SUBRED INTEGRADA DE SERVICIOS DE SALUD CENTRO ORIENTE E.S.E.

1. POLÍTICA DE SEGURIDAD DIGITAL

2. DECLARACIÓN

La Subred Integrada de Servicios de Salud Centro Oriente E.S.E. se compromete a adoptar e implementar la política de Seguridad Digital estableciendo las reglas, los lineamientos, estrategias y mecanismos para garantizar la seguridad y disponibilidad de los activos informáticos, definiendo controles que permitan mitigar los riesgos de delitos informáticos a los que se exponen los usuarios de la Subred al conectarse a la red de datos mediante un dispositivo digital.

01/11/2021
BOGOTÁ D.C

3. OBJETI VO

Adoptar la Política de Seguridad Digital expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones mediante el CONPES 3854 de 2016, el cual tiene como objeto fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

4. ALCANCE

Esta política aplica a todos los funcionarios, contratistas, terceros de la Subred Integrada de Servicios de Salud Centro Oriente E.S.E así como a los entes externos que requieran acceso a la información y la ciudadanía en general.

5. DESARROLLO Y MEDICIÓN DE LA POLÍTICA

La política de seguridad digital de la Subred Integrada de Servicios de Salud Centro Oriente ESE dentro de sus lineamientos incluye el concepto de seguridad digital en la implementación y desarrollo del Plan de Seguridad y Privacidad de la Información, teniendo en cuenta la normatividad vigente y los eventuales cambios que se puedan presentar.

Para el desarrollo de una cultura de seguridad digital se establece un proceso de capacitación permanente en seguridad de la información y seguridad digital a todos los colaboradores de la subred y demás grupos de interés externos que se identifiquen.

Desde la Oficina de Sistemas de Información TIC se fortalecerán y establecerán la infraestructura en hardware y software que permita prevenir, atender y controlar los eventos de seguridad digital que se puedan presentar en el desarrollo de las actividades propias de la entidad.

En el marco de la gestión de riesgos de la entidad se incluirán los identificados con eventos de seguridad informática derivados de las debilidades de los sistemas de información y demás plataformas informáticas, mediante la implementación de estrategias de mejoramiento continuo.

En relación con lo anterior, en los eventos que amerite se continuará con la alianza estratégica con los entes de control de incidentes de seguridad informática para el reporte y documentación de los ataques y/o eventos de seguridad detectados que puedan afectar otras entidades y/o ciudadanos.

Con la implementación de la política la Subred Integrada de Servicios de Salud Centro Oriente ESE pretende:

a. Fortalecer la Seguridad Digital de la institución.
b. Establecer la confianza de los usuarios internos y externos en el uso de los sistemas de información y servicios informáticos que brinda la Subred.
c. Establecer las buenas prácticas que lleven a la confidencialidad, seguridad y disponibilidad de la información digital que permita minimizar el riesgo de pérdida de datos.
d. Generar cultura de seguridad digital en la institución que permita minimizar la ocurrencia de amenazas informáticas que atenten contras los activos de información de la Subred.
e. Alinear las estrategias de la institución a las del orden nacional en materia de seguridad informática.

5.1 INDICADORES DE MEDICIÓN		
NOMBRE	**FÓRMULA**	**PERIODICIDAD**
Proporción de incidentes de seguridad digital gestionados	***No. De eventos de seguridad gestionados / Número de eventos de seguridad identificados * 100***	**Trimestral**

6. ALINEACIÓN DE LA POLÍTICA

La política de Seguridad Digital de la Subred Integrada de Servicios de Salud Centro Oriente E.S.E, se encuentra alineada a la Misión y Visión, ya que garantiza que se cumplan con estándares superiores en el tratamiento de la información generada desde cada uno de los procesos.

Misión; Somos la Subred Integrada de Servicios de Salud Centro Oriente del Distrito Capital, prestamos servicios de salud en el marco de una gestión clínica segura con estándares superiores de calidad, trato humanizado, mejoramiento continuo, gestión interinstitucional e intersectorial, participación comunitaria y generación del conocimiento por medio de la investigación y la docencia para impactar las condiciones de salud de usuarios, familias y comunidades, con talento humano íntegro y calificado.

Visión: En el año 2024 seremos una Subred Integrada de Servicios de Salud reconocida por la gestión de las Rutas Integrales de Atención en Salud, la atención integral, diferencial, territorial, el compromiso con la prestación de servicios seguros, humanizados, el cumplimiento de estándares superiores de calidad y la satisfacción de los usuarios y sus familias.

Adicionalmente se encuentra alineada con las normas internacionales:

- Sistema de gestión de seguridad de la información ISO 27001
- Guía de análisis y gestión de riesgos ISO 27005 y el modelo recomendado por el Ministerio TIC.
- Documento Conpes 3854. Política Nacional de Seguridad Digital.
- Resolución 500 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"*.
- Modelo de Seguridad y privacidad de la información MSPI : *El "Instrumento de Evaluación MSPI" Es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Pública*.

7. LÍNEAS DE DEFENSA

LÍNEA DE DEFENSA	RESPONSABLE	COMPROMISO
PRIMERA	Oficina Sistemas de Información TIC, Líderes de Proceso y sus equipos de trabajo.	*Autocontrol:* Conocer la política, los procedimientos, los protocolos y todas aquellas herramientas institucionales para el aseguramiento de la información en sus grupos de trabajo y los activos de información de los que son responsables.
SEGUNDA	Oficina Asesora de Desarrollo Institucional	*Monitoreo:* Monitorea el cumplimiento de la política ejecutada por la primera línea de defensa. Consolida y analiza la información resultado de la ejecución de la política y retroalimenta a la primera los resultados.
TERCERA	Oficina de Control Interno	*Enfoque evaluación independiente:* La función de la auditoría interna, a través de un enfoque basado en el riesgo, proporcionará aseguramiento objetivo e independiente sobre la eficacia de gobierno, gestión de riesgos y control interno a la alta dirección de la entidad, incluidas las maneras en que funciona la primera y segunda línea de defensa.
ESTRATÉGICA	Alta Gerencia o Comité Institucional de Gestión y Desempeño Y Comité Institucional de Coordinación de Control Interno	La responsabilidad de esta línea de defensa se centra en la emisión, revisión, validación y supervisión del cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión y auditoría interna para toda la entidad.

8. MARCO LEGAL

Documento Conpes 3854. Política Nacional de Seguridad Digital.

MSPI Resolución 500 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”

NTC-ISO /IEC 27001Conpes 3854 Política Nacional De Seguridad Digital

Ley 1712 de 2014, Ley de transparencia y acceso a la información pública.

Ley 734 de 2002 Por la cual se expide el Código Disciplinario Único

Ley 1341 de 2009, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

Decreto 1078 de 2015 artículo 2.2.9.1.2.1 "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

Decreto 2106 de 2019 artículo 16 “Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública”

9. GLOSARIO

Activo de Información: se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

Análisis de Riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo NTC-ISO /IEC 27001.

Confidencialidad: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.

Controles: Medida que permite reducir o mitigar un riesgo.

Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

Integridad: Propiedad de la información que busca preservar su exactitud y completitud.

Sistema de Gestión de Seguridad de la Información: Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

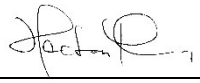
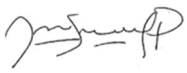
Riesgo: Efecto de la incertidumbre sobre los objetivos.

Tecnologías de la Información (TI): Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.

10. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE CREACIÓN O ACTUALIZACIÓN
001	02-12-2021	Creación de documento

11. CONTROL DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Ing. Héctor Recaman Ing. César Prieto	Nombre: Ing. Jorge Eduardo Sandoval Plazas	Nombre: Claudia Lucia Ardila Torres
Cargo y/o actividad: Líder Data Center Técnico Operativo TIC	Cargo y/o actividad: Jefe Oficina Sistemas de Información TIC	Cargo y/o actividad: Gerente
Fecha: 02/12/2021	Fecha: 02/12/2021	Fecha: 02/12/2021
Firma: 	Firma: 	Firma: