Red Salud Armenia E.S.E.

PA CUIDAR DE TODOS

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024

Código: AP-GT-PL-006 Versión: 1

TABLA DE CONTENIDO

INTRODUCCIÓN

Red Salud Armenia E.S.E. dentro de sus lineamientos de Sistemas de Información tiene establecido primordialmente tener la seguridad y la privacidad de la información de los usuarios que de alguna u otra manera interactúan con el Sistema de Información o mediante cualquier tipo de acceso a los datos institucionales desde alguna estación de trabajo o dispositivo.

Red Salud Armenia E.S.E. en busca de la mejora continua implementa un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados el manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma.

La institución en su quehacer diario utiliza TIC en cuanto a captura, procesamiento y reporte de información tanto internamente como externamente para comunicarse con los diferentes actores del sistema de salud, lo cual implica que la institución sea vulnerable a ataques mal intencionados o mala manipulación de la información lo que acarrea problemas económicos, legales, y administrativos por lo cual este documento busca establecer un línea de trabajo que permita a la entidad sortear los riesgos que lo rodean y lograr que su información este segura.

1. JUSTIFICACIÓN

La administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

2. OBJETIVOS

a. Objetivo general.

Establecer un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información el cual sea una guía para el control y minimización de los de los riesgos dentro de la institución y así proteger la privacidad de la información y los datos tanto de los procesos como de las personas vinculadas con la información de en RED SALUD ARMENIA E.S.E.

b. Objetivos Específicos

- Lograr un diagnóstico real de la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información.

- Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y MINTIC para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

3. ALCANCE

El presente documento pretende determinar la manera en que se llevara a cabo el proceso de protección de acceso a la información institucional de usuarios que de alguna u otra manera interactúan con el Sistema de Información o cualquier tipo de acceso a los datos institucionales desde alguna estación de trabajo o dispositivo, así como también, establecer las políticas corporativas para el uso de los equipos de cómputo y software dentro de toda la red hospitalaria y garantizando su ejecución, cumplimiento y seguimiento y control por medio de indicadores de gestión para estos procesos tan relevantes dentro de la institución.

4. DEFINICIONES

1. **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
2. **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
3. **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
4. **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
5. **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
6. **Ciberespacio:** Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua española). Control Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición

más simple, es una medida que modifica el riesgo.

7. **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
8. **Gestión de incidentes de seguridad de la información** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
9. **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
10. **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
11. **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
12. **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
13. Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
14. **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

15. **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
16. **Parte interesada**: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

5. MARCO NORMATIVO

- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública
- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales
- Ley 594 de 2000 - Ley General de Archivos
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos
- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
- Decreto 2364 de 2012 - Firma electrónica
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos
- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales
- Ley 527 de 1999 - Ley de Comercio Electrónico
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información

6. MÉTODOS DE PROTECCIÓN

Siguiendo estos sencillos consejos se puede aumentar considerablemente la seguridad de una computadora, algunos son:

- Tener el sistema operativo y el navegador web actualizados.
- Tener instalado un antivirus y un firewall y configurarlos para que se actualicen

automáticamente de forma regular ya que cada día aparecen nuevas amenazas.

- Utilizar una cuenta de usuario con privilegios limitados, la cuenta de administrador solo debe utilizarse cuando sea necesario cambiar la configuración o instalar un nuevo software.
- Tener precaución al ejecutar software procedente de Internet o de medios extraíbles como CD o memorias USB. Es importante asegurarse que proceden de algún sitio de confianza.
- Evitar descargar software de redes P2P, ya que realmente no se sabe su contenido ni su procedencia.
- Desactivar la interpretación de Visual Basic Script y permitir Java Script, ActiveX y cookies sólo en páginas web de confianza.
- Utilizar contraseñas de alta seguridad para evitar ataques de diccionario.
- Es recomendable hacer copias de respaldo regularmente de los documentos importantes, a medios extraíbles como CD o DVDs para poderlos recuperaren caso de infección por parte de algún malware.
- Guardar información importante de trabajo en la nube (Google Drive), y haceruna copia cada determinado tiempo, solicitar a sistemas que guarde la información en los Discos duros.

7. AMENZAS DE SEGURIDAD

Se entiende por AMENAZA una condición del entorno del sistema de información (personas, maquinas Etc.) que dada una oportunidad podría dar lugar a que se genere una VIOLACION DE SEGURIDAD.

La violación de seguridad son contrapartes a la certificación de un sistema seguro y se clasifican en

- Confidencialidad
- Integridad
- Disponibilidad
- Uso legitimo

LAS POLITICAS DE SEGURIDAD Y EL ANALISIS DE RIESGOS, habrán identificado las amenazas que deberán de ser contrarrestadas dependiendo del diseño del sistema de seguridad especificando, los servidores y mecanismos de seguridad necesarios para prevenir eventos o enfrentar contingencias. Específicamente su captura, transformación, almacenamiento, protección yrecuperación.

8. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DELA INFORMACION

Red Salud Armenia E.S.E. dentro de sus lineamientos de Sistemas de Informacióntiene establecido primordialmente tener la seguridad y la privacidad de la información de los usuarios que de alguna u otra manera interactúan con el Sistema de Información o mediante cualquier tipo de acceso a los datos institucionales desdealguna estación de trabajo o dispositivo.
Red Salud Armenia E.S.E. en busca de la mejora continua implementa un métodológico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados el manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma.
La institución en su quehacer diario utiliza TIC en cuanto a captura, procesamientoy reporte de información tanto internamente como externamente para comunicarsecon los diferentes actores del sistema de salud, lo cual implica que la institución sea vulnerable a ataques mal intencionados o mala manipulación de la informaciónlo que acarrea problemas económicos, legales, y administrativos por lo cual estedocumento busca establecer un línea de trabajo que permita a la entidad sortear los riesgos que lo rodean y lograr que su información este segura.

La ejecución del plan está acorde a la matriz de riesgos de sistemas de información, anexa a este plan.

Valoración del Riesgo:

Se mide en cuanto a probabilidad e impacto para obtener un dato cuantitativo que permitasu comparación y priorización, como se muestra en las siguientes escalas de valoración:

	Resultados de la calificación del Riesgo de Corrupción				
PROBABILIDAD	**Probabiliad**	**Puntaje**	**Zonas de riesgo de corrupción**		
	Casi Seguro	5	25 Moderada	50 Alta	100 Extrema
	Probable	4	20 Moderada	40 Alta	80 Extrema
	Posible	3	15 Moderada	30 Alta	60 Extrema
	Improbable	2	10 Baja	20 Moderada	40 Alta
	Rara vez	1	5 Baja	10 Baja	20 Moderada
	Impacto		Moderado	Mayor	Catastrófico
	Puntaje		5	10	20

IMPACTO

9. PRIORIDAD DE ASPECTOS CRÍTICOS EN LOS APLICATIVOS INFORMÁTICOS

Se define como aspectos críticos en los aplicativos informáticos los más importantes para continuar con la normal prestación del servicio, aquellos afectan directamente el proceso de atención. Debido a que su prioridad es de importancia vital para la actividad institucional, se determinó que el aplicativo Dinámica Gerencial .Net es la piedra angular del sistema de información y por tanto los esfuerzos deben estar enfocados a restablecer su funcionamiento. Para el óptimo funcionamiento del sistema de información es necesario que se cuente con una copia vigente de las bases de datos, recuperada de las copias de seguridad que se hacen al servidor. Estas bases de datos son el aspecto crítico del sistema de información, pues en ellas se almacenan los datos clínicos, financieros,inventarios y de nómina, entre otros.

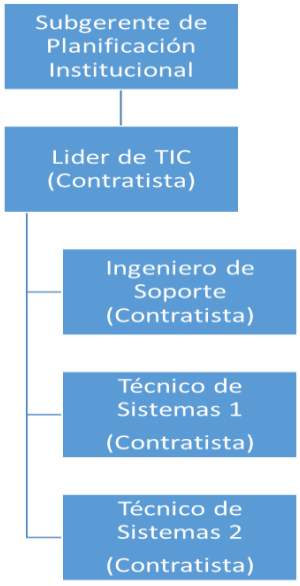
Tenemos como prioridad los siguientes aplicativos informáticos

Según la importancia y frecuencia de uso del software institucional, en caso de calamidad o desastre los aplicativos deben restablecerse en el siguiente orden:

1. Microsoft SQL Server
2. Dinámica Gerencial .Net
3. Antivirus Kaspersky Endpoint Security
4. Microsoft Office u OpenOffice
5. Dinámica Gerencial Fox
6. Sistema de gestión documental Torresoft SGE
7. Infraestructura de microservicios virtualizados en Linux

10. RESPONSABLES

La estructura organizacional en Red Salud Armenia E.S.E. de los procesos responsables de la realización del plan es la siguiente:



11. INDICADORES

1. **PORCENTAJE DE ATAQUES INFORMATICOS EFECTIVOS**
   (Número de ataques informáticos efectivos / Número de ataques informáticos recibidos) * 100

2. **PORCENTAJE DE CUMPLIMIENTO DE LA POLÍTICA DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**
   (Puntaje obtenido de la lista de chequeo gestión de la política de la seguridad y privacidad de la información)

12. GLOSARIO DE TÉRMINOS

Administrar: Gobernar, ejercer la autoridad o el mando sobre un territorio y sobre las personas que lo habitan. Dirigir una institución. Ordenar, disponer, organizar, en especial la hacienda o los bienes.
Arquitectura Empresarial o TI: Describe la estructura y las relaciones de todos los elementos de TI de una organización. Se descompone en arquitectura de información, arquitectura de sistemas de información y arquitectura de servicios tecnológicos. Incluye además las arquitecturas de referencia y los elementos estructurales de la estrategia de TI (visión de arquitectura, principios de arquitectura, lineamientos y objetivos estratégicos).
Gel: Gobierno en línea es el nombre que recibe la estrategia de gobierno electrónico (e-government) en Colombia, que busca construir un Estado más eficiente, más transparente y más participativo gracias a las TIC.
Gestionar: Hacer diligencias conducentes al logro de un negocio o un objetivo.
Gobierno Corporativo: manera en que las entidades son dirigidas, mejorando su funcionamiento interna y externamente, buscando eficiencia, transparencia e integridad, para responder adecuadamente ante sus grupos de interés, asegurando un comportamiento ético organizacional.
Copia de seguridad: Copia los datos o los registros de una base de datos de SQL Server o del registro de transacciones en un dispositivo de copia de seguridad, como un disco, para crear una copia de seguridad de datos o de registros.
Copia de los datos: que se puede usar para restaurar y recuperar los datos después de un error. Las copias de seguridad de una base de datos también se pueden usar para restaurar una copia de la base de datos en una nueva ubicación.
Dispositivo de copia de seguridad: Disco o dispositivo de cinta en el que se escriben las copias de seguridad de SQL Server del que se pueden restaurar.
Copia de seguridad de datos: Copia de seguridad de datos en una base de datos completa (copia de seguridad de base de datos), una base de datos parcial (copia de seguridad parcial) o un conjunto de archivos de datos o grupos de archivos (copia de seguridad de archivos).
Copia de seguridad de base de datos: Las copias de seguridad completas representan la base de datos completa en el momento en que finalizó la copia de seguridad. Las copias de seguridad diferenciales solo contienen los cambios realizados en la base de datos desde la copia de seguridad completa más reciente.
Copia de seguridad diferencial: Copia de seguridad de datos basada en la última

copia de seguridad completa de una base de datos completa o parcial o de un conjunto de archivos de datos o grupos de archivos (base diferencial) y que solo incluye los datos que han cambiado desde dicha base.
Recuperar: Devolver una base de datos a un estado estable y coherente.
Restaurar: Proceso de varias fases que copia todos los datos y páginas del registro desde una copia de seguridad de SQL Server especificada a una base de datos especificada y, a continuación, pone al día todas las transacciones registradas en la copia de seguridad mediante la aplicación de los cambios registrados para poner los datos al día.

13. BIBLIOGRAFIA

MINTIC. (30 de junio de 2014). *Marco de Referencia, Guías, Base del conocimiento*. Obtenido de www.mintic.gov.co/arquitecturati/630/w3-article-9253.html MINTIC. (2015). *Arquitectura TI*. Obtenido de http://www.mintic.gov.co/arquitecturati/630/w3-channel.html

MINTIC. (2015). *Fortalecimiento de la Gestión TI en el Estado*. Obtenido de Modelo de Gestión TI: http://www.mintic.gov.co/gestionti/615/w3-channel.html

MINTIC. (30 de marzo de 2016). G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información - PETI. Bogotá, Colombia.

MINTIC. (s.f.). *Gobierno en Linea*. Obtenido de http://estrategia.gobiernoenlinea.gov.co/623/w3-channel.html

DAFT Guia de administración del riesgo de https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

Control de cambios

Versión	Fecha de actualización	Razón de la actualización	Responsable de la actualización	Verifico/Aprobó
1	22/01/2024	Documento inicial	Sistemas de información	Subgerencia de Planificación