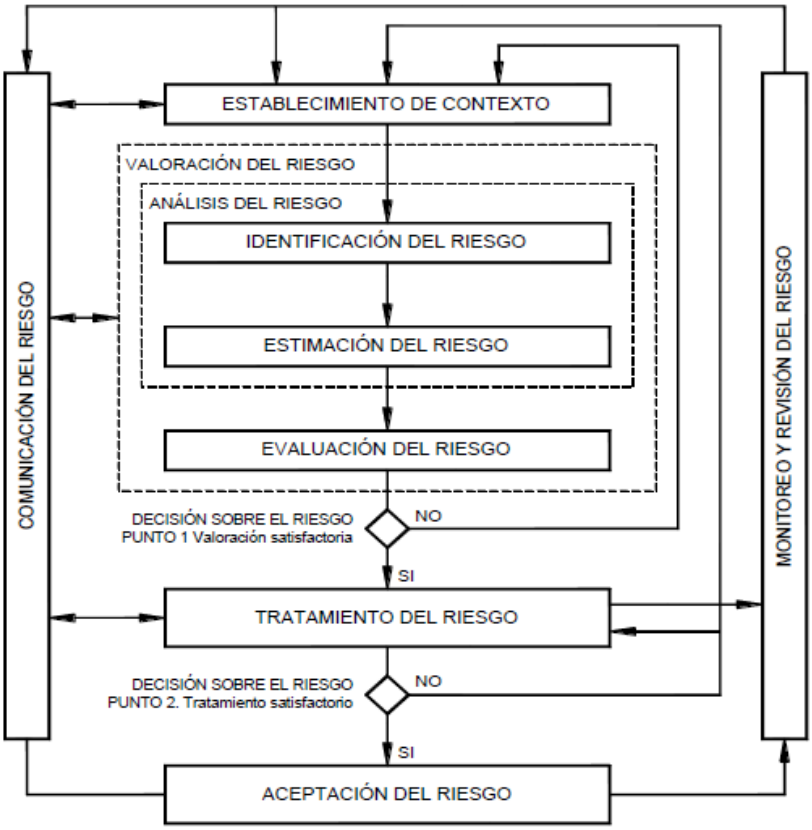
  Implementar controles por deficiencias en el diseño, la implementación o la eficacia operativa que minimice los riesgos identificados.

- La E.S.E Hospital Universitario de Santander implementará procesos de formación y capacitación que posibiliten competencias en gestión del riesgo.

9. DESARROLLO

El proceso de gestión del riesgo en la seguridad de la información consta del establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo, monitoreo y revisión del riesgo.

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñada basada tanto en la norma ISO/IEC 31000 como en la ISO 27005 para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:



9.1. Establecimiento del Contexto.

De acuerdo a la "Política de Planeación institucional" de la dimensión "Direccionamiento estratégico y planeación" del Modelo de Planeación y Gestión – MIPG de la función pública, la metodología para la gestión del riesgo de la E.S.E Hospital Universitario de Santander inicia con el análisis del contexto institucional, en donde se identifican la plataforma estratégica (misión, visión, objetivos, políticas, valores y principios), las prioridades, objetivos, programas y metas, los cuales se hallan definidos en el Plan de Desarrollo de la E.S.E Hospital Universitario de Santander 2018 – 2020.

Por lo anterior, para el análisis del riesgo se debe definir los posibles riesgos asociados al cumplimiento de las prioridades, programas, metas y objetivos de los procesos, estándares, ejes de acreditación y/o sistemas de gestión, los cuales deben ser medibles y deben contar cronogramas de ejecución, responsables e indicadores para monitorear y evaluar su cumplimiento, así como los controles para su mitigación.

Así mismo, dentro del análisis del contexto, las situaciones del entorno pueden ser de carácter interno o externo en los campos social, cultural, económico, financiero, tecnológico, ambiental, político y legal, bien sea internacional, nacional o regional según sea el caso de análisis; a su vez

la E.S.E Hospital Universitario de Santander a nivel interno considera factores como: estructura organizacional, funciones y responsabilidades, políticas, objetivos y estrategias implementadas, recursos y conocimientos con que se cuenta (económicos, personas, procesos, sistemas, tecnología, información, comunicación interna), relaciones con las partes involucradas y cultura organizacional los cuales apoyan el cumplimento de las metas y objetivos institucionales y es donde se identifican los riesgos que afectan la prestación de los servicios.

CONTEXTO		
CONTEXTO	**CATEGORÍA**	**DEFINICIÓN**
EXTERNO	ECONÓMICO	Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
EXTERNO	POLÍTICO	Cambios de gobierno, legislación, políticas públicas, regulación.
EXTERNO	SOCIAL	Demografía, responsabilidad social, orden público.
EXTERNO	TECNOLÓGICO	Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
EXTERNO	MEDIOAMBIENTALES	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
EXTERNO	COMUNICACIÓN EXTERNA	Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.
INTERNO	FINANCIEROS	Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
INTERNO	PERSONAL	Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
INTERNO	PROCESOS	Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
INTERNO	TECNOLOGÍA	Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
INTERNO	ESTRATÉGICOS	Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
INTERNO	COMUNICACIÓN INTERNA	Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
PROCESO	DISEÑO DEL PROCESO	Claridad en la descripción del alcance y objetivo del proceso.
PROCESO	INTERACCIONES CON OTROS PROCESOS	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
PROCESO	TRANSVERSALIDAD	Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
PROCESO	PROCEDIMIENTOS ASOCIADOS	Pertinencia en los procedimientos que desarrollan los procesos.
PROCESO	RESPONSABLES DEL PROCESO	Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
PROCESO	COMUNICACIÓN ENTRE LOS PROCESOS	Efectividad en los flujos de información determinados en la interacción de los procesos.

9.2. Identificación de Riesgos Inherentes de Seguridad Digital.

En la etapa de identificación se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos de información dentro del proceso: "Integridad, confidencialidad y disponibilidad". Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Existirían tres (3) tipos de riesgos:

- Pérdida de confidencialidad.
- Pérdida de la integridad.
- Pérdida de la disponibilidad.

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

9.2.1. Identificación de Amenazas.

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

- Deliberadas (D), fortuito (F) o ambientales (A).

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D

	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

9.2.1.1. Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

FUENTE DE AMENZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego	Piratería Ingeniería Social
Criminal de la computación	Destrucción de la Información Divulgación ilegal de la información	Crimen por computador Acto fraudulento
Terrorismo	Chantaje Destrucción	Ataques contra el sistema DDoS Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otro interés)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de Información
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ganancia monetaria	Asalto a un empleado Chantaje

9.2.1.2. Identificación de vulnerabilidades: la entidad pública puede identificar vulnerabilidades (debilidades) en las siguientes áreas

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad

	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

9.3. Análisis de los Riesgos.

Con el análisis de los riesgos se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (en el caso de procesos se denomina: Riesgo inherente).

Los pasos a seguir para el análisis de los riesgos son los siguientes:

9.3.1. Determinar la Probabilidad

La probabilidad es entendida como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad. Para su determinación se utiliza la tabla de probabilidad.

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

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

En el análisis de la probabilidad se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Clasificación de la Probabilidad

CRITERIOS PARA CALIFICAR LA PROBABILIDAD			
NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

En caso de que la entidad no cuente con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, los integrantes del equipo de trabajo deben calificar en privado el nivel de probabilidad en términos de factibilidad, utilizando la siguiente matriz de priorización de probabilidad.

Matriz de priorización de probabilidad											
N°	**RIESGO**	**DESCRIPCIÓN**	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**TOTAL**	**PROM**	**CALIFICACIÓN**
1	Otros riesgos	El evento podrá ocurrir en algún momento.	5	4	3	5	3	4	24	4	Probable
Convenciones: N°: número consecutivo del riesgo - P1: participante 1 P… - Tot: total puntaje - Prom.: promedio											

La herramienta de priorización indica que cada participante (P1, P2, P3… P6) asigna una calificación de probabilidad a cada riesgo identificado, se promedian los resultados y ese puntaje promedio seria la calificación del riesgo.

El análisis de frecuencia deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre el evento o riesgo identificado. En caso de no contar con datos históricos, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de sus factores internos y externos.

9.3.2. Determinar Consecuencias o Nivel de Impacto

El nivel de impacto es entendido como las consecuencias que puede ocasionar a la E.S.E Hospital Universitario de Santander la materialización del riesgo. Se tienen en cuenta las consecuencias potenciales establecidas en la identificación del riesgo.

Para su determinación se utilizan tablas de niveles de impacto como se muestran a continuación:

NIVEL	VALOR DE IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	2	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
MODERADO	3	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.

MAYOR	4	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
CATASTRÓFICO	5	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Cada entidad deberá adaptar los criterios a su realidad. El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

9.4. CRONOGRAMA

CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS												
ACTIVIDAD	**2022**											
	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
Sensibilización en Riesgos												
Identificación de Riesgos Digitales												
Análisis y tratamiento de los Riesgos												
Implementación de acciones de mejora de Riesgos												
Monitoreo y Revisión												
Informe final del Plan de Tratamiento de Riesgos												

1. DOCUMENTOS DE REFERENCIA

ANEXO 4 LINEAMIENTOS PARA LA GESTION DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS – MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION

GDI-PLA-PG-01 PROGRAMA DE GESTION INTEGRAL DE RIESGO
GUIA PARA ADMINISTRACION DEL RIESGO Y DISEÑO DE CONTROLES EN ENTIDADE PÚBLICAS.

2. ANEXOS

3. SOCIALIZACIÓN

Una vez aprobado este documento, es responsabilidad del líder del macroproceso y el responsable del procesos garantizar su socialización en los grupos primarios que le aplique, y/o mediante la utilización de cualquiera de las herramientas desarrolladas por la institución para tal fin, dejando la evidencia respectiva, las cuales deben ser enviado como soporte al correo institucional procesoscalidad@hus.gov.co.

1. CONTROL DE MODIFICACIONES					
Versión	**Fecha**	**Descripción de la Modificación**	**Actualizado por**	**Revisado por**	**Aprobado por**
NA	MM-AA	NA	NA	NA	NA