1. RESPONSABLE

El responsable de llevar a cabo este plan es el Líder de Sistemas.

2. OBJETIVO

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 Geriátrico y Ancianato San Miguel.

3. ALCANCE

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.

4. DEFINICIONES

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”.

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

5. REF NORMATIVA

Decreto 612 del 4 de abril de 2018.

6. DESARROLLO

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

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:

- 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.

- 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.

- 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.

- 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.

- Hay áreas en el hospital que cuentan con equipos de sistemas ya muy antiguos sin que puedan poseer las aplicaciones o actualizaciones necesarias para su buen funcionamiento y protección de datos.

- 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.

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 manipulacion adecuada de los archivos y de los activos fijos	Vigencia 2019
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 2019

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 2019
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 2019
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 2019

7. ANEXOS

N.A

8. APROBACION

	ELABORO	**REVISO**	**APROBO**
Nombre	MAURICIO GOMEZ	ARIADNA BOLAÑOS	HECTOR FABIO CORTES
Cargo	Lider Sistemas	Responsable Planeación	Gerente
Firma			