PLAN DE TRATAMIENTO DE RIESGO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

EMPRESA SOCIAL DEL ESTADO
HOSPITAL SAN JUAN DE DIOS
ITUANGO, 2023

INTRODUCCION

Para toda entidad es de gran importancia contar con un plan de gestión de riesgos con el fin de garantizar la continuidad de la misma. Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado en La ESE Hospital San Juan de Dios de Ituango. El tratamiento de los riesgos de seguridad de la información se basa en procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Para la realización de este plan la ESE diagnóstico su situación actual, realizando la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información.

La contribución de la realización de este plan a la ESE permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

OBJETIVOS

Objetivo General

Desarrollar un plan de gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en La ESE Hospital San Juan de Dios de Ituango

Objetivos Específicos

- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la Información.
- Definir los principales activos a proteger en la ESE.
- Identificar las principales amenazas que afectan a los activos.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de Implementar el plan de gestión de seguridad de la información

ALCANCES Y LIMITACIONES

ALCANCES

- Lograr el compromiso de la ESE Hospital San Juan de Dios de Ituango para emprender la implementación del plan de gestión del riesgo en la seguridad de la información.

- Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.

- Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

LIMITACIONES

Crear el rubro del presupuesto necesario para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en La ESE Hospital San Juan de Dios de Ituango.

GESTIÓN DE RIESGOS

IMPORTANCIA DE LA GESTIÓN DE RIESGOS

En la actualidad en toda entidad, institución u organización se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo.

La ESE Hospital San Juan de Dios de Ituango, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad de la entidad tras sufrir alguna pérdida o daño en la información de la misma.

Considerando la situación actual de la ESE Hospital San Juan de Dios de Ituango, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

DEFINICION GESTIÓN DEL RIESGO

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como “la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización”.

IDENTIFICACIÓN DEL RIESGO

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.
Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.
Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión

SITUACION NO DESEADA

- ✓ Hurto de información o de equipos informáticos.
- ✓ Hurto de información durante el cumplimiento de las funciones laborales, por intromisión Incendio en las instalaciones de la empresa por desastre natural o de manera intencional. Alteración de claves y de información.
- ✓ Pérdida de información.
- ✓ Daño de equipos y de información
- ✓ Atrasos en la entrega de información
- ✓ Atrasos en asistencia técnica
- ✓ Fuga de información
- ✓ Manipulación indebida de información

ORIGEN DEL PLAN DE GESTION

La ESE Hospital San Juan de Dios de Ituango cuenta con debilidades que se encontraron en el sistema actual, por lo que es necesario crear un plan de gestión de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad; la información.
El gobierno nacional y el ministerio de las TIC han abanderado los proyectos de Gobierno en Línea que permite conocer el funcionamiento de los hospitales y entidades públicas en el país. Es por ello necesario que la ESE Hospital San Juan de Dios de Ituango cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades, a la población y al mismo hospital.

PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

1. Dar soporte al modelo de seguridad de la información al interior de la entidad. Conformidad legal y evidencias de la debida diligencia.
2. Preparación de un plan de respuesta a incidentes.
3. Descripción de los requisitos de seguridad de la información para un producto, un servicio o un mecanismo.
4. Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

DESCRIPCIÓN DE DEBILIDADES

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la ESE Hospital San Juan de Dios de Ituango se encontraron otras amenazas e impactos como los siguientes:

Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos según se va presentando la necesidad.
No existe una estructura o protocolo fijo y establecido para la infraestructura física del hospital.
Algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcance a ser guardada.
En la entidad se presenta incumplimiento del cuidado tanto de los equipos informáticos y como de la información física y digital, algunos de estos son:

- ✓ Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.

- ✓ En algunos papeles reutilizables se encontró información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.

- ✓ En algunas oficinas del hospital no existen los equipos de cómputo suficientes para el uso de la totalidad de su personal. Existe un riesgo de pérdida de información ya que deben compartir los recursos informáticos.

- ✓ La información es llevada en memorias o discos duros portátiles personales, por ende, la información sale de la entidad.

- ✓ No hay control para el uso de memorias portátiles en los equipos del hospital, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.

- ✓ No existe un área de sistemas con personal encargado de revisar, documentar, diseñar y controlar los procesos propios de un modelo de seguridad de la información para el hospital.

- ✓ No existe un historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados por el personal de sistemas en la entidad.

- ✓ Los documentos físicos que se manejan en la institución no se han digitalizado por lo tanto están expuestos a perdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.

MATRIZ DE VULNERABILIDADES Y MITIGACION DEL RIESGO DE LA ESE HOSPITAL SAN JUAN DE DIOS DE ITUANGO

VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACIÓN	CALIFICACIÓN	EVALUACIÓN	MITIGACIÓN DEL RIESGO
Fallas eléctricas	Las conexiones no son suficientes, no cumplen con las exigencias el tamaño de la red de equipos de cómputo (cables sueltos, inadecuada estructura y adecuación)	Inadecuada conexión de cableado eléctrico	Posible pérdida de información	*Riesgo tecnológico *Riesgo físico *Riesgo Humano	40	Riesgo moderado	Plantear un nuevo diseño de la red eléctrica
Afectación de activos de información y activos informáticos	Desconocimiento o de las políticas y normas de seguridad de la información	No socialización No capacitación de las políticas y normas de seguridad.	Acciones no adecuadas en el tratamiento delos activos de información e informáticos	Riesgo Tecnológico *Riesgo en servicio *Riesgo de la información *Riesgo en Personal	60	Riesgo Alto	Diseñar, Socializar e implementar un Manual de políticas y normas de seguridad de la Información en el Hospital.

VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACIÓN	CALIFICACIÓN	EVALUACIÓN	MITIGACIÓN DEL RIESGO
Confidencialidad e integridad de la información	En la entidad se han encontrado dentro del papel reutilizable información personal de pobladores	Exposición de datos personales en papel reutilizable	incumplimiento de confidencialidad	*Riesgo Información	60	Riesgo Alto	Socializar con los funcionarios de la entidad acerca de
Pérdida de información y/o deterioro físico	La documentación e información en papel o física esta siendo archivada en sitios no adecuados para ello	No se ha iniciado la ejecución de digitalización de la información	Daño de documentos y retiro del papel	*Riesgo de información	40	Riesgo Importante	Iniciar la ejecución de la digitalización y almacenamiento de la información contenida en el papel.

VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACIÓN	CALIFICACIÓN	EVALUACIÓN	MITIGACIÓN DEL RIESGO
Incumplimiento de las actividades de seguridad de la información	El personal encargado de los sistemas no es suficiente. No se están siguiendo protocolos y normas para garantizar la seguridad de la	No existe personal encargado del proceso de aseguramiento de la información	Ausencia de transferencia de conocimiento y falta de capacitación	*Riesgo información *Riesgo servicio *Riesgo tecnológico	60	Riesgo alto	Capacitar al personal del hospital para el cumplimiento de procesos y actividades de seguridad de la información

PROPUESTA DE SEGURIDAD

- ✓ Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas y los puestos de trabajo.
- ✓ Establecer políticas de seguridad y privacidad de la información como también las políticas de Seguridad informática.
- ✓ Implementar y socializar las políticas de seguridad y privacidad de la información con el Personal del hospital.
- ✓ Implementar el sistema de documentación digital en el hospital para reducir riesgos de pérdida de información física.

- ✓ Habilitar el software para digitalización de documentos y gestión documental en los próximos meses.

- ✓ Implementar software para realizar copias de seguridad en caliente.
- ✓ Dar inicio a las actividades de Gestión Documental.

PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

Obtener una nube dedicada para la información del hospital con el fin de tener un respaldo en caso de accidentes referentes a pérdidas de estas.

Contar con un plan alternativo que asegure la continuidad de la actividad del negocio en caso que ocurran incidentes graves.

PLAN DE CONTINUIDAD DEL NEGOCIO

- Diseñar un formato de chequeo de acuerdo a las necesidades de la organización que permita realizar las auditorías periódicas con la finalidad de verificar que los objetivos de control, procesos y procedimientos se cumplan.

- Socializar con los empleados de la ESE la importancia del Plan de Continuidad de seguridad de la información, para hacer frente a incidentes graves de seguridad en la institución, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.

- Diseñar estrategias para el proceso de recuperación de la información teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.

- Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:
  Detectar el riesgo
  Plantear controles y efectuar las implementaciones respectivas.
  Mitigar el riesgo.

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN

El análisis permitió identificar que la ESE Hospital San Juan de Dios de Ituango requiere políticas de seguridad de la información; por lo cual debe quedar integrado con el documento actual. Se recomienda entre otros tener en cuenta:

Socialización y capacitación de temas de seguridad.
Ambiente con la seguridad física adecuada.
Sistemas de respaldo para mantener soporte de la información

PLAN DE CAPACITACIÓN

Contar con un plan de capacitación para el personal encargado de la seguridad de la información, en aspectos a fortalecer como:

Detectar los requerimientos tecnológicos
Determinar objetivos de capacitación para personal
Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad.
Elaborar un programa de capacitación en temas de cyber seguridad y políticas de seguridad de la información para todos los funcionarios de la entidad.
Evaluar los resultados de cada actividad.