2026

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

E.S.E CAMU IRIS LÓPEZ DURAN – SAN ANTERO CÓRDOBA

Tabla de contenido

PRESENTACIÓN

Como Gerente de la ESE CAMU Iris López Durán de San Antero – Córdoba, presento el Plan de Seguridad y Privacidad de la Información como un compromiso institucional con la protección de uno de nuestros activos más valiosos: la información y los datos personales de nuestros usuarios, colaboradores y partes interesadas. En el sector salud, la información soporta decisiones clínicas, la continuidad de la atención, la seguridad del paciente y la gestión administrativa y financiera; por ello, garantizar su protección es una responsabilidad ética y legal que fortalece la confianza de la comunidad. Este Plan establece los lineamientos y medidas necesarias para preservar la confidencialidad, integridad y disponibilidad de la información institucional, evitando accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas que puedan afectar la operación y el buen nombre de la ESE.

A través de este instrumento, definimos responsabilidades claras para funcionarios y contratistas, promoviendo una cultura de seguridad basada en buenas prácticas, autocontrol y respeto por la privacidad. El Plan incorpora acciones para el manejo seguro de historias clínicas, bases de datos, documentos contractuales, información financiera y comunicaciones oficiales, así como medidas de control de accesos, respaldos, continuidad operativa y respuesta ante incidentes. De manera especial, prioriza la protección de la información sensible y reservada propia de la prestación de servicios de salud, asegurando que el tratamiento de datos personales se realice bajo criterios de legalidad, finalidad y seguridad. Asimismo, el Plan se articula con el Sistema de Control Interno, la gestión del riesgo institucional y la mejora continua, permitiendo identificar vulnerabilidades, fortalecer controles y evaluar su efectividad mediante seguimiento e indicadores.

Con la implementación del Plan de Seguridad y Privacidad de la Información, reafirmamos nuestro compromiso con la transparencia, la responsabilidad institucional y el cuidado integral de las personas, garantizando que la información esté protegida y disponible cuando se requiera para brindar una atención oportuna y segura. Invito a todo el equipo humano de la ESE CAMU Iris López Durán a asumir este Plan como una tarea compartida, donde cada práctica segura, cada control aplicado y cada decisión responsable contribuye a proteger los derechos de nuestros usuarios y asegurar la sostenibilidad y confiabilidad de nuestra institución.

Luz Suárez

LUZ AIDA SUAREZ
Gerente
E.S.E CAMU IRIS LOPEZ DURAN

INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información de la Empresa Social del Estado CAMU Iris López Durán de San Antero – Córdoba se establece como un instrumento institucional fundamental para garantizar la protección, el uso responsable y la disponibilidad oportuna de la información en el desarrollo de los procesos misionales, estratégicos y de apoyo. En una entidad del sector salud, la información es un activo crítico que soporta la continuidad de la atención, la seguridad del paciente, la toma de decisiones clínicas y la gestión administrativa y financiera; por ello, su protección debe abordarse de manera integral, preventiva y permanente. Este Plan reconoce que la ESE administra información sensible y reservada, como historias clínicas, resultados diagnósticos, bases de datos de usuarios, información contractual, talento humano, facturación y reportes obligatorios, lo que exige controles robustos para evitar accesos no autorizados, pérdidas, alteraciones, divulgaciones indebidas o interrupciones en los sistemas y servicios de información.

En este contexto, el Plan de Seguridad y Privacidad define principios, lineamientos y medidas orientadas a preservar la confidencialidad, integridad y disponibilidad de la información, así como a garantizar la privacidad de los datos personales bajo criterios de legalidad, finalidad, minimización, seguridad y responsabilidad institucional. De igual manera, establece roles y responsabilidades para funcionarios y contratistas, promoviendo una cultura de seguridad basada en la ética, el cumplimiento de protocolos y la corresponsabilidad en el manejo de la información. El Plan incorpora acciones para gestionar los riesgos asociados a amenazas internas y externas, tales como fallas tecnológicas, incidentes de ciberseguridad, errores humanos, pérdida o sustracción de equipos, indisponibilidad de aplicativos, deterioro de archivos físicos y eventos ambientales que puedan afectar la operación.

Asimismo, este instrumento se articula con el Sistema de Control Interno, la gestión del riesgo institucional, la gestión documental y los planes institucionales vigentes, fortaleciendo la mejora continua y la capacidad de respuesta ante incidentes. En consecuencia, su implementación permitirá a la ESE CAMU Iris López Durán consolidar un entorno de confianza para usuarios y partes interesadas, asegurar el cumplimiento de las obligaciones relacionadas con la protección de datos y la reserva legal, y garantizar que la información esté protegida y disponible cuando se requiera, contribuyendo directamente a la calidad, oportunidad y sostenibilidad de los servicios de salud prestados a la comunidad.

ALCANCE PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de Seguridad y Privacidad de la Información de la Empresa Social del Estado CAMU Iris López Durán de San Antero – Córdoba se establece como un instrumento institucional fundamental para garantizar la protección, el uso responsable y la disponibilidad oportuna de la información en el desarrollo de los procesos misionales, estratégicos y de apoyo. En una entidad del sector salud, la información es un activo crítico que soporta la continuidad de la atención, la seguridad del paciente, la toma de decisiones clínicas y la gestión administrativa y financiera; por ello, su protección debe abordarse de manera integral, preventiva y permanente. Este Plan reconoce que la ESE administra información sensible y reservada, como historias clínicas, resultados diagnósticos, bases de datos de usuarios, información contractual, talento humano, facturación y reportes obligatorios, lo que exige controles robustos para evitar accesos no autorizados, pérdidas, alteraciones, divulgaciones indebidas o interrupciones en los sistemas y servicios de información.

En este contexto, el Plan de Seguridad y Privacidad define principios, lineamientos y medidas orientadas a preservar la confidencialidad, integridad y disponibilidad de la información, así como a garantizar la privacidad de los datos personales bajo criterios de legalidad, finalidad, minimización, seguridad y responsabilidad institucional. De igual manera, establece roles y responsabilidades para funcionarios y contratistas, promoviendo una cultura de seguridad basada en la ética, el cumplimiento de protocolos y la corresponsabilidad en el manejo de la información. El Plan incorpora acciones para gestionar los riesgos asociados a amenazas internas y externas, tales como fallas tecnológicas, incidentes de ciberseguridad, errores humanos, pérdida o sustracción de equipos, indisponibilidad de aplicativos, deterioro de archivos físicos y eventos ambientales que puedan afectar la operación.

Asimismo, este instrumento se articula con el Sistema de Control Interno, la gestión del riesgo institucional, la gestión documental y los planes institucionales vigentes, fortaleciendo la mejora continua y la capacidad de respuesta ante incidentes. En consecuencia, su implementación permitirá a la ESE CAMU Iris López Durán consolidar un entorno de confianza para usuarios y partes interesadas, asegurar el cumplimiento de las obligaciones relacionadas con la protección de datos y la reserva legal, y garantizar que la información esté protegida y disponible cuando se requiera, contribuyendo directamente a la calidad, oportunidad y sostenibilidad de los servicios de salud prestados a la comunidad.

OBJETIVO GENERAL

Implementar y mantener un Plan de Seguridad y Privacidad de la Información que garantice la protección integral de los activos de información y de los datos personales administrados por la ESE, preservando su confidencialidad, integridad y disponibilidad mediante controles administrativos, técnicos y físicos, fortaleciendo el cumplimiento normativo, la continuidad operativa y la confianza de los usuarios y partes interesadas.

OBJETIVOS ESPECÍFICOS

1. **Definir y socializar** el marco de políticas, roles y responsabilidades para la seguridad y privacidad de la información, aplicable a funcionarios, contratistas y terceros que traten información de la ESE.
2. **Identificar y clasificar** los activos de información y los datos personales por proceso, determinando su criticidad, nivel de sensibilidad y requisitos de protección.
3. **Implementar controles de acceso** (físicos y lógicos) basados en perfiles, privilegio mínimo y trazabilidad, priorizando la información clínica, financiera y contractual.
4. **Fortalecer la protección tecnológica** mediante medidas de seguridad en equipos, redes y sistemas (actualizaciones, antivirus, restricciones de uso y buenas prácticas), reduciendo vulnerabilidades.
5. **Garantizar la continuidad y disponibilidad** de la información a través de esquemas de copias de seguridad, restauración, contingencias y recuperación, con pruebas periódicas y responsables definidos.
6. **Establecer y aplicar** un procedimiento de gestión de incidentes de seguridad y privacidad (detección, reporte, contención, recuperación y lecciones aprendidas).
7. **Promover la cultura de seguridad y privacidad** mediante capacitación y sensibilización permanente sobre manejo seguro de información, reserva legal, confidencialidad y protección de datos personales.
8. **Asegurar el cumplimiento** de los principios y obligaciones de protección de datos personales, garantizando tratamiento legítimo, seguro y documentado, y atención oportuna de solicitudes de titulares.

9. **Monitorear y evaluar** la eficacia del Plan mediante indicadores, auditorías internas y seguimiento a planes de mejora, asegurando la mejora continua y la reducción progresiva del riesgo.

DEFINICIONES

Plan de Seguridad y Privacidad de la Información: Documento institucional que establece políticas, controles y acciones para proteger la información y los datos personales, garantizando su confidencialidad, integridad y disponibilidad, y asegurando el cumplimiento de obligaciones de privacidad.

Gobierno de la información: Conjunto de decisiones, roles y mecanismos mediante los cuales la entidad dirige y controla el uso de la información, definiendo responsabilidades, prioridades, reglas y supervisión para su manejo seguro.

Dato personal: Información asociada o vinculable a una persona natural que permite identificarla directa o indirectamente, como nombres, identificación, contacto, historial de atención o registros administrativos.

Dato sensible: Tipo de dato personal que, por su naturaleza, puede afectar la intimidad del titular o generar discriminación; en salud incluye, por ejemplo, diagnósticos, tratamientos y antecedentes clínicos.

Clasificación de la información: Proceso de asignar niveles de protección a la información según su sensibilidad, criticidad y requisitos de reserva, determinando quién puede acceder, cómo se almacena y cómo se comparte.

Control de acceso: Medidas y procedimientos que limitan el acceso a la información y sistemas únicamente a usuarios autorizados, según roles y perfiles, asegurando trazabilidad y privilegio mínimo.

Medidas de seguridad (controles): Acciones administrativas, técnicas y físicas implementadas para prevenir, detectar o corregir eventos que pongan en riesgo la información (p. ej., respaldos, antivirus, cerraduras, políticas, monitoreo).

Gestión de incidentes: Proceso para detectar, reportar, analizar, contener y recuperar la operación ante eventos que comprometen la seguridad o privacidad de la información, incorporando acciones correctivas y lecciones aprendidas.

Continuidad operativa: Capacidad institucional para mantener o restablecer rápidamente los servicios y el acceso a la información crítica ante fallas tecnológicas, incidentes de seguridad o eventos físicos, mediante planes y respaldos.

Principio de confidencialidad: Obligación de proteger la información reservada o sensible, evitando su divulgación o uso indebido, y asegurando que sea tratada únicamente por personal autorizado y para fines legítimos.

Misión

Establecer y fortalecer un marco institucional de seguridad y privacidad que proteja integralmente los activos de información y los datos personales administrados por la ESE, mediante políticas, controles y buenas prácticas administrativas, técnicas y físicas, garantizando la confidencialidad, integridad y disponibilidad de la información, el cumplimiento normativo y la continuidad operativa para respaldar una atención en salud segura, oportuna y confiable.

Visión

Para el año 2027, consolidar en la ESE un modelo maduro y reconocido de seguridad y privacidad de la información, con cultura organizacional de protección de datos, controles eficaces y capacidad de prevención y respuesta ante incidentes, que asegure la continuidad de los servicios, fortalezca la confianza de los usuarios y promueva la mejora continua en la gestión institucional de la información.

Objetivos estratégicos y líneas de acción

1) Consolidar la gobernanza de la seguridad y privacidad de la información

Líneas de acción:

- Formalizar roles, responsabilidades y cadena de reporte (dueños de información, TI, líderes de proceso).
- Adoptar políticas y procedimientos (clasificación, acceso, uso aceptable, respaldo, incidentes).
- Integrar el plan al mapa de riesgos institucional, Control Interno y planes de mejoramiento.

2) Proteger la confidencialidad y reserva de la información, especialmente la información en salud

Líneas de acción:

- Implementar control de acceso por perfiles y privilegio mínimo (clínico, administrativo, financiero).
- Establecer reglas de manejo de historia clínica, archivo y documentos reservados.
- Aplicar acuerdos de confidencialidad y buenas prácticas para funcionarios, contratistas y terceros.

3) Asegurar la integridad de la información y la trazabilidad documental y digital

Líneas de acción:

- Estandarizar control de versiones, autorizaciones y validaciones en documentos críticos.
- Fortalecer trazabilidad de cambios en sistemas/aplicativos y custodia de soportes.
- Implementar controles sobre impresión, copias, digitalización y traslado de documentos.

4) Garantizar la disponibilidad y continuidad operativa de los sistemas e información crítica

Líneas de acción:

- Diseñar y ejecutar plan de copias de seguridad con pruebas periódicas de restauración.
- Definir planes de contingencia y continuidad (priorización por procesos críticos).
- Establecer mantenimiento preventivo y controles de infraestructura tecnológica.

5) Fortalecer la protección tecnológica frente a amenazas y vulnerabilidades

Líneas de acción:

- Actualización y hardening básico de equipos (parches, antivirus, bloqueo de puertos/USB).
- Seguridad del correo institucional: prevención de phishing, suplantación y adjuntos maliciosos.
- Gestión de vulnerabilidades y revisión periódica de configuraciones críticas

6) Reducir riesgos derivados de terceros y proveedores que tratan información de la ESE

Líneas de acción:

- Incorporar cláusulas de seguridad y privacidad en contratos (confidencialidad, incidentes, accesos).
- Controlar accesos de terceros (usuarios temporales, trazabilidad, revocación oportuna).
- Evaluar proveedores críticos (soporte TI, software, hosting, redes, digitalización).

7) Fortalecer la cultura organizacional de seguridad y privacidad

Líneas de acción:

- Capacitación anual por roles (asistencial, administrativo, directivo y TI).
- Campañas permanentes: escritorio limpio, contraseñas seguras, manejo de historia clínica.
- Sensibilización sobre reporte temprano de incidentes y responsabilidades disciplinarias.

8) Mejorar la detección, respuesta y recuperación ante incidentes de seguridad y privacidad

Líneas de acción:

- Implementar procedimiento de gestión de incidentes (detectar–reportar–contener–recuperar).
- Establecer matriz de escalamiento y comunicaciones internas ante incidentes.
- Realizar simulacros y lecciones aprendidas para ajustar controles y reducir recurrencia.

9) Medir y mejorar continuamente el desempeño del Plan

Líneas de acción:

Definir indicadores (cumplimiento de controles, backups probados, incidentes, accesos).

Auditorías internas y revisiones semestrales del Plan y sus evidencias.

Ejecución de planes de mejora con responsables, plazos y verificación de eficacia.