1. NOMBRE DE LA POLITICA

POLITICA DE SEGURIDAD DIGITAL - LINEAS DE INTERVENCIÓN

2. PRESENTACION

La Seguridad Digital es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante (datos). Para ello existen una serie de estándares. protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información, Para lograrla, es necesario tomar en cuenta y poner en práctica el tridente defensivo, el cual consta de:

CORTAFUEGOS: Es un sistema que se utiliza para evitar que usuarios desautorizados tengan acceso a las redes privadas conectadas con Internet.

ANTIVIRUS: Previene o evitar la activación de virus, así como su propagación y contagio.

ACTUALIZACIONES DE SEGURIDAD: Para que un sistema operativo esté exento de ataques por parte de virus, gusanos, troyanos e intrusos, hay que actualizarlo periódicamente. Las actualizaciones automáticas se activan por defecto mientras el equipo esté conectado a Internet, de acuerdo a la programación que previamente se haya definido: pero también se realizar de forma manual.

3. MARCO LEGAL - NORMATIVIDAD QUE LA SOPORTA

Ley 1273 de 2009: Modifica el Código Penal colombiano, creando nuevos tipos penales relacionados con la protección de la información y los datos informáticos (Delitos Informáticos). Es la base legal para sancionar accesos no autorizados, daño informático, interceptación ilegal, entre otros.
Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales y se regula su tratamiento. Esta ley establece principios y derechos fundamentales en el manejo de información personal.
Decreto 1377 de 2013: Reglamenta parcialmente la Ley 1581 de 2012 en cuanto al tratamiento de datos personales y las medidas de seguridad que deben adoptar las entidades públicas y privadas.
Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, que obliga a las entidades a garantizar el acceso, integridad, confidencialidad y disponibilidad de la información pública.
Ley 1753 de 2015 (Art. 147 y 148): Plan Nacional de Desarrollo 2014–2018, que introdujo disposiciones para establecer la **estrategia nacional de seguridad digital**.
Documento CONPES 3854 de 2016: Define la **Política Nacional de Seguridad Digital**, cuyo objetivo es fortalecer las capacidades del Estado, del sector privado y de la ciudadanía para gestionar riesgos en el entorno digital.
Decreto 1499 de 2017: Por el cual se actualiza el **Modelo Integrado de Planeación y Gestión (MIPG)** e incluye la Política de Seguridad Digital como parte de la gestión estratégica en las entidades públicas.
Ley 1978 de 2019: Reforma del sector TIC, que impulsa el uso responsable de la tecnología, el desarrollo de servicios digitales seguros y promueve la transformación digital del Estado.
Decreto 612 de 2018: Establece directrices para la gestión del riesgo y control interno, donde la seguridad digital es un componente clave para la administración eficiente y segura de la información.

Política de Gobierno Digital (Resolución MinTIC 500 de 2021): Que reemplazó la política de Gobierno en Línea y establece el marco para el uso estratégico de las TIC, incluyendo la seguridad digital como componente transversal.
Guía para la implementación de la Seguridad Digital en el Estado Colombiano (MinTIC): Documento de referencia para aplicar buenas prácticas, evaluaciones de riesgo y controles de seguridad de la información.

4. ALINEACION DE LA POLITICA CON EL DIRECCIONAMIENTO ESTRATEGICO DE LA ESE

Misión Somos una ESE acreditada por la UNICEF como Institución Amiga de la Mujer y de la Infancia – IAMI; que presta servicios de salud con altos estándares de calidad, que garantiza una atención eficaz, efectiva y oportuna a nuestros usuarios.

Visión En el año 2028 seremos, una organización que presta servicios de primer nivel y segundo nivel de atención, reconocidos por el mejoramiento continuo de sus procesos, centrada en el usuario y su familia, fortalecimiento del talento humano, innovadores en la prestación de servicios de salud, con auto sostenibilidad económica y rentabilidad social.

Propósitos

✓ Compromiso en la gestión de su rol misional.

✓ Garantizar capacitación y actualización.

✓ Mantener el fomento a una población saludable.

✓ Garantía de excelentes servicios de atención y prevención en salud.

✓ Mejoramiento de un sistema de desarrollo organizacional.

✓ Mejoramiento de condiciones laborales, en cuanto a su economía y compensación.

✓ Mejoramiento de la salud y estilos de vida de la población

✓ Garantizar las tecnologías de la información y la comunicación en salud actualizadas para el mejoramiento del hospital.

✓ Trabajar con sentido social y humano.

✓ Trabajar con transparencia, ética y eficiencia.

Valores Institucionales

✓ Compromiso: Lo damos todo para lograr nuestros objetivos.

✓ Cumplimiento: Nos permite llegar lejos como personas, organización y conseguir lo que anhelamos. Adquirimos compromisos, sinceros para concluirlos, es toma responsabilidades y actuar en consecuencia a ellas.

✓ Disciplina: Tenemos la capacidad para poner en práctica una serie de principios relativos al orden y la constancia, tanto para la ejecución de tareas y actividades cotidianas.

✓ Equidad: Tratamos a todos por igual, independiente de su clase social, raza, sexo o religión.

✓ Respeto: Reconocemos y toleramos las creencias, actuaciones, sentimientos y motivos de las personas.

✓ Responsabilidad: Asumir las consecuencias de nuestros actos y cumplir con nuestros compromisos y obligaciones ante los demás.

Principios Institucionales

✓ Vocación de servicio: Actitud de vida de colaboración hacia los demás, en todo momento y en todas partes, que lleva a acciones desinteresadas que contribuyen a hacer más ligera y placentera la vida de los otros sin buscar recompensa, agradecimiento y/o admiración.

✓ Trabajo en equipo: Unir el esfuerzo con quienes participan en los procesos y actividades sin excepción, con armonía, cooperación, compromiso y responsabilidad compartida, para multiplicar el logro de resultados en búsqueda de los objetivos y metas comunes.

✓ Excelencia del servicio: Mantener siempre una actitud de servicio frente a nuestros clientes internos y externos, buscando solucionar de manera oportuna sus necesidades.

✓ Prospectiva de Gestión: Buscamos con nuestras actividades diarias alcanzar el nivel máximo de calidad, eficiencia y efectividad en nuestros compromisos.

Políticas Institucionales

✓ Política Estratégica de Gestión del Talento Humano

✓ Política de Gestión Económica y Financiera:

✓ Política Integral de Gestión de Calidad

✓ Política de Gerencia Tecnologías de Información y Comunicación:

✓ Política de Humanización y Seguridad del Paciente

✓ Política Instituciones Amigas de la Mujer y la Infancia (IAMI)

✓ Política de Renovación Tecnológica, Modernización de Infraestructura, Dotación y Mantenimiento Hospitalario

✓ Política de Fortalecimiento de la Salud Pública

✓ Política de Contingencia Epidemiológica

5. DECLARACIÓN DE LA POLÍTICA

La E.S.E. Hospital del Rosario reconoce la importancia de garantizar un entorno digital confiable, seguro y resiliente que proteja los activos de información institucionales y salvaguarde los derechos de los ciudadanos frente a las amenazas digitales emergentes.

Conscientes del valor de la información como recurso estratégico para la prestación de servicios de salud y el cumplimiento de los objetivos institucionales, la entidad adopta esta Política de Seguridad Digital como una guía para prevenir, detectar, responder y recuperarse ante eventos que comprometan la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

Esta política se fundamenta en los principios de gestión del riesgo, mejora continua, corresponsabilidad y cumplimiento legal, promoviendo una cultura organizacional que fomente el uso seguro y responsable de las tecnologías de la información y la comunicación.

Asimismo, se alinea con la Política Nacional de Seguridad Digital, el Modelo Integrado de Planeación y Gestión – MIPG, la Política de Gobierno Digital, y demás normas nacionales e internacionales que rigen el uso y protección de la información en el sector público.

Con esta declaración, la E.S.E. Hospital del Rosario se compromete a implementar medidas técnicas, administrativas y humanas que fortalezcan su seguridad digital, protejan la privacidad de los datos y aseguren la continuidad de sus procesos misionales.

6. ALCANCE DE LA POLITICA

La presente política aplica a todos los funcionarios, contratistas, proveedores y terceros que manejen información de la E.S.E. Hospital del Rosario, así como a los sistemas, equipos, redes y plataformas utilizadas. Incluye la protección de los activos de información institucional, garantizando su confidencialidad, integridad y disponibilidad. Se aplicará en todas las sedes y puntos de atención, promoviendo el uso seguro de las tecnologías conforme a la normativa vigente y buenas prácticas.

7. OBJETIVO DE LA POLITICA

Objetivo General

Establecer directrices y medidas para proteger la información y los activos digitales de la E.S.E. Hospital del Rosario, garantizando su confidencialidad, integridad y disponibilidad, mediante la gestión adecuada de riesgos y el uso seguro de las tecnologías de la información.

Objetivos Específicos

Fortalecer la cultura de seguridad digital entre los funcionarios y contratistas mediante procesos de sensibilización y capacitación continua.
Implementar controles técnicos y administrativos que mitiguen los riesgos asociados al uso de tecnologías de la información y a la gestión de datos.
Garantizar la disponibilidad y continuidad de los servicios digitales ante incidentes de seguridad o eventos disruptivos.
Promover el cumplimiento normativo en materia de protección de datos personales, delitos informáticos y estándares internacionales de seguridad.

Fomentar la mejora continua en los procesos de seguridad digital mediante auditorías, monitoreo y actualización de políticas y procedimientos.

8. LINEAMIENTO Y ESTRATEGIA DE ACCIÓN DE LA POLITICA

Lineamientos de la Política de Seguridad Digital

1. **Confidencialidad de la información**: Se deben establecer controles para asegurar que solo las personas autorizadas tengan acceso a la información sensible o crítica de la E.S.E.
2. **Integridad de los datos**: Toda la información debe mantenerse completa, precisa y sin alteraciones no autorizadas durante su procesamiento, almacenamiento o transmisión.
3. **Disponibilidad de los servicios**: Se deben garantizar medidas para asegurar que los sistemas de información estén disponibles y operativos ante cualquier eventualidad.
4. **Gestión de riesgos**: Identificar, evaluar y tratar los riesgos asociados al uso de tecnologías de la información, para prevenir incidentes que puedan afectar la operación de la entidad.
5. **Cumplimiento normativo**: Alinear todas las acciones con las leyes y reglamentos vigentes en Colombia sobre protección de datos, delitos informáticos y seguridad digital.
6. **Responsabilidad y control de accesos**: Asignar niveles de acceso a los sistemas de información según roles y funciones, implementando mecanismos de autenticación y trazabilidad.
7. **Educación y sensibilización**: Promover una cultura organizacional enfocada en el uso seguro de las tecnologías mediante campañas de concienciación y formación permanente.
8. **Mejora continua**: Evaluar periódicamente la efectividad de las medidas de seguridad adoptadas, proponiendo ajustes según necesidades, amenazas o avances tecnológicos.

Estrategia de la Política de Seguridad Digital

La estrategia se fundamenta en los siguientes componentes:

Diagnóstico institucional: Identificar el estado actual de la seguridad digital en la E.S.E., evaluando fortalezas, debilidades, amenazas y oportunidades.

Definición de roles y responsabilidades: Establecer un equipo responsable de la seguridad digital, con funciones claras de liderazgo, control, monitoreo y respuesta ante incidentes.

Plan de acción: Diseñar e implementar actividades concretas orientadas a proteger los activos de información, prevenir vulnerabilidades y gestionar eventos de riesgo.

Capacitación y sensibilización: Desarrollar programas de formación para funcionarios y contratistas, enfocados en buenas prácticas y normativas aplicables.

Monitoreo y seguimiento: Aplicar indicadores de desempeño y mecanismos de control que permitan evaluar la eficacia de la política y sus acciones operativas.

Articulación con otras políticas institucionales: Alinear la política de seguridad digital con los planes estratégicos de la entidad, la política de gobierno digital, y los marcos de planeación y gestión pública (como el MIPG).

9. CONCEPTOS GENERALES Y DEFINICIONES PARA LA IMPLEMENTACION DE LA POLITICA

1. Seguridad Digital: Conjunto de prácticas, medidas técnicas, organizacionales y legales adoptadas para proteger los activos de información y garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de los datos en los entornos digitales.

2. Activo de Información: Todo recurso de valor para la entidad que contiene datos o información, incluyendo bases de datos, sistemas, aplicaciones, documentos electrónicos, redes y equipos tecnológicos.

3. Confidencialidad: Principio de seguridad que asegura que la información solo sea accesible por personas autorizadas, previniendo el acceso no autorizado o la divulgación indebida.

4. Integridad: Propiedad que garantiza que los datos no han sido modificados, alterados o eliminados de forma no autorizada, y que se mantienen completos y correctos.

5. Disponibilidad: Asegura que los activos de información y servicios tecnológicos estén accesibles y funcionales cuando sean requeridos por los usuarios autorizados.

6. Gestión de Riesgos de Seguridad Digital: Proceso sistemático de identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos que afectan la seguridad de la información y los sistemas digitales de la entidad.

7. Incidente de Seguridad Digital: Cualquier evento no planificado que afecte o pueda afectar la confidencialidad, integridad o disponibilidad de los activos de información, incluyendo accesos no autorizados, ataques informáticos, pérdidas de datos o fallas de sistemas.

8. Usuario Autorizado: Persona que ha recibido permisos formales para acceder a los sistemas de información de la entidad, en función de su rol o responsabilidad.

9. Políticas de Seguridad de la Información: Conjunto de lineamientos y directrices que regulan el uso adecuado de los recursos tecnológicos y la protección de la información dentro de la organización.

10. Ciberseguridad: Campo relacionado con la protección de sistemas, redes y programas frente a ataques digitales. La ciberseguridad forma parte de la seguridad digital, enfocándose en prevenir amenazas externas.

11. Buenas Prácticas en Seguridad Digital: Acciones y hábitos recomendados para el uso responsable y seguro de las tecnologías, tales como el uso de contraseñas robustas, actualizaciones frecuentes de software, y el reporte oportuno de incidentes.

12. Trazabilidad: Capacidad para rastrear y registrar cada acción realizada sobre los activos digitales, permitiendo identificar quién, cuándo y cómo se accedió o modificó determinada información.

10. ACTIVIDADES OPERATIVAS PARA LA IMPLEMENTACIÓN DE LA POLITICA

SEGURIDAD DE LA RED E INTERNET

1. Toda cuenta de acceso al sistema, a la red y direcciones IP, será asignada por el Área de Sistemas de la ESE Hospital Del Rosario de Campoalegre previa solicitud oral o escrito.
2. Se prohíbe utilizar la red y los equipos de la ESE para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular.
3. En lo relacionado con el uso de correo electrónico, no está permitido el uso del correo personal. Los correos institucionales deben ser para uso exclusivo de las actividades de la ESE Hospital Del Rosario de Campoalegre.
4. Para garantizar la seguridad de la información y el equipo informático. el Área de Sistemas establece filtros y medidas para regular el acceso a contenidos en el cumplimiento de esta normatividad.
5. El acceso a la red interna, se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, y éste será permitido únicamente por el área de Sistemas.
6. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoría de seguridad y un reporte de los hallazgos a la oficina de Control Interno Disciplinario para que se tomen las medidas pertinentes.
7. Los mensajes y la información contenida en los buzones de correo son de propiedad de la ESE Hospital del Rosario.
8. No envío de correo masivo. Se refiere a aquel enviado en un gran número de receptores sin un propósito relacionado con el negocio. Estos tipos de mensajes degradan el desempeño del sistema y consumen recursos valiosos en disco y memoria. Los usuarios deberán borrar todos los correos de cadena y masivos (no relacionados con el negocio) y abstenerse de reenviarlos a otras personas. Así mismo, no reenvíe correo a otra persona sin el previo consentimiento del remitente.

SE PROHIBE:

1. Hacer mal uso de los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso y/o utilizar los recursos de la ESE Hospital Del Rosario de Campoalegre para el acceso no autorizado a redes y sistemas remotos.
2. Acceder remotamente a los equipos de la ESE Hospital Del Rosario de Campoalegre sin previa autorización del Área de Sistemas.
3. Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas, mediante técnicas, comandos o programas a través de la red.
4. Monopolizar los recursos en perjuicio de otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones en masa, uso de recursos de impresión no autorizado e impresión de documentos no institucionales.
5. Poner información en la red que infrinja el derecho a la intimidad de los demás funcionarios y/o contratistas.
6. Utilizar los servicios de la red para la descarga, uso, intercambio y/o instalación de juegos, música, películas, imágenes protectoras o fondos de pantalla, software de libre distribución, información y/o productos que de alguna manera atenten contra la propiedad intelectual de sus actores o que contenga archivos ejecutables.
7. Efectuar cualquiera de las siguientes labores sin previa autorización del Gerente: copiar software para utilizar en sus computadores en casa, proveer copias de software a contratistas, empleados temporales, amigos, parientes o cualquier otra tercera persona, instalar software en cualquier computador o servidor de la Empresa, bajar software de Internet u otro servicio en línea a cualquier

Computador o servidor, modificar, radicar, transformar o adaptar cualquier software o, descompilar o aplicar ingeniería de reverso en cualquier software institucional.

8. Comunicación de Secretos del Negocio: A menos que sea expresamente autorizado por el Gerente, está estrictamente prohibido divulgar, propagar o almacenar información de propiedad del Hospital. secretos del negocio o cualquier otra información confidencial; el incumplimiento de esta norma puede resultar en responsabilidad civil y penal. (Art. 238, 288 y 289 del Código Penal).
9. El acceso a cuentas de correos personales de ningún tipo desde la red del Hospital y solo se podrán utilizar las cuentas de correo electrónico suministradas por la Institución. Algunos ejemplos de los sistemas de correos electrónicos personales no autorizados son Yahoo, Hotmail, Gmail.
10. Utilizar los servicios para acceder a páginas de radio o TV en línea, descargar archivos de música o video, visitar sitios de pornografía, ocio, entre otros que estén fuera de las funciones del usuario. El Hospital puede utilizar software pare identificar y bloquear sitios de Internet con material inadecuado, violento y sexualmente explícito. En el evento, en que el usuario encuentre este tipo de material en Internet, deberá desconectarse del sitio en forma inmediata, sin importar si el sitio fue bloqueado o no por el software.

SEGURIDAD DE SOFTWARE

1. El Área de Sistemas es responsable de la instalación de software informático y de telecomunicaciones.
2. En los equipos de cómputo de la ESE Hospital Del Rosario de Campoalegre, no se permite la instalación de software que no cuente con el licenciamiento apropiado. Está prohibido el uso de aplicaciones ilegales y el uso de "Cracks", "Keygens" y demás aplicativos.
3. Está totalmente prohibido la instalación de juegos. programas de mensajería o aplicativos que no estén relacionados con las labores institucionales que se realizan en la ESE.
4. Con el propósito de proteger la integridad de los equipos y sistemas informáticos y de telecomunicaciones, es obligatorio que todos y cada uno de estos dispongan de software de seguridad (antivirus, filtros de contenido web, controles de acceso, entre otros). Equipo que no cuente con estos aplicativos de seguridad, no puede conectarse a la red de la institución.
5. Las medidas de protección lógica (a nivel de software) son responsabilidad del personal del área de sistemas y el correcto uso de los sistemas corresponde a quienes se les asigna y les compete notificar cualquier eventualidad al Área de Sistemas.
6. La adquisición y actualización de software para los equipos de cómputo y de telecomunicaciones se llevará a cabo de acuerdo al calendario y requerimientos que sean propuestos por el área de Sistemas y a la disponibilidad presupuestal con el que se cuente.
7. El Área de Sistemas administrará los diferentes tipos de licencias de software con la que cuenta la ESE Hospital del Rosario de Campoalegre y vigilará su vigencia de acuerdo a sus fechas de caducidad.
8. Es obligación de todos los usuarios que manejen información masiva y/o crítica, solicitar respaldo correspondiente al Área de sistemas sobre la generación copias de seguridad ya que se considera como un activo de la institución que debe preservarse. Las copias de respaldo a la información generada por el personal y los recursos informáticos de la institución deben estar resguardados en sitios debidamente adecuados para tal fin.

SEGURIDAD DE DATOS E INFORMACIÓN:

La información es de los insumos más importantes dentro de una organización. La seguridad informática debe evitar que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la esta sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando datos errados o incompletos. El objetivo de esta política es la de asegurar el acceso a la información en el momento oportuno.

1. Toda información de relevancia debe contar con copia de seguridad y un tiempo de retención determinado, por lo cual, la información no se debe guardar indefinidamente en un archivo activo ocupando espacio innecesario de almacenamiento, el usuario debe establecer cuándo su información pasará a ser inactiva.
2. Para evitar pérdidas de información debido a uso mal intencionado o causa externa, se deben realizar copias de seguridad de la información o Backups. El Área de Sistemas de la ESE Hospital Del Rosario de Campoalegre se encargará de realizar el respaldo de la base de datos del Sistemas de Información DGH y a toda la información cuya responsabilidad sea resorte del área de sistemas. Los usuarios se harán responsables del respaldo de la información que reposa en cada Computador PC producto de su trabajo de Gestión diaria.

2.1. Esquema de copias de seguridad — Sistemas Integrado DGH. Teniendo en cuenta que los equipos de cómputo no son inmunes a las averías de discos (teniendo en cuenta que estas partes son fungibles), averías de virus (están a la orden del día) o a eliminaciones por accidente de información, se hace necesario tener un sistema de backup robusto que se actualice periódicamente de tal manera que prevenga la pérdida de datos. En este orden de ideas se muestra el esquema actual de seguridad diseñado para la información de la base de datos de Dinámica Gerencial Hospitalaria. y la cual se ampliará pronto a la información o archivos de trabajo almacenados por los usuarios en las unidades compartidas habilitadas en el servidor. A continuación, se presenta el esquema detallado de copias de seguridad, que permite resguardar la información.

Backup Total

Se ejecutará esta copia diariamente cada doce (12) horas. Esta copia se sacará en Disco Duro Externo de 8 TB (intramural) y Disco Duro Externo de 4TB (extramural) destinado para ello. Esta copia se almacenará para archivo histórico de copias de seguridad, con la programación que se muestra a continuación.

Programación Copia	Hora
Sucede Diariamente	00:00
Sucede Diariamente	13:00

Documento: GCO-PD-13V1 Procedimiento para la Realización de Copias de Seguridad.

3. Cualquier aplicación, archivo desconocido o sospechoso que aparezca en la información del usuario (ya sea en el equipo local, correo electrónico), no debe ser abierto o ejecutado sin antes contar con la

asesoría de la oficina de Sistemas de Información, que se encargará de examinar y determinar si la aplicación o archivo es potencialmente peligrosa para el equipo o la red de la entidad.

4. No está permitido extraer información de la institución por ningún medio y bajo ningún motivo.

SEGURIDAD DE USUARIOS

Los usuarios son las personas que utilizan la estructura tecnológica de la Institución, ya sean equipos, recursos de red o gestión de la información. El Área de Sistemas establece normas que buscan reducir los riesgos a la información o infraestructura informática. Estas normas incluyen, restricciones, autorizaciones, denegaciones, perfiles de usuario, protocolos y todo lo necesario que permita un buen nivel de seguridad informática. Todos los funcionarios y contratistas de la ESE Hospital Del Rosario de Campoalegre, deberán cumplir con estos requerimientos de seguridad de la Información. Igualmente, durante el proceso de vinculación deberán recibir inducción sobre lo establecido en este Documento y sobre la responsabilidad del cumplimiento de las políticas, procedimientos y estándares definidos por el Hospital. La información almacenada en los equipos de cómputo del Hospital es propiedad de la ESE Hospital Del Rosario de Campoalegre y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad. No es permitido divulgar, alterar, borrar, eliminar información sin la debida autorización.

Toda información en formato electrónico o impreso del Hospital debe estar debidamente identificada mediante rótulos o etiquetas, lo que permitirá su identificación y clasificación. Con esto se alimenta el inventario y clasificación de los archivos de información. Las claves o los permisos de acceso que les sean asignados a los funcionarios y/o contratista, son responsabilidad exclusiva de cada uno de ellos y no deben utilizar la identificación o contraseña de otro usuario, excepto cuando los funcionarios de Sistemas la soliciten para la reparación o el mantenimiento de algún servicio o equipo.

1. Los permisos a usuarios son personales e intransferibles y serán acordes a las funciones que desempeñen y no deberán tener permisos adicionales a estos. Estos permisos se conceden a solicitud escrita del jefe de la Oficina quien debe velar por su adecuado manejo.
2. Los usuarios deben renovar periódicamente su clave de acceso al sistema, esto deben solicitarlo al Área de Sistemas quienes le facilitarán el acceso y lo acompañarán en el proceso. Está totalmente prohibido: El intento o violación de los controles de seguridad establecidos; El uso sin autorización de los activos informáticos; el uso no autorizado o impropio de la conexión al Sistema: el uso indebido de las contraseñas, firmas, o dispositivos de autenticación e identificación; acceder a servicios informáticos utilizando cuentas, claves, contraseñas de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma
3. El usuario será el directo responsable de cualquier daño producido por medidas o decisiones mal tomadas. mantenimientos, reparaciones o instalaciones realizados por él que no fueran informadas o consultadas a el Área de Sistemas de la ESE Hospital Del Rosario de Campoalegre.
4. Los usuarios son responsables de todas las actividades llevadas a cabo con su código de usuario. Si detectan actividades irregulares con su código, tienen que solicitar una auditoria al área de Sistemas que se encargará de dar soporte e informar al usuario la actividad completa en el período y módulos solicitados y de igual manera informará qué medidas se deben tomar al respecto. (Investigación preliminar, cambio de usuario, proceso disciplinario).

5. Los usuarios de DGH de forma imperativa están asociados a unos roles definidos previamente que le dan acceso a las opciones que aplican a cada módulo de DGH, esto con el fin de que a los usuarios se les habilite automáticamente las opciones propias de su función.
6. Los modelos o folios de historias clínicas deben estar asociadas al personal médico al cual aplique el diligenciamiento de la misma, de tal manera que solo podrán crear o consultar folios de modelos de historia los médicos que apliquen a la especialidad para la cual fue diseñada la historia.
7. Los coordinadores de área deben reportar periódicamente las novedades de retiro o ingreso de nuevo personal que aplique para usos del sistema DGH para de esta manera realizar el respectiva desactivación o creación/activación de usuarios, evitando de esta manera que usuarios que ya no laboran en la institución queden activos en el sistema.
8. Informar inmediatamente al área de Sistemas cualquier anomalía, aparición de virus o programas sospechosos e intentos de intromisión y no intente distribuir este tipo de información interna o externamente. A cualquier infracción a la política de seguridad informática cometida por un funcionario y/o contratista de la ESE Hospital Del Rosario de Campoalegre, será investigado y sancionado según sea el nivel del riesgo. En caso de presentarse un problema critico a nivel informático en horario no laboral afectando el normal funcionamiento de la ESE, el área de Sistemas dispone de un funcionario para atender y solucionar estos inconvenientes.
9. Está prohibido intentar sobrepasar los controles de los sistemas, o tratar de saltar los bloqueos de acceso a internet (cambio de dirección IP, cambio de nombre de equipo, etc.) o introducir intencionalmente software malintencionado que impida el normal funcionamiento de los sistemas.
10. Todo funcionario que utilice los recursos informáticos, tiene la responsabilidad de velar por su integridad, confidencialidad y disponibilidad de la información que maneje, especialmente si dicha información es crítica.
11. El Área de Sistemas es la única encargada y responsable de capacitar a los usuarios en el manejo de las herramientas informáticas que son exclusivas de la misión y función de la institución.
12. Los usuarios de la red de la ESE Hospital Del Rosario de Campoalegre, recibirán capacitación para el manejo de las herramientas desarrolladas en la institución. La asistencia a la capacitación es obligatoria y requisito indispensable para acceder al sistema de información de lo contrario no se le asigna claves y contraseñas. Está totalmente prohibido el uso de contraseñas o claves de otro usuario.
13. No se permitirá el almacenamiento y/o procesamiento de información propiedad del Hospital, en equipos o dispositivos de propiedad de los funcionarios o contratistas. Todos los contratistas y funcionarios deben firmar una cláusula de confidencialidad. que permita al Hospital proteger la información.
14. El usuario renuncia a derechos de privacidad: Los Usuarios renuncian expresamente a la privacidad en relación con cualquier material que ellos creen, almacenen, envíen o reciban en el Computador, a través de Internet o de cualquier otra red. Los Usuarios dan su consentimiento para que, de ser necesario, funcionarios del Hospital puedan acceder a revisar cualquier tipo de material que creen, almacenen, envíen o reciban en el Computador, a través de Internet o de cualquier otra red. Los Usuarios entienden y aceptan que el Hospital puede utilizar procedimientos y recursos manuales o automáticos para monitorear la utilización de sus Recursos de Computación.
15. Material inapropiado o ilegal. El material que tenga carácter fraudulento, que pueda llegar a generar sentimientos de acoso u hostigamiento o que por su naturaleza sea embarazoso, sexualmente explicito, difamatorio, ilegal o inapropiado, no podrá ser enviado por correo electrónico o cualquier otra forma de comunicación electrónica (tales como sistema de boletín, boards, grupos de noticia, grupos

de chat) o exhibido o almacenado en los Computadores del Hospital. Los Usuarios que encuentren o reciban este tipo de material deben reportarlo en forma inmediata a su jefe.

16. Usos prohibidos: Los Recursos de Computación del Hospital no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), material político o cualquier otro uso que no esté autorizado. Tampoco podrán ser usados para escuchar música (sea por cualquier medio y en especial por Internet).
17. Los Usuarios son responsables de salvaguardar sus contraseñas de acceso al sistema; éstas no deben ser impresas, almacenadas en los sistemas o suministradas a cualquier otra persona. Ningún Usuario podrá acceder al sistema utilizando la cuenta o contraseña de otro usuario. Las contraseñas deben contener un mínimo de 8 caracteres en una combinación de letras números y caracteres especiales, tanto en mayúsculas como en minúsculas.
18. Las contraseñas no implican privacidad: El uso de contraseñas para acceder al sistema no implica que los Usuarios tengan la expectativa de privacidad en el material que ellos almacenen en el sistema de cómputo.
19. El uso de Unidades Externas de almacenamiento como Memorias USB, Unidades de CD, Unidades de DVD, y en general todos los dispositivos que se conecten por puertos USB están restringidos para los usuarios en general.
20. El uso de Carpetas Compartidas está restringido para los usuarios en general. Solo se configurará este tipo de acceso por demanda, una vez se justifique ante el área de sistemas su uso y se de viabilidad al mismo.
21. En la utilización de los recursos de computación, los usuarios deberán guardar conformidad con todas las licencias de software, derechos de autor y todas las leyes nacionales e internacionales que regulen la propiedad intelectual y las actividades en línea.
22. Detención de Virus. Los virus pueden causar daño sustancial a los sistemas de cómputo. Cada Usuario tiene la responsabilidad de tomar las precauciones necesarias para asegurar que no introduzca virus en la red del Hospital; por lo tanto. todo archivo y material recibido a través de medio magnético u óptico o bajado de Internet o de cualquier red externa, deberá ser rastreado para detención de virus y otros programas destructivos antes de ser colocados en el sistema de cómputo de la Empresa.
23. Los usuarios no podrán instalar o utilizar software de encriptación en los computadores de la Empresa sin la previa autorización escrita de su jefe inmediato y del administrador de la red. Los usuarios no pondrán contraseñas o llaves de Encriptación que no sean de conocimiento del jefe inmediato o administrador de la red.

11. INDICADORES Y METAS

Objetivo que se desea Alcanzar con la Implementación de la Política	Meta para dar Cumplimiento al objetivo específico de la Política	Nombre del Indicador	Formula
Fortalecer la protección de la información institucional.	Implementar controles de seguridad en el 100% de los sistemas críticos.	Nivel de implementación de controles de seguridad.	(N° de sistemas con controles implementados / Total de sistemas críticos) × 100

Aumentar la conciencia en ciberseguridad del personal.	Capacitar al 100% del personal en buenas prácticas de seguridad digital.	Porcentaje de funcionarios capacitados.	(N° de funcionarios capacitados / Total de funcionarios) × 100
Minimizar los incidentes de seguridad digital.	Reducir en un 80% los incidentes reportados al finalizar el año.	Tasa de reducción de incidentes.	((Incidentes año anterior - Incidentes actuales) / Incidentes año anterior) × 100

12. RESPONSABLES DE EJECUTAR Y REALIZAR SEGUIMIENTO AL CUMPLIMIENTO DE LA POLÍTICA

N°	Responsable (Líder o Coordinador)	Proceso	Dependencia
1	Coordinador de TIC	Gestión de tecnologías de la información y las Comunicaciones	Área TIC

JOSE ALEXANDER MORENO CORDOBA
Gerente E.S.E Hospital del Rosario

Proyecto: *Saul Andrés Murcia Jurado*
Coordinador TIC

Reviso*: Omar Ignacio Casanova Puentes*
Asesor MIPG

NO IMPRIMIR

VERSIÓN	FECHA	RAZON DE LA MODIFICACIÓN
01	16-07-2025	Creación del Formato de adopción de las Políticas Institucionales MIPG

PROYECTADO POR: (firma)	**REVISADO POR:** (firma)	**APROBADO POR:** (firma)
NOMBRE: Omar Ignacio Casanova	**NOMBRE:** Constanza Ofelia Molano Cuellar	**NOMBRE:** Jose Alexander Moreno Córdoba
CARGO: Asesor MIPG	**CARGO:** Profesional Administrativa y Financiera	**CARGO:** Gerente