RESOLUCIÓN No. 146
(27 de diciembre de 2021)
"Por medio de la cual se adopta la Política de Seguridad Digital para la ESE. Hospital Octavio Olivares – Puerto Nare.

EL GERENTE

De la "Empresa Social del Estado ESE. Hospital Octavio Olivares – Puerto Nare – Antioquia", en uso de sus atribuciones legales, y en especial por las conferidas en la Ley 100 de 1993, el Decreto 1499 de 2017, Decreto 1083 de 2015, Decreto 113 de 28 de abril de 2020 de la Junta Directiva del Hospital, y la Resoluciones 710 de 2012, 743 de 2013 y 408 de 2018 y,

CONSIDERANDO

Normatividad	Descripción
Artículo 61 de la constitución Política de 1991.	El Estado protegerá la propiedad intelectual por el tiempo y formalidades que establezcan a Ley.
Ley 23 de 1982	Derechos de Autor.
Ley 57 de 1985	Publicidad de los actos y documentos oficiales.
Decreto Ley 2150 de 1995	Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 594 de 2000	Ley General de Archivos. 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. (Ley 594 de 2000, art 3).
Ley 603 de 2000	Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
Ley 594 de 2004.	Por medio de la cual se dictan la Ley General de Archivo y se dictan otras disposiciones.
Ley 962 de 2005	Racionalización de trámites y procedimientos administrativos procedimientos administrativos.
Ley 1150 de 2007	Seguridad de la información electrónica en contratación en línea.

Ley 1266 de 2008	Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países".
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC– se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 del 30 Julio de 2009.	Por la cual se definen principios y conceptos sobre la sociedad de la información, y organización de las tecnologías de la información y comunicaciones. Parágrafo de su artículo 38 establece que: "Las autoridades territoriales implementarán los mecanismos a su alcance para gestionar recursos a nivel nacional e internacional, para apoyar la masificación de las TIC, en sus respectivas jurisdicciones".
Decreto 235 de enero de 2010.	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Decreto 1151 de 04 de abril de 2008 y Manual para la Implementación de la Estrategia de Gobierno en Línea.	Por medio del cual se establecen los lineamientos generales de la estrategia de gobierno en línea de la República de Colombia. Se reglamenta parcialmente la Ley 962 de 2005 y se dicta otras disposiciones
Ley 1438 de 2011	Por medio del cual se reforma el sistema general de Seguridad Social en Salud y se dictan otras disposiciones. Parágrafo "transitorio" del Artículo 112 "La historia clínica única electrónica será de obligatoria aplicación antes del 31 de diciembre de 2013.
Ley 1437 de 2011	Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
Ley 1474 de 2011	Se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, hace referencia al uso obligatorio de los sitios web de las entidades públicas como mecanismo para la divulgación de información pública.
Ley 1450 de 2011	Artículo 232. La Racionalización de trámites y procedimientos al interior de las entidades públicas. Que: los organismos y entidades de la Rama Ejecutiva del Orden Nacional y Territorial procederán a identificar, racionalizar y simplificar los procesos, procedimientos, trámites y servicios internos, con el propósito de eliminar duplicidad de funciones y barreras que impidan la oportuna, eficiente y eficaz prestación del servicio en la gestión de las organizaciones.
Decreto 2693 de 2012	Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Ley 1581 de 2012	Art. 3. Autorización Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
Decreto 2364 de 2012	Firma electrónica.
Decreto 2609 de 2012	Expediente electrónico Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
Decreto 2693 de 2012	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
Decreto – Ley 019 de 2012	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública, estableció en su artículo 4, en relación con la celeridad en las actuaciones administrativas, que: "Las autoridades tienen el impulso oficioso de los procesos administrativos; deben utilizar: formularios gratuitos para actuaciones en serie, cuando la naturaleza de ellas lo haga posible y cuando sea asunto de su competencia, suprimir los trámites innecesarios, sin que ello las releve de la obligación de considerar y valorar todos los argumentos de los interesados y los medios de pruebas decretados y practicados; deben incentivar el uso de las tecnologías de la información y las comunicaciones a efectos de que los procesos administrativos se adelanten con diligencia, dentro de los términos legales y sin dilaciones injustificadas; y deben adoptar las decisiones administrativas en el menor tiempo posible".
Decreto 1377 de 2013	Art. 3 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. 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
Ley estatutaria 1618 de 2013	Ejercicio pleno de las personas con discapacidad.
Decreto N° 2573 de 2014	Se reglamenta parcialmente la Ley 1341 de 2009 y que en el mismo decreto se define el componente de Privacidad y Seguridad de la información que incluye el modelo de seguridad y privacidad de la información (MSPI), y para ello cuenta con una serie de guías anexas que ayudan a las entidades a cumplir con lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuales son los resultados a obtener y como desarrollarlos.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. 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. (Ley 1712 de 2014, art 4).
Acuerdo 03 de 2015	del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.
Anexo 1 - Resolución 3564 de 2015	Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
Ley Estatutaria 1757 de 2015	Promoción y protección del derecho a la participación democrática.
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.
Decreto 103 de 2015	derogado parcialmente por el decreto 1081 d 2015. Por el cual se reglamenta parcialmente la ley 1712 de 2014
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
NTC-ISO/IEC 27002.	Establece las mejores prácticas para la implementación del Sistema de Gestión de Seguridad de la Información.
NTC-ISO/IEC 27001.	Señala los requerimientos del Sistema de Gestión de Seguridad de la Información.
CONPES - Política Nacional de Seguridad Digital	Se tiene como objetivo: "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".
Decreto 415 de 2016	Se adiciona al decreto único reglamentario de la función pública la definición de lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital.
Decreto 1499 de 2017	Se modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.
Decreto 1413 de 2017	(Título 17, parte 2, libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 612 del 04 de abril de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Ley 1928 de 2018	Por medio de la cual se aprueba el convenio sobre la ciberdelincuencia.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital, la cual tiene por objeto 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.
Ley 1955 de 2019	"POR EL CUAL SE EXPIDE EL PLAN NACIONAL DE DESARROLLO 2018-2022 "PACTO POR COLOMBIA, PACTO POR LA EQUIDAD" **ARTÍCULO 147º. TRANSFORMACIÓN DIGITAL PÚBLICA.** Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. En todos los escenarios la transformación digital deberá incorporar los componentes asociados a tecnologías emergentes, definidos como aquellos de la Cuarta Revolución Industrial, entre otros. Las entidades territoriales podrán definir estrategias de ciudades y territorios inteligentes, para lo cual deberán incorporar los lineamientos técnicos en el componente de transformación digital que elabore el Ministerio de Tecnologías de la Información y las Comunicaciones. Los proyectos estratégicos de transformación digital se orientarán por los siguientes principios: 1. Uso y aprovechamiento de la infraestructura de datos públicos, con un enfoque de apertura por defecto. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales. 3. Plena interoperabilidad entre los sistemas de información públicos que garantice el suministro e intercambio de la información de manera ágil y eficiente a través de una plataforma de interoperabilidad. Se habilita de forma plena, permanente y en tiempo real cuando se requiera, el intercambio de información de forma electrónica en los estándares definidos por el Ministerio TIC, entre entidades públicas. Dando cumplimiento a la protección de datos personales y salvaguarda de la información. 4. Optimización de la gestión de recursos públicos en proyectos de Tecnologías de la Información a través del uso de los instrumentos de agregación de demanda y priorización de los servicios de nube. 5. Promoción de tecnologías basadas en software libre o código abierto, lo anterior, sin perjuicio de la inversión en tecnologías cerradas. En todos los casos la necesidad tecnológica deberá justificarse teniendo en cuenta análisis de costo-beneficio. 6. Priorización de tecnologías emergentes de la Cuarta Revolución Industrial que faciliten la prestación de servicios del Estado a través de nuevos modelos

incluyendo, pero no limitado a, tecnologías de desintermediación, DLT (Distributed Ledger Technology), análisis masivo de datos (Big data), inteligencia artificial (AI), Internet de las Cosas (IoT), Robótica y similares.

7. Vinculación de todas las interacciones digitales entre el Estado y sus usuarios a través del Portal Único del Estado colombiano.
8. Implementación de todos los trámites nuevos en forma digital o electrónica sin ninguna excepción, en consecuencia, la interacción del Ciudadano-Estado sólo será presencial cuando sea la única opción.
9. Implementación de la política de racionalización de trámites para todos los trámites, eliminación de los que no se requieran, así como en el aprovechamiento de las tecnologías emergentes y exponenciales.
10. Inclusión de programas de uso de tecnología para participación ciudadana y gobierno abierto en los procesos misionales de las entidades públicas.
11. Inclusión y actualización permanente de políticas de seguridad y confianza digital.
12. Implementación de estrategias público-privadas que propendan por el uso de medios de pago electrónicos, siguiendo los lineamientos que se establezcan en el Programa de Digitalización de la Economía que adopte el Gobierno nacional.
13. Promoción del uso de medios de pago electrónico en la economía, conforme a la estrategia que defina el Gobierno nacional para generar una red masiva de aceptación de medios de pago electrónicos por parte de las entidades públicas y privadas.

PARÁGRAFO. Los trámites y servicios que se deriven de los anteriores principios podrán ser ofrecidos tanto por personas jurídicas privadas como públicas, incluyendo a la entidad que haga las veces de articulador de servicios ciudadanos digitales, o la que defina el Ministerio TIC para tal fin.

(Ver Directiva Presidencial 03 de 2021)

ARTÍCULO 148º. GOBIERNO DIGITAL COMO POLÍTICA DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL. Modifíquese el artículo 230 de la Ley 1450 de 2011, el cual quedará así:

ARTÍCULO 230. GOBIERNO DIGITAL COMO POLÍTICA DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL. Todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones para la implementación de la política de Gobierno Digital.

	Esta política liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones contemplará como acciones prioritarias el cumplimiento de los lineamientos y estándares para la integración de trámites al Portal Único del Estado Colombiano, la publicación y el aprovechamiento de datos públicos, la adopción del modelo de territorios y ciudades inteligentes, la optimización de compras públicas de tecnologías de la información, la oferta y uso de software público, el aprovechamiento de tecnologías emergentes en el sector público, incremento de la confianza y la seguridad digital y el fomento a la participación y la democracia por medios digitales. El Gobierno implementará mecanismos que permitan un monitoreo permanente sobre el uso, calidad, nivel de satisfacción e impacto de estas acciones.
Decreto 2106 de 2019	**"Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública"** **ARTÍCULO 8. Obligación de uso de los canales digitales entre autoridades.** Cuando las entidades habiliten canales digitales para el cumplimiento de sus competencias deberán relacionarse por dichos medios. Únicamente se utilizarán otros medios cuando la ley así lo exija. **ARTÍCULO 17. Transacciones a través de medios electrónicos.** Las autoridades deberán habilitar medios de pago electrónicos para las transacciones que se realicen a favor del Estado o de la entidad en relación con el pago de las tarifas asociadas a trámites, procesos y procedimientos.
Directiva Presidencial 02 de 2019	Simplificación de la interacción digital entre los ciudadanos y el Estado.

Que, en mérito de lo expuesto,

RESULVE

Artículo 1°. Objeto. La presente Resolución tiene como objeto adoptar la Política de Seguridad Digital para la ESE. Hospital Octavio Olivares – Puerto Nare. El Hospital se compromete con la implementación de la política de Seguridad Digital estableciendo reglas, lineamientos y mecanismos para garantizar seguridad y disponibilidad de los activos informáticos definiendo controles que permitan mitigar los riesgos de delitos informáticos como el uso indebido de información, interceptación, robo o suplantación de identidad, entre otros. Riesgos a los que está expuesto un dispositivo al conectarse a la red del Hospital o al interactuar con otros dispositivos

A partir del artículo 133 de la Ley 1753 de 2015 y del Decreto 1499 de 2017, el Modelo Integrado de Planeación y Gestión (MIPG) integró los sistemas de gestión de la calidad de la Ley 872 de 2003 y de

Desarrollo Administrativo de que trataba la Ley 489 de 1998 y fueron derogados los artículos del 15 al 23 de la Ley 489 de 1998 y la Ley 872 de 2003.

El Modelo Integrado de Planeación y Gestión MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio.

MIPG busca mejorar la capacidad del Estado para cumplirle a la ciudadanía, incrementando la confianza de la ciudadanía en sus entidades y en los servidores públicos, logrando mejores niveles de gobernabilidad y legitimidad del aparato público y generando resultados con valores a partir de una mejor coordinación interinstitucional, compromiso del servidor público, mayor presencia en el territorio y mejor aprovechamiento y difusión de información confiable y oportuna es una de los objetivos de la puesta en marcha del Modelo Integrado de Planeación y Gestión MIPG.

Con la política de Seguridad Digital se pretende fortalecer las capacidades de las 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.

La ESE. Hospital, entendiendo la importancia de una adecuada gestión de la información se ha comprometido con la implementación de un sistema de gestión de seguridad digital de la información buscando fortalecer un arco de confianza en el ejercicio de sus deberes con el estado y los ciudadanos, todo enmarcado en el cumplimiento de la Ley de transparencia y del derecho a la información pública 1712 de 2014.

Para la ESE. Hospital, la protección de la información digital busca la disminución de riesgos sobre la información, con el objeto de mantener un nivel de integridad, confidencialidad y la disponibilidad de la información acorde con las necesidades de los diferentes grupos de interés de la institución.

De acuerdo con lo anterior esta Polltica aplica al hospital, y se basa teniendo en cuenta los procesos y procedimientos que se desarrollan en la institución, y estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Proteger los procesos, procedimientos e instructivos en materia de seguridad de información.

- ♣ Fortalecer la seguridad de la información mediante la instalación de nuevos equipos tecnológicos, para garantizar la continuidad de la prestación de servicios de salud frente a incidentes.
- ♣ Fortalecer el buen manejo de los recursos y unidades de almacenamientos compartidos en la red.

Artículo 2°. OBJETIVO GENERAL. Establecer los lineamientos institucionales para la gerencia y seguridad de la información generada y custodiada por la ESE hospital, asegurando la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés y cumpliendo con los lineamientos de la planificación estratégica para el direccionamiento del modelo de atención integral, confiable, seguro y humanizado para la prestación del servicio de salud.

OBJETIVOS ESPECÍFICOS

- ♣ Establecer y mantener la política de Seguridad Digital.
- ♣ Administrar los riesgos de seguridad de la información.
- ♣ Identificar y dar seguimiento a las amenazas de seguridad de la información.
- ♣ Proteger los activos de información, con base en los criterios de confidencialidad, integridad, disponibilidad.
- ♣ Fomentar y difundir la política de seguridad Digital.
- ♣ Establecer las bases fundamentales para la protección de los activos de la información ya sean físicos o electrónicos.
- ♣ Minimizar el riesgo en la seguridad de la información de los procesos misionales de la entidad.
- ♣ Cumplir con los principios de seguridad de la información, y así mantener la confianza de sus usuarios y colaboradores.
- ♣ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ♣ Fortalecer la cultura de seguridad de la información en los usuarios, funcionarios, ejecutores, terceros, proveedores y la ciudadanía en general de la ESE. Hospital.
- ♣ Garantizar la continuidad de la prestación del servicio misional frente a incidentes, dando sostenibilidad a la prestación del servicio de salud.

Artículo 3°. ALCANCE. Los lineamientos contenidos en la presente política son de observancia obligatoria para todo el personal que labore en, o para el Hospital, que por sus funciones tenga acceso a equipos de cómputo, sistemas y aplicaciones, bases de datos, instalaciones del centro de cómputo y en general, a todos los recursos informáticos de la organización.

Artículo 4°. DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios del hospital y, en consecuencia, debe ser protegido.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000

Acuerdo de Confidencialidad: es un documento en los que los funcionarios o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la entidad, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de

datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación y su uso no autorizado.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Estándar: Es el conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Un estándar se construye a través de consenso y refleja la experiencia y las mejores prácticas en un área en particular, implican uniformidad y normalización y es de obligatorio cumplimiento.

Hardware: Refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Informática: La informática es una ciencia que estudia métodos, procesos, técnicas, con el fin de almacenar, procesar y transmitir información y datos en formato digital.

Integridad: es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes al hospital.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Lineamientos: Directriz o disposición establecida por el Ministerio TIC, que debe ser implementada por las entidades públicas para el desarrollo de la Política de Gobierno Digital y se desarrolla a través de estándares, guías, recomendaciones o buenas prácticas.

Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros, CDs, DVDs y unidades de almacenamiento USB.

Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la institución.

Registros de Auditoría o Log: son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos del hospital. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los altos mandos, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

PSD: Política de Seguridad Digital

Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la

interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la institución o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Sistemas de control ambiental: son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.
Software: Equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Tecnología: Es el conjunto de conocimientos técnicos, ordenados científicamente, que permiten diseñar y crear bienes y servicios que facilitan la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de la humanidad.

Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Vulnerabilidades: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el hospital (amenazas), las cuales se constituyen en fuentes de riesgo.

Artículo 5°. Lineamientos de la Política Gobierno Digital. En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

Con la política se fortalecen 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, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional 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.

En el orden nacional, en los Comités Sectoriales de Gestión y Desempeño se darán las directrices para su implementación. Además, la articulación en materia de Seguridad Digital estará a cargo del enlace sectorial de seguridad digital quien será el encargado de rendir cuentas al Coordinador Nacional de Seguridad Digital acerca de la implementación de la Política Nacional de Seguridad Digital en el respectivo sector.

De otro lado, en el Comité Institucional de Gestión y Desempeño se debe articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política. Para ello, se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área transversal que haga parte de la Alta Dirección. Para las entidades cabeza de sector, el Responsable de Seguridad Digital será el designado como enlace sectorial de seguridad digital.

En el orden territorial, MinTIC definirá los lineamientos para que las entidades territoriales definan la figura del enlace de Seguridad Digital territorial para la implementación de la política de Seguridad Digital, así como las instancias respectivas para la articulación con el Coordinador Nacional de Seguridad Digital.

Artículo 6°. ESTRATEGIAS: La estrategia informática de la institución está orientada hacia los siguientes puntos:

- Plataforma de sistemas abiertos.
- Esquemas de operación bajo el concepto cliente/servidor y web en caso de desarrollos probados.
- Estandarización de hardware, software base, utilitarios y estructuras de datos.
- Intercomunicación entre unidades y equipos mediante protocolos estándares.
- Manejo de proyectos conjuntos con las diferentes áreas.
- Integración de sistemas y bases de datos.
- Programación con ayudas visuales e interactivas. Facilitando interfaces amigables al usuario final.
- Integración de sistemas tele informáticos.
- Para la elaboración de los proyectos informáticos y de sus presupuestos, se tomarán en cuentan tanto las necesidades de hardware y software del área solicitante, como la disponibilidad de recursos con que éstas cuenten.
- Definir e implementar Plan de Seguridad y privacidad de la información que incluya la seguridad digital, soportado en lineamientos claros acordes a las necesidades y a la normatividad.
- Brindar capacitación en seguridad de la información y seguridad digital, a los colaboradores.

- Implementar mecanismos y herramientas que permitan prevenir, atender, controlar y regular los incidentes o emergencias digitales para afrontar las amenazas y los riesgos que atentan contra la seguridad digital.

- Adoptar una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información e infraestructura implementando estrategias de mejoramiento continuo.

- Elaborar procedimientos de acuerdo a la normatividad que permitan minimizar los riesgos asociados con seguridad digital, validando y monitoreando con frecuencia los riesgos.

- Gestionar los incidentes de seguridad digital y en caso de ser necesario dar aviso a autoridades competentes, de acuerdo con las normas legales establecida

Artículo 7°. RESULTADOS ESPERADOS DE LA POLÍTICA

- Fortalecimiento de la Seguridad Digital de la institución.

- Brindar la confianza a nuestros usuarios y colaboradores.

- 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.

- Desarrollo de las estrategias de la Política de Seguridad Digital buscan contrarrestar el incremento de las amenazas informáticas que pueden afectar significativamente el Hospital

Artículo 8°. METAS

- Identificar y actualizar un mapa de riesgos sobre las actividades institucionales en la seguridad de la informática.

- Formular y elaborar y poner en marcha el plan de seguridad y privacidad sobre la información.

- Formular, elaborar e implementar controles de acceso a la información, sistemas y recursos de red.

- Diseñar e implementar un plan de seguridad para el almacenamiento de la información.

Artículo 9°. INDICADORES

- Actualizar un (1) mapa de riesgos sobre la seguridad digital e informática.

- ♣ Elaborar y poner en marcha un (1) plan de seguridad y privacidad en el manejo de la información.
- ♣ Controles de acceso a la información / controles programados *100
- ♣ Elaborar y poner en marcha un (1) plan de seguridad para el almacenamiento de la información.
- ♣ Proporción de incidentes relacionados con seguridad digital
- ♣ Proporción de incidentes relacionados con seguridad digital gestionados

Artículo 10. Vigencia. La presente Resolución rige a partir del día siguiente a la fecha de su expedición y deroga a las demás normas o disposiciones que le sean contrarias.

Se expide en Puerto Nare, Antioquia, a los 27 días del mes de diciembre del año 2021.

COMUNÍQUESE Y CÚMPLASE

CIRO GOMEZ BARRIOS
ESE. Hospital Octavio Olivares – Puerto Nare
Gerente