INDICE

- Introducción 3
- Objetivos 3
- Alcances y limitaciones 4
- Gestión de riesgos 4
- Importancia de la gestión de riesgos 4
- Definición gestión del riesgo 4
- Visión general para la administración del riesgo de seguridad de la información 5
- Identificación del riesgo 5
- Situación no deseada 5
- Origen del plan de gestión 6
- Propósito del plan de gestión de riesgo de la seguridad de la información. 6
- Identificación del riesgo 6
- Análisis de vulnerabilidades 6
- Descripción de vulnerabilidades 6

INTRODUCCION

Es importante contar con un plan de gestión de riesgos con el fin de garantizar el funcionamiento, controles e información entrante y saliente. Con este plan podremos minimizar y conocer los riesgos que la E.S.E. Hospital Geriátrico y Ancianato San Miguel posee actualmente y poder realizar las mejoras correspondientes para no generar perdida de información vital de la ESE, información de clientes internos y externos y los medios por los cuales se manipula la información

Para la realización de este plan la ESE Hospital Geriátrico y Ancianato San Miguel con el apoyo del área de sistemas 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

Desarrollar un plan de gestión de seguridad y privacidad que permita garantizar la seguridad, integridad y privacidad de la información, minimizando el riesgo de pérdida de activos de la información en La E.S.E Hospital Geriátrico y Ancianato San Miguel.

Objetivos Específicos

- Identificar los eventos que pueden generar inconvenientes para la perdida de información o daños físicos en los equipos donde se transmiten los datos.
- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Identificar y definir los principales activos a proteger en la ESE.
- Reconocer los principales riesgos que puedan afectar los activos fijos de la ESE.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- Permitir comparar de acuerdo a las posibles soluciones que muestra el plan para los activos físico e informáticos.

ALCANCES Y LIMITACIONES

ALCANCES

 Lograr obtener compromiso por parte de la ESE Hospital Geriátrico y Ancianato San Miguel realizar las soluciones pertinentes para evitar riesgos físicos e informáticos.

 Dar poder de decisión para poder realizar soluciones rápidas y confiables

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

LIMITACIONES

Tener como carácter primario un presupuesto para adquirir la tecnología y protecciones físicas.

GESTIÓN DE RIESGOS

IMPORTANCIA DE LA GESTIÓN DE RIESGOS

En el tiempo actual las empresas, instituciones están en el proceso de sistematizar todos los procesos para poder generar mejor rendimiento, rapidez en la entrega de la información, información clara y certera. La información es crucial en una empresa, están dentro del primer escalafón de nivel de importancia ya que sin ella la empresa no puede realizar los procesos y su segundo nivel son los equipos tecnológicos que la ESE utiliza para la manipulación de esta información.

Es por eso que se deben de tener parámetros y procesos de seguridad que hagan que una empresa si sufre una pérdida de información o de sus activos por cualquier concepto se riesgos naturales, riesgos de manejo inadecuado de la información, fallas eléctricas, desconocimiento del manejo de la información, virus informáticos, secuestro de información, suplantación de identidades, perdidas administrativas de la información o de los activos fijos. es de suma importancia tener un plan de tratamiento ya que si no se tiene está expuesta a perder su información.

En la actualidad las empresas son atacadas constantemente solo con obtener una brecha de riesgo para afectar toda la información y no solo afecta la información sino la calidad de la información almacenada.

Para ello es importante reiterar tener el plan con soluciones para prevenir todo este tipo de ataques, desastres que no solo afecta la parte física e informática sino también la parte económica de la empresa, ya que los costos por recuperación de datos (si son posibles) son bastantes elevados dependiendo del nivel de afectación que haya tenido la parte física de almacenamiento o que tan alterada o corrupta se encuentre la misma

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”.

VISION GENERAL PARA LA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Proceso para la administración del riesgo.

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 Geriátrico y Ancianato San Miguel cuenta con vulnerabilidades 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.

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

- Dar soporte al modelo de seguridad de la información al interior de la entidad.
- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto, un servicio o un mecanismo.
- Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

IDENTIFICACIÓN DEL RIESGO
ANALISIS DE VULNERABILIDADES

DESCRIPCIÓN DE VULNERABILIDADES

Teniendo en cuenta que la información y los equipos activos son atacados y la información se ve amenazada por varios factores, la ESE Hospital Geriátrico y Ancianato San Miguel ha encontrado diferentes amenazas o inconvenientes que pueden afectar la información, los activos físicos y la calidad de la información como los que se muestran a continuación:

1. No hay regulación de energía en las diferentes áreas del hospital, esto puede afectar que los equipos tecnológicos sufran fallas eléctricas, daños en los sistemas de almacenamiento y pérdida parcial o definitiva de la información.

2. No se han realizado las suficientes capacitaciones al personal para corroborar y aclarar el buen funcionamiento de los equipos tecnológicos, aplicaciones o software que se usan y la forma adecuada de manipular la información.

3. Se han encontrado documentos o papeles que se usan como reciclable con información vital de la empresa o con datos sensibles que deben ser destruidos de manera segura.

4. La entidad cuenta con un sistema de almacenamiento en la nube, pero los documentos físicos que se manejan 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

VULNERABILIDAD	DESCRIPCION	CAUSA	EFECTO	CLASIFICACION	CALIFICACION	EVALUACION	MITIGACION DEL RIESGO	VIGENCIA DE CUMPLIMIENTO
Fallas eléctricas	Las conexiones no son suficientes, no cumplen con las exigencias el tamaño de la red de equipos de cómputo, no hay protección en el momento de perdida de energía o elevación del sistema eléctrico. (cables sueltos, inadecuada estructura y adecuación, ups)	Inadecuada conexión de cableado eléctrico, falta de plata de respaldo	Posible pérdida de información y daños físicos en los equipos	*Riesgo tecnológico *Riesgo físico *Riesgo humano	70	Riesgo Alto	Plantear renovación de cableado eléctrico y poseer UPS de respaldo para todos los equipos de sistemas	por determinar
Afectación de activos de información y activos informáticos.	desconocer la forma adecuada de manipular la información y los equipos de sistemas adecuadamente	no realizar capacitación, socialización de manipulación de equipos políticas y seguridad	manipulación no adecuada que genere perdida, alteración o eliminación de la información y daños físicos en las estaciones de trabajo	*Riesgo Tecnológico *Riesgo en la información *Riesgo Personal *Riesgo Físico	40	Riesgo Moderado	Diseñar, implementar realizar seguimiento al manipulación adecuada de los archivos y de los activos fijos	Vigencia 2021
Confidencialidad e integridad de la información	Hallar en papel reciclable información vital de la empresa o datos de usuarios internos y externos	Exponer información privada de usuarios internos y externos	incumplimiento de confidencialidad e integridad de la información	*Riesgo en la información *Riesgo Personal	38	Riesgo Moderado	Informar a los usuarios que manipulan la información realizar la eliminación correctiva de la información interna y externa	Vigencia 2021

VULNERABILIDAD	DESCRIPCION	CAUSA	EFECTO	CLASIFICACION	CALIFICACION	EVALUACION	MITIGACION DEL RIESGO	VIGENCIA DE CUMPLIMIENTO
Pérdida de información y/o deterioro físico	La documentación e información en papel o física está siendo archivada en sitios no adecuados para ellos	No se ha iniciado la ejecución de digitalización de la información	Daño de documentos y deterioro del papel	*Riesgo de información	40	Riesgo Moderado	Iniciar la ejecución de la digitalización almacenando los archivos en la nube y almacenamiento de la información contenida en el papel	Vigencia 2021
incumplir con las políticas de derecho de autor en el software	Tener software operativo (Windows) y software de procesos (office) no licenciados o que no cumplan con las normas de licenciamiento para empresa y hogar	no tener el presupuesto para la adquisición de licencias corporativas	perdida de la información, errores en la actualización de la aplicación	*Riesgo de la información.	100	Riesgo Alto	La ESE Hospital Geriátrico y Ancianato San Miguel cuenta en todos sus equipos con licencias corporativas para los sistemas operativos y procesadores de datos	Vigencia 2021
VULNERABILIDAD	**DESCRIPCION**	**CAUSA**	**EFECTO**	**CLASIFICACION**	**CALIFICACION**	**EVALUACION**	**MITIGACION DEL RIESGO**	**VIGENCIA DE CUMPLIMIENTO**

VULNERABILIDAD	DESCRIPCION	CAUSA	EFECTO	CLASIFICACION	CALIFICACION	EVALUACION	MITIGACION DEL RIESGO	VIGENCIA DE CUMPLIMIENTO
No poseer un software para la protección de virus e infecciones cibernéticas	Contar con un software que proteja, vacune, supervise, informe y verifique la información del usuario cuando ingresa a páginas web o introduce dispositivos externos en los equipos de sistemas.	no tener el presupuesto para la adquisición de licencias corporativas	Perdida de la información, secuestro de la información, divulgación de la información, alteración de la información, daños físicos en los equipos de sistemas, suplantación de identidades, robos virtuales.	*Riesgo de la información *Riesgo Personal *Riesgo Físico *Riesgo privacidad *Riesgo Económico	100	Riesgo Alto	La ESE cuenta con software para la protección de datos virtuales y realiza seguimiento en todas las entradas y salidas de información mediante sus motores de búsqueda.	Vigencia 2021

ANEXOS

N/A

APROBACIÓN

ELABORADO POR	REVISADO POR	APROBADO POR
Daniel Piedrahita Soporte Sistemas	Carolina Osorio González Subgerente Administrativa y Financiera	Sandra Marentes Astaiza Gerente

Control de cambios				
Versión	Fecha	pagina	Solicitante	Comentarios
1	14/02/2019	Documento Original	Subgerencia Administrativa y Financiera	N.A
2	04/01/2021	6-8	Subgerencia Administrativa y Financiera	N.A
3	30/01/2023	2	Subgerencia Administrativa y Financiera	Ajuste al objetivo del plan.