PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

CENTRO DE SALUD DE GUACHAVES – E.S.E

SANTACRUZ – NARIÑO

2020

TABLA DE CONTENIDO

INTRODUCCIÓN.

El Plan de Seguridad y Privacidad de la Información, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, 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.

Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios del Centro de Salud de Guachaves – E.S.E.

1. OBJETIVOS.

1.1. OBJETIVO GENERAL.

Desarrollar un plan de gestión de seguridad y privacidad de la información, que permita minimizar los riesgos de pérdida de activos de la información en el Centro de Salud de Guachaves – E.S.E.

1.2. OBJETIVOS ESPECÍFICOS.

- ✓ Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de seguridad digital en toda la institución.
- ✓ Determinar el alcance del plan de seguridad y privacidad de la información.
- ✓ Definir las principales amenazas que afecten la seguridad y privacidad de la información.
- ✓ Proponer soluciones para minimizar los riesgos a los que se encuentra expuesta la información.

2. ALCANCES Y LIMITACIONES.

2.1. ALCANCES.

- ✓ Lograr el compromiso del Centro de Salud de Guachaves – E.S.E, para emprender la implementación del plan de seguridad y privacidad de la información.
- ✓ Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de seguridad y privacidad de la información.
- ✓ Capacitar al personal de la entidad en el proceso de plan de seguridad y privacidad de la información.

2.2. LIMITACIONES.

Crear el rubro del presupuesto necesario para apoyar la implementación del plan de seguridad y privacidad de la información en el Centro de Salud de Guachaves E.S.E, del Municipio de Santacruz.

3. 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

3.1. SITUACIÓN 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

4. ORIGEN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Centro de Salud de Guachaves E.S.E, se encuentra expuesto a vulnerabilidades que se encontraron en el sistema actual, por lo que es necesario crear un plan de seguridad y privacidad de la información que permita protegerla.

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 el Centro de Salud De Guachaves E.S.E, cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades, a la población y mima Institución.

4.1. PROPÓSITO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

- ✓ Dar soporte al plan de seguridad y privacidad de la información al interior de la entidad. De Conformidad con lo establecido con lo legal y las evidencias de la debida diligencia.
- ✓ 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.

5. ANÁLISIS DE VULNERABILIDAD DE LA INFORMACIÓN.

5.1. DESCRIPCIÓN DE VULNERABILIDADES.

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en el Centro de Salud de Guachaves ESE, se encontraron otras amenazas e impactos como los siguientes:

a) Algunos de los puntos de red ubicados en el área asistencial no se encuentran debidamente ubicados e instalados bajo las normas establecidas.

b) Algunos cables de energía están sueltos, no están cerca a los escritorios y existe el 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.

c) 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 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 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 Centro de Salud.

- 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 entidad 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.

5.2. PROPUESTA DE SEGURIDAD DE LA INFORMACIÓN.

- ✓ Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.
- ✓ 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.

5.3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

En el centro de Salud de Guachaves ESE, se requiere políticas de seguridad de la información y Se recomienda 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 en caso de eventualidades catastróficas.

5.4. CAPACITACIÓN.

Contar con un plan de capacitación para el personal encargado de la seguridad de la información y fortalecer aspectos tales como:

a) Detectar los requerimientos tecnológicos.

b) Determinar objetivos de capacitación para personal.

c) Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad.

d) Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los funcionarios de la entidad.

e) Evaluar los resultados de cada actividad.