E.S.E HOSPITAL ANA SILVIA MALDONADO JIMENEZ DE COLOMBIA - HUILA

Plan De Seguridad y Privacidad En la información

Colombia, Enero de 2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Hospital Ana Silvia Maldonado Jiménez de Colombia - Huila, las mejoras prácticas dadas por el Departamento de Administrativo de la Función Pública con su estrategia MIPG y el Ministerio de las Tecnologías e Información en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información.

El Modelo de Seguridad y Privacidad de la Información, pretende lograr en la institución y sus clientes internos, externos y partes interesadas confianza en el manejo de la información garantizando para cada uno la privacidad, continuidad, integralidad y disponibilidad de los datos.

2. OBJETIVOS

2.1. Objetivo General

Realizar un documento institucionales guiado en de lineamientos de buenas prácticas en seguridad y Privacidad de la información.

2.2. Objetivos Específicos

- Ajustar el uso de mejores prácticas de seguridad de la información en la institución.
- Eficacia en la gestión de la seguridad de la información al interior de le entidad.
- Ejecutar de manera correcta la legislación relacionada con la protección de datos personales.
- Optimizar la labor de acceso a la información pública.

3. ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional. La Política de Seguridad de la Información aplica para todos los usuarios internos en todos los niveles jerárquicos, usuarios externos, proveedores y terceros; que produzcan, administren, custodien o que tengan acceso a la información.

4. RESPONSABLES

La estructura organizacional de los procesos responsables de la realización del plan es la siguiente:

GERENTE
ASESORES
EQUIPO ADMINISTRATIVO
EQUIPO ASISTENCIAL

5. MARCO CONCEPTUAL

5.1 Seguridad De La Información

La Seguridad Informática se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos. Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección.

Destacamos que, aunque se diferencia entre la Seguridad de la Información y la Protección de Datos como motivo u obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas. En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación no autorizada. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo, existen más requisitos como por ejemplo la autenticidad entre otros. El motivo o el motor para implementar medidas de protección, que responden a la Seguridad de la Información, es el propio interés de la institución o persona que maneja los datos, porque la pérdida o modificación de los datos, le puede causar un daño (material o inmaterial). Entonces en referencia al ejercicio con el banco, la pérdida o la modificación errónea, sea causado intencionalmente o simplemente por negligencia humana, de algún récord de una cuenta bancaria, puede resultar en pérdidas económicas u otras consecuencias negativas para la institución.

5.2 Protección de Datos.

La Protección de Datos, el objetivo de la protección no son los datos en sí mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta. Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la institución o persona que maneja los datos, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información. En muchos Estados existen normas jurídicas que regulan el tratamiento de los datos personales, como por ejemplo en España, donde existe la "Ley Orgánica de Protección de Datos de Carácter Personal" que tiene por objetivo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

Sin embargo, el gran problema aparece cuando no existen leyes y normas jurídicas que evitan el abuso o mal uso de los datos personales o si no están aplicadas adecuada o arbitrariamente. Pero una buena Gestión de riesgos no es una tarea única sino un proceso dinámico y permanente que tiene que estar integrado en los procesos (cotidianos) de la estructura institucional, que debe incluir a todas y todos los funcionarios -¡¡la falla el eslabón más débil de la cadena!!- y que requiere el reconocimiento y apoyo de las directivas. Sin estas características esenciales no están garantizados, las medidas de protección implementadas no funcionarán y son una pérdida de recursos.

5.3 Amenazas

Siempre hay riesgo de que ocurra cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

Generalmente se distingue y divide tres grupos

- **Criminalidad:** son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.

- **Sucesos de origen físico:** son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.

- **Negligencia y decisiones institucionales:** son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

5.4 Vulnerabilidades

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño. Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades en grupos característicos: Ambiental, Física, Económica, Social, Educativo, Institucional y Política

5.5 Obtención Y Almacenamiento De Copias De Seguridad (Backups)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la ESE.

- .

6. 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.
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática.
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad.
- 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.

- 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

- 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

7. DESCRIPCIÓN DEL PLAN

Política De Seguridad Y Confidencialidad De La Información

El equipo de colaboradores y el Gerente de la Hospital Ana Silvia Maldonado Jiménez de Colombia – Huila, se comprometen a garantizar la confidencialidad, seguridad e integralidad de la información de los usuarios y su familia, clientes internos y externos en cuanto a seguridad lógica y física de los activos de la información, fomento de canales de comunicación que garanticen acceso y transparencia de la información pública a través de uso adecuado de las TICS, cumpliendo con las disposiciones generales para la protección de datos, aportando al cumplimiento de la Misión, Visión y objetivos estratégicos de la institución.

Objetivos De La Política De Gestión De Calidad

- Garantizar la protección de datos personales de usuarios, clientes, proveedores y trabajadores tanto en los medios físicos como electrónicos.
- Controlar el uso efectivo de equipos de cómputo que garantice la confidencialidad, seguridad e integralidad de la información de los usuarios incluyendo.
- Fortalecer el conocimiento y la adherencia en el plan de contingencia en caso de caída del sistema de información

8. CONTROL DE RESPONSABILIDADES

FIRMA:
Nombre: EDUARDO MAHECHA REYES
Cargo: Gerente E.S.E
Fecha: Enero 2025