PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION VIGENCIA 2026

PLA-GIN-05

INTRODUCCION

Para El HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DEL VALLE E.S.E y con base en lo estipulado en la guía de gestión de riesgos de MINTIC, la gestión de los riesgos es un método sistemático que permite establecer a las entidades sean públicas o privadas, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos en función de la tecnología, equipos, infraestructura etc., asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

La entidad es consciente de que todo el equipo humano del HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DEL VALLE E.S.E, en cumplimiento de sus funciones, está expuesto a riesgos, por lo tanto, se hace necesario establecer una estructura y metodología en conjunto con lo dictaminado por el Ministerio de las TIC´s, para identificar las causas y consecuencias evitando la materialización de los eventos detectados, teniendo como fin la seguridad de la información bajo los principios de Integridad, Disponibilidad y Confidencialidad de la información.

Por lo anterior y dando cumplimiento a las políticas de seguridad y privacidad de la información se define este documento como el conjunto de actividades que se deben gestionar para dar el correcto tratamiento a los riesgos que la entidad tiene frente a la gestión tecnológica de toda su infraestructura y la información, alineando todo a la ISO 27005 como guía metodológica de la aplicación de las actividades gestión de riesgos.

1. OBJETIVO

Establecer la estructura metodológica para la administración de riesgos en el HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DEL VALLE E.S.E. Así como definir y ejecutar las acciones requeridas para generar una conciencia preventiva e integral en el tratamiento de los riesgos de Seguridad y Privacidad de la Información en la entidad, lo anterior manteniendo la protección de la integridad, confidencialidad y disponibilidad de la información.

2. ALCANCE

El presente documento está enfocado en mejorar la estrategia para el análisis, diseño, ejecución y control de los riesgos, generados en las actividades cotidianas por el uso frecuente de información en el HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DEL VALLE E.S.E.

La mitigación de los riesgos como debe ser establecida bajo un proceso estructurado y sistemático es por ello que esta guía contiene desde la definición de los roles y responsabilidades hasta los formatos que deben ser diligenciados en el proceso de identificación, y aplica a todas las dependencias y procesos de la entidad.

3. CONDICIONES GENERALES

No aplican condiciones generales al plan

4. TÉRMINOS Y DEFINICIONES

Acciones asociadas: son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
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 (análisis del riesgo inherente).
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.
Contexto estratégico: son las condiciones internas y del entorno, que pueden generar eventos que originen oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
Control: acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
Control preventivo: acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
Control correctivo: acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
Debilidad: situación interna que la entidad puede controlar y que puede afectar su operación.
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 identificados.
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
Opciones de manejo: posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
Plan de contingencia: conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
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 de corrupción: posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
Riesgo inherente: es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
Riesgo institucional: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

- Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
- Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
- Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
- Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción serán considerados como riesgos de tipo institucional.

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 necesario.

5. MARCO LEGAL

Constitución Política de Colombia. Artículos 15, 209 y 269.
Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las empresas de certificación y se dictan otras disposiciones.
Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
CONPES 3995 DE 2019. Política nacional de confianza y seguridad digital.

6. DESCRIPCION (DESARROLLO DEL PLAN)

6.1 ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACION DEL RIESGO

El éxito de la administración del riesgo depende de diversos factores, aun así, la participación de la alta dirección en este caso los líderes de los procesos del Hospital, permite que el proceso se desarrolle con mayor fluidez y efectividad es por ello que en la identificación de los roles no solo se observa el equipo técnico que hará las labores de análisis y tratamiento del riesgo.

- Gerente General: aprueba las directrices para la administración del riesgo en la Entidad.
- Directores de los procesos: Apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos.
- Servidores públicos y contratistas: ejecutar los controles y acciones definidas para la administración de los riesgos tratados, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos de la entidad.
- Oficina de Control Interno: debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos en conjunto con el Oficial de Seguridad y Privacidad de la Información.

En cuanto al equipo de trabajo del área de tecnología se cuenta con un equipo definido bajo los siguientes roles:

DOMINIO TI	ROLES
CIO (Chief Information Officer) - jefe Responsable de Gestión de la Información.	Profesional Universitario
Responsable de los Sistemas de Información	Profesional Universitario
Responsable de la Infraestructura Telecomunicaciones	Técnico Administrativo
Responsable de la Seguridad de la Información	Profesional Universitario

Tabla 1: Roles Oficina Sistemas

6.2 COMPROMISOS EN LA ADMINISTRACION DEL RIESGO

El HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DEL VALLE E.S.E, adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, mediante el apoyo la alta dirección del Hospital en conjunto con los líderes de proceso, funcionarios y contratistas; es por ello que se comprometen a:

- Conocer y cumplir la política de seguridad de la información de la entidad
- Replicar con sus equipos de trabajo fortaleciendo el trabajo mancomunado con la oficina de Sistemas fortaleciendo la conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
- Aprobar la revisión frecuente de los procesos y procedimientos para la identificación de nuevos riesgos o control de los existentes.
- Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

Para mitigar y lograr lo mencionado anteriormente es necesario que sean asignados recursos humanos, presupuestales y tecnológicos que permitan cerrar las brechas detectadas y mejorar los controles existentes.

6.3 ETAPAS PARA LA ADMINISTRACION DEL RIESGO

A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

6.3.1 Análisis contexto estratégico

Definir el contexto estratégico marca la pauta o ruta que la entidad debe asumir frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, evitando establecer las condiciones ideales para la materialización.

Para la definición del contexto estratégico es fundamental tener claridad sobre cuál es el plan estratégico de la entidad, hacia dónde va el hospital y cuáles son los planes programas o proyectos a ejecutarse, así mismo las oficinas o dependencias de cada proceso deben trabajar de forma responsable en conjunto con la oficina de sistemas lo cual mitigaría la toma de decisiones errada en cuanto a tecnología se refiere ya que se identifican de forma temprana los posibles riesgos que se puedan presentar.

6.3.2 Identificación de riesgos

En esta fase del documento el objetivo es evaluar todos los activos que se encuentran, considerando las dependencias existentes entre ellos y realizando una valoración sobre estos. De esta forma se definirá claramente un punto de salida de todos los activos, sean estos tangibles o no, dentro de la entidad y pudiendo analizar a qué amenazas podrían estar expuestos estos activos.

Una vez disponemos de un listado de las amenazas reales que pueden afectar a los activos, estaremos en disposición de poder realizar la evaluación del impacto que sufrirá la entidad en caso de que se materialicen estas amenazas.

El impacto, junto con los resultados anteriormente explicados dará una serie de datos que permitirán priorizar el plan de acción y, al mismo tiempo, evaluar como se ve modificado este valor una vez se apliquen las contramedidas o bien, el riesgo que estamos dispuestos a asumir (riesgo residual) por parte del Hospital.

Como resultado de esta fase, podremos obtener:

- Un análisis detallado de los activos relevantes de seguridad de la Entidad.
- Un estudio de las posibles amenazas sobre los sistemas de información, así como su impacto.
- El resultado final, será el impacto potencial que tendrá la materialización de las diferentes amenazas a las que están expuestos nuestros activos.

6.3.3 Inventario de activos

El primer punto para el análisis es estudiar los activos vinculados a la información. Es habitual agrupar los activos por grupos para ello. En nuestro caso, podemos agrupar los activos por grupos en los que nos centraremos son:

- [L] Lugar

- [HW] Hardware
- [SW] Software
- [COM] Red
- [O] Organización
- [P] Personal

Los resultados de este estudio se recogerán en una tabla que facilitará posteriores estudios. La tabla se dividirá en dos columnas donde se recogerá la información aquí dispuesta y clasificada. Para la primera columna se encontrará el ámbito del activo con el objetivo de realizar las agrupaciones y, en la segunda columna se encontrará el activo concreto.

Valoración del riesgo

Se realizará en esta fase la valoración del riesgo basados en los niveles de impacto y probabilidad que se enmarcan en la política de tratamiento del riesgo de la entidad.

Comunicación y consulta

Esta fase es en la que se realiza la comunicación tanto de la política de tratamiento del riesgo como los resultados de las valoraciones en la entidad cuando se han ejecutado las actividades de este plan.

Monitoreo y seguimiento del riesgo

En esta fase se ejecutarán actividades que para el plan de tratamiento son permanentes, es decir son controles periódicos que se agendan con el fin de mantener un control de los resultados frente al cumplimiento de los objetivos de este plan de la entidad, se deben dar con períodos de tiempo no mayores a 3 meses, como recomendación, sin embargo, estos tiempos pueden ser determinados por la Oficina de Sistemas.

6.3.4 DIMENSIONES DE SEGURIDAD

Desde el punto de vista de la seguridad, junto a la valoración de los activos, se ha de indicar cuál es el aspecto de la seguridad más crítico. Esto será de gran ayuda en el momento de pensar en posibles medidas de prevención, ya que serán enfocadas en aquellos aspectos más críticos.

Una vez identificados los activos, se ha de realizar la valoración de estos. Esta valoración mide la criticidad a las cinco dimensiones de la seguridad de la información gestionada por el proceso del HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DEL VALLE E.S.E. Esta valoración nos permitirá, a posteriori, valorar el impacto que tendrá la materialización de la amenaza sobre la parte del activo expuesto.

El valor que reciba el activo puede ser propio o acumulado. El valor propio se asignará a la información, quedando el resto de los activos subordinados a las necesidades de explotación y protección de la información. De esta manera, los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos. Cada activo de información puede tener un valor diferente en cada una de las diferentes dimensiones para la organización que deseamos analizar.

Las tres dimensiones de las que se habla son:

- [C] Confidencialidad. Únicamente las personas autorizadastienen acceso a la información sensible o privada.

- [I] Integridad. La información y los métodos de procesamiento de esta información son exactos y completos, y no se han manipulado sin autorización
- [D] Disponibilidad. Los usuarios que están autorizados pueden acceder a la información cuando lo necesiten.

Una vez detalladas las tres dimensiones se ha de tener presente la escala en que se realizarán las valoraciones. En este caso se utilizará una escala de valoración de 1 – 4 siguiendo los siguientes criterios.

CRITERIO	VALOR
Zona de riesgo bajo	1
Zona de riesgo moderado	2
Zona de riesgo alto	3
Zona de riesgo extremo	4

Tabla 2. Tabla de zonas

6.3.5 ANALISIS DE AMENAZAS

Las amenazas pueden afectar diferentes aspectos de la seguridad de los activos, por tanto, uno de nuestros objetivos es el análisis de qué amenazas pueden afectar los activos del HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DEL VALLE E.S.E. Una vez hecho esto se ha de estimar la vulnerabilidad de cada activo respecto a las amenazas potenciales.

El primer paso para realizar este análisis es disponer de una tabla de amenazas, para obtener este listado de amenazas se cruza con los activos que detallados en el punto anterior.

En último lugar, para valorar el impacto de las amenazas en los activos definidos, se debe asignar valores al impacto que produciría en el hospital la materialización de la amenaza, este valor será estimado de 1 – 4 y se define en la siguiente tabla:

CRITERIO	VALOR
Leve	1
Menor	2
Moderado	3
Mayor	4
Catastrófico	5

Tabla 3. Valoración de impacto

Se hacen las siguientes aclaraciones adicionales para comprender la clasificación realizada:

- Se ha realizado la división o agrupación de activos según ámbito (Instalaciones, hardware, software, etc.). Sin embargo, por darle más sentido al análisis, en algunos de los ámbitos se ha procedido a agrupar los activos según quién accede a ellos. Como las principales actividades son servicios orientados a la comunidad, se han dividido los activos que se

acceden desde el exterior y los activos que únicamente se accede desde el interior. Un ejemplo de esto sería una aplicación web, donde se accede a ella desde cualquier red mundial, un portátil o un sistema operativo, donde únicamente se puede acceder desde la red de la organización. También se ha de tener en cuenta que no todas las dimensiones de la seguridad se ven afectadas por una amenaza, existirán amenazas dirigidas a vulnerar la integridad de un sistema y en cambio otras, únicamente a la disponibilidad, así como combinaciones de varias dimensiones afectadas.

- Otra decisión ha sido la de separar los datos y servicios de logs del resto de servicios, ya que la función de esta se aleja del objetivo de los servicios ofrecidos por la organización y, por tanto, no sería realista juzgarlos de igual forma y otorgar amenazas que no les involucran.
- Para cada uno de los activos y sus agrupaciones, se han intentado escoger las amenazas con más sentido. Un ejemplo de esto es en algunos casos de amenazas que, por estructura o lógica del HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DEL VALLE E.S.E, estas no aplican. Se detallan algunas de estas en los siguientes puntos.
- Los datos de las aplicaciones se han separado del resto de datos, ya que a estos datos se pueden acceder desde el exterior, porque son gestionados por terceros que tiene acceso a ella, por tanto, no pueden tener el mismo nivel de impacto una amenaza sobre estos que sobre los datos que gestionan los funcionarios del HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DEL VALLE E.S.E, como por ejemplo los datos del sistema operativo, antivirus, etc.
- Es decir, se ha dado sentido a los datos, agrupando los activos según qué tipo de servicio ofrecen y quién podrá acceder a ellos. De esta manera, se enriquecen los números y se ajusta más a la realidad, ya que no es lo mismo acceder a un servicio interno como un antivirus, que a un servicio externo al que se puede acceder desde el exterior y manipular datos en ellos. Este es el motivo principal por el que se ha optado a agrupar los activos según las tablas que se presentan a continuación.

6.3.6 AMENAZAS QUE PUEDEN INDENTIFICAR EN LA INFRAESTRUCTURA

ACTIVO	AMENAZA
[L] Lugar	Daño en los equipos y servidores por falta de un Equipo climatización centro de datos
	Mal estado de Equipos extintores
[HW] Hardware	Alteración, suplantación, eliminación o Divulgación Datos Servidor correo
	Pérdida o robo dispositivos móviles
	Daño o alteración Equipos de Escritorio
	Daño, alteración o fuga de información Equipos Portátiles
	Daño o alteración Impresoras
	Daño, alteración o fuga de información Servidor Aplicaciones
	Daño, alteración o fuga de información Servidor Backup
	Daño, alteración o fuga de información Servidor Bases de datos

ACTIVO	AMENAZA
	Daño, alteración o fuga de información Servidor de correo
	Malware, troyano, gusanos, descargas o visitas a través de Unidades extraíbles
[SW] Software	Daño Aplicación Sistemas Operativos
	Daño o alteración Aplicaciones ofimática
	Alteración, eliminación o Divulgación Base de datos de Contraseñas
	Alteración, Suplantación o eliminación Correo electrónico
	Alteración, eliminación o Divulgación Datos Backup
	Alteración, eliminación o Divulgación Programas de administración (contabilidad, manejo de personal, etc.)
	Daño o alteración Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)
	Alteración, eliminación o Divulgación Programas de producción de datos
	Alteración, eliminación o Divulgación Programas manejo documental
	Daño o alteración Servidor Antivirus
[COM] Red	Defacing, XSS, DOSs, SQLinjection Página Web externa
	Daño o alteración Equipos de la red cableada (router, switch, etc.)
	Daño o alteración Equipos de la red inalámbrica (router, punto de acceso, etc.)
	Malware, troyano, gusanos, descargas o visitas a través de Navegación en Internet
	Inclusiones a PBX (Sistema de telefonía convencional)
	Daño o alteración Servidor Firewall
[O] Organización	Alteración o eliminación Archivo Contractual
	Alteración o eliminación Archivo de Gestión
	Alteración o eliminación Archivo RRHH
	Alteración o eliminación Autorizaciones Planeación
	Alteración o eliminación Bases de datos internos
	Alteración o eliminación Contables
	Alteración o eliminación Contractuales

ACTIVO	AMENAZA
	Alteración, eliminación o Divulgación Datos Desplazados
	Alteración, eliminación o Divulgación Datos Usuarios SISBEN
	Alteración o eliminación Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)
	Alteración o eliminación Financieros
	Alteración o eliminación Jurídicos
	Alteración o eliminación Licencias y Permisos
[P] Personal	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Administrativos
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de gerencia y Asesores
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Auxiliares
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Proveedores
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Contratistas
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Informática / Soporte técnico interno
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Mensajería interna (personal que radica documentos)
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Personal técnico
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de secretarios y directores
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Servicio de limpieza de planta
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Servicio de limpieza externo
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Servicio de mensajería de externo
	Acceso no autorizado a personal ajeno, Manejo Inadecuado de equipos, negligencia en la prestación del servicio por parte de Servicio de vigilancia
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Soporte técnico externo

6.3.7 IMPACTO POTENCIAL

Una vez terminado el análisis de los activos, presentado en las tablas anteriores y el análisis de las amenazas, podemos calcular el impacto potencial que pueden suponer para el HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DEL VALLE E.S.E la materialización de estas amenazas.

En este apartado y, para el cálculo del impacto, no se tienen en cuenta contramedidas, por tanto, el resultado que obtengamos de este cálculo se podrá extraer un valor de referencia que ayudará para determinar y priorizar un plan de acción. Al aplicar las contramedidas, este valor se verá modificado. Para realizar el cálculo del impacto potencial, se utiliza la siguiente fórmula:

Impacto Potencial = Activo x Impacto

Donde, es el valor de cada dimensión y el impacto es la degradación en cada dimensión en la que se ve afectado el activo también en caso de materializarse. En la tabla siguiente se presentan los resultados.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización
Menor - 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Tabla 5: Valoración de Impacto - Niveles de impacto en riesgos de procesos y seguridad de la información.
Fuente: Guía para la administración del Riesgo y el diseño de controles en entidades públicas, versión 5.

6.3.8 EVALUACION DEL RIESGO

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

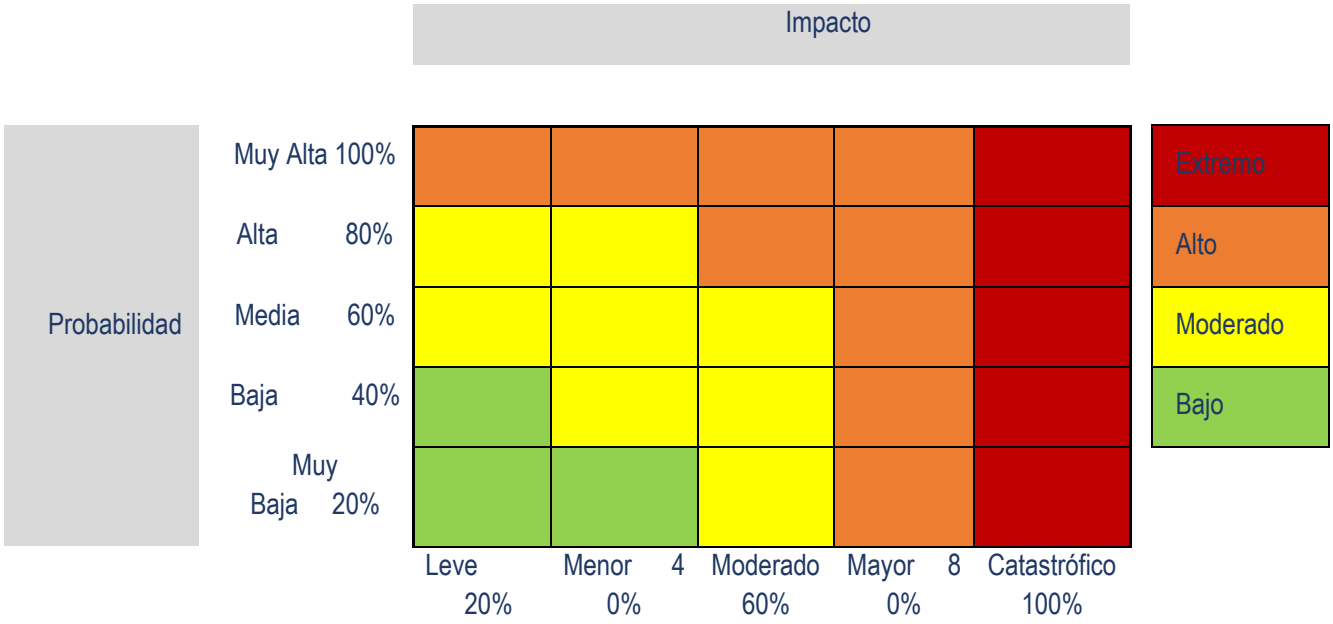

Tabla 6: Valoración del Riesgo - Nivel y Matriz de Calor del Riesgo.
Fuente: Guía para la administración del Riesgo y el diseño de controles en entidades públicas, versión 5.

CRITERIO	VALOR
Zona de riesgo bajo	B
Zona de riesgo moderado	M
Zona de riesgo alto	A
Zona de riesgo extremo	E

Tabla 7. Zona de riesgo

6.3.9 VALORACION DE LOS RIESGOS

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo.
Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

6.4 IDENTIFICACION DE CONTROLES

Es crucial para la implementación adecuada de un SGSI la aplicación de controles existentes según la norma ISO 27001. Estos salen como resultado del análisis de riesgo efectuado en la etapa inicial (plain), en la mayoría de los casos para la aplicación de los controles es necesario personal experto en diversas áreas pues si bien es cierto que la implantación de un sistema de

seguridad de la información está ligada al personal encargado de TI según la norma se trabaja sobre los dominios existentes los cuales incluyen desde recursos humanos hasta la legislación.
Para cada uno de los dominios existen controles que deberán ser aplicados para la mitigación del riesgo depende de la clasificación inicial.

6.5 MANEJO DE RIESGOS

Estructuralmente el HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DEL VALLE E.S.E manejará los riesgos identificados de la siguiente manera:

- **Controles de clase técnica**: Estos controles se basan prácticamente en la gestión operativa y de aseguramiento, de zonas físicas, accesos, manipulación de hardware y software, accesos a sitios web, manejo de la información, etc. Esta es la fase de la implementación de mayor cuidado y costo, pues en este proceso es donde está en juego la información y el éxito de la implantación del sistema de gestión y la mitigación del riesgo.
- **Controles de clase documental**: En esta fase los controles son dirigidos a reglamentar, aplicar, sensibilizar a todo el personal que labora en las organizaciones además son los controles más complicados pues con base en ello es que se les informa y distribuye el respectivo funcionamiento a los demás funcionarios. Usualmente estas políticas, instructivos, reglamentos no son muy tenidos en cuenta por los funcionarios dejando de forma incompleta la implantación del sistema de gestión de seguridad. Es aquí donde los planes de capacitación y sensibilización deben ser planificados de la mejor manera para tener la mayor aceptación en cada uno de los funcionarios de la compañía para dar el máximo cumplimiento y sacar el máximo de efectividad con la aplicación de controles técnicos
- **Implementar programas de capacitación y sensibilización**: Es ideal que se programen las fechas desde el inicio y las respectivas capacitaciones y sensibilizaciones, pues de esto depende en gran parte el éxito de la implementación del sistema. Al aplicar algunos controles se deberá realizar el debido seguimiento para verificar y cuantificar la funcionalidad del mismo, sin embargo, esto no aplica para todos los controles; Es ahí donde la sensibilización entra a jugar un papel fundamental en la compañía pues por desconocimiento los funcionarios pueden interferir o estropear el funcionamiento real del control, pues si bien es cierto que el sistema puede ser estable los usuarios son parte fundamental del éxito de cada uno.
- **Implementación de procedimiento de manejo de incidentes de seguridad**: Cuando se habla de incidente informático, se hace referencia a un suceso que se presentó o que tiene una gran posibilidad de darse en un momento determinado. Este suceso puede ser llevado a cabo a voluntad o accidental. Dependiendo de la gravedad de la situación esto puede afectar el funcionamiento normal de la organización. Por lo general el manejo del incidente implica que este se debe solucionar en el menor tiempo posible para evitar una afectación mayor y se debe buscar documentar cada uno de los eventos presentados y el tiempo que transcurrió entre cada uno de ellos, con el fin de poderlo analizar posteriormente y aplicar correcciones del caso para que en un futuro este no se vuelva a presentar o al menos su impacto sea lo menor posible. Para ello, se pueden seguir los seis pasos ideales para mantener el orden adecuado.
- **Preparación**: En este punto, se debe tener una lista de chequeo la cual ayuda a organizar la reacción ante un incidente, para esto es necesario tener conceptos claros como son:
  - Políticas de la organización. Si estas existen, se debe determinar que está permitido y que no. Conducto regular de comunicación, lista de contactos, la posibilidad o no de dar información a terceros, quien está en capacidad de hacerlo entre otros.
  - Recurso humano. No basta con saber que se cuenta con determinadas áreas dentro de la organización, se necesita saber quiénes son las personas que están capacitadas para afrontar un incidente, sus números de teléfono, el escalamiento en la comunicación, entre otros.
  - Información: El manejo que se le debe dar a la misma, forma de almacenamiento, importancia según el negocio, confidencialidad, integridad y disponibilidad.

- Software – Hardware: Con qué elementos contamos como antivirus, firewall, ubicación de estos, servidores, etc. Comunicaciones. Con qué elementos cuenta la organización para llevar a cabo la prestación de los servicios ante un incidente, medios de comunicación alternos, etc.
- Ups – Plantas Eléctricas – controles: Determinar claramente cuáles son los dispositivos que cuenta la organización, cuales son principales y cuáles de respaldo, el comportamiento de estos, tiempos de funcionamiento, plan de contingencia entre otros.
- Formatos o Plantillas. Se debe contar con elementos para registrar los sucesos, el tiempo en que ocurren, como se afrontan, observaciones, etc.

- **Detección y análisis**: La detección se puede dar por llamada de algún usuario, cliente, administrador, etc., alarma presentada por algún dispositivo dispuesto para ello, como un firewall, IDS, IPS. Alteración de información, observación, medios informativos, caída de un sistema, base de datos, etc. Una vez detectado se procede a analizar el impacto de este, con ello se disponen los elementos que se requieran para solucionar el impase. Determinar si no son falsos positivos, validar la evidencia en este caso ver logs de registros, bitácoras.
- **Contención**: En esta fase se procede a neutralizar el incidente, para ello es necesario tener cautela de no eliminar evidencia que posteriormente nos ayude a analizar el origen, el posible atacante, desde cuándo está llevando a cabo el proceso, en fin, información que posteriormente se estudiará. Aquí se toman decisiones de cómo plantear la estrategia de contención, fundamentados en importancia del activo, disponibilidad para la operación de la organización, elementos alternos o sustitutos, grado del ataque.
- **Erradicación y recuperación**: Con base en la información tomada en la detección y contención es necesario tomar las medidas del caso para que no se vuelvan a presentar. Es posible que la organización tenga que invertir en elementos de protección adicionales. Pero esta decisión debe ser fundamentada en hechos y datos, ser lo más objetivos posibles. En el proceso de recuperación puede ser necesario restaurar las copias de respaldo, cambio de contraseñas, cambios de direcciones IP.
- **Reporte y cierre**: Se hace necesario llevar a cabo un informe en el cual se documente los procesos realizados, siendo muy claros en los pasos llevados a cabo. Esta información puede servir más adelante para resolver nuevos impases o determinar si las decisiones tomadas fueron acordes al incidente. Se debe generar un documento de lecciones aprendidas el cual debe estar redactado por el equipo que afrontó el incidente, estas lecciones aprendidas se analizaran posteriormente por una junta la cual se informará y hará los aportes para prevenir futuras situaciones. Por último, dar a conocer las recomendaciones del caso y llevar a cabo las implementaciones a que haya lugar. Es bueno volver a hacer una revisión periódica tanto a las decisiones tomadas como a las inversiones hechas por la organización. Con ello evitamos que una solución planteada hoy mañana sea obsoleta y se nos presente un incidente nuevamente.

6.6 SEGUIMIENTO DE RIESGOS

Cuando sea solicitado por el comité, se presentarán avances sobre el funcionamiento y manejo de los riesgos en la entidad en cuanto al cumplimiento de las políticas y directrices para la administración del riesgo y la administración de los riesgos por proceso. Los resultados de la evaluación y las observaciones deben ser posteriormente solucionadas y entregadas a la alta dirección en cabeza del gerente general o un designado, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la Entidad.

ACTIVIDADES

Las siguientes actividades son parte del plan de acción en la identificación y gestión de riesgos del HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DEL VALLE E.S.E para la vigencia 2026.

GESTION	ACTIVIDAD	DESCRIPCION	INICIO	FIN
GESTIÓN OPERATIVA DEL RIESGO	Socializar al interior de TIC´s los lineamientos de riesgos	Realizar la socialización con el equipo de TIC's y los funcionarios de la entidad, los lineamientos de gestión del riesgo como la política de seguridad, los informes de vigencias anteriores para el tratamiento de riegos, y los resultados de procesos anteriores.	Enero 2026	Diciembre 2026
	Sensibilización de los elementos de la gestión del riesgo en la entidad	Gestionar actividades con todas las áreas para socializar los lineamientos para la gestión del riesgo, y los resultados de los riesgos residuales con la dependencia que gestiona el riesgo institucional y con las demás áreas.	Enero 2026	Diciembre 2026
	Identificación de riesgos de seguridad y privacidad de la información.	Crear y ejecutar actividades para la Identificación de riesgos de seguridad y privacidad de la información, Privacidad de datos personales, continuidad del negocio y seguridad digital con la matriz de gestión de riesgos FOR-DES-14.	Enero 2026	Diciembre 2026
	Evaluación y aceptación de riesgos residuales	Realizar análisis y evaluación de los riesgos residuales de las matrices y basados en el apetito aprobado de riesgo de la política de gestión y tratamiento de riesgos elaborar el documento de aceptación del riesgo. por medio de la matriz FOR-DES-14.	Enero 2026	Diciembre 2026
	Publicación del riesgo	Publicar las matrices e informes de la gestión y tratamiento del riesgo a los interesados internos y externos por medio del informe de tratamiento de riesgos.	Enero 2026	Diciembre 2026

	Implementación de controles para el tratamiento de riesgos	Definir e implementar los controles más adecuados para tener un nivel de riesgo aceptable para los procesos incluidos en el alcance del MSPI. Aplicar acciones para cumplir con el plan de tratamiento de riesgos incluyendo los de Seguridad de la información, detallando el tratamiento que aplica a los riesgos. Aprobar el plan de tratamiento de riesgos por parte de los dueños de cada riesgo, buscando la participación de las diferentes áreas incluidas en el proceso y finalmente de la Alta Dirección.	Enero 2026	Diciembre 2026
	Mejoramiento	Identificar oportunidades de mejora según los resultados obtenidos de los análisis y evaluaciones de riesgos y de los resultados de los controles implementados. Generar un informe de mejoramiento para la aprobación e implementación.	Enero 2026	Diciembre 2026
		Realizar el seguimiento y monitoreo de los controles implementados, y de las acciones de mejora aprobadas para el tratamiento de riesgos.	Enero 2026	Diciembre 2026
		Realizar actualización del plan de gestión y tratamiento de riesgos según los resultados obtenidos.	Enero 2026	Diciembre 2026
	Monitoreo y Revisión	Generar, reportar y presentar informes de indicadores en el tratamiento de riesgos.	Enero 2026	Diciembre 2026
		Presentar mejoras al plan de gestión y tratamiento de riesgos para la siguiente vigencia.	Enero 2026	Diciembre 2026

METAS

- Ejecutar el plan de trabajo propuesto en materia de identificación, valoración y tratamiento de riesgos propuesto para la vigencia 2026.
- Revisar detalladamente el plan de tratamiento de riesgos y ajustar a la realidad de la entidad los aspectos que en mejora continua se puedan presentar.

INDICADORES DE MEDICION Y CONTROL

Para el cumplimiento del plan de tratamiento de riesgos de la entidad es preciso monitorear y controlar las actividades por lo cual se formulan dos (2) indicadores de medición del plan, estos son:

Indicador 1: Porcentaje de Activos valorados y gestionados

- Variables: Total de Activos valorados
- Fórmula de medición: Porcentaje de activos valorados = (#total de activos vinculados y ejecutados al proceso de valoración) / (# total de activos tecnológicos de la entidad) *100
- Resultado: Se tendrá en cuenta el porcentaje de activos valorados en el proceso, lo que permite medir el objetivo para la vigencia 2026, que es el 100% del total de activos CRITICOS actuales. Lo anterior según la importancia de los activos involucrados en la gestión de la entidad en sus procesos más críticos a los menos críticos.

Indicador 2: Porcentaje de ejecución del plan de tratamiento de riesgos.

- Variables: Actividades # de ejecutadas y # de Actividades programadas.
- Fórmula de Medición: Porcentaje de ejecución del plan= (# de actividades ejecutadas/# actividades planeadas) *100
- Resultado: El resultado será el porcentaje de cumplimiento del plan, para posteriormente aplicar actividades de medición, control y valoración de las mejoras que deban hacerse para las vigencias futuras.

7. ANEXOS

NA

Elaborado por:	Revisado por:	Aprobado por:
ORIGINAL FIRMADO	***ORIGINAL FIRMADO***	***ORIGINAL FIRMADO***
Leydi Marcela Martínez Turriago Profesional Universitario Sistemas	**Berenice Rivera Trujillo** Líder ISC	**Stella Tafur Guerreo** Subgerente Administrativa y Financiera
Fecha: 14 de enero de 2026	**Fecha:** 16 de enero de 2026	**Fecha:** 19 de enero de 2026

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA DE VIGENCIA
01	Creación del documento	Enero de 2026