

**RESOLUCIÓN N° 501 DE 2024**  
(27 de noviembre de 2024)

**“POR LA CUAL SE ADOPTA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PSI) EN LA E.S.E  
HOSPITAL ROSARIO PUMAREJO DE LÓPEZ”**

La suscrita Agente Especial Interventora de la E.S.E. Hospital Rosario Pumarejo de López; en uso de sus facultades constitucionales, legales y reglamentarias, designadas por la Superintendencia Nacional de Salud a través de la Resolución N° 2024420000003001-6 del 02 de abril de 2024, “Por la cual se acepta una renuncia y se designa Agente Interventor, y se dictan otras disposiciones”, con Acta de Posesión DPSS – I – 002 de 2024 del 02 de abril de 2024; y

**CONSIDERANDO:**

Que, Ley 1273 de 2009: Protección de la información como bien jurídico en los siguientes artículos:

Artículo 269A: *Acceso abusivo a un sistema informático.* El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: *Intercepción de datos informáticos.* El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: *Daño Informático.* El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: *Uso de software malicioso.* El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: *Violación de datos personales.* El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: *Suplantación de sitios web para capturar datos personales.* El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: *Circunstancias de agravación punitiva:* Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Que, mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1º, tiene por objeto "(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de

datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".

Que, Ley 1341 de 2009: Uso responsable de las TIC, determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.

Que, la Norma ISO 27001 aportan un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a proteger la información, indistintamente del formato de la misma, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa.

Que la E.S.E Hospital Rosario Pumarejo de López, con el fin de dar cumplimiento a la normatividad vigente en términos de Seguridad de la Información, requiere adoptar la Política de Seguridad de la Información, con el fin proporcionar un entorno tecnológico seguro que soporte los objetivos estratégicos de la organización, previniendo incidentes cibernéticos que puedan generar pérdidas económicas, daño reputacional o afectación en la prestación de servicios.


Que, en mérito de lo anterior,

#### RESUELVE:


**ARTÍCULO PRIMERO. OBJETO:** Adoptar los lineamientos establecidos en la Ley 1273 de 2009, específicamente en sus artículos (269A; 269B; 269C; 269D; 269E; 269F; 269G; 269H) que permitan proteger los activos informáticos de la ESE Hospital Rosario Pumarejo de López, garantizando la confidencialidad, integridad y disponibilidad de la información crítica relacionada con pacientes, procesos clínicos, administrativos y financieros. Esta política busca prevenir accesos no autorizados, asegurar el cumplimiento normativo, y mitigar riesgos que puedan afectar la prestación de los servicios de salud.

**ARTÍCULO SEGUNDO. DEFINICIÓN:** La Política de Seguridad Información de la ESE Hospital Rosario Pumarejo de López es el conjunto de principios, normas y procedimientos que rigen la protección de los activos tecnológicos y la información digital del hospital. Busca garantizar la confidencialidad, integridad y disponibilidad de los datos, especialmente los relacionados con pacientes, procesos clínicos y administrativos. Esta política establece lineamientos para la gestión de riesgos informáticos, la prevención de accesos no autorizados, y el cumplimiento de las normativas vigentes, promoviendo un entorno tecnológico seguro y eficiente que soporte la misión del hospital.

**ARTÍCULO TERCERO. ALCANCE:** Esta política aplica a todos los sistemas, equipos, aplicaciones y datos utilizados en el ESE Hospital Rosario Pumarejo de López, abarcando procesos clínicos, administrativos y financieros. Su cumplimiento es obligatorio para empleados, contratistas, proveedores y terceros con acceso a los activos informáticos del hospital. Incluye la protección de redes, bases de datos, historiales clínicos

Dirección calle 16 Avenida la popa N 17-192 

E-mail: contacto@hrplopez.gov.co 

Hospitalrosariovalledupar 

electrónicos, correos electrónicos y demás recursos tecnológicos. Adicionalmente, considera la seguridad en la gestión de información sensible y confidencial, promoviendo buenas prácticas y el cumplimiento normativo en todas las áreas operativas del hospital.

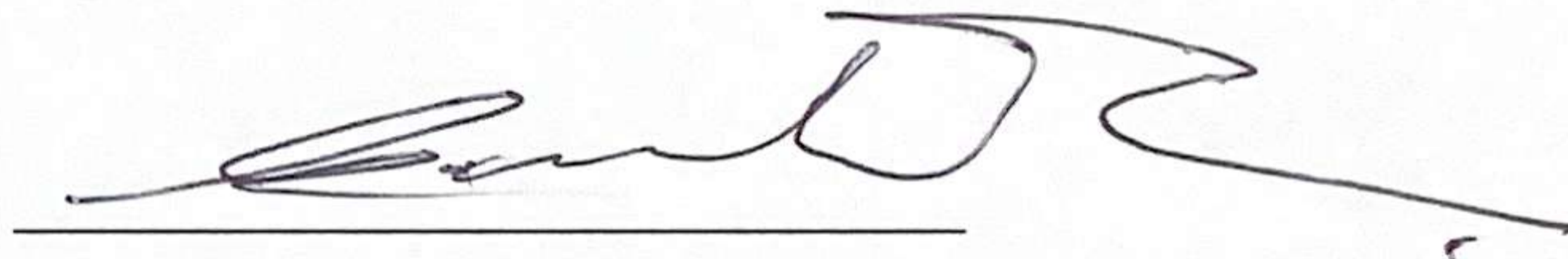
**ARTÍCULO CUARTO. RESPONSABLE.** Desígnese como referente de la Política de Seguridad de Información al Profesional Universitario de Sistemas de la ESE Hospital Rosario Pumarejo de López.

**ARTÍCULO QUINTO: DIVULGACIÓN:** La presente Resolución se divulgará por medio de la página WEB de la institución y de la socialización en los procesos de inducción y reinducción, así mismo permanecerá exhibida en los espacios oficiales de la ESE Hospital Rosario Pumarejo de López.




**ARTÍCULO SEXTO. VIGENCIA:** el contenido de la presente resolución rige a partir de la fecha de publicación.

**COMUNÍQUESE, PUBLÍQUESE y CÚMPLASE**

Dado en Valledupar cesar, a los veintisiete (27) días del mes de noviembre del 2024.



**CARMEN SOFÍA DAZA OROZCO**  
Agente Especial Interventor

Elaboró	Edwar Enrique Suárez Cujia – Profesional de Apoyo al SIGR (c)	
Revisó:	Aarol Lee Ovalle – jefe de la Oficina de Planeación, Calidad y Sistemas de información	
Aprobó:	Cesar Enrique Carrillo Urbina – jefe Oficina Asesora Jurídica y Control Interno Disciplinario	
Los arriba firmantes declaramos que hemos revisado el documento, cuyo contenido se encuentra ajustado a las disposiciones legales vigentes, bajo nuestra responsabilidad lo presentamos para firma.		