PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION

2019

CONTENIDO

1. INTRODUCCIÓN

Hoy en día se hace indispensable gestionar los riesgos de todo tipo en las organizaciones y la Seguridad de la Información no es la excepción. De igual manera, la estrategia de Gobierno Digital dispone la necesidad de establecer e implementar una Metodología de la gestión de Riesgos, el cual es la base para la elaboración de este documento.

Uno de los ejes principales de la acreditación en salud es la “gestión de riesgo” y a continuación se presenta el enfoque para ello:

La gestión de riesgos comprende tres procesos:

- **Análisis de calificación y valoración**: Comprende las actividades de **análisis de riesgo**, la cual incluye identificar el riesgo (activos, amenazas, vulnerabilidades y determinar que podrá suceder (riesgos), **estimar el riesgo** (obtener la indicación del riesgo cualitativo/cuantitativo) y la **evaluación de riesgos,** sus impactos y las recomendaciones para la reducción de los riesgos.
- **Administración del riesgo**: Se refiere a la priorización, implementación y mantenimiento de las medidas de reducción de riesgos apropiadas.
- **Monitoreo continuo**: Es la labor de repetir los pasos anteriores a intervalos de tiempo específicos o cuando se identifiquen cambios significativos en la organización, ya sea por la modificación y/o adición de servicios, cambios en la infraestructura tecnológica o por nueva reglamentación.

La metodología de análisis y evaluación de riesgos está enfocada principalmente en:

1. Caracterización de sistemas
2. Criterios de evaluación de riesgos
3. Identificación de amenazas
4. Identificación de vulnerabilidades
5. Determinación de probabilidades
6. Análisis de impacto
7. Determinación de alcance
8. Análisis de calificación y valoración del riesgo
9. Metodología para el tratamiento de riesgos
10. Recomendaciones de control
11. Documentación de resultados
12. Observaciones

El presente estudio se realizó siguiendo los pasos anteriormente descritos.

2. PRESENTACIÓN

2.1. Objetivos

2.1.1. Objetivo General

Realizar una adecuada gestión de los riesgos de la Seguridad de la Información en el Hospital Universitario Hernando Moncaleano Perdomo.

2.1.2. Objetivos específicos

- Presentar a la alta dirección del hospital un panorama general del estado de riesgos asociados a la seguridad de la información, que apoye en la toma de decisiones encaminadas al logro de los objetivos estratégicos.
- Priorizar y justificar las inversiones en cuanto a la implementación de controles para el mejoramiento de la seguridad de la información.
- Dar a conocer a la alta dirección de los riesgos residuales, las consecuencias y el impacto para la organización, para su aceptación o gestión.
- Brindar protección a los activos de información críticos del Hospital.

2.2. Alcance

Este plan, proporciona la metodología establecida por el Hospital para la administración y gestión de los riesgos a nivel de procesos; orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

2.3. Marco normativo

Norma NTC – ISO/IEC 27001
Norma NTC – ISO/IEC 27002
Norma NTC – ISO/IEC 27005

2.4. Definiciones

Administración de riesgos: Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
Amenaza: Situación externa que no controla la entidad y que puede afectar su operación.
Análisis del riesgo: Etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles.

Asumir el riesgo: Opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
Causa: Medios, circunstancias y/o agentes que generan riesgos.
Calificación del riesgo: Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
Compartir o transferir el riesgo: Opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
Consecuencia: Efectos que se pueden presentar cuando un riesgo se materializa.
Control: Acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
Evaluación del riesgo: Resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
Evitar el riesgo: Opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
Frecuencia: Ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
Identificación del riesgo: Etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
Impacto: Medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
Mapa de riesgos: Documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
Materialización del riesgo: Ocurrencia del riesgo identificado
Probabilidad: Medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
Procedimiento: Conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
Proceso: Conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.
Riesgo: Eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
Riesgo residual: Nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
Valoración del riesgo: Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

3. CONTENIDO

3.1. Caracterización de sistemas

Alcance

La gestión de riesgos abarca los procesos de la entidad y sistemas de información que hacen uso de la información “HISTORIA CLINICA”, como activo de información relevante para la atención de salud a usuarios, desde la recolección de datos, procesamiento, almacenamiento y disposición final.

Ante esto, los procesos relacionados son los siguientes:

Atención ambulatoria especializada, atención de urgencias, atención unidades de cuidado crítico, atención quirúrgica y sala de partos, atención hospitalización, gestión de apoyo diagnóstico y complementación terapéutica, gestión farmacéutica, referencia y contra referencia, gestión de la información.

Queda excluido las instalaciones de la universidad Surcolombiana (Salud) y aplicaciones de ámbito docencia-Servicio.

Activos de información

Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.

Información: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.

Se refiere a información de carácter sensible y/o crítica de la Entidad. Ejemplos de activos primarios podrías ser:

- Historias clínicas
- Información personal de trabajadores, contratistas, etc.
- Datos intercambiados entre aplicaciones (laboratorio, patología, Imagenología)
- Procesos, procedimientos, etc.
- Información contable y financiera.

Software: Se conoce como al soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

Ejemplos de activos de software podría ser:

- Sistemas Operativos (Servidores – PC)
- Antivirus
- Software de Firewall
- MS Office (en todas sus versiones)
- CAL de acceso
- Gestor de Base de Datos (SQL Server)
- Correo electrónico (Outlook)
- Software Biomédico

Interfaces del sistema (conectividad interna y externa)

Se refiere a aspectos de integración de aplicaciones o sistemas de información para mantener la integridad y unicidad con la historia clínica. Ejemplos de activos interfaces podrían ser:

- Interface entre INDIGO – DGH
- Interface entre INDIGO – LABCORE
- Interface entre INDIGO – PATCORE
- Interface entre INDIGO - CARESTREM

Recurso humano: Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.

Personas que soportan y usan el sistema de TI

Personas son activos de información que aportan el proceder. Ejemplos de activos personas podrían ser:

- Personal TIC (Sistemas de información, mesa de servicio, redes e infraestructura, mantenimiento de equipos)
- Personal Médico – Asistencial
- Personal Administrativo

Servicio: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.

Misión del sistema (Procesos ejecutados por el sistema)

SERVICIOS	DESCRIPCION	IMPORTANCIA
DGH	Maneja toda la información del ERP. Facturación, cartera, inventarios, etc.	MUY ALTA
INDIGO CRYSTAL	Maneja toda la información de Historias clínicas.	MUY ALTA
INDIGO VIE	Contiene toda la información de nómina y glosas	ALTA
COMODIN	Contiene la información contable histórica hasta el 2012.	BAJA
SIIGOS	Contienen Historias Clínicas Oncología.	NORMAL
IMÁGENES DIAGANOSTICAS	Información de imágenes diagnósticas. Rx, TAC, Resonancia.	MUY ALTA
Página Web	Página Web institucional	BAJA
Exchange	Servidor de Correo antiguo. No está en uso. Se deja como de consulta.	BAJA
Servidor de Archivos	Archivos compartidos o del usuario.	ALTA
SharePoint	Nuevo servicio de gestión documental y portales.	MUY ALTA
Plataforma Documental	Plataforma para la gestión de correspondencia.	BAJA
GEDAC	Aplicación para el control de derechos de peticiones	BAJA
LABCORE	Gestión de laboratorio clínico	MUY ALTA
PATCORE	Gestión de patologías	ALTA
ECLIPSE	Software de Digitalización Historias clínicas	BAJA
INTERNET	Servicio que provee el internet	MUY ALTA

Hardware: Se define al hardware como el conjunto de los componentes que conforman la parte material (física) de una computadora, dentro de los cuales no sólo se definen a los componentes físicos internos (disco duro, tarjeta board, microprocesador, circuitos, cables, etc.), sino también a los periféricos (escáners, impresoras).

Ejemplo de los activos de hardware son:

- Servidores
- Dispositivos de almacenamiento externos.
- Equipos activos de red (Router, Switch, Firewall, Acces Point, etc.)
  Computadores portátiles, de torre, All in One, Impresoras, escáners

Otro: Activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso.

Ejemplo: Sitios, Armarios RF, cajas fuertes, archivadores, estanterías, salas refrigeradas para servidores, cuartos de archivo, CPDs... son otros activos físicos que podemos tener en nuestra institución, y deberemos identificar.

Criticidad del sistema y de los datos (Valor del sistema o importancia para la entidad)

De todas las aplicaciones en el hospital, las más críticas son:

- DGH-Dinámica Gerencial Hospitalaria (Contabilidad, facturación, etc.)
- INDIGO CRYSTAL: (Historias Clínicas)
- LABCORE (Laboratorio Clínico)
- CARESTREM (Imágenes diagnosticas)
- PATCORE (Patología)

Sensibilidad del sistema y de los datos

La sensibilidad se refiere al nivel de protección requerida para mantener la integridad, confidencialidad y disponibilidad.

SERVICIOS	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD
DGH	MUY ALTA	ALTA	MUY ALTA
INDIGO CRYSTAL	MUY ALTA	MUY ALTA	MUY ALTA
INDIGO VIE	MEDIA	ALTA	ALTA
COMODIN	BAJA	BAJA	ALTA
SIIGOS	BAJA	MUY ALTA	MUY ALTA
IMÁGENES DIAGANOSTICAS	MUY ALTA	MUY ALTA	MUY ALTA
Página Web	BAJA	BAJA	ALTA
Exchange	BAJA	ALTA	ALTA
Servidor de Archivos	ALTA	MEDIA	ALTA
SharePoint	ALTA	MEDIA	ALTA
Plataforma Documental	BAJA	MEDIA	ALTA
GEDAC	BAJA	BAJA	ALTA
LABCORE	MUY ALTA	MUY ALTA	MUY ALTA
PATCORE	ALTA	ALTA	MUY ALTA
ECLIPSE	BAJA	MUY ALTA	MUY ALTA

Requerimientos funcionales del sistema de TI

Los requerimientos funcionales del sistema de información son direccionados directamente a los proveedores de software. A estos se les realiza seguimiento estricto del mismo y son tenidos en cuenta en la elaboración del presente documento.

Políticas de seguridad del sistema y de gobierno de TI

Las políticas se seguridad del sistema de información están contenidas en el Manual de Seguridad de la Información.

Arquitectura de seguridad del sistema

Se tiene definido el inventario de hardware y servidores en el inventario de activos de información.

Flujo de información

Con el mejoramiento organizacional, la administración del Hospital Universitario Hernando Moncaleano Perdomo requiere tomar decisiones cada vez con una mayor base de conocimiento para así reducir la incertidumbre; es por eso que el flujo de información representa el movimiento de la información a través de la institución. Anexo 2 del Plan de Gerencia de la Información (Flujo de información entre procesos).

3.2. Criterios de evaluación de riesgos

La gestión de riesgos de seguridad de la información del Hospital se deberá enfocar en escenarios o enfoques como los siguientes

- El valor estratégico del proceso de información para el negocio,
- La criticidad de los activos de información se basa en su clasificacion,

Clasificación de acuerdo con la confidencialidad: La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, Esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad, a manera de ejemplo en la guía se definieron tres (3) niveles alineados con los tipos de información declarados en la ley 1712 del 2014:

INFORMACION PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACION PUBCLCA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACION PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Clasificación de acuerdo con la integridad: La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles:

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA

Clasificación de acuerdo con la disponibilidad: La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles:

1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

COFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACION PUBLICA RESERVADA	**A (ALTA)**	**1 (ALTA)**

INFORMACION PUBCLCA CLASIFICADA	M (MEDIA)	2 (MEDIA)
INFORMACION PÚBLICA	B (BAJA)	3 (BAJA)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Una vez clasificados los activos estos son analizados en la matriz de riesgo.

- Los requisitos legales y reglamentarios, así como las obligaciones contractuales,
- La importancia de la disponibilidad, confidencialidad e integridad para las operaciones y el negocio,
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación.

3.3. Identificación de amenazas

Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información. Algunos ejemplos de amenazas se muestran a continuación:

Fuente de amenaza	Motivos	Amenazas
Hacker, Craker	Reto, Ego, Rebelión	Hacking, ingeniería social, intrusión a los sistemas, acceso no autorizado a los sistemas
Criminales Informáticos	Destrucción de información, divulgación ilegal de información, ganancia económica, alteración no autorizada de datos	Crimen con el computador (CiberStalking), Actividades fraudulentas (reenvío, suplantación, intercepción, desfalcos), Robo de información, Intrusión al sistema
Terroristas	Destrucción, Explotación, Venganza	Terrorismo, Guerra de información, Ataques del sistema (negación del servicio), Penetración al sistema

Espionaje Industrial	Ventaja competitiva, Espionaje económico	Explotación económica, Robo de información, Intrusión en la privacidad personal, Ingeniería Social, Penetración al sistema, Acceso no autorizado al sistema (Acceso a información, tecnologías o propiedades clasificadas)
Internos (pobremente entrenados, disgustados, maliciosos, negligentes, deshonestos o empleados despedidos)	Curiosidad, Ego, Inteligencia, Ganancia Económica, Venganza, Errores y omisiones no intencionales (errores en la entrada de datos, errores de programación)	Asalto a un empleado, Abuso del computador, Fraude y Robo, Robo de información (Soborno), Entrada de datos falsos o corruptos, Intercepción código malicioso (virus, bombas lógicas, caballos de Troya), Venta de información personal y/o de la entidad, Errores del sistema, Intrusiones al sistema, Sabotaje al sistema, Acceso no autorizado al sistema.
Naturales	N/A	Inundaciones, terremotos, tornados, deslizamientos de tierra, avalanchas, tormentas eléctricas y otros eventos similares
Ambientales	N/A	Faltas prolongadas de energía eléctrica, polución, químicos, dispersión de líquidos.

3.4. Identificación de vulnerabilidades

Una vulnerabilidad es un defecto o debilidad en los procedimientos de seguridad, diseño, implementación o en los controles internos del sistema que podrían ser explotadas.

Los métodos para la identificación de vulnerabilidades del sistema comprenden el uso de fuentes de vulnerabilidades, la realización de pruebas a la seguridad del sistema y el desarrollo de listas de chequeo (Checklist) de requerimientos de seguridad.

Siguiendo la recomendación de la guía en donde afirma que “Sí el sistema aún no se ha diseñado, la búsqueda de vulnerabilidades se debe centrar en las políticas de seguridad de la entidad, procedimientos de seguridad planeados, en la definición de requerimientos del sistema y en los análisis de los proveedores y desarrolladores de sistema (White papers).”, se listan las siguientes vulnerabilidades.

Vulnerabilidad	Fuente de amenaza	Amenazas
No se realiza pruebas de seguridad. No se revisan de forma periódica los log de auditoria	Hacker, Craker	Hacking, Ingeniería social, Intrusión a los sistemas, Acceso no autorizado a los sistemas
Violación de la reserva de la historia clínica por parte de los usuarios con acceso al sistema	Criminales Informáticos	Crimen con el computador (CiberStalking), Actividades fraudulentas (reenvío, suplantación, intercepción, desfalcos), Robo de información, Intrusión al sistema
La página web y sus servicios no cuentan con mecanismos de seguridad adecuados. (Página obsoleta).	Terroristas	Bombas/Terrorismos, Guerra de información, Ataques del sistema (negación del servicio), Penetración al sistema

La información se maneja en los equipos de forma local y se desconoce qué datos son copiados en medios extraíbles. No existe políticas en el manejo de celulares o Smartphone a nivel interno. La información no está debidamente clasificada. Se desconoce qué datos son confidenciales (a excepción de la HC) y por lo tanto no se protege de forma adecuada.	Espionaje Industrial	Explotación económica, Robo de información, Intrusión en la privacidad personal, Ingeniería Social, Penetración al sistema, Acceso no autorizado al sistema (Acceso a información, tecnologías o propiedades clasificadas)
El proceso de ingreso y retiro de usuarios se cumple se debe hacer auditoria. No se realiza capacitación de ingreso a los usuarios nuevos del sistema de información No existe un manual de uso del sistema informático. No se realiza auditoria a los sistemas informáticos No se realiza capacitación de seguridad informática a los usuarios externos.	Internos (pobremente entrenados, disgustados, maliciosos, negligentes, deshonestos o empleados despedidos)	Asalto a un empleado, Abuso del computador, Fraude y Robo, Robo de información (Soborno), Entrada de datos falsos o corruptos, Intercepción código malicioso (virus, bombas lógicas, caballos de Troya), Venta de información personal y/o de la entidad, Errores del sistema, Intrusiones al sistema, Sabotaje al sistema, Acceso no autorizado al sistema.
No está socializado un plan de continuidad y contingencia. El plan de contingencia no es evaluado ni probado	Naturales	Inundaciones, terremotos, tornados, deslizamientos de tierra, avalanchas, tormentas eléctricas y otros eventos similares
El plan de continuidad del negocio no está socializado. El plan de continuidad no se evalúa.	Ambientales	Fallas prolongadas de energía eléctrica, polución, químicos, dispersión de líquidos.
Falta maquinas trituradoras de papel	Espionaje	La maquinas trituradoras, evita que las personas arrojen documentos importantes con información personal a la basura, que puedan ser usados para crear perfiles de ataque.

3.5. Determinación de probabilidades

Se entiende como la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia.

TABLA DE PROBABILIDAD

Nivel	Descriptor	Descripción	Frecuencia
3	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año
2	Posible	El evento podría ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años

3.6. Análisis de impacto

El paso más importante en la medición del nivel de riesgo es determinar el impacto adverso resultante que una amenaza explote exitosamente una vulnerabilidad.

En sí, el impacto se entiende como las consecuencias que pueden ocasionar a la organización la materialización del riesgo. A continuación, se muestra escala de medida cualitativa estableciendo las categorías y la descripción.

IMPACTO

No.	Rango	Descripción
3	Severo	Si el hecho llegara a presentarse, tendría alto impacto o efectos sobre la entidad (altas pérdidas económicas, alto riesgo la imagen de la entidad, entre otros)
2	Moderado	Si el hecho llegara a presentarse, tendría mediano impacto o efectos sobre la entidad (pérdida moderada, no amenaza la imagen de la entidad, entre otros)
1	Leve	Si el hecho llegara a presentarse, tendría bajo impacto o efectos mínimos sobre la entidad.

3.7. Determinación del alcance

Se determina el área de afectación afectada por la materialización del riesgo.

ALCANCE

No.	Rango	Descripción
3	Global	Eventos que puede afectar transversalmente la ejecución de varios procesos de la entidad
2	Local	Eventos que pueden afectar la ejecución del proceso.
1	Puntual	Eventos que suceden puntualmente y que se pueden tratar dentro de los límites donde se ejecutan las actividades propias del procedimiento.

3.8. Análisis de calificación y valoración del riesgo

Zona de riesgo: Una vez realizado el análisis de riesgo con base a los aspectos de probabilidad, impacto y alcance, se determina la priorización de la zona de riesgo con base en las fórmulas establecidas en la matriz, lo que permite determinar cuáles requieren de un tratamiento inmediato.

ZONA DEL RIESGO

No.	Rango	Descripción
> = 2,5	ALTO	La zona de riesgo supera los límites establecidos en cuanto a impacto y alcance afectando las actividades que realiza la entidad para lo cual se debe reducir, evitar, compartir o transferir el riesgo implementando o estableciendo controles adicionales
> 2,0 a < 2,5	MEDIO	La zona de riesgo se encuentra en los límites permisibles en cuanto a impacto y alcance, para lo cual se debe asumir o reducir el riesgo se materialice implementando los controles adecuados
< = 2,0	BAJO	La zona de riesgo se encuentra dentro de los rangos establecidos por la entidad en cuanto alcance e impacto permitiendo asumir el control del riesgo.

Valoración del Control: la determinación del control existente al interior de los diferentes procesos y procedimientos que se realizan.

VALORACION DEL CONTROL

No.	Rango	Formula
3	INEFECTIVO	El control no existe, o existe, pero no se aplica, o existe y se aplica, pero el mismo no es efectivo.
2	ADECUADO	El Control existe y está en implementación, pero aún no se evidencia su efectividad.
1	EFECTIVO	El control existe y se aplica de manera efectiva, asegurando la no materialización del riesgo

Valoración del Riesgo: la determinación del nivel de riesgo es el resultado de confrontar el impacto y la probabilidad y el alcance con los controles existentes al interior de los diferentes procesos y procedimientos que se realizan. Se debe tener muy claros los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones, estos niveles de riesgos son:

VALORACION DEL RIESGO

No.	Rango	Descripción
> = 6	INACEPTABLE	El control con el que actualmente se cuenta para la mitigación del riesgo no asegura que la materialización del mismo no se presente, por lo cual la entidad debe adelantar las acciones inmediatas con el fin de asegurar la efectividad del control (establecer el control, reevaluarlo, establecer unos nuevos, entre otros).
>3 y <6	MODERADO	El Control existente debe evaluarse mediante auditorias o seguimiento permanente con el fin de garantizar el resultado satisfactorio del proceso mediante la mitigación del riesgo.
<=3	ACEPTABLE	Ya la entidad evaluó el control y se está asegurando el resultado del proceso, el riesgo no se ha materializado y mediante la aplicación de estos controles se puede asegurar que el riesgo es aceptable y se controlará a través de seguimiento de auditorías de gestión y externas por parte de los entes de control.

3.9. Metodología para el tratamiento de riesgos

Una vez se culmina la identificación, valoración y la definición del tratamiento de riesgos, se deben establecer cuáles son los controles o medidas que se van a diseñar, establecer, implementar o mejorar para cada riesgo que no haya quedado en los niveles tolerables o aceptables.

El conjunto de controles que se definen para mitigar los riesgos debe hacer parte de un plan de tratamiento de riesgos corporativo, de tal forma que se pueda traducir dicho plan a proyectos específicos en donde sea posible identificar como mínimo:

- Nombre del proyecto (implementación de control).
- Objetivo.

- Responsable.
- Recursos requeridos (Humanos, Tecnológicos, Servicios, Bienes, etc.).
- Tiempo.
- Inversión.
- Riesgos que mitiga.
- Impactos actuales de los riesgos que mitiga.
- Análisis costo - beneficio de su implementación.
- Tipo de controles involucrados (Prevención, contención, detección, recuperación, reacción, notificación)
- Normatividad interna existente y requerida que apoya la implementación de los controles (Políticas, procedimientos).
- Controles, objetivos de control o procesos de normas del Anexo A de ISO 27001 (Declaración de Aplicabilidad), marcos de gobierno de seguridad o TI, cláusulas de regulaciones que apoya el proyecto
- Nivel de prioridad del proyecto.

Posterior a esto, se deben tomar las medidas adecuadas para hacer frente a los mismos y para ello se dispone de las siguientes opciones:

- La primera opción, **evitar** la acción que da origen al riesgo particular. Se evalúa y determina la viabilidad de si se puede o no evitar el riesgo en la entidad mediante el impacto que esto generaría.
- La segunda opción consiste en **transferir** el riesgo a entidades como aseguradoras o proveedores que puedan gestionar de manera eficaz el riesgo particular, siempre que no resulte un costo superior al del riesgo mismo. Para seleccionar una tercerización de un riesgo se evalúa el costo beneficio; es decir, sea la opción adecuada y económica en su implementación, adicionalmente se debe verificar que el riesgo residual este en los niveles de aceptación de la compañía tras su implementación.
- La tercera alternativa para hacer frente a un riesgo es **asumir o aceptar**. Ello implica que no se van a tomar medidas de protección contra ese riesgo. La decisión ha de ser tomada y firmada por la dirección de la empresa y sólo es viable en el caso de que la organización controle el riesgo y vigile que no aumenta.
- La última opción es **reducir o mitigar** el riesgo. Para ello la empresa debe implantar una serie de medidas que actúen de salvaguarda para los activos. Todas las medidas implantadas han de ser documentadas y gestionadas por la organización.

3.10. Criterios de aceptación del riesgo

La decisión de recibir, reconocer, tolerar o admitir un riesgo, es decisión del Hospital y posterior al estudio de los diferentes escenarios posibles y del establecimiento de los procedimientos posibles para contrarrestar sus efectos y probabilidad de ocurrencia.

Por lo tanto, el Hospital Universitario Hernando Moncaleano Perdomo considera que para la aceptación del riesgo, se deberá tener en cuenta los siguientes elementos de evaluación de impacto y especialmente, cuando éste sea de nivel BAJO (Aceptable):

- Aspectos legales y reglamentarios,
- Operaciones,
- Tecnología,
- Finanzas,
- Factores sociales y humanitarios.

La escala de riesgos definidos serán los niveles Alto, Medio, y Bajo, que representarán el grado o nivel a que se encuentra expuesto el activo de información que está siendo evaluado. También representa las acciones que debe tomar la alta dirección y los responsables del logro de la misión, en cada uno de los niveles como se indica en la siguiente ilustración:

Nivel de riesgo	Descripción del riesgo y acciones necesarias
ALTO (INACEPTABLE)	Requiere fuerte medidas preventivas. Planes de tratamiento implementados en corto tiempo, reportados y controlados con atención directa de la alta dirección de la mano con los líderes de áreas.
MEDIO (MODERADO)	Se requieren acciones preventivas controladas por grupos de manejo de incidentes en un periodo de tiempo razonable.
BAJO (ACEPTABLE)	El propietario del activo lo administra con procedimientos rutinarios o decide aceptar el riesgo.

Los criterios de aceptación de riesgo, establece que el riesgo de nivel “alto” se considera inaceptable y debe ser tratado de forma inmediata con los recursos necesarios requeridos. Así mismo, para el nivel “medio” se considera moderado y deben ser tratados de forma controlada por grupos de manejo de incidentes y riesgo de nivel “bajo” se considera aceptable y se administra con procedimientos rutinarios o se decide aceptar el riesgo.

4. EVALUACIÓN

Matriz de análisis de gestión de riesgos

5. ANEXOS

A continuación, se presenta el esquema a utilizar para el análisis de la gestión de riesgos del área TIC.

ANEXO A. ESQUEMA ANALISIS DE GESTIÓN DE RIESGOS AREA TIC

(0) TIPO DE ACTIVO DE INFORMACION	(1) ACTIVOS INFORMACION	(2) AMENAZA	(3) VULNERABILIDAD (CAUSA)	(4) RIESGO	(5) FRECUENCIA	(6) IMPACTO	(7) ALCANCE	(8) CALIFICACION (5+6+7)	(9) ZONA DE RIESGO

ACCIONES DE CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLES	(10) VALORACION DEL CONTROL	(11) RIESGO Vs. CONTROL	(12) VALORACION DEL RIESGO	(16) TRATAMIENTO DE RIESGO	(17) ACCION DE CONTROL PROPUESTA	(18) EFICACIA DEL CONTROL ESPERADA	(19) COSTO DE LA IMPLEMENTACION ($)

(20) TIEMPO ESTIMADO DE LA IMPLEMENTACION	(21) RESPONSABLE DEL CONTROL	(22) PRIORIZACION DE LA IMPLEMENTACION	(23) ESTADO DE IMPLEMENTACION	(24) FRECUENCIA RESIDUAL	(25) IMPACTO RESIDUAL	(26) ALCANCE RESIDUAL	(27) CALIFICACION (24+25+26)		SEGUIMIENTO EFICACIA

6. CUADRO DE CONTROL DE RESPONSABILIDADES

ELABORÓ	REVISÓ	APROBÓ
NOMBRE: Alejandro Polania Cárdenas	**NOMBRE:** Marleny Quesada Losada	**NOMBRE:** Jesús Antonio Castro Vargas
CARGO: Jefe Oficina Asesora Sistemas De Información	**CARGO:** Jefe oficina de Planeación, Calidad y Desarrollo Institucional	**CARGO:** Gerente E.S. E
FECHA: Diciembre 2019	**FECHA: Diciembre 2019**	**FECHA: Diciembre 2019**

7. CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS
01	JULIO 2018	Emisión de los documentos
02	DICIEMBRE 2019	Se realiza la actualización del plan de tratamiento de riesgos incluyendo los activos de información además se establece la criticidad.