E.S.E. HOSPITAL SAN JOSÉ

TECNOLOGÍAS
HOSPITAL SAN JOSÉ DE RESTREPO VALLE

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Restrepo Valle, Enero de 2024

"Hospital San José, un Hospital más cerca de ti!"
contactenos@hsjrestrepo.gov.co
Tel. (2) 2522722 - 2522773
Calle 9 15-10, Restrepo Valle
www.hsjrestrepo.gov.co

TABLA DE CONTENIDO

Pagina.

INTRODUCCIÓN

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.

1. PRESENTACIÓN

El presente plan se elabora con el fin de dar a conocer como se realizará la implementación y socialización del componente de Gobierno en línea en el Eje Temática de la Estrategia en **Seguridad y Privacidad de la Información**, el cual busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

2. DEFINICIONES

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados.[1]

Activo: Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.[2]

Activo de Información: Se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.[3]

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.[4]

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.[5]

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.[6]

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.[7]

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento.[8]

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.[9]

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.[10]

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.**

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.[11]

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.[12]

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público.

[1] Ley 1712 de 2014, art 4
[9] CONPES 3701
[10] Resolución CRC 2258 de 2009
[11] Ley 1712 de 2014, art 6
[12] Ley 1581 de 2012, art 3
[13] Decreto 1377 de 2013, art 3

[8] Ley 1581 de 2012, art 3
[2] ISO/IEC 27000
[3] Ley 594 de 2000, art 3
[4] ISO/IEC 27000
[5] ISO/IEC 27000
[6] ISO/IEC 27000
[7] Ley 1581 de 2012, art 3

Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.[13]

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.[14]

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.[15]

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.[16]

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural.[17]

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.[18]

[26] ISO/IEC 27000
[27] ISO/IEC 27000
[28] ISO/IEC 27000
[29] Ley 1581 de 2012, art 3
[30] ISO/IEC 27000

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.[19]

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio,

particular y privado o semiprivado de una persona natural o jurídica por lo que su/ acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.[20]

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. [21]

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.[22]

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. [23]

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL[24] la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

[26] ISO/IEC 27000
[27] ISO/IEC 27000
[28] ISO/IEC 27000
[29] Ley 1581 de 2012, art 3
[30] ISO/IEC 27000

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.[25]

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.[26]

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. [27]

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o 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. [28]

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento.[29]

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. [30]

3. OBJETIVOS

3.1. Objetivo General

Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en la E.S.E. Hospital San José, con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

[26] ISO/IEC 27000
[27] ISO/IEC 27000
[28] ISO/IEC 27000
[29] Ley 1581 de 2012, art 3
[30] ISO/IEC 27000

3.2. Objetivos Específicos

- Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente en la E.S.E. Hospital San José para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.

- Aplicar las metodologías del Departamento Administrativo de la Función Pública DAFP e ISO respectivamente en seguridad y riesgo de la información en la E.S.E. Hospital San José.

4. RECURSOS

- **Humano**:
  - Gerente General
  - Líderes del Proceso
  - Profesional Tecnología
  - Personal Externo

- **Físico:**
  - PC
  - Equipos de comunicación

- **Financiero**

5. RESPONSABLES

- Gerente General
- Líderes del Proceso
- Profesional de Tecnología

6. METODOLOGÍA DE IMPLEMENTACIÓN

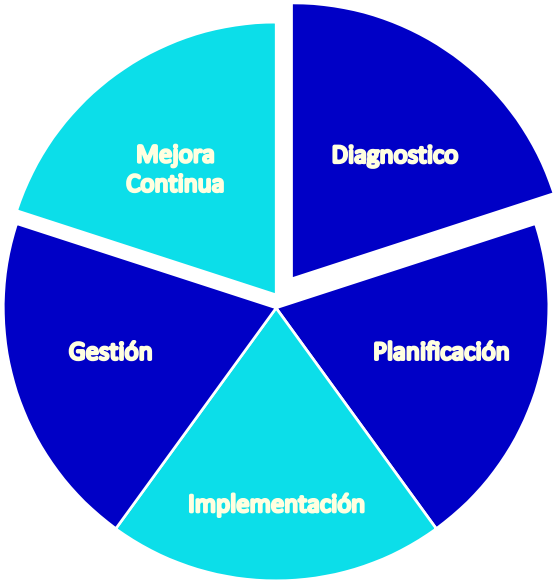
Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la E.S.E. Hospital San José, se toma como base la metodología Planear, Hacer, Verificar y Actuar "PHVA" y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

[26] ISO/IEC 27000
[27] ISO/IEC 27000
[28] ISO/IEC 27000
[29] Ley 1581 de 2012, art 3
[30] ISO/IEC 27000

De acuerdo con esto, se definen las siguientes fases de implementación del Modelos de Seguridad y Privacidad de la Información MSPI para identificar el nivel de madurez:

- Diagnosticar
- Planear
- Hacer
- Verificar
- Actuar

Gráfico: Marco de Seguridad y Privacidad de la Información[31]



[31] Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC

[26] ISO/IEC 27000
[27] ISO/IEC 27000
[28] ISO/IEC 27000
[29] Ley 1581 de 2012, art 3
[30] ISO/IEC 27000

7. ACTIVIDADES

- Realizar Diagnóstico
- Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
- Realizar la Identificación de los Riesgos con los líderes del Proceso
- Entrevistar con los líderes del Proceso
- Valorar del riesgo y del riesgo residual
- Realizar Mapas de calor donde se ubican los riesgos
- Plantear al plan de tratamiento de riego aprobado por los lideres

8. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los plazos de implementación de acuerdo a lo establecido por la E.S.E. Hospital San José.

- Revisión y/o Modificación de la actual Política de Seguridad
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información

[26] ISO/IEC 27000
[27] ISO/IEC 27000
[28] ISO/IEC 27000
[29] Ley 1581 de 2012, art 3
[30] ISO/IEC 27000

- Aspectos de seguridad de la información en la gestión de continuidad del negocio

9. CRONOGRAMA

ACTIVIDAD	JULIO				AGOST				SEPT				OCT				NOV				DIC			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Realizar Diagnostico																								
Elaborar el Alcalde del Plan																								
Realizar Identificación de los Riesgos																								
Entrevista con los Lideres del Proceso																								
Valoración del Riesgo Residual																								
Mapas de Calor donde se ubican los riesgos																								
Seguimiento y Control																								

10. SEGUIMIENTO Y EVALUACIÓN

Al finalizar cada etapa se realizará una reunión del **Comité de Seguridad TIC (Tecnologías de Información y Comunicaciones)** para presentar el informe del avance del proyecto y de esta manera evaluar todos los pasos se han ido realizado.

[26] ISO/IEC 27000
[27] ISO/IEC 27000
[28] ISO/IEC 27000
[29] Ley 1581 de 2012, art 3
[30] ISO/IEC 27000

11. ENTREGABLES

- Informe de avance o resumen ejecutivo
- Acta de Reunión
- Plan de tratamiento de riego aprobado por los líderes
- Política de Seguridad
- Productos de cada etapa

[26] ISO/IEC 27000
[27] ISO/IEC 27000
[28] ISO/IEC 27000
[29] Ley 1581 de 2012, art 3
[30] ISO/IEC 27000

Revisó:	Aprobó:
Sandra Noguera Perafán Subgerencia Administrativa y Financiera Comité de Gestión y Desempeño	Luz Ayda Zuleta Valencia Gerente
Fecha: Enero de 2024	Fecha: Enero de 2024