HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E.

ACREDITACION EN SALUD

¡Trabajamos por mi Nariño,
tu salud,
nuestro compromiso!

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

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E.

2024

TABLA DE CONTENIDO

1 INTRODUCCIÓN 4
2 OBJETIVO 5
3 PROCEDIMIENTO GESTION DE RIESGOS DE SEGUR. PRIVA. DE LA INFORMACION 5
4 MATRIZ DE RIESGOS INSTITUCIONAL 5
5 INDICADORES 10
6 EJECUCIÓN 10
7 MONITOREO 10
8 MEJORAMIENTO CONTINUO 11
CONTROL DE CAMBIOS 12

INDICE DE TABLAS

Tabla 1 Riesgos de Proceso_____ 6
Tabla 2 Riesgos Anticorrupción_____ 6
Tabla 3 Riesgos de sistemas de información_____ 6
Tabla 4 Riesgos de seguridad y salud en el trabajo_____ 7
Tabla 5 Matriz de Riesgos Institucional_____ 8

1. INTRODUCCIÓN

Toda información que maneja una entidad pública es muy importante para la relación con el ciudadano, por lo tanto, el resguardo de todo tipo de información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de una Entidad.

Teniendo en cuenta lo anterior dentro del Modelo de Seguridad y Privacidad de la información (MSPI), la Gestión de riesgos se convierte en un tema decisivo y por otra parte se tiene la metodología presentada en la "Guía para la administración del riesgos y el diseño de controles en entidades públicas" versión 7 de noviembre 2020 del DAFP, a parte de esta guía la oficina de Gestión de la Información se permite presentar la Metodología de Análisis y Gestión de Riesgos de Sistemas de Información MAGERIT – V3, siempre buscando que haya una integración y de este modo aprovechar el trabajo adelantado en la identificación de Riesgos para ser complementados con los Riesgos de Seguridad y Privacidad de la Información.

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación de la Confidencialidad, Integridad y Disponibilidad.

2. OBJETIVO

Establecer de manera interna un reglamento que permita identificar, medir, controlar, monitorear y comunicar toda clase de riesgos relacionados con la seguridad y privacidad de la información y que de alguna manera interfieren en el cumplimiento de los objetivos estratégicos.

3. PROCEDIMIENTO PARA LA GESTION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Con lo relacionado al procedimiento para la gestión de riesgos asociados a la seguridad y privacidad de la información, la organización ha adelantado estos pasos y ha logrado establecer dicho procedimiento el cual se encuentra aprobado por el SIG con el código PRGES-011 V04 GESTIÓN INTEGRAL DEL RIESGO del 26 de Octubre de 2018 y su última actualización del 4 de diciembre de 2023, el cual se encuentra vigente y tiene como objetivo "Establecer la metodología para la gestión integral de los riesgos del HUDN, en cuanto a su identificación, análisis, valoración y tratamiento y para la identificación de las oportunidades de los Sistemas de Gestión". Dentro de dicho procedimiento se ha establecido como alcance el siguiente "Aplica para la gestión de riesgos y oportunidades del SGC, SGSST, SST y SGA, y para la gestión de riesgos de Seguridad de la Información y de Anticorrupción en todos los procesos del HUDN".

Como se puede observar el procedimiento establecido y vigente abarca los riesgos asociados a la Seguridad y privacidad de la información.

4. MATRIZ DE RIESGOS INSTITUCIONAL

La organización ha establecido un procedimiento para la gestión integral del riesgo y como producto de su aplicación ha elaborado la matriz de riesgos institucional, la cual se encuentra identificada dentro de la página web institucional en la siguiente ruta

https://www.hosdenar.gov.co/index.php/transparencia/matriz-de-riesgo-institucional/matrices-de-riesgo-institucional-actualizadas/, con fecha de aprobación del 26 de octubre de 2018 y su última actualización del 1 de marzo de 2023, y se encuentra vigente. La matriz Mapa de riesgos GEST INFOR muestra el consolidado de los riesgos del proceso de Gestión de Información, clasificados así:

Tabla 1: Riesgos de Proceso

ITEM	RIESGO DE PROCESO
1	Incumplimiento de actividades programadas en el Plan Estratégico de Tecnologías de la Información (PETI).
2	Ausencia de suministros técnicos.
3	Caída del sistema de información DGH.
4	Afectación del rack de comunicaciones por fenómenos naturales.
5	Incumplimiento en la entrega de desarrollos de software propios del hospital
6	Perdida de información.
7	Documentos que ingresan a la unidad de correspondencia incompletos o no digitalizados
8	Duplicidad en el número de historia clínica según consecutivo o varios pacientes
9	Desalineación del PETI con la estrategia.

Tabla 2: Riesgos Anticorrupción

ITEM	RIESGO ANTICORRUPCIÓN
1	Pliegos de condiciones hechos a la medida.
2	Tráfico de influencias.
3	Designar supervisores que no cuentan con conocimientos suficientes para desempeñar la función.

Tabla 3: Riesgos de sistemas de información

ITEM	RIESGOS DE SISTEMAS DE INFORMACIÓN
1	Daño por agua o polvo en servidor de cuarto de Urgencias.
2	Colapso estructural por movimiento sísmico que pueda causar daño en los servidores.
3	Espionaje remoto de bases de datos de historias clínicas y financiera.

4	Hurto de servidores en finanzas y sistemas cuarto piso.
5	Hurto de servidores primero, cuarto y quinto.
6	Pérdida de información vital para la operación del negocio.
7	Incumplimiento en la disponibilidad del personal de soporte.

Tabla 4: Riesgos de seguridad y salud en el trabajo

ITEM	RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO
1	Trabajo en Espacios confinados en cuarto de comunicaciones y cielo falso.
2	Posturas prolongadas sedentes.
3	Movimientos repetitivos.
4	Riesgo eléctrico (baja tensión).
5	Mecánico.
6	Manejo de cargas livianas: Hombres: <ó=25kg y Mujeres: <ó= 12.5kg
7	Ejecución de actividades con posibilidad de ser golpeado, atrapado por objetos que caen o en movimiento.
8	Utilizar herramientas corto punzante.
9	Exposición sustancias químicas no peligrosas.
10	Presencia de microorganismos en el ambiente laboral.
11	Falta de Iluminación.

Para un total de 30 Riesgos identificados para el proceso de Gestión de Información.

Para efectos del presente Plan de Tratamiento de Riesgos tomamos los seis (6) riesgos de gestión de la información y haciendo énfasis en estos riesgos que implican un riesgo potencial para Gestión de la información, en la Matriz mapa de riesgo GEST INFOR no se tuvo en cuenta el % de riesgo o Zona de riesgo Inherente, se tiene en cuenta todos los riesgos asociados a Gestión de la Información.

Tabla 5: Matriz de Riesgos Institucional

Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de impacto	Impacto Inherente	%	Zona de Riesgo Inherente	Atributos: Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento	Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado
1	Reputacional	Incumplimiento de actividades programadas en el Plan Estratégico de Tecnologías de la Información (PETI)	1. Desconocimiento del PETI 2. Priorización de otras actividades fuera del plan 3. Cambios en los turnos laborales en todas las áreas del hospital.	Posibilidad de pérdida Reputacional por incumplimiento de actividades programadas en el Plan Estratégico de Tecnologías de la Información (PETI), debido a desconocimiento del mismo, priorización de otras actividades fuera del plan , cambios en los turnos laborales en todas las áreas del hospital.	Ejecucion y Administracion de procesos	2	Muy Baja	20%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	Menor	40%	Bajo	Preventivo	Manual	40%	Documentado	Aleatoria	Con Registro	Muy Baja	12%	Menor	40%	Bajo	Aceptar	Mantener controles que se vienen trabajando	Coordinador de GI	1/01/2023	31/12/2023		En curso
2	Económico y Reputacional	Ausencia de suministros tecnicos	1. Falta de asignación de presupuesto 2. Ausencia de planeación del plan anual de adquisiciones (PAA)	Posibilidad de pérdida Económica y Reputacional por ausencia de suministros tecnicos, debido a falta de asignación de presupuesto y ausencia de planeación del plan anual de adquisiciones (PAA)	Ejecucion y Administracion de procesos	2	Muy Baja	20%	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	Probabilidad	Preventivo	Manual	40%	Documentado	Aleatoria	Con Registro	Muy Baja	12%	Moderado	60%	Moderado	Aceptar	Mantener controles que se vienen trabajando	Coordinador de GI	1/01/2023	31/12/2023		En curso
3	Económico y Reputacional	Caída del sistema de información DGH	1. Destinación presupuestal 2. Fallas de fluido eléctrico.	Posibilidad de pérdida Económica y Reputacional por caída del sistema de información DGH, debido a destinación presupuestal y fallas de fluido eléctrico.	Ejecucion y Administracion de procesos	60	Media	60%	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	Probabilidad	Preventivo	Manual	40%	Documentado	Aleatoria	Con Registro	Baja	36%	Moderado	60%	Moderado	Aceptar	Mantener controles que se vienen trabajando	Coordinador de GI	1/01/2023	31/12/2023		En curso
4	Económico y Reputacional	Afectación del rack de comunicaciones por fenómenos naturales	1. Inundaciones 2. Incendios 3. Fenómenos volcánicos 4. Terremotos	Posibilidad de pérdida Económica y Reputacional por afectación del rack de comunicaciones por fenómenos naturales, debido a inundaciones, incendios, fenómenos volcánicos y terremotos.	Ejecucion y Administracion de procesos	2	Muy Baja	20%	Mayor a 500 SMLMV	Catastrófico	100%	Extremo	Probabilidad	Preventivo	Manual	40%	Documentado	Aleatoria	Con Registro	Muy Baja	12%	Catastrófico	100%	Extremo	Reducir (mitigar)	Realizar solicitud de implementación de backup externo o cluster en la nube y rack de comunicaciones sea antisísmico.	Coordinador de GI	1/01/2023	31/12/2023		En curso
5	Económico y Reputacional	Incumplimiento en la entrega de desarrollos de software propios del hospital	1. Falta de planeación en el cronograma de actividades 2. Insuficiencia en la priorización del cronograma de desarrollo de software de alto impacto en la organización	Posibilidad de pérdida Económica y Reputacional por incumplimiento en la entrega de desarrollos de software propios del hospital, debido a la falta de planeación en el cronograma de actividades e insuficiencia en la priorización del cronograma de desarrollo de software de alto impacto en la organización	Ejecucion y Administracion de procesos	20	Baja	40%	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	Probabilidad	Detectivo	Manual	30%	Documentado	Continua	Con Registro	Baja	28%	Moderado	60%	Moderado	Aceptar	Mantener controles que se vienen trabajando	Coordinador de GI	1/01/2023	31/12/2023		En curso

Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de impacto	Impacto Inherente	%	Zona de Riesgo Inherente	Afectación	Atributos						Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento	Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado
														Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia												
6	Económico y Reputacional	Perdida de información	1.Error humano 2. Falla eléctrica 3.Falla del sistema	Posibilidad de pérdida Económica y Reputacional por perdida de información, debido a errores humanos, fallas eléctricas y del sistema.	Ejecucion y Administracion de procesos	2	Muy Baja	20%	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Muy Baja	12%	Moderado	60%	Moderado	Reducir (mitigar)	Mantener controles que se vienen trabajando	Coordinador de GI	1/01/2023	31/12/2023		En curso
													Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Muy Baja	7%	Moderado	60%	Moderado	Aceptar	Mantener controles que se vienen trabajando	Coordinador de GI	1/01/2023	31/12/2023		En curso

5. INDICADORES

Como se observa en la tabla anterior por cada riesgo y por cada control propuesto se han fijado indicadores individuales, pero a nivel general es pertinente establecer un indicador que agrupe todas las actividades el cual quedaría de la siguiente manera y sirve para medir la eficacia en la ejecución del plan:

$$ICA = \frac{\text{No. de Actividades cumplidas}}{\text{No. de actividades programadas}} * 100$$

Donde ICA es el Índice de Cumplimiento de Actividades

6. EJECUCIÓN

La ejecución consiste en llevar a cabo la implementación de los controles propuestos en el cuadro anterior, procurando que se realicen dentro de los tiempos establecidos y sean desarrolladas por los responsables asignados.

Para poder llevar a cabo con éxito la ejecución es importante recalcar el compromiso de la Alta y Media dirección para asignar los recursos económicos necesarios a las actividades que así lo requieran.

7. MONITOREO

Le corresponde a la organización y a cada una de las tres líneas de defensa que establece MIPG hacer un seguimiento al presente plan para determinar su efectividad, para lo cual debe realizar las siguientes actividades:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.

- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

8. MEJORAMIENTO CONTINUO

Es responsabilidad de la organización dar garantía para la mejora continua en la gestión de riesgos en este caso de los asociados a la seguridad y privacidad de la información, teniendo en cuenta lo anterior se debe fijar cuando haya hallazgos, falencias o incidentes de seguridad y privacidad de la información se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos, por otra parte es importante que la organización establezca y haga frente a las consecuencias que se derivan de lo que llegó a materializarse.

Deben definirse las acciones para mejorar continuamente la gestión de riesgos de seguridad y privacidad de la información de la siguiente manera:

- Revisar y evaluar los hallazgos encontrados en los informes de los entes de control.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad o de los servicios que presta al ciudadano.
- Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

CONTROL DE CAMBIOS

E: Elaboración del documento.

M: Modificación de del documento

X: Eliminación del documento

VERSIÓN	CONTROL DE CAMBIOS AL DOCUMENTO	INFORMACIÓN DE CAMBIOS					ACTO ADMINISTRATIVO/NORMA DE ADOPCIÓN
		E	M	X	Actividades o Justificación	Elaboró / Actualizó	
V-01	Plan - TRSPI	X			Se modifica el documento en todos sus numerales y tablas	ROBERTO E FREIRE BURBANO	Decreto 612/2018, Ley 1474/2011 Art. 74
V-02	Plan - TRSPI		X		Se modifica la matriz de riesgos de proceso, se ajusta la tabla 3.	ROBERTO E FREIRE BURBANO	Decreto 612/2018, Ley 1474/2011 Art. 74

Realizo

ROBERTO EDUARDO FREIRE BURBANO
Ing. Sistemas Esp.
HUDN - 2023

Reviso

HENRY LUIS RODRIGUEZ CARDENAS
Coordinador Gestión de Información