La Ceja del Tambo

Empresas Públicas de La Ceja E.S.P

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

DIRECCIÓN PLANEACIÓN ESTRATÉGICA Y TIC

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	**CÓDIGO**	**PL01-PG-06**
	VERSIÓN	**03**
	FECHA	**08/01/2026**
	PÁGINA	**1 de 1818**

Contenido

1. INTRODUCCIÓN

El *Plan de Tratamiento de Riesgos de la Seguridad y Privacidad de la Información* de Empresas Públicas de La Ceja E.S.P. Constituye una herramienta estratégica para garantizar la protección de los datos institucionales y personales que gestiona la entidad. Este plan se fundamenta en la necesidad de prevenir, mitigar y responder a los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, en un entorno cada vez más digital y regulado.

Este documento responde a las exigencias legales establecidas en Colombia, en particular por la **Ley 1581 de 2012** sobre protección de datos personales, la **Ley 1266 de 2008** en el contexto del habeas data financiero y comercial, y las disposiciones técnicas del **Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC)**. Asimismo, se articula con marcos internacionales como el **Reglamento General de Protección de Datos (GDPR)** y con estándares técnicos como la **norma ISO/IEC 27001**, orientada a la gestión de la seguridad de la información.

Desde una perspectiva de gestión pública, este plan se encuentra alineado con el **Modelo Integrado de Planeación y Gestión (MIPG)**, especialmente en los componentes de Gestión de la Información, Control Interno, Talento Humano y Transparencia, promoviendo una cultura institucional orientada a la protección de la información y el cumplimiento normativo.

A través de la identificación, análisis y tratamiento de los riesgos, así como del establecimiento de controles técnicos, organizativos y procedimentales, este plan busca fortalecer la capacidad institucional para prevenir incidentes, garantizar la continuidad operativa, asegurar el cumplimiento normativo y preservar la confianza de los ciudadanos y demás partes interesadas.

2. OBJETIVO

2.1 Objetivo General

Establecer un marco sistemático para la identificación, evaluación, tratamiento y monitoreo de los riesgos relacionados con la seguridad y privacidad de la información en Empresas Públicas de La Ceja E.S.P., con el fin de garantizar la confidencialidad, integridad y disponibilidad de los datos institucionales y personales, conforme a la normativa legal vigente, los lineamientos del MINTIC, los principios del Modelo Integrado de Planeación y Gestión (MIPG) y las normas técnicas ISO aplicables.

2.2 Objetivos Específicos

- Identificar los riesgos que puedan comprometer la seguridad y privacidad de la información, tanto en medios físicos como digitales.
- Evaluar los riesgos en función de su probabilidad de ocurrencia e impacto, priorizando aquellos que representen mayores amenazas para la organización.
- Definir estrategias de tratamiento de riesgos mediante acciones de mitigación, transferencia, aceptación o eliminación, asignando responsables y plazos.
- Establecer planes de respuesta ante incidentes que aseguren la continuidad operativa y minimicen los impactos sobre la información crítica.
- Fortalecer la cultura organizacional en materia de seguridad de la información mediante programas de capacitación, concienciación y buenas prácticas.
- Asegurar el cumplimiento de las obligaciones legales y reglamentarias en materia de protección de datos personales, tanto en el contexto nacional como internacional.
- Promover la mejora continua mediante auditorías, monitoreo y revisión periódica de los riesgos y controles implementados.

---

3. ALCANCE

El *Plan de Tratamiento de Riesgos de la Seguridad y Privacidad de la Información* aplica a todas las áreas, procesos, sistemas y actores involucrados en la gestión de información dentro de Empresas Públicas de La Ceja E.S.P. Abarca tanto los datos institucionales como los datos personales de clientes, usuarios, contratistas y empleados, en todas sus fases: recolección, almacenamiento, procesamiento, transmisión y disposición final.

El alcance del plan se define según los siguientes criterios:

3.1 Ámbito Geográfico

Aplica a todas las instalaciones físicas y sedes operativas de Empresas Públicas de La Ceja E.S.P., incluyendo oficinas principales, estaciones técnicas, centros de operación remotos, entornos virtuales y cualquier otra infraestructura donde se gestione información institucional.

3.2 Ámbito Operativo

Involucra todos los procesos misionales, estratégicos, de apoyo y evaluación que hagan uso o generen información, ya sea en formato físico o digital. Se incluyen los sistemas tecnológicos, servicios en la nube, software institucional, bases de datos, redes internas y externas, así como cualquier canal de comunicación oficial.

3.3 Usuarios y Personal Alcanzado

Este plan es de aplicación obligatoria para todos los servidores públicos, contratistas, proveedores, pasantes y terceros que tengan acceso, directo o indirecto, a la información gestionada por la entidad. Incluye a quienes participan en la creación, consulta, edición, custodia o eliminación de información.

3.4 Tipos de Información Cubierta

- Datos personales y sensibles (de empleados, usuarios, clientes, proveedores).
- Información institucional crítica y estratégica.
- Documentación legal, financiera, técnica y operativa.
- Registros del Sistema Integrado de Gestión (SIG).

3.5 Sistemas y Plataformas Tecnológicas

El plan aplica a todos los sistemas de información, servidores, dispositivos móviles, estaciones de trabajo, redes, bases de datos, aplicativos webs, sistemas SCADA y cualquier tecnología que soporte la operación institucional.

3.6 Cumplimiento Normativo

Este plan garantiza el cumplimiento de:

- **Ley 1581 de 2012** y sus decretos reglamentarios.
- **Ley 1266 de 2008** (habeas data financiero).
- **Lineamientos MINTIC** en seguridad digital y privacidad.
- **Normas ISO** aplicables: 27001, 9001, 14001 y 45001.
- **Directrices de MIPG**, especialmente en gestión de la información, control interno y cultura organizacional.

3.7 Formación y Cultura Organizacional

Comprende acciones de capacitación y concienciación continúa dirigidas a todo el personal, para garantizar el uso adecuado de la información y el cumplimiento de las políticas institucionales en seguridad y privacidad.

3.8 Respuesta ante Incidentes

Incluye la gestión de eventos que comprometan la seguridad de la información, mediante protocolos de notificación, contención, recuperación, análisis forense y mejora continua.

4. MARCO NORMATIVO Y REFERENCIAL

Este plan se fundamenta en un conjunto de normas legales, técnicas y organizacionales que establecen las obligaciones y buenas prácticas para la gestión segura y responsable de la información institucional y de los datos personales tratados por Empresas Públicas de La Ceja E.S.P. A continuación se presenta el marco normativo que sustenta su diseño e implementación:

4.1 Normativa Nacional

- **Ley 1581 de 2012** – *Ley de Protección de Datos Personales:* Establece los principios, derechos, deberes y procedimientos para el tratamiento adecuado de datos personales en Colombia.
- **Decreto 1377 de 2013:** Regula aspectos operativos de la Ley 1581, como el consentimiento del titular, políticas de tratamiento, medidas de seguridad y derechos de los titulares.
- **Ley 1266 de 2008** – *Ley de Habeas Data Financiero:* Regula el tratamiento de la información financiera, crediticia y comercial de personas naturales y jurídicas.
- **Ley 1273 de 2009:** Modifica el Código Penal para tipificar delitos informáticos y establece sanciones para la afectación de datos y sistemas.
- **Lineamientos del MINTIC:** Guías y directrices sobre seguridad digital, tratamiento de datos personales, gobernanza de TI y gestión de riesgos tecnológicos en entidades públicas.

4.2 Estándares Internacionales

- **ISO/IEC 27001:2022** – *Gestión de Seguridad de la Información:* Norma internacional que establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo control de accesos, análisis de riesgos, gestión de incidentes y mejora continua.
- **ISO 9001:2015** – *Gestión de la Calidad:* Aplica a través de la gestión documental, seguimiento a procesos críticos, tratamiento de no conformidades, control de registros y mejora continua.
- **ISO 14001:2015** – *Gestión Ambiental:* Aplica de manera transversal en la protección de información ambiental sensible, cumplimiento legal y control de riesgos asociados al entorno.
- **ISO 45001:2018** – *Seguridad y Salud en el Trabajo:* Aplica en la protección de información relacionada con SST, gestión de incidentes laborales y continuidad operativa.
- **Reglamento General de Protección de Datos (GDPR):** En caso de tratamiento de datos de ciudadanos de la Unión Europea, este reglamento exige principios como el consentimiento explícito, derecho al olvido y evaluaciones de impacto.

4.3 Lineamientos Institucionales y de Gestión Pública

- **Modelo Integrado de Planeación y Gestión (MIPG):** Este plan contribuye al cumplimiento de las políticas de Gestión de la Información, Control Interno, Talento Humano, Transparencia y Servicio al Ciudadano, asegurando el uso responsable, seguro y ético de la información institucional.
- **Políticas internas de seguridad de la información y protección de datos personales:** Adoptadas por la entidad para asegurar el cumplimiento legal y técnico.
- **Sistema Integrado de Gestión (SIG):** Este plan se articula con los procesos documentados del SIG institucional, incluyendo gestión de riesgos, gestión documental, control de cambios, continuidad operativa, entre otros.

---

5. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

La identificación y el análisis de riesgos constituyen la base del presente plan, permitiendo anticipar eventos que puedan afectar la seguridad, disponibilidad, integridad y privacidad de la información de Empresas Públicas de La Ceja E.S.P.

Para este propósito, la entidad cuenta con el **Mapa de Riesgos Institucional – Formato FO01-PG-16**, el cual constituye el instrumento oficial para la **identificación, análisis, evaluación, tratamiento y seguimiento de los riesgos**, incluyendo aquellos asociados a la gestión financiera, los procesos institucionales, la seguridad de la información y la protección de datos personales.

Dicho mapa contempla el análisis del **riesgo inherente y residual**, la valoración de **probabilidad e impacto**, la definición de **controles**, **estrategias de tratamiento**, **planes de reducción**, responsables y mecanismos de **monitoreo y seguimiento**, tanto por parte del proceso de Planeación como del Órgano de Control Interno (OCI).

La gestión de riesgos se desarrolla bajo los principios establecidos en la **norma ISO/IEC 27001:2022**, en alineación con el **Modelo Estándar de Control Interno (MECI)** y las **directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)**, garantizando coherencia con el Sistema Integrado de Gestión y el marco de control institucional.

5.1 Tipos de Riesgos a Considerar

Se contemplan los siguientes tipos de riesgo en el entorno institucional:

Riesgos de seguridad informática:	✓ Ataques cibernéticos (phishing, malware, ransomware). ✓ Accesos no autorizados a sistemas o redes. ✓ Exposición de credenciales.
Riesgos físicos:	✓ Robo de equipos. ✓ Daños por incendios, inundaciones o fallas eléctricas. ✓ Acceso no controlado a áreas restringidas. ✓ Obsolescencia tecnológica
Riesgos organizacionales:	✓ Fallas en la capacitación del personal. ✓ Errores humanos en el manejo de la información. ✓ Ausencia o desactualización de políticas.
Riesgos relacionados con la privacidad de datos personales:	✓ Divulgación no autorizada de información. ✓ Tratamiento de datos sin consentimiento válido. ✓ Pérdida o modificación indebida de datos personales sensibles.

5.2 Metodología de Evaluación de Riesgos

La evaluación de riesgos se realiza con base en dos criterios:

- **Probabilidad de ocurrencia:** Posibilidad de que el riesgo se materialice, considerando amenazas previas, vulnerabilidades existentes o frecuencia del evento.
- **Impacto potencial:** Consecuencias que tendría la materialización del riesgo sobre la organización, sus procesos, sus sistemas o su reputación.

Se utiliza una escala cualitativa de 5 niveles para cada criterio:

Probabilidad:	**Rara Vez:** Riesgos extremadamente raros, con casi ninguna probabilidad de ocurrir.
	Improbable: Riesgos que son relativamente poco frecuentes, pero que tienen una pequeña probabilidad de manifestarse.
	Posible: Riesgos que son más típicos, con alrededor de un 50/50 de probabilidades de tener lugar.
	Probable: Riesgos que son muy probables que ocurran.
	Definido: Riesgos que es casi seguro que se manifestarán. Aborde estos riesgos primero.
Impacto	**Insignificante:** Riesgos que no conllevan consecuencias negativas reales o que no representan una amenaza significativa para la organización o el proyecto.
	Menor: Riesgos que tienen un pequeño potencial de consecuencias negativas, pero que no afectarán significativamente el éxito general.
	Moderado: Riesgos que podrían traer consecuencias negativas, lo que representa una amenaza moderada para el proyecto u organización.

	Mayor: Riesgos con consecuencias negativas sustanciales que afectarán seriamente el éxito de la organización o proyecto.
	Catastrófico: Riesgos con consecuencias negativas extremas que podrían hacer que todo el proyecto falle o afecte gravemente las operaciones diarias de la organización. Estos son los riesgos de mayor prioridad a abordar.

5.3 Proceso de Identificación y Valoración de Riesgos

1. **Identificación de activos de información críticos:** Aplicaciones, bases de datos, servidores, redes, archivos físicos, etc.
2. **Detección de amenazas relevantes:** Basadas en historial institucional, informes técnicos, alertas nacionales (ColCERT) y evaluación interna.
3. **Identificación de vulnerabilidades:** Fallas de seguridad, debilidades en políticas, falta de control físico o digital.
4. **Valoración del riesgo:** Combinación entre probabilidad e impacto.
   Se categoriza así:

Nivel de riesgo	Descripción	Acción sugerida
Alto	Riesgo crítico. Alta probabilidad e impacto	Requiere tratamiento inmediato.
Medio	Riesgo significativo, pero controlable	Gestionar en el corto o mediano plazo.
Bajo	Riesgo tolerable o aceptable	Monitoreo y revisión periódica.

Los riesgos identificados, su valoración, controles, tratamiento y seguimiento se documentan y actualizan en el Mapa de Riesgos Institucional (FO01-PG-16), el cual sirve como insumo para la definición de los planes de acción y las estrategias de tratamiento descritas en el presente plan.

6. TRATAMIENTO DE LOS RIESGOS

Una vez identificados y valorados los riesgos que afectan la seguridad y privacidad de la información, Empresas Públicas de La Ceja E.S.P. adopta mecanismos de tratamiento con el fin de reducir su impacto o probabilidad, garantizar la continuidad del servicio y mantener el cumplimiento normativo.

El tratamiento de riesgos se puede aplicar bajo cuatro enfoques principales:

6.1 Estrategias de Tratamiento

a) Mitigación del riesgo	Reducción del riesgo mediante la implementación de controles técnicos, administrativos y organizativos. **Ejemplos de controles:** • Autenticación multifactor. • Cifrado de datos sensibles. • Políticas de contraseñas seguras. • Capacitación en manejo de información. • Copias de respaldo automáticas
b) Transferencia del riesgo	Asignación del riesgo, total o parcialmente, a un tercero mediante: • Contratación de seguros. • Externalización de servicios tecnológicos (con acuerdos de nivel de servicio - SLA). • Inclusión de cláusulas contractuales sobre protección de datos y seguridad.
c) Aceptación de riesgo	Aplicable cuando el riesgo tiene bajo impacto o el costo de mitigación es mayor que sus efectos. Se documenta y se monitorea periódicamente.
d) Eliminación del riesgo	Aplicación de medidas que eliminan la fuente del riesgo, como: • Descontinuar procesos o tecnologías obsoletas. • Modificar procedimientos críticos. • Reorganizar flujos de información.

6.2 Plan de Acción y Seguimiento

Para cada riesgo clasificado, se define un plan de acción que incluye:

Riesgo Identificado	Acción Correctiva o Preventiva	Tipo de Tratamiento	Responsable	Plazo
Acceso no autorizado a bases de datos	Implementar autenticación multifactor y control de acceso	Mitigación	Técnico Operativo de las TIC	3 meses
Pérdida de datos por fallo en servidor	Establecer respaldo automático y redundancia	Mitigación	Técnico Operativo de las TIC	2 meses
Ciberataque (ransomware)	Instalar antivirus y capacitar empleados	Mitigación	Técnico Operativo de las TIC	1 mes
Incumplimiento de la Ley 1581	Realizar auditoría y actualizar políticas de privacidad	Mitigación / Cumplimiento	OCI	4 meses

Riesgo Identificado	Acción Correctiva o Preventiva	Tipo de Tratamiento	Responsable	Plazo
Software desactualizado	Establecer protocolo de actualización periódica	Eliminación	Técnico Operativo de las TIC	1 mes
Phishing a empleados	Implementar filtros de correo y simulacros de phishing	Mitigación	Técnico Operativo de las TIC	2 meses

6.3 Procedimiento para la Gestión del Tratamiento

1. **Definición del tratamiento:** Selección de la estrategia más adecuada para cada riesgo.
2. **Asignación de responsables:** Designación formal del líder de implementación de cada acción.
3. **Establecimiento de plazos:** Cronograma definido para cada medida.
4. **Monitoreo y seguimiento:** Verificación del cumplimiento y efectividad del tratamiento.
5. **Revisión periódica:** Revaluación del riesgo postratamiento y ajustes si son necesarios.

---

7. PLAN DE CONTINUIDAD Y RECUPERACIÓN ANTE INCIDENTES

El presente componente establece las medidas preventivas, reactivas y correctivas necesarias para garantizar la continuidad operativa y la recuperación efectiva de los sistemas de información y datos críticos en caso de un incidente que afecte la seguridad de la información o los servicios tecnológicos institucionales.

7.1 Objetivo

Asegurar la restauración oportuna de los procesos críticos, los activos de información y los servicios asociados, minimizando el impacto de eventos disruptivos (como ciberataques, fallos técnicos, desastres naturales o errores humanos) sobre la operación y los ciudadanos.

7.2 Componentes Clave

a) Respaldo y protección de información crítica

- Implementación de copias de seguridad automáticas (backup).
- Almacenamiento de respaldos en ubicaciones seguras o entornos en la nube.

- Replicación en tiempo real de bases de datos sensibles.

b) Redundancia tecnológica

- Servidores de respaldo para asumir la operación en caso de falla.
- Configuraciones de alta disponibilidad y balanceo de carga.

c) Planes de recuperación ante desastres (DRP)

- Procedimientos documentados para restaurar la infraestructura tecnológica.
- Priorización de servicios y sistemas críticos para recuperación secuencial.

d) Plan de comunicación durante incidentes

- Protocolos para informar a empleados, usuarios y partes interesadas.
- Canales oficiales definidos: correo, mensajería interna, sitio web.
- Portavoces designados para evitar información contradictoria.

e) Roles y responsabilidades

Rol	Responsabilidad
Responsable de Continuidad	Coordinar implementación y actualización del plan
Equipo de Respuesta a Incidentes	Ejecutar acciones técnicas de recuperación
Equipo de Comunicación	Informar interna y externamente sobre el incidente

7.3 Simulacros y Pruebas

- **Simulacros periódicos** de recuperación ante incidentes tecnológicos (al menos una vez al año).
- **Evaluaciones post-simulacro** para identificar oportunidades de mejora.
- **Pruebas de recuperación de respaldos**, para verificar integridad y tiempos de restauración.

7.4 Capacitación al personal

- Entrenamiento a líderes de proceso sobre su rol en caso de incidente.
- Manuales rápidos de actuación ante pérdida de acceso a sistemas.
- Cultura de reporte inmediato de incidentes o anomalías.

7.5 Mejora continua del plan

- Revisión anual o posterior a cada incidente.
- Actualización ante:

- Cambios en la infraestructura tecnológica.
- Nuevas amenazas identificadas.
- Resultados de auditorías o simulacros.

8. CAPACITACIÓN Y CONCIENCIACIÓN EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8.1 Objetivo

Fortalecer las competencias del talento humano de Empresas Públicas de La Ceja E.S.P. en relación con el manejo seguro de la información institucional y la protección de los datos personales, promoviendo una cultura organizacional orientada al cumplimiento normativo, la prevención de incidentes y la mejora continua.

8.2 Plan Anual de Formación

El plan de formación en seguridad de la información y protección de datos será liderado por el área de TIC en articulación con Talento Humano y se ejecutará con base en el nivel de exposición al riesgo de cada proceso.

Actividades principales:

Actividad	Frecuencia	Público objetivo	Modalidad
Talleres de concienciación general	Trimestral	Todo el personal	Presencial / virtual
Inducción en seguridad de la información	En el ingreso	Nuevos funcionarios y contratistas	Presencial / virtual
Actualización normativa (Ley 1581, ISO, MINTIC)	Anual o cuando haya cambios	Responsables de procesos	Presencial
Simulacros de ciberataques (phishing)	Semestral	Personal con acceso a sistemas críticos	Virtual / interna
Buenas prácticas en contraseñas y uso de dispositivos	Bimestral	Todo el personal	Comunicaciones internas

8.3 Estrategias de Sensibilización

- Campañas visuales en carteleras, pantallas y correo institucional.
- Boletines mensuales con tips sobre seguridad digital.
- Videos educativos breves.
- “Día de la Seguridad de la Información”.
- Reconocimiento a buenas prácticas por parte del personal.

8.4 Evaluación de Conocimientos

- Cuestionarios post-capacitación.
- Encuestas de satisfacción y efectividad.
- Registro de participación y seguimiento.
- Simulaciones de incidentes y análisis de respuesta.

8.5 Responsables y Recursos

Responsable	Función
Área TIC	Diseño del contenido técnico y actualizaciones
Talento Humano	Ejecución del plan de formación y logística
Líderes de proceso	Verificación del cumplimiento por su equipo
Mesa Técnica de Gobierno Digital	Monitoreo y revisión del avance del plan

Se asignará un presupuesto anual específico para soportar las actividades formativas y de sensibilización, incluyendo materiales, plataformas virtuales y facilitadores externos si es necesario.

---

9. MONITOREO, AUDITORÍA Y MEJORA CONTINUA

9.1 Objetivo

Establecer un sistema sistemático de seguimiento, evaluación y mejora continua de las medidas de seguridad y privacidad de la información, con el fin de verificar su eficacia, detectar debilidades, garantizar el cumplimiento normativo y fortalecer los mecanismos de control institucional.

9.2 Actividades de Monitoreo Continuo

Actividad	Descripción	Herramienta / Responsable	Frecuencia
Monitoreo de accesos	Revisión de logs de ingreso a sistemas, bases de datos y redes internas	Sistema de gestión de eventos e información de seguridad (SIEM) – Área TIC	Semestral
Detección de anomalías	Identificación de comportamientos sospechosos (malware, tráfico inusual)	IDS/IPS, antivirus, firewall – Área TIC	Tiempo real
Seguimiento de incidentes	Registro, análisis y trazabilidad de los eventos de seguridad reportados	Bitácora de incidentes / Mesa Técnica de Gobierno Digital	Permanente
Revisión de respaldos	Verificación de integridad, frecuencia y recuperación	Plataforma de backup – Jefe de Infraestructura	Semanal

9.3 Auditorías Internas y Externas

Tipo de auditoría	Objetivo	Responsable	Frecuencia
Auditoría interna de seguridad de la información	Verificar cumplimiento de políticas, controles y normativas	Comité de Seguridad / Control Interno	Semestral
Auditoría de cumplimiento legal (Ley 1581, ISO 27001)	Evaluar conformidad normativa y contractual	Responsable de Cumplimiento / Jurídica	Anual
Auditoría externa especializada (opcional)	Validar robustez del SGSI y controles tecnológicos	Firma externa / MINTIC (si aplica)	Según plan

9.4 Acciones Correctivas y Preventivas

- **Acciones correctivas:** Se aplican cuando se detectan desviaciones, fallos o incumplimientos.
- **Acciones preventivas:** Se anticipan a posibles riesgos o debilidades detectadas en el monitoreo o evaluación.

Cada acción debe estar documentada, con responsable, fecha de implementación y evaluación posterior.

9.5 Indicadores de Desempeño

Indicador	Fórmula	Meta
% de incidentes cerrados dentro del plazo	(Incidentes resueltos a tiempo / Total de incidentes) × 100	≥ 90%
% de cumplimiento del plan de capacitación	(Capacitaciones realizadas / Programadas) × 100	100%
Frecuencia de respaldo verificado con éxito	(Respaldos correctos / Respaldos ejecutados) × 100	≥ 95%
Nivel de cumplimiento auditorías	(Hallazgos resueltos / Total hallazgos) × 100	≥ 90%

9.6 Ciclo de Mejora Continua (PHVA)

El plan adopta el ciclo de **Planear – Hacer – Verificar – Actuar** para garantizar su mejora progresiva:

- **Planear:** Identificación de riesgos, controles y políticas.
- **Hacer:** Implementación del plan, formación y controles.
- **Verificar:** Auditorías, seguimiento y evaluación.
- **Actuar:** Ajustes, lecciones aprendidas y actualizaciones.

10. CIERRE DEL PLAN

10.1 Conclusión

El *Plan de Tratamiento de Riesgos de la Seguridad y Privacidad de la Información* de Empresas Públicas de La Ceja E.S.P. representa un compromiso institucional con la protección de los datos, la seguridad de los sistemas de información y el cumplimiento de las obligaciones legales y normativas vigentes.

Este plan proporciona una hoja de ruta clara para identificar, evaluar y gestionar los riesgos relacionados con la información, fortaleciendo la capacidad institucional para prevenir incidentes, responder ante eventos disruptivos y proteger la integridad, confidencialidad y disponibilidad de los activos informáticos y documentales.

La participación activa de todas las dependencias, el liderazgo del La Mesa Técnica de Gobierno Digital es fundamentales para el éxito del presente plan y su alineación con el Modelo Integrado de Planeación y Gestión (MIPG) y las normas internacionales como ISO 27001, ISO 9001, e ISO 45001.

10.2 Revisión y Actualización del Plan

Este plan será revisado y actualizado:

- **Anualmente**, como mínimo.
- **Posterior a incidentes críticos** que afecten la seguridad de la información.
- **Cuando haya cambios relevantes** en la normatividad, procesos, tecnologías o estructura organizacional.

Responsables:

- Mesa Técnica de Gobierno Digital.
- Responsable de Cumplimiento.
- Área de Tecnología de la Información.
- Coordinador del SIG.

10.3 Compromiso de la Alta Dirección

La alta dirección de Empresas Públicas de La Ceja E.S.P. reafirma su compromiso con la implementación, seguimiento y mejora del presente plan, e invita a todos los funcionarios, contratistas y partes interesadas a asumir con responsabilidad el cumplimiento de las disposiciones aquí establecidas.

La seguridad de la información es un componente transversal del buen gobierno, la sostenibilidad y la confianza ciudadana.

HOJA CONTROL DE CAMBIOS

VERSIÓN	FECHA	REVISÓ	ELABORÓ	APROBÓ	MODIFICACIONES
01		P.U. Tics	P.U. Tics	Dir. Planeación	Plan Inicial
02	07/07/2025	P.U. Tics	P.U. Proyectos Estratégicos y del SIG	Dir. Planeación	La versión actual del Plan fue **reorganizada, fortalecida y alineada** con el Modelo Integrado de Planeación y Gestión (MIPG) y las normas técnicas ISO (27001, 9001, 45001).
03	08/01/2026	P.U. Proyectos de Gestión Integral y TIC	T.O de las TIC	Dir. Planeación y TIC	Se agrega en el 5.1 Tipos de Riesgos a Considerar, riesgos físicos un literal "Obsolescencia tecnológica en el parque tecnológico" SE agrega Mesa Técnica de Gobierno Digital