PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – AÑO 2026

E.S.E CAMU IRIS LÓPEZ DURÁN SAN ANTERO CÓRDOBA

Tabla de contenido

PRESENTACIÓN

Como Gerente de la ESE CAMU Iris López Durán de San Antero – Córdoba, presento el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información como una herramienta estratégica para proteger uno de nuestros activos más sensibles y valiosos: la información institucional y los datos personales de nuestros usuarios. En el sector salud, la información soporta la continuidad de la atención, la seguridad del paciente, la toma de decisiones clínicas y la transparencia administrativa; por ello, su protección no es opcional, sino un compromiso permanente con la comunidad y con el cumplimiento normativo. Este plan consolida el enfoque preventivo que requiere la ESE frente a amenazas internas y externas, como accesos no autorizados, pérdida o alteración de datos, fallas tecnológicas, incidentes de ciberseguridad, errores humanos y eventos físicos que puedan comprometer nuestros sistemas y archivos.

A través de este instrumento, la ESE identifica los riesgos prioritarios, evalúa su probabilidad e impacto, y define controles y acciones concretas para reducirlos, fortaleciendo la confidencialidad, integridad y disponibilidad de la información. El Plan establece responsables, actividades y cronogramas, de manera que cada proceso asuma su papel en la protección de la información, desde la gestión clínica y administrativa hasta las áreas de soporte tecnológico y archivo. Asimismo, impulsa la cultura institucional de seguridad y privacidad, promoviendo prácticas seguras en el manejo de historias clínicas, bases de datos, documentos contractuales, información financiera y comunicaciones oficiales. Este Plan se articula con el Sistema de Control Interno y la mejora continua, permitiendo anticiparnos a incidentes, responder de forma ordenada y recuperar la operación con rapidez cuando se presenten contingencias.

Con la implementación del Plan de Tratamiento de Riesgos, ratificamos nuestro compromiso con el respeto a la privacidad, el uso responsable de la información y la confianza de nuestros usuarios, asegurando que los servicios de salud se presten con calidad, oportunidad y respaldo documental seguro. Invito a todos los funcionarios y contratistas a asumir este plan como una responsabilidad compartida, donde cada acción preventiva cuenta y cada control aplicado protege la integridad institucional y el derecho fundamental de nuestros ciudadanos a la seguridad de sus datos.

Luz Suárez

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

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Empresa Social del Estado CAMU Iris López Durán de San Antero – Córdoba se constituye en un instrumento esencial para proteger uno de los activos más críticos de la institución: la información. En una entidad del sector salud, la información no solo soporta los procesos administrativos y financieros, sino que garantiza la continuidad del servicio, la seguridad del paciente y la toma de decisiones clínicas oportunas. Por ello, asegurar la confidencialidad, integridad y disponibilidad de los datos se convierte en una responsabilidad institucional permanente, especialmente cuando la ESE gestiona información sensible como historias clínicas, resultados de laboratorio, datos personales, facturación, contratación y reportes obligatorios a entes de control.

Este plan se formula con el propósito de identificar, evaluar y tratar los riesgos que puedan afectar la seguridad de la información y la privacidad de los datos personales, considerando amenazas internas y externas como accesos no autorizados, pérdida o alteración de documentos, fallas tecnológicas, incidentes de ciberseguridad, errores humanos, indisponibilidad de sistemas, fuga de información y eventos físicos que comprometan los archivos y equipos. En coherencia con las buenas prácticas de gestión del riesgo y con el marco de protección de datos personales y gobierno de la información, el Plan de Tratamiento establece controles, responsables, recursos y cronogramas que permitan reducir la probabilidad de ocurrencia y el impacto de estos riesgos, priorizando los procesos críticos y la información clasificada como reservada o sensible.

Asimismo, el Plan fortalece la cultura institucional de seguridad y privacidad, definiendo lineamientos para el manejo adecuado de la información por parte de funcionarios y contratistas, promoviendo la responsabilidad, la ética y el cumplimiento de protocolos, y articulándose con el Sistema de Control Interno, los planes institucionales, el Modelo Integrado de Planeación y Gestión y la estrategia de mejora continua. En consecuencia, la implementación de este Plan permitirá a la ESE CAMU Iris López Durán robustecer su capacidad de prevención, respuesta y recuperación ante incidentes, asegurar el cumplimiento normativo, mejorar la confianza de usuarios y partes interesadas, y consolidar un entorno de gestión de la información seguro, confiable y acorde con los desafíos actuales del sector salud.

ALCANCE DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información** de la **ESE CAMU Iris López Durán de San Antero – Córdoba** tiene como alcance la identificación, priorización, definición e implementación de controles para mitigar los riesgos que puedan afectar la **confidencialidad, integridad y disponibilidad** de la información institucional, así como la **privacidad de los datos personales** que se recolectan, almacenan, procesan, transmiten o custodian en el desarrollo de los procesos misionales, estratégicos y de apoyo. Aplica a **todas las dependencias, sedes, procesos, funcionarios y contratistas** que gestionen información en cualquier formato (físico, digital, electrónico, audiovisual), incluyendo la información clínica (historias clínicas y soportes asistenciales), administrativa, financiera, contractual, de talento humano, de atención al usuario y reportes a entes de control.

El alcance comprende los activos de información y los recursos tecnológicos asociados, tales como **equipos de cómputo, servidores, redes, sistemas de información, correo electrónico, dispositivos de almacenamiento, aplicativos, bases de datos, plataformas de comunicación**, así como los **archivos físicos** y espacios de custodia documental. Incluye la definición de medidas preventivas, correctivas y de mejora relacionadas con el **control de accesos**, gestión de usuarios y perfiles, copias de seguridad, continuidad y recuperación ante desastres, control de cambios, protección contra malware, manejo seguro de documentos, trazabilidad, clasificación de la información, y cumplimiento de principios de protección de datos personales y reserva legal. El Plan cubre tanto riesgos internos (errores humanos, fallas de procedimiento, uso inadecuado de información, pérdida o sustracción) como riesgos externos (ciberataques, accesos no autorizados, eventos físicos o ambientales, fallas de terceros), y se articula con el **Sistema de Control Interno**, el **MIPG**, la gestión documental y los planes institucionales vigentes, estableciendo responsables, actividades, recursos, cronograma e indicadores para asegurar su implementación y seguimiento.

OBJETIVO GENERAL

Implementar y mantener un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que permita identificar, priorizar y controlar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional y los datos personales, mediante la aplicación de medidas administrativas, técnicas y físicas, fortaleciendo el cumplimiento normativo, la continuidad operativa y la confianza de usuarios y partes interesadas.

OBJETIVOS ESPECÍFICOS

1. **Identificar y actualizar** el inventario y la clasificación de los activos de información y datos personales, determinando su criticidad y nivel de sensibilidad por proceso.
2. **Evaluar y priorizar** los riesgos de seguridad y privacidad, estableciendo niveles de probabilidad e impacto y definiendo el apetito/tolerancia al riesgo institucional.
3. **Definir e implementar controles** preventivos, detectivos y correctivos para reducir la probabilidad de ocurrencia y/o el impacto de incidentes de seguridad (acceso no autorizado, pérdida, fuga, alteración o indisponibilidad).
4. **Fortalecer la gestión de accesos** mediante lineamientos de usuarios, perfiles, contraseñas, autenticación, trazabilidad y privilegios mínimos, especialmente para información clínica y financiera.
5. **Asegurar la continuidad y recuperación** de la información a través de políticas y procedimientos de copias de seguridad, restauración, contingencias y recuperación ante desastres, priorizando procesos críticos.
6. **Establecer un procedimiento de respuesta a incidentes** que incluya detección, reporte, análisis, contención, recuperación y lecciones aprendidas, con responsabilidades claras por dependencia.
7. **Promover la cultura de seguridad y privacidad** mediante capacitación y sensibilización periódica a funcionarios y contratistas sobre manejo seguro de información, protección de datos y reserva legal.

8. **Monitorear y verificar** la eficacia de los controles implementados mediante indicadores, auditorías internas y seguimiento del plan de acción, asegurando mejora continua.
9. **Asegurar el cumplimiento** de los principios y obligaciones relacionadas con protección de datos personales, confidencialidad y reserva de la información en el marco del sector salud.

DEFINICIONES

Seguridad de la información: Conjunto de medidas y controles orientados a proteger la información frente a accesos no autorizados, pérdida, alteración o indisponibilidad, garantizando su uso seguro en la institución.

Privacidad de la información: Principio y práctica que asegura que los datos personales se recolecten, usen, almacenen y compartan de manera legítima, limitada y respetuosa de los derechos del titular.

Riesgo de seguridad de la información: Posibilidad de que una amenaza explote una vulnerabilidad y genere un impacto negativo sobre la confidencialidad, integridad o disponibilidad de la información.

Activo de información: Cualquier elemento que tenga valor para la entidad por contener o soportar información, como bases de datos, historias clínicas, archivos físicos, sistemas, aplicativos, servidores o documentos.

Confidencialidad: Propiedad de la información que evita su divulgación a personas no autorizadas, garantizando que solo accedan quienes tienen permiso y necesidad funcional.

Integridad: Propiedad que asegura que la información se mantenga completa, exacta y sin modificaciones no autorizadas durante su almacenamiento, procesamiento o transmisión.

Disponibilidad: Propiedad que garantiza que la información y los servicios tecnológicos estén accesibles y operativos cuando se requieren para la atención en salud y la gestión institucional.

Tratamiento del riesgo: Conjunto de decisiones y acciones para modificar el riesgo, mediante controles que lo reduzcan, lo eviten, lo transfieran, lo acepten o lo mitiguen según su priorización.

Control de seguridad: Medida administrativa, técnica o física implementada para prevenir, detectar o corregir incidentes, reduciendo la probabilidad o el impacto de los riesgos de información.

Incidente de seguridad de la información: Evento que compromete o puede comprometer la seguridad o privacidad de la información (por ejemplo, fuga de datos, malware, pérdida de equipos, acceso indebido o borrado accidental)

Misión

Gestionar de manera preventiva y sistemática los riesgos de seguridad y privacidad de la información, mediante la identificación, evaluación y tratamiento de amenazas que afecten la confidencialidad, integridad y disponibilidad de los datos institucionales y personales, asegurando controles eficaces, cumplimiento normativo y una cultura organizacional de protección de la información que respalde la continuidad y calidad de los servicios de salud.

Visión

Para el año 2027, consolidar un modelo institucional robusto y maduro de seguridad y privacidad de la información, reconocido por su capacidad de prevenir y responder a incidentes, proteger la información sensible y los datos personales, y garantizar la continuidad operativa y la confianza de los usuarios, mediante controles integrados, mejora continua y buenas prácticas alineadas con los estándares de seguridad de la información en el sector salud.

Metodología de tratamiento (ciclo anual)

1. **Inventariar activos**: historias clínicas, bases de datos, carpetas compartidas, correos, servidores, archivo físico, aplicativos.
2. **Clasificar información**: pública / interna / reservada / sensible (salud).
3. **Identificar amenazas y vulnerabilidades**: acceso indebido, phishing, malware, pérdida de equipos, errores humanos, fallas eléctricas, inundación, terceros.
4. **Valorar riesgo**: probabilidad x impacto.
5. **Definir tratamiento** por riesgo: **mitigar**, **evitar**, **transferir** o **aceptar** (con justificación).

6. **Implementar controles** (administrativos, técnicos y físicos).
7. **Monitorear** con indicadores y auditorías.
8. **Mejorar**: lecciones aprendidas y ajuste trimestral del plan

Líneas de acción y controles (núcleo del plan)

A. Gobernanza y políticas (administrativo)

- Política de seguridad y privacidad, clasificación de información, uso aceptable, escritorio limpio.
- Roles: líder TI, responsable de datos, dueños de activos, responsables de proceso.
- Cláusulas de confidencialidad y seguridad para contratistas y proveedores.

B. Control de accesos (confidencialidad)

- Acceso por perfiles y privilegio mínimo (no "todos ven todo").
- Bloqueo automático de pantalla, contraseñas robustas, revisión mensual de usuarios.
- Registro de préstamos/consulta de archivos físicos; control de llaves.

C. Continuidad, respaldos y disponibilidad

- Backups programados (diario/semanal), copia fuera del equipo principal.
- Pruebas de restauración mensuales (si no se prueba, "no existe").
- Plan de contingencia por caída de internet/sistema: formatos manuales y posterior carga.

D. Integridad y trazabilidad

- Control de versiones y autorizaciones para documentos críticos.
- Bitácoras de cambios (cuando aplique): quién accedió, qué modificó y cuándo.
- Procedimiento de digitalización y custodia de soportes.

E. Ciberseguridad básica (técnico)

- Antivirus actualizado, parches del sistema, bloqueo de USB o autorización controlada.
- Filtrado de correo y capacitación anti-phishing (simulacros sencillos).
- Segmentación mínima de red (si es posible) y Wi-Fi con claves seguras.

F. Gestión de incidentes (respuesta)

- Canal de reporte (correo/WhatsApp interno oficial), responsable y tiempos.
- Pasos: detectar → contener → analizar → recuperar → documentar → mejorar.
- Plantillas: acta de incidente, evidencias, acciones correctivas.

G. Privacidad y protección de datos (legal y operativo)

- Minimización: recolectar solo lo necesario.
- Consentimientos y avisos de privacidad donde aplique.
- Procedimiento para solicitudes de titulares (consulta/actualización).
- Control reforzado de historia clínica: reserva, autorizaciones, custodia.

Ver matriz de tratamiento de riegos de seguridad y privacidad de la información

ID	Proceso/Área	Activo de información	Riesgo	Amenaza
1	Asistencial / Historia Clínica	Historia clínica (física y/o sistema)	Acceso no autorizado a historia clínica	Uso indebido de credenciales / acceso interno
2	TI / Sistemas	Bases de datos clínicas y administrativas	Pérdida de información por falla de equipos o borrado accidental	Falla de disco / error humano
3	Administrativa / Archivo	Archivo físico (contratos, actos, HC en físico)	Deterioro o pérdida de documentos por humedad/plagas/inundación	Evento ambiental / condiciones inadecuadas
4	Todas las áreas	Correo institucional / comunicaciones	Suplantación / phishing y robo de credenciales	Phishing
5	Asistencial / Urgencias-Consulta	Aplicativo clínico y red	Indisponibilidad del sistema afecta continuidad de atención	Caída de internet o del aplicativo
6	Contratación / Jurídica	Información contractual y de proveedores	Fuga de información por terceros (soporte TI / proveedor software)	Acceso externo sin control
7	Talento Humano	Historias laborales y datos de personal	Exposición de datos personales de empleados	Acceso indebido / envío por canales no autorizados
8	Atención al Usuario / PQRS	Base de datos PQRS y registros de usuarios	Divulgación indebida de datos en respuestas o publicaciones	Error humano
9	Todas las áreas	Equipos portátiles / memorias USB	Pérdida o robo de equipos con información	Hurto/extravío
10	Control Interno / Todas	Plan y controles de seguridad	Controles no se sostienen en el tiempo (incumplimiento)	Falta de seguimiento

Vulnerabilidad (causa)	Impacto (1-5)	Probabilidad (1-5)	Nivel de riesgo (IxP)	Tratamiento (Mitigar/Evitar/Transferir/Aceptar)
Perfiles de usuario amplios; ausencia de revisión de usuarios; contraseñas débiles	5	3	15	Mitigar
No existen backups programados o no se prueban restauraciones	5	3	15	Mitigar
Almacenamiento sin control ambiental; falta de limpieza; estantería insuficiente	4	3	12	Mitigar
Baja sensibilización; ausencia de protocolo de reporte; falta de filtros/alertas	4	4	16	Mitigar
No hay plan de contingencia; no se priorizan procesos críticos	5	3	15	Mitigar
No se formalizan cláusulas; cuentas temporales sin revocación	4	3	12	Mitigar
Almacenamiento en carpetas compartidas sin control; uso de WhatsApp personal	4	3	12	Mitigar
Falta de revisión; desconocimiento de reserva y minimización	3	3	9	Mitigar
Sin cifrado; sin inventario; sin política de reporte	4	2	8	Mitigar
No hay indicadores ni auditoría; no se reporta a comité	4	3	12	Mitigar

Controles/Acciones de tratamiento	Tipo de control (Adm/Téc/Fís)	Responsable	Evidencia/Soporte
Definir perfiles por rol (mínimo privilegio); revisar y depurar usuarios mensualmente; bloquear cuentas inactivas; política de contraseñas y bloqueo de pantalla.	Adm/Téc	TI + Coordinación Asistencial	Matriz de perfiles; actas de revisión mensual; evidencias de bloqueo; política socializada
Implementar copias de seguridad diarias/semanales; almacenar copia fuera del equipo principal; realizar prueba mensual de restauración; bitácora de backups.	Téc	TI	Bitácora de backups; actas de pruebas de restauración; evidencias de almacenamiento externo/seguro
Diagnóstico de condiciones; plan de conservación preventiva (limpieza, control de humedad y plagas); organización y estantería; señalización; restricción de acceso.	Fís/Adm	Archivo + Servicios Generales	Informe diagnóstico; registros de limpieza/fumigación; actas de organización; control de acceso
Capacitación y campañas trimestrales; instructivo de verificación y reporte; simulacro trimestral; restricción de apertura de adjuntos sospechosos.	Adm/Téc	TI + Talento Humano	Listas de asistencia; piezas de campaña; reportes de simulacros; instructivo publicado
Adoptar plan de contingencia (formatos manuales + cargue posterior); definir RTO/RPO; simulacro semestral; mantenimiento preventivo.	Adm/Téc	Calidad + TI + Coordinación Asistencial	Procedimiento de contingencia; formatos; actas de simulacro; registros de mantenimiento
Incluir cláusulas de confidencialidad y seguridad; accesos temporales y trazables; revocación al cierre del servicio; checklist de evaluación de proveedores críticos.	Adm/Téc	Jurídica + TI	Contratos con cláusulas; actas de revocación; checklist proveedores; registros de accesos
Definir repositorio seguro con permisos; prohibir envío por canales no autorizados; capacitación en privacidad; acuerdos de confidencialidad.	Adm/Téc	Talento Humano + TI	Matriz de permisos; circular de lineamientos; listas de asistencia; compromisos firmados
Guía de respuesta segura; revisión de respuestas por responsable; capacitación en minimización; control de anexos.	Adm	Atención al Usuario + Jurídica	Guía; actas de revisión; evidencias de capacitación; checklist de anexos
Inventario de equipos; etiquetado; política de no almacenar info sensible localmente; procedimiento de reporte inmediato; bloqueo de USB o autorización.	Adm/Téc	TI + Almacén	Inventario; actas de entrega; política; registros de bloqueo/autorización USB
Definir tablero de indicadores; seguimiento trimestral; auditoría interna semestral; plan de mejora con responsables y fechas.	Adm	Control Interno + TI	Tablero; informes trimestrales; informes de auditoría; planes de mejora

Fecha inicio (2026-ISO)	Fecha fin (2026-ISO)	Indicador de seguimiento	Meta 2026	Estado (Planificado/En curso/Completado)	Observaciones
2026-02-01	2026-12-15	% usuarios con perfil definido	≥ 90%	Planificado	
2026-02-01	2026-12-31	# pruebas de restauración exitosas	12	Planificado	
2026-01-15	2026-10-30	% medidas preventivas implementadas	≥ 80%	Planificado	
2026-02-15	2026-12-15	% personal capacitado en phishing	≥ 90%	Planificado	
2026-03-01	2026-11-30	# simulacros realizados	2	Planificado	
2026-01-20	2026-12-10	% contratos críticos con cláusulas	100%	Planificado	
2026-02-01	2026-12-01	% repositorios con permisos aplicados	≥ 90%	Planificado	
2026-03-01	2026-12-15	% respuestas revisadas con checklist	≥ 95%	Planificado	
2026-02-10	2026-10-31	% equipos inventariados y etiquetados	100%	Planificado	
2026-03-15	2026-12-20	# informes de seguimiento	4	Planificado	