Plan operacional de seguridad de la información

2024-2028

(Versión 3)

Elaborado por:
Ing. Eliany Rocío Montejo Carrascal – Profesional Especializado

En revisión:
Ing. Gustavo Carvajal Millan – Jefe de Oficina TIC

Septiembre del 2026

Tabla de contenido

PLAN DE SEGURIDAD DE LA INFORMACIÓN 3

1. Introducción 3
2. Alcance 4
3. Responsabilidades sobre activos de información ..... **¡Error! Marcador no definido.**
4. Análisis de riesgos actuales ..... **¡Error! Marcador no definido.**
5. Proyectos e iniciativas ..... **¡Error! Marcador no definido.**

PLAN DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

La seguridad y privacidad de la información constituyen condiciones esenciales para la continuidad de los servicios, la confianza de la ciudadanía y el cumplimiento de las obligaciones institucionales de la Alcaldía Municipal de Chía. El presente Plan Operacional de Seguridad de la Información actualiza el documento 2024-2028 y transforma los lineamientos de la Política de Seguridad de la Información en actividades concretas, medibles y trazables, articuladas con el Modelo de Seguridad y Privacidad de la Información (MSPI), el PETI, el Modelo de Gestión y Gobierno TI (MGGTI), el Modelo de Arquitectura Empresarial (MAE), el Modelo de Gestión de Proyectos TI (MGPTI) y la gestión institucional de riesgos.

La Política de Seguridad de la Información 2024-2027, versión 3 actualizada en mayo de 2026, amplió y precisó controles relacionados con recursos humanos, activos, permisos y privilegios, control de acceso, seguridad física, criptografía, operaciones, comunicaciones, adquisición y desarrollo de sistemas, proveedores, internet, correo electrónico, identidad, contraseñas, incidentes, riesgos, cumplimiento, sensibilización y auditoría. Por lo tanto, el plan operacional debe pasar de una relación general de riesgos e iniciativas a un esquema de ejecución que indique responsables reales, periodicidad, evidencias, indicadores y mecanismos de seguimiento.

La actualización también incorpora aprendizajes derivados del autodiagnóstico MSPI realizado en 2026, de los seguimientos a riesgos y controles de la Oficina TIC, de la formalización de procedimientos como gestión de cambios, desarrollo seguro y conectividad inalámbrica, de los ejercicios de sensibilización y de la revisión de la infraestructura física y tecnológica del datacenter. Se priorizan acciones de alto impacto que puedan ejecutarse con recursos existentes, sin trasladar responsabilidades operativas a personas que no cuenten con los accesos, competencias o autoridad técnica para ejecutar el control.

2. Objetivos

2.1 Objetivo general

Implementar de manera gradual y verificable los lineamientos de la Política de Seguridad de la Información de la Alcaldía Municipal de Chía, fortaleciendo la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, la gestión de riesgos, la continuidad de los servicios, la respuesta a incidentes y la cultura institucional de seguridad y privacidad.

2.2 Objetivos específicos

- Convertir los lineamientos de la Política de Seguridad de la Información en actividades operativas con responsables, metas, periodicidad y evidencias definidas.
- Mantener actualizado el MSPI mediante autodiagnóstico, cierre de brechas y seguimiento de acciones de mejora.
- Fortalecer la identificación, clasificación, custodia y protección de los activos de información con participación de los propietarios de los procesos.
- Mejorar la gestión de identidades, accesos, privilegios y transiciones laborales, aplicando mínimo privilegio y trazabilidad.
- Fortalecer la seguridad de redes, infraestructura, endpoints, respaldos, continuidad y condiciones físicas del datacenter.
- Integrar seguridad en el ciclo de vida de proyectos, desarrollo de software y gestión de cambios tecnológicos.
- Mejorar la prevención, detección, documentación, escalamiento y aprendizaje derivado de incidentes de seguridad.
- Fortalecer la seguridad en la contratación y en la relación con proveedores, sin sustituir las responsabilidades de supervisores, Contratación y áreas dueñas del proceso.
- Promover una cultura de seguridad mediante sensibilización breve, práctica y continua, considerando la resistencia al cambio identificada en la alcaldía.
- Establecer indicadores y evidencias que permitan demostrar la ejecución y eficacia de los controles ante auditorías y seguimientos institucionales.

3. Alcance

El plan aplica a todos los procesos, personas, tecnologías, datos y sistemas de información involucrados en la gestión pública de la Alcaldía Municipal de Chía, de acuerdo con el alcance definido por la Política de Seguridad de la Información. Comprende funcionarios, contratistas, proveedores, pasantes y terceros; infraestructura tecnológica; plataformas, aplicativos y servicios digitales; información generada, procesada, almacenada o transmitida; sedes físicas; acceso remoto y servicios en nube cuando apliquen.

La ejecución es institucional y distribuida. La Oficina TIC lidera los componentes de gobierno y seguridad tecnológica bajo su competencia, pero cada Secretaría, Dirección, Oficina, supervisor, propietario de activo y líder técnico conserva la responsabilidad sobre la información, los accesos, los tratamientos y las actividades operativas que administra. El plan no concentra en Gobierno TI actividades técnicas

que requieran accesos o atribuciones propias de Infraestructura, Desarrollo, Soporte, Contratación, Función Pública u otras áreas.

4. Marco de referencia y articulación institucional

El presente plan se articula con la Política de Seguridad de la Información, la Política de Gobierno Digital, la Política de Seguridad Digital, el MSPI, la gestión institucional de riesgos y los instrumentos de planeación de la alcaldía. Para efectos operativos, se aplicarán las versiones vigentes de los documentos institucionales.

- Política de Seguridad de la Información 2024-2027, versión 3, actualizada mayo de 2026.
- Plan Estratégico de Tecnologías de la Información (PETI 2024-2028).
- Modelo de Gestión y Gobierno TI (MGGTI).
- Modelo de Arquitectura Empresarial (MAE) y su hoja de ruta.
- Modelo de Gestión de Proyectos TI (MGPTI).
- Metodología de Gestión del Cambio TIC y formato institucional de Control de Cambios.
- Procedimiento de Desarrollo Seguro de Software.
- Procedimiento de Conectividad Inalámbrica y formato de Solicitud de Conexión Wi-Fi.
- Matriz vigente de riesgos y controles de la Oficina TIC en Kawak.
- Autodiagnóstico MSPI 2026.
- Catálogo de servicios TIC, Mesa de Servicios - GLPI y procedimientos de operación.
- Instrumentos institucionales de gestión documental, contratación, talento humano, continuidad, privacidad y atención al ciudadano, según competencia.

5. Criterios de actualización frente al plan anterior

El plan anterior contenía una matriz estática de catorce riesgos y una relación de proyectos e iniciativas. La actualización 2026 conserva su propósito, pero modifica el enfoque para evitar duplicidad con la matriz oficial de riesgos y para responder a la política vigente.

Aspecto	Ajuste 2026
Riesgos	La matriz de riesgos vigente en Kawak se convierte en la fuente oficial. El plan no replica de forma rígida riesgos que pueden cambiar; establece actividades de seguimiento y tratamiento alineadas a dicha matriz.
Responsables	Se precisan responsables según capacidad real de ejecución. Gobierno TI coordina, consolida y hace seguimiento en Kawak; los líderes técnicos ejecutan y evidencian controles operativos cuando tienen acceso y autoridad sobre la plataforma o servicio.
MSPI	Se incorpora el autodiagnóstico 2026 como línea.
Procedimientos	Se incluyen los documentos formalizados o actualizados: Gestión de Cambios, Desarrollo Seguro, Conectividad Inalámbrica y gestión de incidentes, entre otros.
Evidencias	Cada actividad debe producir evidencia verificable: tickets, formatos, actas, reportes, logs, matrices, aprobaciones, registros de capacitación o resultados de pruebas.
Indicadores	Se establecen indicadores mínimos para medir cobertura, cumplimiento y eficacia, no solo existencia documental.
Cultura	Se incorpora una estrategia de adopción gradual, con comunicaciones cortas, acompañamiento a líderes y aprovechamiento de espacios existentes para disminuir resistencia al cambio.

6. Modelo de gobernanza y responsabilidades

La gobernanza del plan se basa en el principio de corresponsabilidad. La asignación de una actividad deberá respetar la competencia, el acceso a la información y la capacidad operativa del responsable. Cuando una actividad involucre varias áreas, el líder del control deberá obtener y conservar las evidencias de los responsables técnicos o funcionales que ejecutan el trabajo.

Instancia / rol	Responsabilidad operacional en el plan
Comité Institucional de Gestión y Desempeño	Aprobar políticas y lineamientos institucionales; respaldar la implementación del MSPI y efectuar decisiones de alto nivel.
Comité de Seguridad de la Información	Analizar situaciones relevantes de seguridad, coordinar decisiones interdependencias y apoyar respuestas a incidentes o requerimientos que requieran participación institucional.

Instancia / rol	Responsabilidad operacional en el plan
Jefe Oficina TIC	Liderar el MSPI; priorizar actividades; gestionar recursos; validar lineamientos, requerimientos técnicos y planes de mejora.
Gobierno TI – Oficina TIC	Coordinar actualización de políticas y estrategias; consolidar autodiagnóstico MSPI; articular riesgos, y seguimiento; acompañar la adopción. No sustituye la ejecución técnica de controles que dependen de accesos administrados por otras áreas.
Infraestructura y Redes – Oficina TIC	Administrar redes, servidores, VPN, firewalls, conectividad, segmentación, respaldos, cuentas técnicas, alta disponibilidad, Datacenter y controles de infraestructura conforme a su competencia.
Soporte Técnico / Mesa de Servicios	Registrar, clasificar, escalar y documentar incidentes y requerimientos; apoyar seguridad de endpoints, inventarios, mantenimiento y evidencias operativas.
Desarrollo de Sistemas de Información	Aplicar desarrollo seguro, segregación de ambientes, control de código, pruebas, gestión de vulnerabilidades y despliegues; ejecutar y evidenciar los cambios de aplicaciones.
Especialista / enlace de seguridad informática	Apoyar análisis de riesgos técnicos, monitoreo, incidentes, hardening, configuración de herramientas de seguridad y coordinación técnica.
Función Pública	Articular inducción, retiro, novedades de personal y formación; suministrar oportunamente información que permita altas, cambios y bajas de accesos.
Contratación y supervisores	Incorporar y verificar obligaciones de seguridad y confidencialidad en contratos; efectuar seguimiento contractual dentro de su competencia.
Servicios Administrativos / responsables de sedes	Apoyar controles de seguridad física, acceso, videovigilancia, condiciones locativas y mantenimiento de sistemas físicos cuando corresponda.
Propietarios de activos / líderes de proceso	Identificar, clasificar y mantener actualizados sus activos; definir necesidad de acceso y validar tratamiento, conservación y uso de la información.
Control Interno	Realizar evaluación independiente, auditoría y seguimiento conforme a sus funciones.
Todos los usuarios	Cumplir políticas, proteger credenciales, utilizar adecuadamente los recursos y reportar incidentes o debilidades.

7. Diagnóstico y línea base

La línea base se construye con el autodiagnóstico MSPI 2026, los seguimientos de riesgos, la evidencia aportada por los responsables técnicos y los documentos formalizados en la Oficina TIC. Los resultados muestran avances documentales importantes, pero también la necesidad de fortalecer la ejecución repetible y la trazabilidad operativa.

Tema	Avance / evidencia base	Prioridad de fortalecimiento
Riesgos y controles	Seguimiento periódico a riesgos y controles de la Oficina TIC; durante 2026 se consolidaron reportes y evidencias.	Mantener la matriz oficial en Kawak como fuente única y documentar materialización o no materialización con criterios verificables.
Gestión de cambios	Metodología y formato institucional formalizados; socialización realizada.	Aumentar evidencia de uso real mediante tickets, formatos diligenciados, validación posterior y lecciones aprendidas.
Desarrollo seguro	Procedimiento actualizado y en proceso de formalización; ambientes diferenciados y controles existentes.	Completar publicación, aplicación uniforme y evidencias de pruebas de seguridad, repositorio y trazabilidad.
Redes	Procedimiento de conectividad inalámbrica y formato de solicitud formalizados; segmentación y controles de red existentes.	Consolidar revisión periódica de reglas, acceso de terceros, segmentación y evidencia de monitoreo.
Activos de información	Matrices de activos actualizadas en diferentes dependencias.	Completar cobertura institucional, propietarios, clasificación y revisiones periódicas.
Sensibilización	Jornadas realizadas en 2026 y material de sensibilización disponible.	Formalizar programa anual con cobertura, evaluación, refuerzos y medición de apropiación.

Tema	Avance / evidencia base	Prioridad de fortalecimiento
Datacenter y continuidad	Informes técnicos 2026 evidencia UPS, climatización, control de acceso, CCTV, detección y extinción de incendios.	Atender hallazgos de mantenimiento, escalamiento de alarmas, extintores y documentación técnica; fortalecer DRP, RTO, RPO y pruebas.
Incidentes	Gestión a través de mesa de servicios; experiencia 2025 con incidente de defacement para reporte externo.	Consolidar clasificación, escalamiento, reporte externo oportuno, lecciones aprendidas y simulacros.
Identidad y accesos	Política define mínimo privilegio, usuarios individuales y gestión de accesos.	Fortalecer la verificación periódica y evidencia operativa por los administradores reales de sistemas y cuentas.

8. Líneas operacionales 2026-2028

Las siguientes líneas traducen la Política de Seguridad de la Información en actividades ejecutables. Los plazos se expresan como frecuencia o meta para permitir su programación anual. Cuando una actividad dependa de otra dependencia, la Oficina TIC deberán solicitar el insumo y consolidar la evidencia, sin asumir como propia una ejecución que corresponde al responsable funcional o técnico.

#	Línea / política	Numerales política	Actividad operacional	Responsable líder	Apoyo	Periodicidad / meta	Evidencia mínima
1	Gobernanza y mejora continua del MSPI	5.2.2.3	Actualizar cuando sea necesario MSPI.	Gobierno TI	Jefe TIC, líderes técnicos, responsables de proceso	Anual	Matriz de autodiagnóstico.
2	Gestión de riesgos de seguridad	5.1.4	Revisar la matriz vigente de riesgos y controles, documentar materialización o no materialización y actualizar tratamientos ante cambios o incidentes.	Responsables de riesgo vs control; Gobierno TI consolida	Líderes técnicos	Según cronograma institucional; mínimo cuatrimestral	Kawak, evidencias, actas, reportes de control
3	Activos de información	5.10	Completar y mantener inventario, clasificación de activos por dependencia, identificando propietario, custodio, criticidad, privacidad y cambios relevantes.	Propietarios de activos y líderes de proceso	Oficina TIC, Gestión Documental	Revisión anual y por cambios significativos	Matriz de activos

#	Línea / política	Numerales política	Actividad operacional	Responsable líder	Apoyo	Periodicidad / meta	Evidencia mínima
4	Identidad, accesos y privilegios	5.11, 5.12, 5.21, 5.22	Formalizar altas, cambios, bajas y recertificación de privilegios; aplicar mínimo privilegio y eliminar cuentas innecesarias.	Administradores de cada Sistema, Datacenter y Desarrollo e Innovación	Función Pública, supervisores, Gobierno TI seguimiento	Altas/bajas por evento; vrificación trimestral en sistemas críticos	Solicitudes, tickets, matriz de accesos, reportes de verificación.
5	Transiciones laborales	5.9	Asegurar notificación oportuna de retiros, cambios de rol y revocación de accesos, devolución de activos y transferencia de información.	Función Pública, jefes y supervisores para notificación; TIC ejecuta accesos bajo su administración	Soporte, Infraestructura, propietarios de sistemas	Por evento; revisión mensual de pendientes	Lista de chequeo, ticket de baja o cambio, acta de entrega
6	Seguridad de endpoints y software	5.4, 5.15	Definir línea base de seguridad de equipos, software autorizado, parches, antimalware, bloqueo, conexión de terceros y controles sobre medios removibles.	Soporte Técnico, Datacenter	Seguridad informática	Monitoreo mensual; línea base anual	Inventario, reportes de parches, antimalware, checklist de cumplimiento

#	Línea / política	Numerales política	Actividad operacional	Responsable líder	Apoyo	Periodicidad / meta	Evidencia mínima
7	Seguridad de redes y acceso de terceros	5.12, 5.13.9, 5.16	Mantener segmentación, reglas de firewall, VPN y redes para contratistas, visitantes sin acceso a la LAN; revisar excepciones y trazabilidad.	Datacenter y Redes	Seguridad informática, Soporte	Revisión trimestral y por cambio	Diagramas, respaldos de configuración, tickets, reportes de reglas, segmentación
8	Criptografía y comunicaciones seguras	5.14, 5.16	Mantener cifrado en tránsito, VPN/certificados y controles de claves; documentar estándares criptográficos mínimos y ciclo de vida de certificados.	Datacenter, administradores de plataformas	Seguridad informática, Desarrollo	Revisión semestral; renovación por vigencia	Inventario de certificados, configuración aprobada, evidencias de renovación
9	Respaldo, recuperación y continuidad	5.15.4, 5.13, 5.24	Formalizar esquema de backups, retención y restauración; definir servicios críticos, RTO, RPO y DRP; ejecutar pruebas de restauración y recuperación.	Datacenter y Redes	Jefe TIC, Desarrollo, dueños de servicio	Backups según criticidad; prueba restauración trimestral; DRP anual	Logs de backup, actas de restauración, DRP, resultados de pruebas

#	Línea / política	Numerales política	Actividad operacional	Responsable líder	Apoyo	Periodicidad / meta	Evidencia mínima
10	Datacenter y seguridad física	5.13	Hacer seguimiento al plan de mantenimiento, climatización, UPS, control de acceso, alarmas, detección, extinción, CCTV y hallazgos físicos; documentar responsables de escalamiento.	Datacenter y Redes, responsables de instalaciones según competencia	Servicios Administrativos, SST, Obras Públicas	Inspección mensual; mantenimiento según fabricante, contrato	Checklist, informes de mantenimiento, registros de acceso, reportes de alarmas
11	Gestión de incidentes	5.24	Operar un flujo único de reporte, clasificación, contención, recuperación, documentación, escalamiento a COLCERT/CSIRT cuando aplique y lecciones aprendidas.	Mesa de Servicios, Seguridad informática, líder técnico del servicio	Jefe TIC, Jurídica, según evento	Continuo; revisión mensual de indicadores; simulacro anual	Tickets GLPI, ficha de incidente, reporte externo, lecciones aprendidas

#	Línea / política	Numerales política	Actividad operacional	Responsable líder	Apoyo	Periodicidad / meta	Evidencia mínima
12	Gestión de cambios	5.10.4, 5.18.2	Aplicar la metodología de Gestión de Cambios a cambios no rutinarios, con análisis de riesgos, aprobación, pruebas, plan de implementación, rollback y revisión posterior.	Líder técnico del área donde se origina el cambio	Mesa de Servicios	Por cambio; consolidado trimestral	Formato de cambio, ticket GLPI, pruebas, aprobación, cierre
13	Desarrollo seguro	5.17	Formalizar y aplicar el procedimiento de Desarrollo Seguro; documentar requisitos de seguridad, segregación de ambientes, pruebas, versiones, dependencias y vulnerabilidades.	Líder de Desarrollo y equipo de Desarrollo	Seguridad informática, proveedores	Por proyecto; revisión semestral del procedimiento	Requerimientos, casos de prueba, repositorio, reportes de vulnerabilidades, evidencias de despliegue

#	Línea / política	Numerales política	Actividad operacional	Responsable líder	Apoyo	Periodicidad / meta	Evidencia mínima
14	Proyectos y arquitectura segura	5.17.1, 5.17.2	Incorporar revisión de seguridad y arquitectura en el inicio de proyectos TIC, definiendo requisitos no funcionales, riesgos, controles, interoperabilidad y responsables.	Líder técnico del Proyecto, responsable del proyecto	Gobierno TI, Arquitectura Empresarial, Desarrollo, Datacenter	Por proyecto; seguimiento trimestral de hoja de ruta	Formato de inicio.
15	Proveedores y contratación	5.7, 5.18	Mantener cláusulas de confidencialidad y seguridad; verificar obligaciones durante la ejecución y retiro del proveedor.	Supervisor del contrato, Contratación	Oficina TIC según componente tecnológico	Por contrato; revisión periódica según supervisión	Contrato, cláusulas, informe, de supervisión, evidencias de retiro de accesos

#	Línea / política	Numerales política	Actividad operacional	Responsable líder	Apoyo	Periodicidad / meta	Evidencia mínima
16	Correo, internet y servicios digitales	5.19, 5.20	Mantener controles de filtrado, navegación, correo institucional, monitoreo autorizado y uso institucional; revisar excepciones y capacidad de continuidad.	Datacenter, administradores de servicios	Jefe TIC, Seguridad informática	Monitoreo continuo; revisión trimestral	Reportes de seguridad, reglas, alertas, tickets de excepción
17	Privacidad y protección de datos	5.5.3 a 5.5.6, 5.25	Aplicar controles técnicos de privacidad, acceso restringido, confidencialidad y seguridad de datos personales; apoyar la gobernanza institucional sin concentrar en TIC responsabilidades jurídicas o misionales de tratamiento.	Responsables de tratamiento, dependencias competentes	TIC componente técnico, Jurídica, Atención al Ciudadano, Gestión Documental	Según tratamiento; revisión anual de controles	Inventario de tratamientos cuando exista, controles de acceso, cláusulas, evidencias de privacidad

#	Línea / política	Numerales política	Actividad operacional	Responsable líder	Apoyo	Periodicidad / meta	Evidencia mínima
18	Sensibilización y cultura	5.5, 5.8, 6, 8	Ejecutar plan anual de concienciación con contenidos breves, prácticos y segmentados; medir cobertura y apropiación; reforzar temas derivados de incidentes.	Gobierno TI coordina; áreas TIC aportan contenidos	Función Pública, Prensa, Jefe TIC	Plan anual; mínimo actividades semestrales	Cronograma, asistencia, piezas, evaluación, indicadores
19	Cumplimiento y auditoría	5.25, 7, 9, 10	Consolidar evidencias, atender auditorías, revisar cumplimiento de políticas y gestionar hallazgos mediante acciones correctivas con responsable y fecha.	Jefe TIC, responsables de cada control	Control Interno, Planeación	Revisión anual y según auditorías	Informes, planes de mejora, cierres, evidencias de eficacia

#	Línea / política	Numerales política	Actividad operacional	Responsable líder	Apoyo	Periodicidad / meta	Evidencia mínima
20	Gestión documental y evidencia	5.15.2, 5.25	Definir repositorio y convención para conservar evidencias de controles sin duplicidad, con fechas, responsable, periodo y relación con riesgo/política.	Gobierno TI para esquema; cada responsable conserva evidencia de su control	Calidad, Gestión Documental, líderes técnicos	Implementación 2026; revisión trimestral	Índice de evidencias, carpetas/expedientes, trazabilidad en Kawak/GLPI

9. Hoja de ruta de implementación

Fase	Horizonte	Prioridades	Criterio de implementación
Fase 1 - Consolidar y ordenar	0 - 90 días	Cerrar control documental: autodiagnóstico MSPI, responsables reales de controles, procedimientos pendientes de publicación, matriz de activos y definición de indicadores.	Uso de herramientas existentes (Kawak, GLPI, correo, repositorios institucionales).

Fase	Horizonte	Prioridades	Criterio de implementación
Fase 2 - Ejecutar controles repetibles	3 - 6 meses	Verificación de accesos críticos, revisión de reglas de red, pruebas de restauración, seguimiento de cambios, incidentes, proveedores, mantenimiento de datacenter y sensibilización trimestral.	Priorizar disciplina operativa y evidencias antes que nuevas adquisiciones.
Fase 3 - Probar eficacia y continuidad	6 -12 meses	Simulacro de incidente, prueba de DRP, restauración, revisión de RTO, RPO, auditoría interna, evaluación de apropiación, revisión de desarrollo seguro y cierre de hallazgos.	Medir resultados y ajustar controles que no sean eficaces.
Fase 4 - Madurez 2027-2028	Anual	Automatizar mediciones cuando exista capacidad, fortalecer DLP, SIEM, PAM u otras herramientas si el análisis de riesgo y presupuesto lo justifican; mantener mejora continua del MSPI.	Inversión condicionada a riesgo, viabilidad y disponibilidad presupuestal.

10. Indicadores de seguimiento

Indicador	Fórmula / criterio	Frecuencia	Meta de referencia
Cumplimiento del plan operacional	Actividades ejecutadas / actividades programadas x 100	Cuatrimestral	>= 85%

Indicador	Fórmula / criterio	Frecuencia	Meta de referencia
Cobertura de activos actualizados	Activos revisados / activos inventariados x 100	Semestral	>= 90%
Verificación de accesos críticos	Sistemas críticos recertificados / sistemas críticos definidos x 100	Cuatrimestral	100%
Éxito de respaldos	Backups exitosos / backups programados x 100	Mensual	>= 98%
Pruebas de restauración exitosas	Pruebas exitosas / pruebas programadas x 100	Cuatrimestral	100% de las programadas
Cambios con trazabilidad completa	Cambios con registro, aprobación, prueba y cierre / cambios sujetos al procedimiento x 100	Cuatrimestral	>= 90% y mejora continua
Incidentes documentados oportunamente	Incidentes registrados y clasificados / incidentes detectados x 100	Mensual	100%
Cobertura de sensibilización	Participantes alcanzados / población objetivo x 100	Semestral	>= 80% anual
Cierre de hallazgos	Hallazgos cerrados en plazo / hallazgos con plazo vencido o cumplido x 100	Cuatrimestral	>= 85%
Cumplimiento de mantenimiento crítico	Mantenimientos ejecutados / mantenimientos programados x 100	Cuatrimestral	>= 90%
Revisión de proveedores críticos	Proveedores críticos revisados / proveedores críticos identificados x 100	Semestral	100%

11. Gestión de evidencia y trazabilidad

El principal cambio metodológico del plan es que cada control debe dejar evidencia proporcional a la actividad. La existencia de una política o procedimiento demuestra diseño, pero la eficacia debe demostrarse mediante registros de aplicación cuando corresponda. Para reducir carga administrativa, se priorizarán evidencias generadas naturalmente por la operación.

- Tickets GLPI, solicitudes de servicio, incidentes y cambios.
- Formatos institucionales de gestión de cambios, inicio de proyectos, listas de chequeo y actas.
- Reportes de herramientas de seguridad, respaldos, parches, monitoreo, firewall y antivirus.
- Registros de acceso, matrices de permisos y evidencia de recertificación.
- Informes de mantenimiento, inspección, pruebas de restauración y de continuidad.
- Correos institucionales de solicitud, aprobación o validación cuando sean la evidencia formal disponible.
- Registros de capacitación, material divulgado, evaluaciones y resultados de encuestas.
- Contratos, cláusulas, informes de supervisión y evidencia de retiro de accesos de terceros.
- Informes de auditoría, seguimiento de riesgos, acciones correctivas y cierres.

La evidencia debe indicar como mínimo: control o actividad a la que corresponde, periodo, responsable, fecha, resultado y ubicación del soporte. Se evitará duplicar archivos innecesariamente cuando el documento ya repose en Kawak, GLPI o un repositorio institucional con trazabilidad.

12. Gestión del cambio y apropiación

La implementación del MSPI y de la Política de Seguridad de la Información implica cambios de comportamiento y coordinación entre áreas. Considerando la resistencia al cambio identificada en la organización, el plan adopta un enfoque gradual, práctico y de baja fricción, evitando que la seguridad se perciba como una carga documental adicional.

Estrategia	Aplicación práctica
Aprovechar espacios existentes	Utilizar reuniones mensuales, comités y mesas técnicas ya programadas para socializar controles; evitar crear reuniones adicionales salvo necesidad.
Microcontenidos	Utilizar piezas breves, ejemplos reales, preguntas rápidas, juegos de máximo 5 -10 minutos para reforzar prácticas de seguridad.
Solicitudes simples de evidencia	Pedir al responsable el soporte que ya genera la operación, evitando formatos nuevos cuando un ticket, reporte o acta sea suficiente.
Responsabilidad realista	Asignar controles a quien cuenta con acceso y capacidad para ejecutarlos. Gobierno TI acompaña y consolida, pero no reemplaza al líder técnico.
Implementación por prioridad	Empezar por brechas críticas y acciones sin costo o de bajo costo; justificar inversiones con riesgo, impacto y beneficio.
Retroalimentación	Antes de formalizar nuevos controles, validar con los responsables técnicos si son aplicables y qué evidencia pueden producir.
Reconocimiento de avances	Mostrar resultados y mejoras alcanzadas para aumentar apropiación.
Aprendizaje de incidentes	Usar incidentes y hallazgos como casos de aprendizaje sin personalizar culpas; priorizar acciones correctivas y preventivas.

13. Iniciativas prioritarias actualizadas

Consolidación del MSPI y plan de mejora basado en brechas.

- Actualización y clasificación de activos de información por dependencia.
- Fortalecimiento de identidad, accesos privilegiados y transición de usuarios.
- Operación y evidencia de la Metodología de Gestión de Cambios.
- Aplicación del Procedimiento de Desarrollo Seguro y pruebas de seguridad.
- Fortalecimiento de conectividad inalámbrica, segmentación y acceso de terceros.
- DRP, RTO, RPO, pruebas de restauración y alta disponibilidad de servicios críticos.
- Mantenimiento y seguimiento de infraestructura física del Datacenter.
- Gestión integral de incidentes, escalamiento y lecciones aprendidas.

- Programa anual de concienciación y formación en seguridad y privacidad.
- Revisión periódica de proveedores críticos y obligaciones contractuales de seguridad.
- Consolidación de indicadores y repositorio de evidencias de controles.

14. Seguimiento, revisión y mejora continua

El seguimiento será coordinado por la Oficina TIC conforme a las competencias definidas, sin perjuicio de las responsabilidades de cada dependencia y responsable de control. Se propone una evaluación anual integral asociada al autodiagnóstico MSPI y a la revisión de la Política de Seguridad de la Información.

- Cada responsable actualizará el estado de las actividades que le correspondan y suministrará la evidencia mínima definida.
- Gobierno TI consolidará avances, brechas, indicadores y acciones pendientes para conocimiento del Jefe de la Oficina TIC.
- Los hallazgos de auditorías, incidentes, cambios tecnológicos significativos o modificaciones normativas podrán originar ajustes extraordinarios al plan.
- Las actividades no ejecutadas deberán registrar causa, riesgo asociado, acción compensatoria cuando aplique y nueva fecha objetivo.
- La eficacia de los controles se evaluará no solo por existencia documental, sino por su aplicación y resultados verificables.
- Los cambios de responsable deben quedar formalmente comunicados para evitar vacíos o asignaciones a personas sin capacidad operativa.

14.1 Reporte de avance

Formato propuesto registro de avance:

Actividad	Responsable	Periodo	Estado	Evidencia	Observación / acción
Actividad 1	Responsable	Cuatrimestral	No iniciada, en curso, cumplida, reprogramada	Enlace o soporte	Observación
Actividad 2	Responsable	Cuatrimestral	No iniciada, en curso, cumplida, reprogramada	Enlace o soporte	Observación

15. Referencias documentales

- Política de Seguridad de la Información 2024-2027, versión 3, actualizada mayo de 2026.
- Plan Operacional de Seguridad de la Información 2024-2028.
- Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), 2026.
- Matriz vigente de riesgos y controles de la Oficina TIC.
- Metodología de Gestión del Cambio TIC y Formato de Control de Cambios.
- Procedimiento de Desarrollo Seguro de Software.
- Procedimiento de Conectividad Inalámbrica y Formato de Solicitud de Conexión Wi-Fi.
- Informe Datacenter 2026.
- Catálogo de servicios TIC.
- PETI 2024-2028, MGGTI, MAE y MGPTI.

16. Control de cambios

Fecha	Versión	Descripción del cambio
Diciembre 2024	1	Elaboración del plan
Diciembre 2025	2	Actualización plantilla institucional
Septiembre 2026	3	Actualización plan operacional