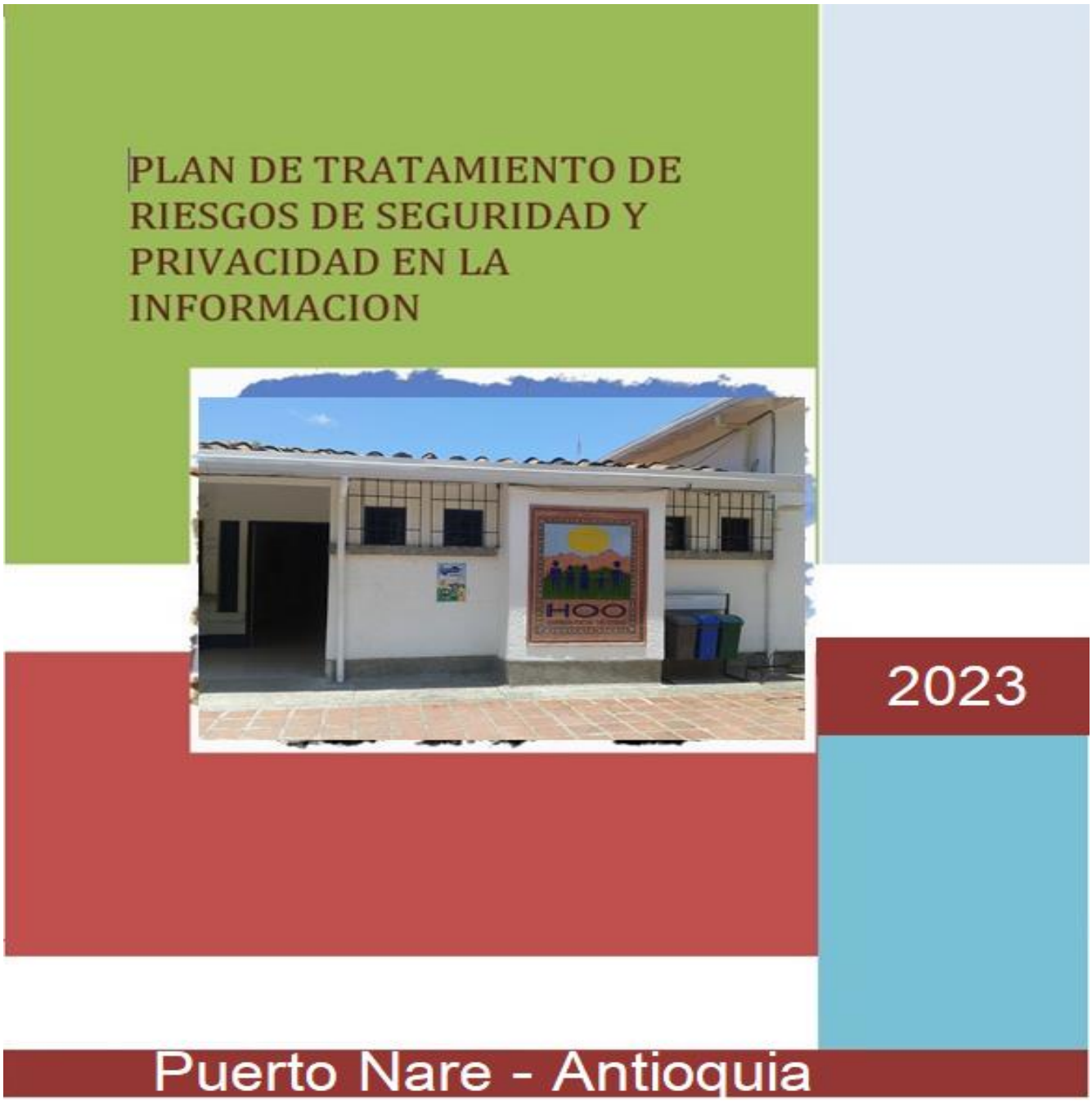
ESE HOSPITAL OCTAVIO OLIVARES PUERTO NARE - ANTIOQUIA



ELABORÓ: **Jeisson Palacio**	REVISÓ: **Leonor Avendaño**	APROBÓ: **Ciro Gómez**
CARGO: **Asesor Informático**	CARGO: **Asesor Calidad**	CARGO: **Gerente**
FECHA: **enero de 2023**	FECHA: **enero de 2023**	FECHA: **enero de 2023**

Datos de Contacto:

Institución	ESE HOSPITAL OCTAVIO OLIVARES
NIT	890.985.810-5
Gerente	Ciro Gómez Barrios
Preparado por	Ing. Jeisson Alberto Palacio Diaz
Conmutador	5905935 EXT 2006
Fax	
Código	05585
Correo Notificaciones Judiciales	josellinas70@gmail.com
Correo contacto y PQRD	siauhoo@gmail.com
Sitio Web	www.hospitalhoo.gov.co
Horario de Atención al Público	Salud urgencias 24 horas continua Administrativo Lunes a sábado 8:00 am a 12:00 pm y de 2:00 pm a 5:00 pm
Dirección	Calle 5 N.º 45-103 Fondo Obrero

1. RESUMEN EJECUTIVO

Mediante la definición del Plan de Tratamiento de Riesgos la **ESE Hospital Octavio Olivares de Puerto Nare**, busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad, Perdida de Integridad y Perdida de Disponibilidad), en la información digital, evitando aquellas situaciones que impidan el logro Estratégicos delHospital.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes en los activos de información delHospital, estas acciones son organizadas en forma de medias de seguridad denominados controles, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

Las anteriores medidas se definen teniendo en cuenta la información del análisis de riesgos, sobre la plataforma informática y las necesidades del Proceso de Gestión de laInfraestructura de TIC del Hospital, en cuanto a la seguridad de la información yproporciona las herramientas necesarias para definir cada una de las características delas medidas y la definición de los pasos a seguir para su ejecución.

El presente plan se realiza con el objeto de dar a conocer cómo se desarrollará la implementación y socialización del componente de la Estrategia en **seguridad y privacidad dela información**, el cual busca guardar los datos de los usuarios como un tesoro, garantizando la seguridad de la información.

2. INTRODUCCIÓN

La Seguridad de la Información, según ISO 27001, describe la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan; hoy en día la gran mayoría de las entidades cuenta con un sistema de información y reconoce la importancia que esta tiene para su funcionamiento y como esta debe estar adecuadamente identificada y protegida.

La E.S.E Hospital Octavio Olivares, es una entidad proveedora de gran cantidad de información tanto magnética como física, la cual se encuentra en continuo procesamiento para el reporte de diferentes informes tanto internos como externos, hecho que implica un riesgo a la negligente manipulación de la información o a la perdida de la misma, lo que podría traer problemas económicos, legales y/o administrativos por lo cual este documento busca establecer una línea de trabajo que permita a la entidad sortear los riesgos a la cual está expuesta y lograr que su información este segura.

Por lo anterior es fundamental que la E.S.E Octavio Olivares de Puerto Nare, vincule el plan de tratamiento de riesgos de seguridad y privacidad de la información en cumplimiento al decreto 612 de 2018, como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible

3. DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información, en beneficiode unificar criterios dentro de la Agencia.

- **Acceso a la Información Pública:** Derecho fundamental definido como la facultad que tienen todas las personas de conocer sobre la existencia y accedera la información pública en custodia 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/IEC27000).

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere,obtenga, adquiera, transforme o controlar en su calidad de tal.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel ordenpara servir como testimonio e información a la persona o institución que los produce y a los usuarios, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, lainformación, la investigación y la cultura. (Ley 594 de 2000, art 3).

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

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo ydeterminar el nivel de riesgo. (ISO/IEC 27000).

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

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los usuarios, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivelde riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **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 usuario, 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).

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- **Declaración de Aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vidapersonal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- **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).

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia deun sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las

circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.(Ley 1712 de 2014, art 6).

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de latotalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.(Ley 1712 de 2014, art 6).

- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **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 dela 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 de proteger dicha información en observancia del marco legal vigente.

- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **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).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o 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).
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).
- **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).

4. OBJETIVOS

a. Objetivo General

- Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en la ESE Hospital Octavio Olivares de Puerto Nare, con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

b. Objetivos Específicos

1. Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana en materia de seguridad de la información.
2. Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital, de acuerdo con los contextos establecidos en la Entidad.
3. Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital.
4. 4. Alinear el Plan de Desarrollo Municipal, Plan de Desarrollo de la ESE Hospital Octavio Olivares de Puerto Nare y Plan de Seguridad y Privacidad del Hospital con este plan de tratamiento de riesgos.
5. Emplear un enfoque de sistemas para planificar, implementar, monitorizar y gestionar los riesgos de seguridad digital.

5. RECURSOS

- **Humano**: Gerente, subdirector Administrativo, Líderes del Proceso, Profesionales de Sistema y Tecnología, Personal Externo.
- **Físico:** Firewall, PC y equipos de comunicación
- **Financieros**: $00.000.000 (Millones)

6. RESPONSABLES

- Gerentes
- Subdirector Adm
- Líderes del Proceso
- Profesionales de Sistema y Tecnología

7. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la ESE Hospital Octavio Olivares de Puerto Nare, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – Min TIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar

8. ACTIVIDADES

1. Realizar Diagnóstico

2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información

3. Realizar la Identificación de los Riesgos con los líderes del Proceso.

4. Entrevistar con los líderes del Proceso.

5. Valorar del riesgo y del riesgo residual

6. Realizar Mapas de calor donde se ubican los riesgos

7. Plantear al plan de tratamiento del riesgo aprobado por los líderes.

9. MARCO REFERENCIAL POLÍTICA DE ADMINISTRACION DE RIESGOS

El Hospital Octavio Olivares a través de su Modelo de Seguridad y Privacidad, se compromete a mantener una cultura de la gestión del riesgo digital, con un enfoque basado en los riesgos de seguridad digital en los procesos y proyectos luchando continuamente contra la corrupción, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de los de seguridad y privacidad de la Información y Seguridad Digital de manera Integral. La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores del Hospital. Se deben tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

• Evitar: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo del activo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de archivos se retiran los permisos de acceso.

• Prevenir: corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las

inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos.

• Reducir o mitigar: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo.

• Dispersar: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos.

• Compartir: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros.

10. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por la ESE Hospital Octavio Olivares de Puerto Nare

a. Revisión y/o Modificación de la actual Política de Seguridad
b. Aspectos organizativos de la seguridad de la información
c. Seguridad Ligada a los recursos humanos
d. Revisión del Control de acceso
e. Seguridad en la operatividad
f. Seguridad en las telecomunicaciones
g. Gestión de Incidentes de Seguridad de la Información
h. Aspectos de seguridad de la información en la gestión de continuidad de la ESE Hospital Octavio Olivares.

11. CRONOGRAMA

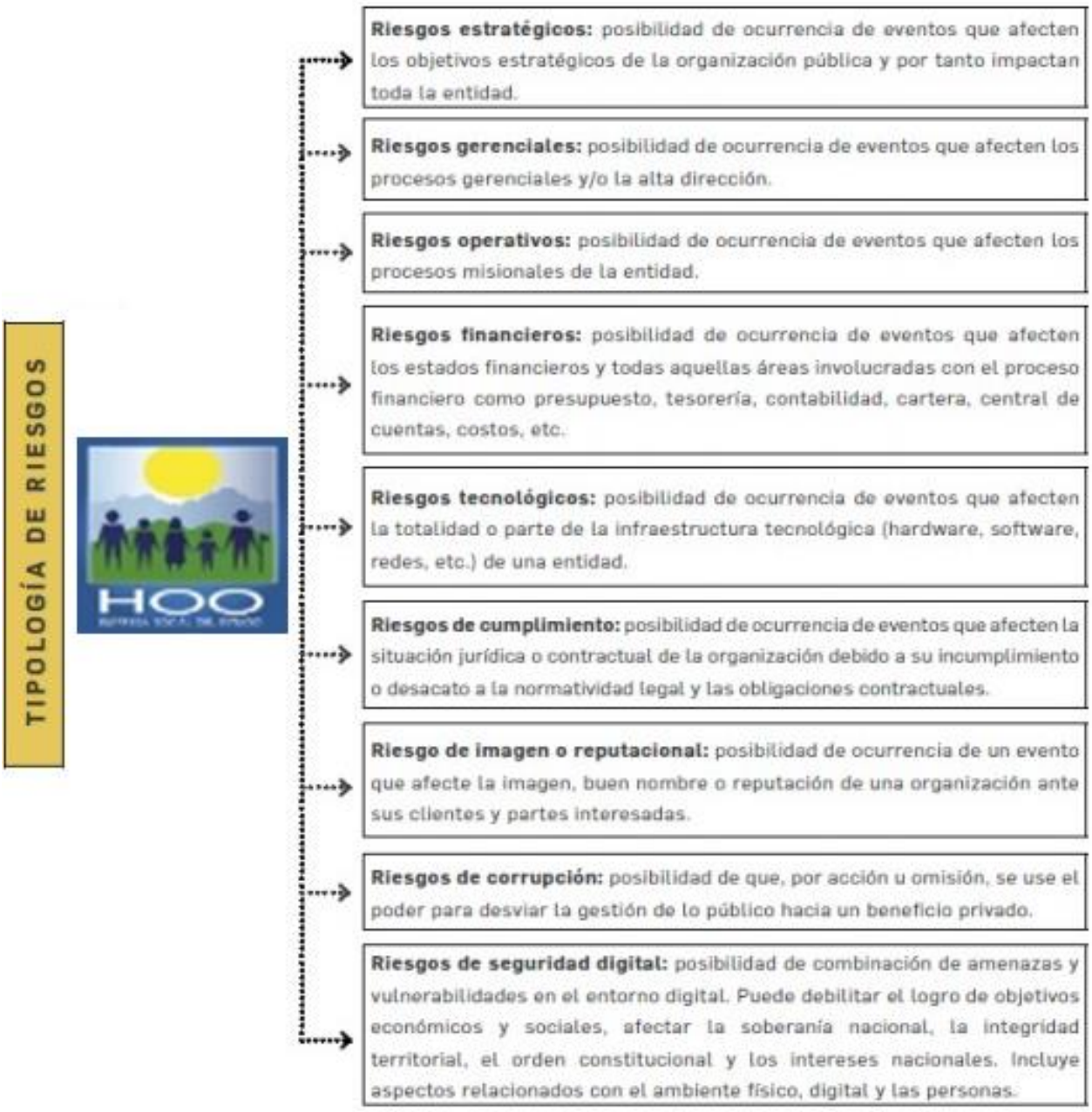
El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de información de los diferentes procesos de la ESE Hospital Octavio Olivares de Puerto Nare, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del Hospital.

FECHA	ACTIVIDADES	RESPONSABLE	FECHA DE INICIO	FECHA FIN
Fase 1 Planeación de la gestión del Riesgo.	Revisar y ajustar metodología para la gestión de Riesgo de Seguridad Digital acorde a las necesidades del HGM. Revisión Guía de Gestión de Riesgos de Seguridad Digital HGM.	Equipo Sistemas	Enero 2023	Marzo 2023
Fase 2 Identificación y valoración de Activos.	Identificación de Activos de Información. Clasificación de Activos de Información. Valoración de Activos de Información.	Equipo Sistemas	Marzo 2023	Abril 2023
Fase 3 Identificación de Amenazas y Vulnerabilidades	Identificación de Amenazas y Vulnerabilidades	Equipo Sistemas	Mayo 2023	Mayo 2023
Fase 4 Determinación de Riesgos	Determinación del Impactos de las amenazas por activo Determinación de Probabilidad de Ocurrencia por	Equipo Sistemas	Junio 2023	Junio 2023
Fase 5 Análisis de Riesgos	Cálculo de Riesgos Identificación de Riesgos superiores al NRA	Equipo Sistemas	Julio 2023	Julio 2023
Fase 6 Gestión de Riesgos	Determinación de Controles Tratamiento de Riesgos Diseño de controles. Priorización de Controles	Equipo Sistemas	Agosto 2023	Agosto 2023
Fase 7 Planificación de controles	Implementación de Controles que no requieren recursos. Planificación de Controles (Presupuesto próximo año).	Equipo Sistemas y áreas responsables	Septiembre 2023	Septiembre 2023
Fase 8 Monitoreo	Medición de la eficacia de los controles	Equipo Sistemas y áreas responsables	Octubre 2023	Diciembre 2023

Los controles seleccionados serán confrontados con los establecidos en el Anexo A del estándar ISO 27001:2013 como pilar fundamental del Modelo de Seguridad y Privacidad del Hospital.

12. IDENTIFIACACION DEL RIESGO

Se identifica los tipos de riesgo y su magnitud con la que pueden afectar a la seguridad y privacidad de la información. Los tipos de riesgo se nombran a continuación.


TIPOLOGÍA DE RIESGOS
Riesgos estratégicos: posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
Riesgos gerenciales: posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
Riesgos operativos: posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
Riesgos financieros: posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
Riesgos tecnológicos: posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
Riesgos de cumplimiento: posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
Riesgo de imagen o reputacional: posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
Riesgos de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Riesgos de seguridad digital: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

13. PLAN DE INTERPRETACION

Infraestructura Data Center

Es el sitio principal donde se encuentran ubicados los equipos de plataforma de IT que apoya el core del negocio, es de vital importancia ejecutar las siguientes mejoras:

- ✓ La data center se encuentra en estado deficiente, es necesario realizar reubicación de Rack, este ítem se refiere a que el rack que contiene los equipos está ubicado de costado y afecta el acceso a los equipos.

Impacto de la mejora:

- ✓ Al reorganizar el rack y reubicarlo les permite un mejor acceso a los equipos, minimizando errores al momento de dar soporte.
- ✓ Mejora la circulación de aire frio evitando fallos por incremento de temperatura.

INFRAESTRUCTURA TI

Servidor

La infraestructura actual de servidores en el Hospital consta de:

1 servidores HP Proliant ML110 Generación 9, ubicados en el rack.

- ✓ Servidor de Aplicación.
- ✓ Servidor de Base de Datos.

El equipo tiene varios riesgos tecnológicos y que deben ser mitigados:

- ✓ Obsolescencia Tecnológica
- ✓ Falta de garantía ante el fabricante
- ✓ Combinación de roles

Para mitigar dichos riesgos se propone una actualización adquiriendo nuevos equipos y determinando que los equipos anteriores serán usados para la implementación de un plan DRP (Plan de recuperación a desastres) como plataforma de respaldo ante alguna falla física, electrónica o desastre.

Se propone la adquisición de un servidor con las siguientes características:

- Procesador XEON Decacore
- Memoria de 64 Gigas
- Tarjeta controladora de Disco Smart de 512 o superior.
- Discos para sistema operativo de 300 Gigas 7.2 RPM
- Discos de 1.2 Teras de 10k RPM en RAID 5

Se propone la adquisición de equipos de almacenamiento y seguridad perimetral con las siguientes características:

- ✓ NAS Buffalo de 8 Teras
- ✓ PFSENSE Firewall

Impacto de la mejora:

- ✓ Al ser equipos nuevos se cuenta con garantía de fabricante a 2 años, minimizando los costos de reparación y soporte.
- ✓ Mejoran los tiempos de procesamiento de aplicaciones en el hospital, redundando en una mejor calidad de servicio a los usuarios finales.
- ✓ Minimiza los tiempos de soporte, ya que se reducen los fallos por obsolescencia. El hospital puede crecer en nuevas aplicaciones o procesos, al contar con una buena infraestructura de servidores.
- ✓ Al contar con una solución de recuperación de desastres, se minimiza el tiempo de no-disponibilidad de los servicios informáticos del hospital, redundando en una buena imagen para el hospital.
- ✓ Al contar con una NAS en la red del hospital, tendrán acceso rápido a datos respaldados, confiabilidad en la información debido a que el software de respaldo es de muy buena calidad en el proceso de copiado.
- ✓ Al contar con un firewall en la red, se tendrá protección perimetral desde y hacia internet de todos y cada uno de los usuarios del hospital que estén permitidos a usar los recursos de red, esto le permitirá al hospital minimizar los riesgos de pérdida de información.

Redes & Telecomunicaciones

La infraestructura actual de redes y telecomunicaciones en el Hospital consta de: Dichos equipos tienen varios riesgos tecnológicos y que deben ser mitigados:

- ✓ Obsolescencia Tecnológica
- ✓ Falta de garantía ante el fabricante
- ✓ Puertos Dañados
- ✓ Falta de capacidad para gestión remota
- ✓ Hubs instaladados en los puestos de trabajo

Para mitigar dichos riesgos se propone una actualización adquiriendo nuevos equipos y determinando que los equipos anteriores serán usados para la implementación de un plan DRP (Plan de recuperación a desastres) como plataforma de respaldo ante alguna falla física, electrónica o desastre.

Se proponen equipos de red con las siguientes características:

1. 3 switches L2 (capa 2) administrables de 48 puertos y 4 puertos SFP
2. Servicios de VLAN
3. Servicios de bloqueo de puertos
4. Servicios de Fail-Over

Impacto de la mejora:

- ✓ Al ser equipos nuevos se cuenta con garantía de fabricante a 2 años, minimizando los costos de reparación y soporte.
- ✓ Mejoran los tiempos de respuesta de las aplicaciones en el hospital, redundando en una mejor calidad de servicio a los usuarios finales.
- ✓ Minimiza los tiempos de soporte, ya que se reducen los fallos por obsolescencia.
- ✓ El hospital puede crecer en nuevas aplicaciones o procesos, al contar con una buena infraestructura de Redes.
- ✓ Permite centralizar todos los equipos de red en un solo sitio, minimizando los tiempo de soporte por fallos en la red.
- ✓ Se incrementan los niveles de seguridad lógica, tanto de los equipos mismo como los datos de usuarios y aplicaciones.
- ✓ Se eliminan los puntos de fallo por equipos instalados en cascada, al no generarse colisiones de datos en la red, obteniendo un mejor desempeño en la red.
- ✓ Seguridad Electrónica CCTV

El hospital cuenta actualmente con seguridad electrónica y se propone hacer ajustes en algunos puntos muertos adquiriendo cámaras para mejor protección, además de reubicar unas cuentas que no están cumpliendo con buenas normas.

Impacto de la mejora:

- ✓ Mejora toda la disposición de la red de cámaras.
- ✓ Minimiza los tiempos soporte ante fallos de la red.
- ✓ Al cubrir puntos muertos mejora el cubrimiento de seguridad en el hospital.
- ✓ Permite identificar a todo el personal interno y ajeno del hospital por contar con cámaras de mejor calidad de imagen.

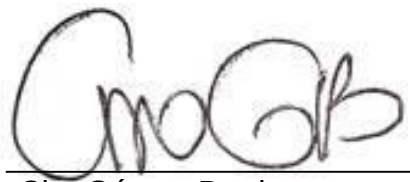
Aprobación.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Versión 2 de la vigencia 2023 de la E.S.E. HOSPITAL OCTAVIO OLIVARES DE PUERTO NARE, fue aprobado por la Asesora de Calidad y la Gerencia, el día 29 de enero de 2023 dando cumplimiento a la Ley de transparencia y acceso a la información pública, este será publicado en la respectiva página web.

14. SEGUIMIENTO Y EVALUACIÓN

Al finalizar cada etapa se realizará una reunión con la Oficina de Control Interno para presentar el informe del avance del proyecto y de esta manera evaluar todos los pasos se han ido realizado.

Jeisson Alberto Palacio Diaz
Ingeniero en Sistemas
ESE Hospital Octavio Olivares
Puerto Nare



Ciro Gómez Barrios
Gerente General
ESE Hospital Octavio Olivares