**EMPRESA SOCIAL DEL ESTADO CARMEN EMILIA OSPINA**

**GERENTE: JULIO CESAR QUINTERO VIEDA**

# PLAN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

**Neiva**

## TABLA DE CONTENIDO


1. **INTRODUCCIÓN** ..... 3
2. **OBJETIVOS** ..... 4
   - 2.1. **Objetivos específicos** ..... 4
3. **ALCANCE** ..... 6
4. **DEFINICIONES** ..... 7
5. **DOCUMENTOS DE REFERENCIA** ..... 10
6. **METODOLOGÍA** ..... 12
   - 6.1. **Identificación del contexto** ..... 12
   - 6.2. **Análisis de la situación actual** ..... 14
7. **CRONOGRAMA** ..... 16

## 1. INTRODUCCIÓN

En la actualidad, la seguridad en la información es una de las preocupaciones más grandes que puede llegar a tener cualquier organización, ya que se refiere a garantizar la calidad, disponibilidad, veracidad y confidencialidad del activo más preciado: la información.

El Plan de Seguridad y Privacidad de la Información, de la ESE Carmen Emilia Ospina, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a los funcionarios y clientes externo acerca de la adecuada gestión de riesgos.

Este Plan está diseñado de acuerdo a los lineamientos de La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente.

## 2. OBJETIVOS

Garantizar la protección, seguridad y privacidad de la información, de los ciudadanos y funcionarios de la ESE Carmen Emilia Ospina, todo esto acorde con lo expresado en la legislación Colombiana, mediante la gestión y uso de controles y mecanismos que contribuyan a alcanzar los niveles requeridos de calidad, seguridad, privacidad y trazabilidad de los componentes de información.

### 2.1. Objetivos específicos

- Optimizar los niveles de madurez y fortalecer las capacidades en la apropiación de aspectos de seguridad y privacidad de la información.
- Generar confianza en las entidades y en los ciudadanos respecto al uso y apropiación de TI en el Estado.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Disminuir la probabilidad de ocurrencia e impacto de los incidentes de Seguridad y Privacidad de la Información de forma efectiva.
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, y privacidad de la información de la ESE Carmen Emilia Ospina.
- Asegurar y hacer uso eficiente y seguro de los recursos de Tecnologías de Información y Comunicaciones
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la Información, Seguridad Digital y protección de la información personal.
- Minimizar el riesgo de vulnerabilidad de la información en el desarrollo de los procesos.

- Asegurar la continuidad de funcionamiento de la plataforma informática.
- Cumplir con la legislación nacional e institucional sobre seguridad de la información.
- Garantizar la disponibilidad de la información para la eficiente toma de decisiones.
- Fortalecer la cultura de la seguridad de la información a nivel de clientes internos y externos.
- Proteger los activos tecnológicos y apoyar su desarrollo.

## 3. ALCANCE

La ESE Carmen Emilia Ospina, registra, almacena, ofrece, intercambia, divulga y actualiza información clasificada, reservada y pública, relacionada con la prestación de servicios de salud de población colombiana, sus funcionarios, contratistas y/o terceros contratados.

Dicha información que se encuentra bajo la custodia de Entidad, la cual representa un valor histórico e importante para tener en cuenta en temas reserva y privacidad de la misma.

## 4. DEFINICIONES

- **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)
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Antivirus:** Software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.
- **Ataques Web:** Es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.
- **Contraseña:** Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados

- **Confidencialidad:** Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000).
- **Disponibilidad:** Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).
- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).
- **Encriptación:** La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos.
- **Firewall:** Es una aplicación de seguridad física y/o lógica diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.
- **Malware:** Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras.
- **Plan de tratamiento de Gestión de Riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación
- **Procedimiento:** Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de detección de intrusos:** Es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red.
- **Virus:** Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario.
- **Vulnerabilidad:** Es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.

## 5. DOCUMENTOS DE REFERENCIA

- **Decreto 1078 de 2015 – MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES**

  Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **NTC / ISO 27001:2013 - ICONTEC**

  Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.
- **NTC/ISO 27002:2013- ICONTEC**

  Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.
- **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 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 1581 de 2012**

  “Por la cual se dictan disposiciones generales para la protección de datos personales.”
- **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.”

- **Ley 1978 de 2019**

  “Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.”

- **Resolución 184 del 2017 – ESE Carmen Emilia Ospina**

  “Por medio de la cual se adopta la Política de tratamiento y protección de datos personales de la ESE CARMEN EMILIA OSPINA.” Con el fin de implementar y dar cumplimiento a la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013.”

## 6. METODOLOGÍA

Para llevar a cabo el Plan de seguridad y privacidad de la información, se tendrá en cuenta la metodología y los lineamientos establecidos por el Ministerio de la TIC, a través del documento “modelo de seguridad”. El cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

La metodología usada para el diseño y desarrollo de este Plan de Seguridad y Privacidad de la Información, fue llevar a cabo las siguientes fases que se detallan a continuación:

### 6.1. Identificación del contexto

En esta fase se hace un reconocimiento de los principales aspectos, características, procesos y arquitectura funcional de la institución, para determinar un eficiente funcionamiento del plan propuesto en el presente documento.

- **Misión**

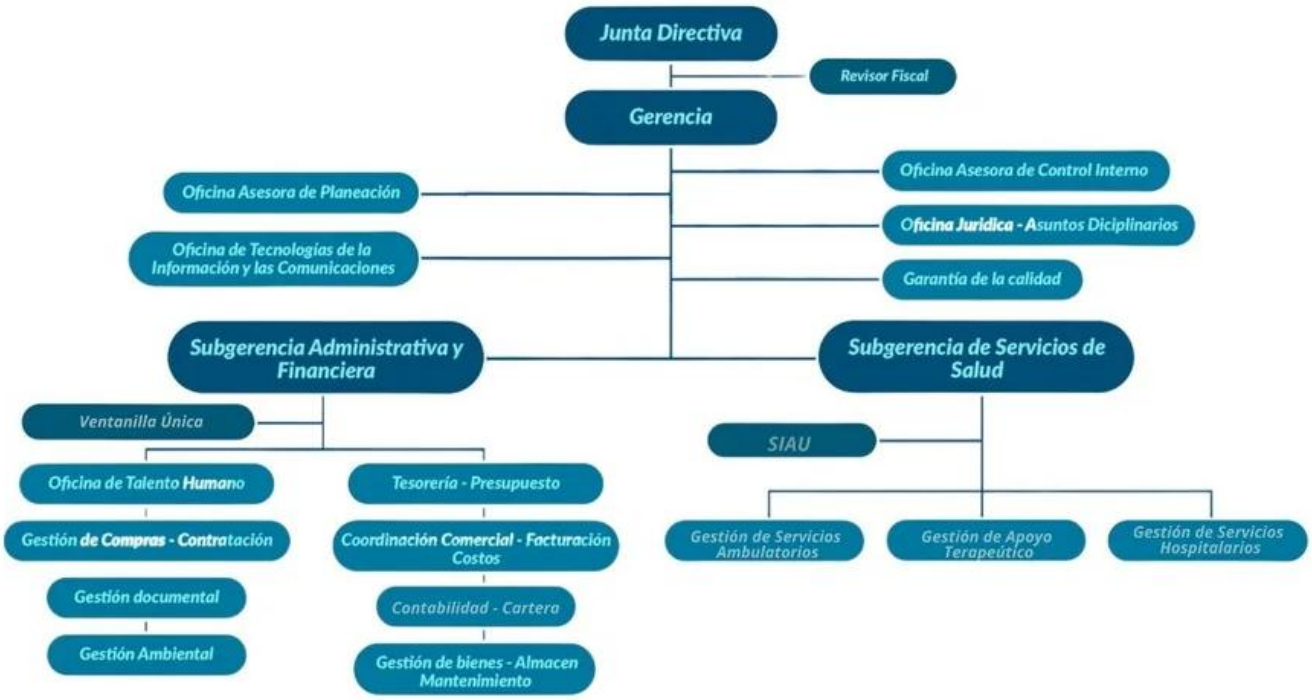
Institución de atención primaria en salud accesible y de alta calidad, dedicada a mejorar la calidad de vida de usuarios y sus familias.

- **Visión**

Para el año 2028, seremos reconocidos como la institución de atención primaria referente en prevención y mantenimiento de la salud, destacada por su efectividad y compromiso social; así como, por la integralidad en la prestación de servicios de baja y mediana complejidad, a través

de una red de centros de atención enfocados en la gestión del conocimiento y la generación de valor social, mientras avanzamos hacia nuestra acreditación de alta calidad.

- **Organigrama**




- **Identidad organizacional**

**Honestidad:** En la E.S.E Carmen Emilia Ospina promovemos y exigimos que tanto los comportamientos individuales como colectivos, se caractericen por la ética, rectitud y transparencia.

**Compromiso con la Calidad:** En la E.S.E Carmen Emilia Ospina, desarrollamos nuestro trabajo garantizando que el servicio prestado sea mejor día tras día. Afianzamos nuestro rol dentro de la organización logrando las metas propuestas.

**Responsabilidad:** En la E.S.E Carmen Emilia Ospina, desempeñamos nuestro rol con diligencia, seriedad y prudencia, asumiendo los objetivos de la entidad como propios.

**Justicia:** En la E.S.E Carmen Emilia Ospina, actuamos con imparcialidad garantizando los derechos a los usuarios, con equidad, igualdad y sin discriminación.

**Excelencia en el Servicio:** En la E.S.E Carmen Emilia Ospina, mantenemos una destacada actitud de servicio frente a nuestros clientes internos y externos, buscando soluciones eficaces a sus necesidades y construyendo relaciones duraderas.

### 6.2. Análisis de la situación actual

Actualmente la ESE Carmen Emilia Ospina, presenta algunas debilidades de tipo documental que permitan evidenciar el crecimiento proporcional de los avances realizados en el Dominio de Seguridad y privacidad de la información, de acuerdo a los lineamientos establecidos por el Ministerio de la TIC, a través de la estrategia Gobierno en Línea. Al igual existen múltiples procedimientos y procesos definidos para el tratamiento y manejo de la información, los cuales no se encuentran debidamente documentados y socializados al personal de la organización. Sin Embargo es importante resaltar los logros actuales:

La ESE CARMEN EMILIA OSPINA, cuenta con sistemas de información, integrales y robustos que cumple con los módulos de seguridad para el acceso y clasificación de perfiles para cada una de las opciones de los mismos.

Se cuenta con un dispositivo unificado de amenazas (UTM) el cual controla a través de políticas, los accesos internos y externos, así como la navegación por Internet.

Copias de seguridad a los sistemas de información, con periodicidad de 8 horas, replicada en línea a un segundo disco externo; Se cuenta con la política de Privacidad y Confidencialidad de la información.

## 7. CRONOGRAMA

| ACTIVIDAD | 2025 |
|---|---|
| Actualizar política de seguridad y privacidad de la información según tecnologías emergentes. | X |
| Realizar seguimiento a través la plataforma de antivirus para la identificación de las posibles vulnerabilidades de los sistemas de información. | X |
| Actualizar catálogo de los componentes de la información. | X |
| Actualizar política de seguridad digital de la información | X |
| Adoptar y difundir el procedimiento para la integridad autenticidad, disponibilidad y preservación de los activos de información. | X |
| Diseñar estrategia para el uso y apropiación de las tecnologías de la información. | X |

| **CONTROL DE CAMBIOS** | | |
|---|---|---|
| Versión | Descripción el Cambio | Fecha de aprobación |
| 1 | Elaboración del documento: | 29/01/2021 |
| 2 | Modificación del documento: Se modifica documento con el fin de obtener una mejora continua en el subproceso “Sistemas informáticos”, se realizaron los siguientes ajustes:<br>1. Actualización de la vigencia.<br>2. Actualización del contenido en general.<br>3. Ajustes estructurales. | 29/12/2022 |
| 3 | Modificación del documento: Se modifica documento con el fin de obtener una mejora continua en el subproceso “Sistemas informáticos”, se realizaron los siguientes ajustes:<br>1. Actualización de la vigencia.<br>2. Actualización del contenido en general.<br>3. Ajustes estructurales. | 30/01/2025 |
| Nombre: Luis Fernando Correa Calderón.<br>Contratista área Sistemas de Información.<br><br>Nombre: Jose Yamil Laguna Rojas<br>Contratista área Sistemas de Información. | Nombre: Liliana Carolina Gonzalez.<br>Cargo: Coordinadora área Sistemas de Información. | Nombre: Julio Cesar Quintero.<br>Cargo: Gerente. |
| **Elaboró** | **Revisó** | **Aprobó** |