PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

1. VALIDACIÓN:

	Nombre	Cargo	Fecha	Firma
Elaboro	DIEGO ALEXANDER MORALES	ING. SISTEMAS	27/01/2023	
Reviso	ALDO RODRIGUEZ	SUBGERENTE ADMINISTRATIVO	27/01/2023	
Reviso	MARISOL JARA QUITERO	COORDINADORA ASISTENCIAL Y LIDER DE CALIDAD	27/01/2023	
Aprobó	JULIA ISABEL MUELLE PLAZAS	GERENTE	27/01/2023	

2.CONTROL DE LA VIGENCIA DEL DOCUMENTO:

Tipo de Copia: Controlada ___ No Controlada ___

(Se deben hacer revisiones cada dos años a la fecha de aprobación)

Fecha de revisión 1_____ Vigente SI____ NO____ Fecha de revisión 2_____ Vigente SI__NO____

Fecha de revisión 3_____ Vigente SI____NO_____ Fecha de revisión 4_____ Vigente SI___NO___

3. CONTROL DE CAMBIOS DEL DOCUMENTO:

FECHA	RESPONSABLE	NOMBRE DEL DOCUMENTO QUE MODIFICA	CONTROL DE CAMBIO	CÓDIGO Y VERSIÓN
27/01/2023	DIEGO MORALES	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACION Y COMUNICACIONES	Actualización Por Vigencia 2023	1

4.CONTROL DE ORIGINAL Y COPIAS DEL DOCUMENTO:

Copia Nro.	Nombre de Quién Tiene Copia del Documento	Cargo	Fecha Recibido	Firma
ORIGINAL	MARISOL JARA QUINTERO	COORDINADORA ASISTENCIAL Y LIDER DE CALIDAD	ORIGINAL FIRMADO	
COPIA	DIEGO ALEXANDER MORALES	LIDER DE PROCESO	COPIA	

TABLA DE CONTENIDO

Contenido

1. VALIDACIÓN: 2

2.CONTROL DE LA VIGENCIA DEL DOCUMENTO: 2

3. CONTROL DE CAMBIOS DEL DOCUMENTO: 2

(Cuando el Documento es versión 1 este literal no aplica) ..... **¡Error! Marcador no definido.**

4.CONTROL DE ORIGINAL Y COPIAS DEL DOCUMENTO: 2

5. INTRODUCCION 4

6. OBJETIVO 4

7. DESCRIPCIÓN DE LA POLÍTICA 5

DEFINICIONES 5

8. MARCO LEGAL 8

9. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 9

10. BIBLIOGRAFIA 10

5. INTRODUCCION

La política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital. Según el manual, la implementación de la política de gobierno digital se ha definido en dos componentes: TIC para el estado y TIC para la sociedad.

6. OBJETIVO

Establecer un marco de acción para aportar a la implementación del Modelo de Seguridad y Privacidad de la información, desde el enfoque de la seguridad informática frente a ciber amenazas sobre los activos de tecnologías de información que soportan la prestación de servicios digitales de la Entidad, en atención al contexto organizacional del E.S.E HOSPITAL SALAZAR DE VILETA. las capacidades y recursos disponibles, para fortalecer la confianza de los ciudadanos, usuarios, funcionarios y demás partes interesadas.

7. DESCRIPCIÓN DE LA POLÍTICA

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de ESE Hospital Salazar de Villeta con respecto a la protección de la información y su tratamiento, con el fin de mantenerla disponible, íntegra y confidencial.

DEFINICIONES

Administración de incidentes de seguridad: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la
Infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos
Y recursos gerenciales que tiene la entidad.

Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base
en tres pilares fundamentales:

- Detectar cualquier alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio.

Alcance: Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la
Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con
El entorno, sobre todo si sólo incluye una parte de la organización.

Almacenamiento en la Nube: Del inglés cloud storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet. Esos lugares de Internet son aplicaciones o servicios que almacenan o guardan esos archivos.

Amenaza: Según [ISO IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: A partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

Características de la Información: las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.

Cifrar: Transcribir en guarismos, letras o símbolos, de acuerdo con una clave; un mensaje o texto cuyo contenido se quiere proteger.

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - Sistema de Gestión de la Seguridad de la Información.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en

que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

Directiva: Según [ISO IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Según [ISO IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evento: Según [ISO IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la
Red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: Definición en la cual se establece el compromiso de la Dirección y el enfoque De la organización en la gestión de la seguridad de la información.

8. MARCO LEGAL

La Constitución Política de Colombia, en su artículo 15, consagra que todas las personas tienen derecho a su intimidad personal, familiar y al buen nombre, debiendo el Estado respetarlos y hacerlos respetar. Del mismo modo, en el artículo 74 señala que es un derecho fundamental acceder a la información pública, salvo las excepciones que establezca la ley.

Ley 1712 de 2014, que regula el acceso a la información pública, dispuso que toda información en posesión, control o custodia de una entidad del Estado es pública, y no podrá ser reservada salvo disposición legal. Así mismo, definió que la información en posesión de una entidad pública que pertenezca al ámbito propio, particular, privado o semiprivado de una persona natural o jurídica se considerará como clasificada y gozará de protección.

El Decreto 1499 de 2017 modificó el Decreto 1083 de 2015 (Decreto Único Reglamentario del Sector de Función Pública), y adoptó el Modelo Integrado de Planeación y Gestión - MIPG.

El Copes 3854 de 2016 y la Política de Seguridad Digital se desarrollan con la implementación del "Modelo de Gestión de Riesgos de Seguridad Digital -MGRSD-".

En el Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018, en su artículo 2.2.9.1.1.3 definió la seguridad de la información como principio de la Política de Gobierno Digital.

En la Resolución 00500 de 2021 "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital."

En el Decreto 767 de 2022 "por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

En consecuencia, se convierte en prioridad establecer el marco en el cual la ESE HSV haga efectivo el derecho al acceso a la información pública de los ciudadanos y la protección de aquella que se considera reservada o clasificada.

9. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Plan de Seguridad y Privacidad de la Información			
NO.	ACTIVIDADES	META	SEGUIMIENTO (%)
1	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Acto administrativo	
2	Definir la política de seguridad y privacidad de la información	Política por aprobar	
3	Actualización y Seguimiento al Plan de Tratamiento de Riesgos de Seguridad Informática frente a Ciber amenazas	Líder TICS	
4	Definir cronograma de backups por cada uno de los equipos y manual o procedimiento para esto	Cronograma y procedimiento	
5	Revisar y asegurar que todos los equipos tienen acceso restringido	Cronograma y procedimiento	

10. BIBLIOGRAFIA

Departamento Administrativo de la Función Pública (2020). Guía para la administración del riesgo y el diseño de controles en entidades públicas.

NTC – ISO/IEC- 27001 (2013), anexo A. Objetivos de control y controles de referencia.

Ministerio de Tecnologías de la Información y las Comunicaciones (2016). Modelo de Seguridad y Privacidad de la Información versión *3.0.2*. Recuperado de https://www.mintic.gov.co/gestionti/615/articles5482_Modelo_de_Seguridad_Privacidad.pdf.

Ministerio de Tecnologías de la Información y las Comunicaciones. Política General de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones. Recuperado de https://www.mintic.gov.co/portal/604/articles62124_Politica_Seguridad_Privacidad_Informacion.pdf

Política General de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones.