CONTROL DE REVISIONES			
	ELABORÓ	**REVISÓ**	**APROBÓ**
NOMBRE Y APELLIDO / CARGO	Profesionales oficina de Sistemas	Profesional Apoyo Calidad	Coordinador oficina de Sistemas
FIRMA			
FECHA	01/11/2020	01/11/2020	01/11/2020

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA**	**MOTIVO DEL CAMBIO**	**DESCRIPCIÓN DEL CAMBIO**
1	01/11/2020		Se creó la primera versión del documento

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

2020

INTRODUCCIÓN

La Administración de 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.

Todo el equipo humano del Hospital Regional de la Orinoquía ESE, 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 Tecnologías y las Comunicaciones MINTIC, 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.

OBJETIVOS

OBJETIVO GENERAL

Generar un documento para establecer la estructura metodológica y las buenas prácticas en cuanto a la administración del riesgo, Seguridad y Privacidad de la Información, para el Hospital Regional de la Orinoquía ESE.

OBJETIVOS ESPECÍFICOS

- Generar pautas para la determinación de los riesgos en el Hospital Regional de la Orinoquía ESE.
- Fomentar el uso y apropiación de la Política de Seguridad y Privacidad de la Información vigente en los funcionarios y contratistas del Hospital Regional de la Orinoquía ESE.
- Involucrar y comprometer a todos los funcionarios y contratistas en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

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 Regional de la Orinoquía ESE.

La mitigación de los riesgos como debe ser establecida bajo un proceso estructurado y sistemático es por ello por lo que el presente documento contiene desde la definición de los roles y responsabilidades hasta los formatos que deben ser diligenciados en el proceso de identificación.

DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes 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 originan 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 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.

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 necesita.

ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACION DEL RIESGO.

El éxito de la administración del riesgo depende de varios factores, aun así la participación de la alta dirección, en cabeza del gerente, subgerentes, líderes de procesos y demás servidores públicos y contratistas, permite que el proceso se desarrolle con mayor efectividad y fluidez, es por ello que la identificación de los roles es fundamental.

Alta Dirección: Aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.

Sistema Integrado de Gestión: Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.

Responsables de los procesos: Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos) al menos una vez al año. Si bien el personal del SIG apoya la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

Servidores públicos y contratistas: Ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

Quien haga las veces de Control Interno: Debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos.

Equipo de trabajo del área de tecnología: Se debe designar un responsable competente que esté a cargo de la seguridad de la información.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

El Hospital Regional de la Orinoquía E.S.E. Define su política de Gestión del riesgo atendiendo los lineamientos establecidos en Guía para la Administración del riesgo del DAFP, articulada con las normas aplicables a la entidad, el Modelo Integrado de Planeación y Gestión, el MSPI, como mecanismo para identificar, analizar, valorar, monitorear, administrar y tratar los riesgos que pudieran afectar el logro de los objetivos institucionales.

ALCANCE DE LA POLÍTICA

La política de Gestión del Riesgo es aplicable a todos los servicios, procesos y a todas las Actividades realizadas por los diferentes funcionarios que laboran en la entidad, no importa el tipo de contratación.

OBJETIVO GENERAL DE LA POLÍTICA

Fortalecer la implementación y desarrollo de la política de Gestión del Riesgo a través del adecuado tratamiento de los riesgos para garantizar el cumplimiento de la misión y objetivos institucionales.

OBJETIVOS ESPECIFICOS DE LA POLITICA

- Proteger los recursos del Estado, resguardándolos contra la materialización de los Riesgos. Introducir en la caracterización de cada uno de los procesos, los riesgos identificados en la matriz de riesgo institucional, para su control y seguimiento en la herramienta adoptada por la entidad. Involucrar y comprometer a todos los servidores del Hospital, en la búsqueda de acciones encaminadas a prevenir, reducir o mitigar los riesgos.
- Valorar cada uno de esos riesgos detectados clasificándolos de acuerdo con su importancia relativa.
- Diseñar el mapa de riesgo Institucional
- Determinar el plan de manejo de riesgos, en el cual se consignen las acciones de seguimiento y control para cada uno de los riesgos detectados y valorados.

ETAPAS PARA LA ADMINISTRACIÓN 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.

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 de desarrollo hacia dónde va la entidad y cuáles son los planes programas o proyectos a ejecutarse, así mismo las

dependencias y líderes de proceso deben trabajar de forma responsable en conjunto con la oficina de sistemas (gerencia de la información), 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.

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 nuestros 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 nos 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 Regional de la Orinoquía ESE.

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.

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 los siguientes:

- [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.

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 los mismos. Esta valoración mide la criticidad a las cinco dimensiones de la seguridad de la información gestionada por el proceso. 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 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 uno de las diferentes dimensiones para la organización que deseamos analizar. Por esto, se ha de tener presente siempre que representa cada dimensión.

Las cinco dimensiones de las que se habla son:

- **[C] Confidencialidad:** Únicamente las personas autorizadas tienen 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.
- **[A] Autenticidad:** Hay garantía de la identidad de los usuarios o procesos que gestionarán la información.
- **[T] No repudio:** Hay garantía de la autoría de una determinada acción y está asociada a quien ha producido esta acción.

Una vez detalladas las cinco 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.

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

Análisis 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 de la entidad. 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 las cruzaremos con los activos que hemos detallado en el punto anterior.

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

VALOR	IMPACTO
1	Insignificante
2	Menor
3	Moderado
4	Mayor
5	Catastrófico

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. Se han dividido los activos que se acceden desde el exterior y los activos que únicamente se acceden desde el interior. 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.

- 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 de la entidad, estas no aplican. Se detallan algunas de estas en los siguientes puntos.

Es decir, se ha intentado dar un poco de 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.

AMENAZAS Y VULNERABILIDADES

ACTIVO	AMENAZA	VULNERABILIDAD
[HW] Hardware	Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento
	Destrucción de equipos y medios	Ausencia de esquemas de reemplazo periódico
	Polvo, corrosión y congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad
	Radiación electromagnética	Sensibilidad a la radiación electromagnética
	Error en el uso	Ausencia de un eficiente control de cambios en la configuración
	Perdida del suministro de energía	Susceptibilidad a las variaciones de voltaje
	Fenómenos meteorológicos	Susceptibilidad a las variaciones de temperatura
	Hurtos de medios o documentos	Almacenamiento sin protección
		Falta de cuidado en la disposición final
		Copia no controlada
[SW] Software	Abuso de los derechos	Ausencia o insuficiencia de pruebas de software
	Corrupción de datos	Defectos bien conocidos en el software
	Error en el uso	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo
	Falsificación de derechos	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado

	Procesamiento ilegal de datos	Ausencias de pistas de auditoria
	Mal funcionamiento del software	Asignación errada de los derechos de acceso
	Hurto de medios o documentos	Software ampliamente distribuido
	Uso no autorizado del equipo	En términos de tiempo utilización de datos errados en los programas de aplicación
	Software ilegal	Interfaz de usuario compleja
	Error en el uso	Ausencia de documentación
	Error en el uso	Configuración incorrecta de parámetros
	Error en el uso	Fechas incorrectas
	Falsificación de derechos	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario
	Falsificación de derechos	Tablas de contraseñas sin protección
	Falsificación de derechos	Gestión deficiente de las contraseñas
	Procesamiento ilegal de datos	Habilitación de servicios innecesarios
	Mal funcionamiento del software	Software nuevo o inmaduro
	Mal funcionamiento del software	Especificaciones incompletas o no claras para los desarrolladores
	Mal funcionamiento del software	Ausencia de control de cambios eficaz
	Error en el uso	Descarga y uso no controlado de software
	Manipulación con software	Ausencia de copias de respaldo
	Hurto de medios o documentos	Ausencia de protección física de la edificación, puertas y ventanas
	Uso no autorizado del equipo	Fallas en la producción de informes de gestión
[COM] Red	Negación de acciones	Ausencia de pruebas de envío o recepción de mensajes
	Escucha encubierta	Líneas de comunicación sin protección
	Escucha encubierta	Tráfico sensible sin protección
	Fallas del equipo de telecomunicaciones	Conexión deficiente de los cables
	Fallas del equipo de telecomunicaciones	Punto único de fallas
	Falsificación de derechos	Ausencia de identificación y autentificación de emisor y receptor
	Espionaje remoto	Arquitectura insegura de la red
	Espionaje remoto	Transferencia de contraseñas en claro
	Saturación del sistema de información	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)
	Uso no autorizado del equipo	Conexiones de red pública sin protección

[O] Organización	Abuso de derechos	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Abuso de derechos	Ausencia de proceso formal para la revisión de los derechos de acceso
	Abuso de derechos	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)
	Abuso de derechos	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información
	Abuso de derechos	Ausencia de auditorias
	Abuso de derechos	Ausencia de procedimientos de identificación y valoración de riesgos
	Abuso de derechos	Ausencia de reportes de fallas en los registros de administradores y operadores
	Incumplimiento en el mantenimiento del sistema de información	Respuesta inadecuada de mantenimiento del servicio
	Incumplimiento en el mantenimiento del sistema de información	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos
	Incumplimiento en el mantenimiento del sistema de información	Ausencia de procedimientos de control de cambios
	Incumplimiento en el mantenimiento del sistema de información	Contrato de soporte del sistema de información no renovado
	Corrupción de datos	Ausencia de procedimiento formal para la documentación del MSPI
	Corrupción de datos	Ausencia de procedimiento formal para la supervisión del registro del MSPI
	Datos provenientes de fuentes no confiables	Ausencia de procedimiento formal para la autorización de la información disponible al público
	Negación de acciones	Ausencia de asignación adecuada de responsabilidades en seguridad de la información
	Falla del equipo	Ausencia de planes de continuidad
	Error en el uso	Ausencia de políticas sobre el uso de correo electrónico
	Error en el uso	Ausencia de procedimientos para introducción del software en los sistemas operativos
	Error en el uso	Ausencia de registros en bitácoras

	Error en el uso	Ausencia de procedimientos para el manejo de información clasificada
	Error en el uso	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos
	Hurto del equipo	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información
	Hurto del equipo	Ausencia de política formal sobre la utilización de computadores portátiles
	Hurto del equipo	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Hurto de medios o documentos	Ausencia de política sobre limpieza de escritorio y pantalla
	Hurto de medios o documentos	Ausencia de autorización de los recursos de procesamiento de información
	Hurto de medios o documentos	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad
	Uso no autorizado de equipo	Ausencia de revisiones regulares por parte de la gerencia
	Uso no autorizado de equipo	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
	Uso de software falsificado o copiado	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales
[P] Personal	Incumplimiento en la disponibilidad del personal	Ausencia del personal
	Destrucción de equipos y medios	Procedimientos inadecuados de contratación
	Error en el uso	Entrenamiento insuficiente en seguridad
	Error en el uso	Uso incorrecto de software y hardware
	Error en el uso	Falta de conciencia acerca de la seguridad
	Procesamiento ilegal de los datos	Ausencia de mecanismos de monitoreo
	Hurto de medios o documentos	Trabajo no supervisado del personal externo o de limpieza
	Uso no autorizado del equipo	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería

[L] Lugar		Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
		Ubicación en área susceptible de inundación
		Red energética inestable
		Ausencia de protección física de la edificación (Puertas y ventanas

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 Regional de la Orinoquía ESE, 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:

Probabilidad	Impacto				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Raro					
Improbable					
Posible					
Probable					
Casi Seguro					

Evaluación 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.

Matriz de Calificación, Evaluación y respuesta a los Riesgos

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía de Riesgos DAFP

Valoración 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.

Identificación 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 (planificación), 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.

Manejo de riesgos

Estructuralmente el Hospital Regional de la Orinoquía ESE, manejara 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 trabajadores.

Usualmente estas políticas, instructivos, reglamentos no son muy tenidos en cuenta por los trabajadores 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 trabajadores de la entidad 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 entidad pues por desconocimiento los trabajadores 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 este 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.

- Recursos 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 que elementos contamos como antivirus, firewall, ubicación de los mismos, servidores, etc.

- Comunicaciones: Con que 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 los mismos, tiempos de funcionamiento, plan de contingencia entre otros.

- Formatos o Plantillas: Se debe contar con elementos para registras los sucesos, el tiempo en que ocurren, como se afrontaron, 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 del mismo, 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 cuando está llevando a cabo el proceso, en fin, información que posteriormente se estudiara. Aquí se toman decisiones de como 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 IPs.

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 afronto el incidente, estas lecciones aprendidas se analizaran posteriormente por una junta la cual se informara 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 las inversiones hechas por la organización. Con ello evitamos que una solución planteada hoy mañana sea obsoleta y se nos presente un incidente nuevamente.