INFORME DE IMPLEMENTACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA PARA LA CONSECUCIÓN DE SISTEMAS INSTITUCIONALES.

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

PERIODO 2025

Índice de contenidos

INFORME DE IMPLEMENTACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA PARA LA CONSECUCIÓN DE SISTEMAS INSTITUCIONALES.

1. ANTECEDENTES

En el contexto ecuatoriano actual, caracterizado por la creciente necesidad de modernizar los servicios públicos y privados para garantizar su eficiencia, transparencia y seguridad, las instituciones se enfrentan a retos significativos en materia de infraestructura tecnológica. Factores como la acelerada transformación digital, las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP) y los lineamientos establecidos por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) obligan a las organizaciones a fortalecer sus plataformas tecnológicas para garantizar la continuidad operativa y la integridad de su información.

La Prefectura de Cotopaxi, consciente de estas exigencias, ha identificado diversas debilidades que limitaban el desarrollo de sus actividades: equipos de cómputo obsoletos, servidores con baja capacidad de procesamiento, conexiones de red inestables, falta de sistemas de respaldo actualizados y ausencia de mecanismos robustos de ciberseguridad. Estos hallazgos fueron confirmados mediante diagnósticos internos, auditorías de gestión tecnológica y reportes de incidentes documentados por las áreas usuarias. Asimismo, el crecimiento institucional, las nuevas dinámicas de trabajo remoto impulsadas a raíz de la pandemia de COVID-19 y la necesidad de integrar plataformas interoperables (en cumplimiento de las estrategias nacionales de Gobierno Electrónico impulsadas por la Secretaría de Transformación Digital) evidenciaron la urgencia de emprender una reestructuración integral de la infraestructura tecnológica.

En respuesta a este escenario, se ha diseñado un plan estratégico de implementación que contempla la adquisición de equipamiento de última generación, el fortalecimiento de la red interna, la migración progresiva hacia servicios de nube bajo estándares internacionales, y la incorporación de prácticas de gestión tecnológica orientadas a la eficiencia, sostenibilidad y cumplimiento normativo en el Ecuador. Esta modernización es fundamental no solo para sostener el crecimiento institucional, sino también para garantizar servicios de calidad a la ciudadanía y a los usuarios internos, en un entorno seguro, ágil y tecnológicamente actualizado.

La ejecución de este proyecto no solo representa un avance técnico, sino también un compromiso con la excelencia institucional y el alineamiento a las mejores prácticas nacionales e internacionales en materia de infraestructura tecnológica y gestión de la información.

2. GENERALIDADES

La infraestructura tecnológica constituye el conjunto de componentes físicos y virtuales que soportan el funcionamiento de los sistemas de información institucionales, permitiendo la gestión eficiente, segura y continua de los procesos administrativos, operativos y de servicio a la ciudadanía. Su adecuada implementación es esencial para garantizar la disponibilidad, integridad y resiliencia de los servicios digitales que forman parte de la actividad pública.

En Ecuador, el fortalecimiento de la infraestructura tecnológica en las instituciones públicas responde a las disposiciones establecidas en marcos regulatorios como la Ley Orgánica de Protección de Datos Personales (LOPDP), el Esquema Gubernamental de Seguridad de la Información (EGSI) emitido por la Secretaría de Transformación Digital, y las directrices técnicas de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). Adicionalmente, se promueve la adopción de estándares internacionales como la ISO/IEC 27001:2022 y la ISO/IEC 20000-1:2018, homologados por el Instituto Ecuatoriano de Normalización (INEN), los cuales establecen prácticas recomendadas para la gestión de servicios de TI y la protección de la información.

La modernización de la infraestructura tecnológica institucional fortalece el cumplimiento de los principios de transparencia, eficiencia, seguridad y protección de datos personales, en consonancia con los objetivos estratégicos de la administración pública ecuatoriana. Para la Prefectura de Cotopaxi, esta implementación representa un paso clave en su compromiso por ofrecer servicios de calidad a la ciudadanía, asegurar la continuidad operativa, y posicionarse como un referente de innovación y transformación digital a nivel provincial.

2.1. Descripción de las políticas de implementación de la infraestructura tecnológica para la consecución de sistemas institucionales

La implementación de la infraestructura tecnológica en la Prefectura de Cotopaxi se rige por un conjunto de políticas orientadas a garantizar la adecuada planificación, desarrollo, operación y sostenibilidad de los sistemas institucionales. Estas políticas aseguran que los

proyectos tecnológicos se ejecuten de manera eficiente, segura y alineada a los objetivos estratégicos institucionales. A continuación, se detallan los principales ejes de acción:

- **Administración de proyectos informáticos**

Consiste en la planificación, organización, dirección y control de los proyectos tecnológicos que involucran la adquisición, instalación, configuración y puesta en marcha de infraestructura y sistemas institucionales. Se aplica el uso de metodologías de gestión de proyectos (como PMI o metodologías ágiles) para garantizar el cumplimiento de plazos, costos, alcance y calidad.

- **Administración de la configuración de software base**

Comprende la gestión estructurada de la instalación, parametrización, actualización y mantenimiento del software fundamental sobre el cual operan los sistemas institucionales. Incluye sistemas operativos, bases de datos, servidores de aplicaciones y herramientas de virtualización, asegurando su correcta integración y compatibilidad.

- **Administración de comunicaciones**

Se refiere al manejo integral de las redes de comunicación de datos, voz y video que soportan la operación de los sistemas tecnológicos. Abarca el diseño, implementación, monitoreo y optimización de redes LAN, WAN e inalámbricas, garantizando su disponibilidad, seguridad y rendimiento de acuerdo a los requerimientos institucionales.

- **Administración de seguridad**

Establece los procedimientos y controles necesarios para proteger la infraestructura tecnológica y los sistemas de información institucionales frente a amenazas internas y externas. Comprende la implementación de políticas de acceso seguro, sistemas de firewall, gestión de vulnerabilidades, copias de respaldo, planes de recuperación ante desastres y cumplimiento de normativas como la LOPDP.

- **Capacitación y soporte a los usuarios en los nuevos sistemas o mejoras que se hayan desarrollado**

Incluye la planificación y ejecución de programas de formación dirigidos al personal institucional, con el fin de garantizar un uso eficiente y seguro de las nuevas herramientas tecnológicas implementadas. Asimismo, contempla la provisión de soporte técnico

oportuno ante incidentes, problemas o consultas derivados de la operación de los sistemas.

- **Informe técnico en el ámbito de su competencia**

  Implica la elaboración y presentación periódica de informes técnicos que documenten el estado, avances, incidentes, mejoras y recomendaciones relacionados con la infraestructura tecnológica. Estos informes son fundamentales para la toma de decisiones estratégicas, auditorías internas y cumplimiento de requisitos de control institucional.

2.2. Objetivo

Establecer un marco técnico y operativo que garantice la adecuada implementación, gestión y sostenibilidad de la infraestructura tecnológica en la Prefectura de Cotopaxi, facilitando la operatividad de los sistemas institucionales de forma eficiente, segura y conforme a las normativas vigentes. Este lineamiento busca asegurar el cumplimiento de estándares internacionales y regulaciones nacionales, tales como la Ley Orgánica de Protección de Datos Personales (LOPDP), el Esquema Gubernamental de Seguridad de la Información (EGSI) y los estándares ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018, promoviendo buenas prácticas en administración de proyectos tecnológicos, comunicaciones, seguridad informática, soporte al usuario y control de calidad. Asimismo, establece directrices claras para la gestión de activos tecnológicos, la protección de la infraestructura crítica, la continuidad operativa frente a contingencias, y la capacitación permanente del personal técnico y administrativo.

2.3. Ámbito De Aplicación

El presente instrumento regirá para todos los servidores, servidoras, funcionarios y funcionarias de la Prefectura de Cotopaxi, así como para proveedores externos que mantengan relaciones contractuales, convenios o acuerdos con la institución en el ámbito de implementación, gestión o soporte de infraestructura tecnológica.

Su aplicación abarca todas las actividades relacionadas con la planificación, adquisición, instalación, configuración, operación, mantenimiento y mejora de la infraestructura tecnológica que soporta los sistemas institucionales. De igual manera, su cumplimiento se enmarca en las disposiciones del Esquema Gubernamental de Seguridad de la Información

(EGSI), la Ley Orgánica de Protección de Datos Personales (LOPDP), y demás normativas vigentes aplicables en el Ecuador.

Todos los usuarios internos y externos con acceso a los recursos tecnológicos institucionales deberán actuar en estricto apego a las políticas, procedimientos y controles establecidos, conforme a los roles, perfiles y responsabilidades asignadas. De esta manera, se asegura una gestión segura, eficiente y alineada a los principios de transparencia, responsabilidad y protección de activos tecnológicos e informáticos de la Prefectura de Cotopaxi.

2.4. Conceptos y Definiciones

- **Actualización de sistemas:**

  Acción de instalar mejoras, parches de seguridad o nuevas versiones en los sistemas tecnológicos para mantener su rendimiento y seguridad.
- **Administración de proyectos:**

  Gestión organizada de actividades, recursos, costos y plazos para alcanzar objetivos específicos en el desarrollo tecnológico.
- **Capacitación:**

  Proceso sistemático de formación dirigido a los usuarios institucionales para garantizar el uso eficiente y seguro de los sistemas tecnológicos.
- **Comunicaciones de red:**

  Infraestructura física y lógica que permite la transmisión de datos entre dispositivos, usuarios y sistemas a través de redes internas y externas.
- **Configuración:**

  Proceso técnico de instalación, ajuste, personalización y parametrización de software o hardware de acuerdo a las necesidades funcionales.
- **Gobierno electrónico:**

  Uso de tecnologías digitales por parte de las entidades públicas para ofrecer servicios más eficientes, transparentes y accesibles a la ciudadanía.
- **Gestión de riesgos tecnológicos:**

  Identificación, análisis y mitigación de amenazas potenciales que podrían afectar la operatividad y seguridad de los sistemas tecnológicos.
- **Infraestructura tecnológica:**

Conjunto de componentes físicos, lógicos y de red que soportan el funcionamiento de los sistemas de información institucionales.

- **Informe técnico:**

  Documento formal que registra de manera estructurada las actividades, resultados, incidentes y propuestas de mejora en el ámbito tecnológico.

- **Protección de datos personales:**

  Aplicación de medidas legales, administrativas y tecnológicas destinadas a resguardar la confidencialidad, integridad y disponibilidad de información sensible.

- **Registro diario:**

  Documento operativo que recopila de forma sistemática las actividades ejecutadas por el personal técnico cada jornada laboral.

- **Seguridad informática:**

  Conjunto de políticas, controles y tecnologías que protegen los activos de información frente a accesos no autorizados y amenazas cibernéticas.

- **Sistema institucional:**

  Plataforma tecnológica diseñada para automatizar y gestionar procesos administrativos, operativos o de servicio público dentro de la organización.

- **Software base:**

  Conjunto de sistemas esenciales como sistemas operativos, bases de datos y plataformas de virtualización que sostienen las aplicaciones.

- **Soporte técnico:**

  Servicio de asistencia prestado a los usuarios para resolver incidencias, consultas o fallos en los sistemas tecnológicos de la institución.

3. ADMINISTRACIÓN DE PROYECTOS INFORMÁTICOS.

La administración de proyectos informáticos en la Prefectura de Cotopaxi es clave para garantizar el desarrollo estructurado y exitoso de iniciativas tecnológicas vinculadas a la implementación y fortalecimiento de la infraestructura institucional. Esta administración permite una ejecución técnica, financiera y operativa eficiente, asegurando que cada iniciativa contribuya al cumplimiento de los objetivos estratégicos institucionales.

3.1. OBJETIVO DE LA ADMINISTRACIÓN DE PROYECTOS INFORMÁTICOS

Descripción:

Establecer una guía clara para planificar, ejecutar, supervisar y cerrar proyectos tecnológicos de forma eficiente, cumpliendo con los plazos, presupuestos y estándares de calidad establecidos.

3.2. LINEAMIENTOS GENERALES

Descripción:

Son las directrices que rigen la forma en que se deben gestionar los proyectos tecnológicos en la institución. Incluyen el uso de metodologías, la planificación detallada, la gestión de riesgos, la coordinación interinstitucional y la evaluación de resultados.

- **Metodologías de gestión de proyectos:**
  Aplicación de estándares internacionales como PMBOK o enfoques ágiles para adaptar los proyectos a la realidad institucional.
- **Definición de objetivos y entregables:**
  Establecimiento claro de lo que se espera lograr y cómo se medirá su cumplimiento.
- **Gestión de riesgos:**
  Identificación y mitigación anticipada de situaciones que puedan afectar el éxito del proyecto.
- **Participación interdepartamental:**
  Coordinación entre todas las áreas involucradas para garantizar un desarrollo armónico del proyecto.
- **Control de calidad:**
  Evaluación constante para asegurar el cumplimiento de los requisitos técnicos y funcionales definidos.

3.3. PLAN ESTRATÉGICO DE ADMINISTRACIÓN DE PROYECTOS INFORMÁTICOS

Descripción:

Esquema general que organiza las fases y actividades del proyecto, desde su inicio hasta su cierre, asegurando orden, trazabilidad y cumplimiento.

Tabla 1

Descripción de fases y actividades

Etapa	Actividad	Descripción
Inicio	Identificación del proyecto	Detectar una necesidad institucional y formular un proyecto que aporte valor.
Planificación	Elaboración del plan del proyecto	Definir cronograma, presupuesto, responsables, matriz de riesgos y plan de comunicación.
Ejecución	Implementación de actividades	Desarrollar las tareas según el plan, gestionar recursos y asegurar cumplimiento técnico.
Monitoreo y Control	Seguimiento y control de calidad	Evaluar el avance, aplicar correctivos y monitorear costos, tiempos y riesgos.
Cierre	Evaluación y documentación	Verificar entregables, recopilar documentación, elaborar informe final y cerrar el proyecto formalmente.

3.4. ROLES Y RESPONSABILIDADES

Descripción:

Define los actores clave que participan en el proyecto, sus funciones específicas y su nivel de responsabilidad durante el ciclo de vida del proyecto.

- **Director de Proyecto:**

  Responsable general de la planificación, ejecución y seguimiento.

- **Equipo Técnico:**

  Encargado de la implementación tecnológica y configuraciones especializadas.

- **Usuarios Clave:**

  Representantes de las áreas beneficiarias que validan requerimientos y entregables.

- **Unidad de Tecnologías de la Información:**

Asegura el cumplimiento normativo, técnico y de ciberseguridad.

3.5. GESTIÓN DE RIESGOS

Descripción:

Proceso sistemático para anticipar, analizar y reducir posibles eventos negativos que puedan afectar el éxito del proyecto.

- **Identificación:**

  Registro temprano de posibles problemas (tecnológicos, presupuestarios, legales).

- **Mitigación:**

  Diseño de planes de contingencia, adquisición de soporte técnico o alternativas tecnológicas.

- **Monitoreo:**

  Revisión continua de los riesgos para actualizar la matriz de riesgos según evolución del proyecto.

3.6. DOCUMENTACIÓN OBLIGATORIA EN CADA PROYECTO

Descripción:

Conjunto de documentos esenciales que respaldan la gestión, control y evaluación del proyecto.

- **Acta de inicio:**

  Formaliza el inicio del proyecto, autorizando recursos y responsables.

- **Plan de gestión:**

  Documento guía con cronograma, presupuesto, matriz de riesgos y alcance.

- **Informes de avance:**

  Reportes periódicos del estado del proyecto.

- **Informe de cierre:**

  Documento que resume resultados, aprendizajes y cumplimiento de metas.

- **Matriz de riesgos actualizada:**

Herramienta de control para identificar y gestionar riesgos.

- **Registro de cambios:**

Documento que detalla cualquier modificación al alcance, tiempo o presupuesto.

3.7. INDICADORES DE ÉXITO

Descripción:

Métricas utilizadas para medir el nivel de cumplimiento del proyecto con base en su eficiencia, calidad y satisfacción de los usuarios.

- **Cumplimiento de cronograma:**

Porcentaje de actividades realizadas dentro del plazo planificado.

- **Desviación presupuestaria:**

Diferencia entre lo ejecutado y lo aprobado.

- **Satisfacción del usuario final:**

Nivel de conformidad de los beneficiarios con el sistema entregado.

- **Reducción de incidentes:**

Comparativa del número de fallos o interrupciones antes y después del proyecto.

4. ADMINISTRACIÓN DE LA CONFIGURACIÓN DE SOFTWARE BASE.

La administración de la configuración de software base en la Prefectura de Cotopaxi constituye un pilar fundamental para garantizar la estabilidad, seguridad, compatibilidad y rendimiento de los sistemas tecnológicos que soportan los servicios institucionales. El software base comprende los sistemas operativos, gestores de bases de datos, servidores de aplicaciones, plataformas de virtualización y herramientas fundamentales que permiten el funcionamiento adecuado de toda la infraestructura tecnológica.

4.1. OBJETIVO DE LA ADMINISTRACIÓN DE LA CONFIGURACIÓN DE SOFTWARE BASE

Descripción:

Asegurar la correcta instalación, parametrización, actualización, mantenimiento y monitoreo

del software base, garantizando su óptima operación, compatibilidad entre sistemas y cumplimiento de los estándares de seguridad y normativas vigentes.

4.2. LINEAMIENTOS GENERALES

Descripción:

Normas que orientan la gestión ordenada y segura del software base institucional, asegurando la trazabilidad de cambios y reduciendo riesgos de vulnerabilidades.

Inventario actualizado: Mantener un registro detallado de todo el software base instalado en la infraestructura institucional.

Configuración estandarizada: Establecer parámetros de instalación uniformes según buenas prácticas (por ejemplo, estándares de CIS Benchmarks).

Actualizaciones controladas: Planificar e implementar actualizaciones periódicas de software, minimizando riesgos de incompatibilidad o interrupción de servicios.

Gestión de parches de seguridad: Aplicar parches críticos de seguridad de manera oportuna conforme a boletines de fabricantes o normativas de ciberseguridad nacionales.

Control de cambios: Registrar y aprobar cualquier modificación de configuración, instalación o actualización en ambientes productivos.

Pruebas de compatibilidad: Verificar previamente en entornos de prueba cualquier nueva configuración o actualización antes de aplicarla en producción.

4.3. PLAN ESTRATÉGICO DE ADMINISTRACIÓN DE CONFIGURACIÓN DE SOFTWARE BASE

Tabla 2

Plan de administración de configuración de software base

Etapa	Actividad	Descripción
Identificación	Registro de plataformas base	Elaborar inventario de sistemas operativos, servidores de aplicaciones, bases de datos, virtualizadores y otros softwares críticos.

Estandarización	Definición de configuraciones base	Establecer configuraciones mínimas de seguridad, rendimiento y compatibilidad para cada tipo de software.
Implementación	Instalación y configuración	Realizar la instalación de software base conforme a los estándares definidos, asegurando integridad y seguridad.
Actualización	Aplicación de parches y mejoras	Gestionar actualizaciones periódicas de versiones y parches críticos siguiendo un calendario aprobado.
Monitoreo y Control	Verificación de estado y funcionamiento	Supervisar el estado de los sistemas base, analizar vulnerabilidades y corregir desviaciones detectadas.
Auditoría	Revisión y validación de configuraciones	Realizar auditorías internas periódicas para asegurar que las configuraciones se mantienen dentro de los parámetros autorizados.

4.4. ROLES Y RESPONSABILIDADES

Descripción:

Define las funciones y compromisos de los equipos y usuarios involucrados en la gestión del software base:

- **Administrador de Infraestructura Tecnológica:** Responsable de instalar, configurar y documentar las plataformas base, garantizando su correcta operación.
- **Unidad de Tecnologías de la Información:** Encargada de definir las políticas de actualización, control de cambios y gestión de vulnerabilidades.
- **Proveedor de soporte externo (cuando aplique):** Apoya en actualizaciones mayores o configuraciones especializadas, bajo supervisión institucional.

- **Usuarios de sistemas:** Reportan incidencias que puedan estar relacionadas a fallas de software base.

4.5. PROCESOS DE GESTIÓN DE CONFIGURACIÓN

Tabla 3

Procesos de gestión de configuración

Proceso	Descripción	Herramienta de Apoyo
Gestión de inventarios	Registro detallado de software instalado, versiones y parámetros de configuración.	Base de datos de inventario institucional.
Control de cambios	Procedimiento de solicitud, evaluación, aprobación y documentación de cambios de configuración.	Sistema de Gestión de Cambios (SGC)
Monitoreo de actualizaciones	Seguimiento de boletines de seguridad, nuevas versiones y mejoras recomendadas.	Herramientas de monitoreo de actualizaciones (por ejemplo, WSUS, Linux Patch Management).
Gestión de incidentes	Atención de fallas o vulnerabilidades relacionadas a la configuración del software base.	Mesa de ayuda institucional.

4.6. DOCUMENTACIÓN OBLIGATORIA

Descripción:

Archivos y reportes necesarios para un control adecuado de la configuración tecnológica:

- Inventario de software base.
- Políticas de instalación y configuración estándar.
- Calendario de actualizaciones de parches y versiones.

- Historial de cambios aplicados en software base.
- Informes de auditorías de configuración.
- Registros de incidencias corregidas.

4.7. INDICADORES DE ÉXITO

Descripción:

Métricas que permiten medir el nivel de eficiencia y control en la administración de software base:

- 100% de los activos tecnológicos registrados en el inventario de software.
- Al menos 95% de los parches críticos aplicados dentro de los 30 días posteriores a su publicación.
- Reducción del 50% en incidentes de vulnerabilidad derivados de software desactualizado.
- Cumplimiento del 100% de las auditorías de configuración sin hallazgos críticos.

4.8. RESUMEN DE ADMINISTRACIÓN DE LA CONFIGURACIÓN DE SOFTWARE BASE

Tabla 4

Administración de la configuración de software base

Elemento	Detalle
Objetivo	Asegurar la correcta gestión del software base garantizando estabilidad, compatibilidad y seguridad.
Áreas Clave	Inventario, estandarización, actualizaciones, monitoreo, auditoría.
Responsables	Administradores de infraestructura, Unidad de TI, soporte externo.
Procesos Principales	Gestión de inventarios, control de cambios, actualización de parches, gestión de incidentes.

Documentos Requeridos	Inventario, historial de cambios, políticas de configuración, informes de auditoría.
Indicadores de Éxito	Inventario completo, parches aplicados a tiempo, reducción de vulnerabilidades, auditorías positivas.

5. ADMINISTRACIÓN DE COMUNICACIONES.

La administración de las comunicaciones en la Prefectura de Cotopaxi es una función crítica para garantizar la conectividad, estabilidad y disponibilidad de los servicios de información institucionales. La red de comunicaciones (física y lógica) soporta el funcionamiento de todos los sistemas tecnológicos y permite la interacción eficiente entre servidores, estaciones de trabajo, usuarios y sistemas externos.

Una infraestructura de comunicaciones sólida asegura la transmisión confiable de datos, la protección de la información y la disponibilidad de servicios estratégicos como internet, VPN, correo electrónico, voz sobre IP, videoconferencias, entre otros.

5.1. OBJETIVO DE LA ADMINISTRACIÓN DE COMUNICACIONES

Garantizar la operación eficiente, segura y continua de la red institucional de comunicaciones, incluyendo todos sus componentes físicos (cableado estructurado, routers, switches, puntos de acceso) y lógicos (protocolos, direcciones IP, accesos remotos), a fin de mantener interconectados los servicios, usuarios y sistemas de información de la Prefectura.

5.2. LINEAMIENTOS GENERALES

- **Diseño estructurado de la red:**

  Planificar la topología de red basada en criterios de escalabilidad, redundancia y segmentación por áreas críticas.
- **Segmentación de red:**

  Separar los segmentos de red según tipo de tráfico (administrativo, voz, videovigilancia, servidores) para mejorar el rendimiento y la seguridad.
- **Monitoreo constante:**

Utilizar herramientas de supervisión en tiempo real para detectar caídas, cuellos de botella, intentos de intrusión o sobrecargas.

- **Redundancia y tolerancia a fallos:**

  Implementar enlaces alternos o equipos de respaldo para asegurar continuidad del servicio en caso de fallos físicos o lógicos.

- **Documentación y trazabilidad:**

  Mantener planos actualizados de la red, configuraciones de equipos, reglas de firewall, tablas de enrutamiento y bitácoras de cambios.

5.3. PLAN ESTRATÉGICO DE ADMINISTRACIÓN DE COMUNICACIONES

Tabla 5

Administración de comunicaciones

Etapa	Actividad	Descripción
Diagnóstico	Auditoría de red institucional	Evaluar cobertura, capacidad, puntos críticos, obsolescencia y vulnerabilidades.
Diseño	Reestructuración y documentación	Redefinir topología si es necesario, segmentar redes, definir protocolos, VLANs, direccionamiento.
Implementación	Mejora o ampliación de red	Sustitución de equipos obsoletos, instalación de nuevos nodos, reconfiguración de dispositivos.
Monitoreo	Vigilancia continua	Supervisar tráfico, latencia, disponibilidad y alertas mediante sistemas NMS (como Zabbix o PRTG).
Mantenimiento	Soporte correctivo y preventivo	Atender incidencias de red, renovar cableado, actualizar firmware, limpiar racks y reorganizar equipos.

Evaluación	Indicadores y reportes	Medir desempeño, documentar cambios, proponer mejoras, validar cumplimiento de objetivos.

5.4. PLAN OPERATIVO DE ADMINISTRACIÓN DE COMUNICACIONES – ANUAL

Tabla 6

Administración de comunicaciones

Periodo	Actividad principal	Responsable	Objetivo
Enero - Febrero	Diagnóstico de red y validación de topología	Unidad de TI	Identificar fallos, puntos de mejora y actualizar el inventario
Marzo - Abril	Actualización de equipos (switches/AP/firewalls)	Infraestructura tecnológica	Reforzar los puntos críticos o vulnerables
Mayo - Junio	Segmentación y gestión de tráfico	Administrador de red	Mejorar el rendimiento mediante VLANs y reglas de QoS
Julio - Agosto	Pruebas de redundancia y simulacros de caída	Infraestructura + Soporte	Validar continuidad operativa
Septiembre - Octubre	Auditoría de accesos y políticas de red	Seguridad informática	Verificar configuraciones y reglas de firewall
Noviembre - Diciembre	Evaluación anual e informe técnico	Unidad de TI	Documentar estado actual, incidentes, propuestas de mejora

5.5. ROLES Y RESPONSABILIDADES

Tabla 7

Roles y responsabilidades

Rol	Función
Administrador de Red	Configurar, monitorear y mantener los dispositivos de red (routers, switches, firewalls).
Unidad de Tecnologías de la Información	Definir políticas de acceso, controlar cambios, auditar incidentes.
Equipo de soporte técnico	Atender fallos físicos, verificar conectividad, intervenir en puntos de red.
Usuarios institucionales	Reportar incidentes de conexión o accesibilidad.

5.6. PROCESOS DE GESTIÓN DE COMUNICACIONES

Tabla 8

Procesos de gestión de comunicaciones

Proceso	Descripción	Herramienta de Apoyo
Gestión de direcciones IP	Asignación ordenada y segura de IPs por departamentos o dispositivos.	DHCP + Planificador IP
Control de accesos a red	Autenticación de dispositivos y usuarios, con monitoreo de sesiones activas.	Portal cautivo o autenticación RADIUS
Registro de eventos y tráfico	Recolección de logs para análisis de comportamiento y detección de incidentes.	Syslog centralizado

Mantenimiento preventivo	Revisión física, limpieza de racks, ventilación, actualización de firmware.	Plan de mantenimiento interno

5.7. DOCUMENTACIÓN OBLIGATORIA

- Mapa lógico y físico actualizado de red.
- Listado de dispositivos y configuraciones (firewalls, switches, routers).
- Registro de cambios en la red.
- Manual de incidentes y planes de respuesta.
- Bitácora de mantenimiento preventivo y correctivo.
- Informes mensuales de estado de la red.

5.8. INDICADORES DE ÉXITO

Tabla 9

Indicadores de éxito

Indicador	Meta
Disponibilidad de red	≥ 99.5% mensual
Tiempo medio de respuesta ante incidentes de red	≤ 2 horas
% de puntos críticos con conectividad redundante	≥ 80%
Número de incidentes graves por fallos de red	0
Actualización de firmware y configuraciones documentadas	100% semestral

6. ADMINISTRACIÓN DE SEGURIDAD.

La administración de la seguridad tecnológica en la Prefectura de Cotopaxi tiene como propósito salvaguardar la integridad, confidencialidad y disponibilidad de la información institucional, así como proteger los activos tecnológicos contra amenazas internas y externas. Esta función es crítica para garantizar la continuidad de los servicios institucionales y asegurar

el cumplimiento de las normativas vigentes nacionales e internacionales en materia de seguridad de la información.

6.1. OBJETIVO DE LA ADMINISTRACIÓN DE SEGURIDAD

Descripción:

Establecer las políticas, procedimientos y controles necesarios para prevenir, detectar, responder y recuperar ante incidentes de seguridad que puedan comprometer la infraestructura tecnológica o la información de la Prefectura de Cotopaxi, cumpliendo con los principios de protección de datos, resiliencia operativa y gestión de riesgos.

6.2. LINEAMIENTOS GENERALES

Descripción:

Conjunto de directrices estratégicas que orientan todas las acciones de seguridad tecnológica en la institución.

- Seguridad desde el diseño: Incluir controles de seguridad en todas las fases de adquisición, implementación y operación de tecnologías.
- Gestión de accesos: Establecer políticas estrictas de creación, uso, control y eliminación de cuentas de usuario y contraseñas.
- Protección de datos personales: Aplicar medidas técnicas que aseguren el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP).
- Monitoreo de amenazas: Implementar sistemas de detección de intrusiones (IDS/IPS) y análisis de logs.
- Respuesta ante incidentes: Definir procedimientos claros para la atención, investigación, notificación y recuperación ante incidentes de seguridad.
- Capacitación constante: Fomentar la formación de todos los funcionarios en buenas prácticas de seguridad informática.

6.3. PLAN ESTRATÉGICO DE ADMINISTRACIÓN DE SEGURIDAD

Tabla 10

Plan estratégico de seguridad

Etapa	Actividad	Descripción

Evaluación	Análisis de riesgos tecnológicos	Identificación de activos críticos, amenazas, vulnerabilidades y medidas de mitigación.
Planificación	Definición de políticas y controles	Establecimiento de reglas de acceso, cifrado de información, protección de redes y equipos.
Implementación	Aplicación de medidas de seguridad	Configuración de firewalls, antivirus, políticas de contraseñas, cifrado de dispositivos, etc.
Monitoreo	Supervisión continua de eventos	Detección de incidentes mediante alertas, revisión de logs, y sistemas SIEM.
Respuesta y recuperación	Gestión de incidentes de seguridad	Activación de protocolos de respuesta, contención de daños y restauración de servicios.
Auditoría	Evaluación de cumplimiento	Revisiones periódicas de políticas, controles aplicados, incidentes reportados y mejoras necesarias.

6.4. PLAN OPERATIVO ANUAL DE ADMINISTRACIÓN DE SEGURIDAD

Tabla 11

Plan operativo de administración de seguridad

Periodo	Actividad principal	Responsable	Objetivo
Enero - Febrero	Actualización de matriz de riesgos	Responsable de Seguridad TI	Identificar nuevos riesgos y actualizar controles.
Marzo - Abril	Capacitación de usuarios en ciberseguridad	Unidad de TI	Sensibilizar sobre amenazas y buenas prácticas.

Mayo - Junio	Simulacro de respuesta ante incidentes	Equipo de Infraestructura	Evaluar tiempos de reacción y efectividad de protocolos.
Julio - Agosto	Auditoría interna de cumplimiento de políticas	Seguridad TI + Auditoría Interna	Revisar cumplimiento de controles de seguridad.
Septiembre - Octubre	Actualización de sistemas de seguridad (firewall, antivirus)	Infraestructura TI	Mantener protecciones actualizadas y efectivas.
Noviembre - Diciembre	Informe de seguridad anual	Responsable de Seguridad TI	Documentar incidentes, acciones correctivas y plan de mejoras.

6.5. ROLES Y RESPONSABILIDADES

Tabla 12

Roles y responsabilidades

Rol	**Función**
Responsable de Seguridad TI	Diseñar políticas de seguridad, gestionar incidentes, coordinar auditorías de seguridad.
Administrador de Red	Aplicar configuraciones seguras en dispositivos de red, controlar accesos y conexiones remotas.
Equipo de soporte técnico	Mantener dispositivos actualizados, aplicar parches de seguridad y respaldar información crítica.
Usuarios institucionales	Cumplir las políticas de uso seguro de los sistemas y reportar anomalías de seguridad.

6.6. PROCESOS DE GESTIÓN DE SEGURIDAD

Tabla 13

Procesos de gestión de seguridad

Proceso	Descripción	Herramienta de Apoyo
Gestión de accesos	Control de creación, modificación y eliminación de usuarios y permisos.	Active Directory, Políticas de grupo (GPO).
Protección de endpoint	Instalación y actualización de antivirus, control de dispositivos USB.	Soluciones antivirus corporativas.
Gestión de copias de seguridad	Respaldo regular de información crítica y validación de recuperación.	Sistemas de backup automáticos.
Detección y respuesta ante incidentes	Monitoreo, análisis y contención de eventos de seguridad.	SIEM, análisis de logs.
Auditoría y evaluación de controles	Revisión sistemática del cumplimiento de las políticas y normativas de seguridad.	Checklists de cumplimiento.

6.7. DOCUMENTACIÓN OBLIGATORIA

- Políticas de seguridad de la información.
- Matriz de riesgos tecnológicos.
- Plan de respuesta ante incidentes de seguridad.
- Registros de incidentes de seguridad y su tratamiento.
- Bitácoras de acceso a sistemas críticos.
- Informes de auditoría de seguridad.
- Reportes de capacitación en ciberseguridad.

6.8. INDICADORES DE ÉXITO

Tabla 14

Indicadores de éxito

Indicador	Meta
Número de incidentes críticos de seguridad	0
Cumplimiento de actualizaciones de seguridad	≥ 98% de parches aplicados en tiempo
Tiempo medio de respuesta ante incidentes	≤ 4 horas
Usuarios capacitados anualmente en seguridad	≥ 90% del personal
Auditorías de seguridad sin hallazgos críticos	100%

7. CAPACITACIÓN Y SOPORTE A LOS USUARIOS EN LOS NUEVOS SISTEMAS O MEJORAS QUE SE HAYAN DESARROLLADO.

La introducción de nuevas herramientas tecnológicas o la mejora de sistemas existentes en la Prefectura de Cotopaxi debe ir necesariamente acompañada de procesos estructurados de capacitación y soporte técnico. La correcta apropiación tecnológica por parte de los usuarios institucionales es fundamental para garantizar que las soluciones implementadas cumplan su propósito, mejoren la productividad y no generen resistencia al cambio.

Este eje estratégico busca preparar a los funcionarios y personal vinculado para utilizar de forma efectiva los sistemas institucionales, reducir el margen de error operativo y asegurar una transición fluida hacia entornos digitales cada vez más automatizados y seguros.

7.1. OBJETIVO

Brindar capacitación efectiva y soporte técnico continuo a los usuarios institucionales, asegurando la correcta adopción de los nuevos sistemas o mejoras tecnológicas implementadas, optimizando su uso y garantizando la continuidad operativa de los servicios.

7.2. LINEAMIENTOS GENERALES

La estrategia de capacitación y soporte técnico en la Prefectura de Cotopaxi se rige por los siguientes principios:

- **Formación oportuna y dirigida:**

  Toda implementación tecnológica debe ir acompañada de sesiones de capacitación previas y posteriores, diferenciadas por nivel de usuario (básico, intermedio, avanzado) y perfil funcional.

- **Capacitación práctica:**

  Se prioriza el enfoque aplicado, utilizando manuales, videos, ejercicios guiados y resolución de casos reales para fomentar la comprensión y el dominio del sistema.

- **Registro diario de capacitaciones:**

  Toda jornada de formación debe ser documentada, con control de asistencia, temas cubiertos, incidencias detectadas y retroalimentación de los participantes. Este registro se mantiene bajo la figura de "registro de capacitaciones realizado – diario ordinario", cumpliendo con estándares operativos internos.

- **Soporte post-capacitación:**

  Se brinda acompañamiento técnico continuo mediante una mesa de ayuda, atención presencial o remota, orientada a resolver dudas, corregir errores de operación o brindar refuerzo a quienes lo requieran.

- **Evaluación del aprendizaje:**

  Al final de cada proceso de capacitación, se realizan encuestas, pruebas de validación o entrevistas breves que permiten verificar el nivel de comprensión y detectar necesidades adicionales.

7.3. DESARROLLO DEL PLAN DE CAPACITACIÓN

Cada capacitación parte de un plan diseñado desde la Unidad de Tecnologías de la Información, el cual considera:

- **Diagnóstico inicial:**

Se identifican los usuarios que interactuarán con el nuevo sistema o mejora, sus funciones y nivel de dominio tecnológico.

- **Diseño del programa:**

  Se elabora un cronograma con sesiones presenciales o virtuales, se preparan los contenidos formativos (manuales, guías, videos, simuladores) y se asignan instructores responsables.

- **Ejecución:**

  Las capacitaciones se desarrollan en grupos pequeños para permitir una atención más personalizada, considerando las funciones del área.

- **Seguimiento:**

  Se registra diariamente la asistencia y participación, así como cualquier dificultad detectada. Estos registros permiten ajustar los contenidos en tiempo real.

- **Evaluación y retroalimentación:**

  Se aplican pruebas prácticas o encuestas de satisfacción para determinar la efectividad de la formación y realizar mejoras en el proceso.

7.4. SOPORTE TÉCNICO A USUARIOS

Una vez que el sistema ha sido implementado, se activa el soporte operativo, que incluye:

- **Atención de incidentes:**

  Se responde a reportes de fallas, errores de uso, bloqueos de cuenta, etc., a través de correo electrónico, plataforma de tickets, soporte telefónico o presencial.

- **Acompañamiento en tiempo real:**

  Durante los primeros días del uso de un nuevo sistema, se asigna personal técnico de acompañamiento para brindar apoyo directo a los usuarios clave.

- **Actualización de contenidos de ayuda:**

  Se mantienen disponibles recursos como tutoriales, preguntas frecuentes (FAQ) y guías rápidas dentro del portal institucional o en repositorios digitales.

7.5. REGISTRO OPERATIVO DIARIO

El registro de actividades de capacitación se lleva de manera diaria y ordinaria, mediante una plantilla interna que detalla:

- Fecha, tema impartido, nombre del sistema o mejora abordada.

- Participantes y sus respectivas áreas.
- Instructores a cargo.
- Observaciones sobre el desarrollo de la sesión.
- Evaluación general del grupo.

Este documento sirve como respaldo institucional y como insumo para auditorías o revisiones internas.

7.6. ROLES Y RESPONSABILIDADES

- **Unidad de TI:**

  Planifica, organiza y supervisa los procesos de capacitación y soporte.
- **Equipo de instructores:**

  Encargado de impartir las sesiones y generar materiales didácticos.
- **Usuarios institucionales:**

  Participan activamente en la formación, aplican lo aprendido y reportan dificultades.
- **Soporte técnico:**

  Responde consultas y da solución a problemas operativos o técnicos derivados del uso de los sistemas.

7.7. INDICADORES DE ÉXITO

La efectividad de la capacitación y el soporte se evalúa con indicadores como:

- Porcentaje de usuarios capacitados en relación al total requerido.
- Nivel de satisfacción expresado por los participantes.
- Reducción de errores operativos en los primeros 30 días tras el despliegue del sistema.
- Tiempo promedio de resolución de incidentes reportados.
- Número de capacitaciones registradas correctamente en el sistema.

8. INFORME TÉCNICO EN EL ÁMBITO DE SU COMPETENCIA.

La elaboración de informes técnicos diarios en la Prefectura de Cotopaxi constituye una práctica de gestión fundamental para garantizar el control, la trazabilidad y la mejora continua de las actividades vinculadas a la infraestructura tecnológica y los sistemas institucionales.

Estos informes permiten documentar incidencias, avances, actividades de mantenimiento, resultados de proyectos y recomendaciones para la optimización de los servicios tecnológicos.

La gestión de informes técnicos diarios ordinarios asegura una comunicación efectiva entre las áreas técnicas, facilita la toma de decisiones basada en datos objetivos y promueve la rendición de cuentas sobre las actividades realizadas.

8.1. OBJETIVO

Documentar de manera sistemática y continua todas las actividades técnicas ejecutadas en el ámbito de tecnologías de la información, proporcionando información relevante sobre el estado de los sistemas, infraestructura, soporte, incidentes, capacitaciones y proyectos, para fortalecer la gestión operativa, la transparencia y la toma de decisiones informadas en la Prefectura de Cotopaxi.

8.2. LINEAMIENTOS GENERALES

- **Periodicidad diaria:**

  Se debe generar un informe técnico diario ordinario, sin excepción, para todas las actividades ejecutadas dentro del área de tecnologías de la información.
- **Contenido estructurado:**

  Cada informe debe incluir actividades realizadas, incidencias atendidas, resultados obtenidos, análisis breve de desempeño y recomendaciones.
- **Responsabilidad individual:**

  Cada técnico, administrador o responsable de un área tecnológica debe elaborar su propio informe correspondiente a las actividades de su competencia.
- **Sistema de registro:**

  Los informes deben archivarse digitalmente en una carpeta institucional organizada por fecha y categoría de actividad, y reportarse semanalmente para revisión consolidada.
- **Veracidad y trazabilidad:**

  Toda información registrada en los informes debe ser verificable, respaldada por evidencias como capturas de pantalla, registros de tickets, reportes de monitoreo, actas de capacitaciones, etc.

8.3. ESTRUCTURA BÁSICA DEL INFORME TÉCNICO DIARIO

La estructura estándar para el informe técnico es la siguiente:

Tabla 15

Informe técnico diario

Sección	Descripción
Encabezado	Fecha, nombre del responsable, unidad, sistema o infraestructura involucrada.
Actividades Realizadas	Descripción breve y específica de las tareas ejecutadas. Ejemplo: configuración de servidor, instalación de actualizaciones, capacitación impartida.
Incidencias Detectadas	Reporte de fallas o vulnerabilidades identificadas, con su respectivo análisis preliminar.
Soluciones Aplicadas o Recomendadas	Acciones correctivas implementadas o sugerencias de solución futura.
Anexos	Evidencias documentales o gráficas (capturas de pantalla, bitácoras, logs, etc.).
Observaciones	Comentarios adicionales relevantes para la gestión técnica o propuestas de mejora.

8.4. PLAN OPERATIVO DE GESTIÓN DE INFORMES TÉCNICOS

Tabla 16

Plan operativo de gestión de informes técnicos

Periodo	Actividad	Responsable	Objetivo

Diario ordinario	Elaboración y registro de informes técnicos de actividades ejecutadas	Técnicos de TI, Administradores de sistemas, Soporte TI	Documentar las actividades diarias y asegurar la trazabilidad de la gestión tecnológica.
Semanal	Consolidación de informes diarios para revisión	Coordinador de TI	Analizar tendencias, identificar incidencias recurrentes, proponer mejoras.
Mensual	Análisis de desempeño técnico	Unidad de TI y Direcciones superiores	Evaluar productividad, cumplimiento de tareas, y proponer ajustes estratégicos.

8.5. ROLES Y RESPONSABILIDADES

Tabla 17

Roles y responsabilidades

Rol	Función
Responsables técnicos	Redactar diariamente su informe detallado de actividades y remitirlo en los plazos establecidos.
Coordinador de TI	Consolidar los informes, identificar patrones de incidencias o problemas sistémicos, reportar hallazgos relevantes a instancias superiores.
Unidad de Tecnologías de la Información	Supervisar la calidad de los informes, emitir lineamientos de mejora, y asegurar su almacenamiento seguro y ordenado.
Dirección Administrativa	Recibir reportes consolidados y tomar decisiones estratégicas basadas en la información suministrada.

8.6. PROCESOS DE GESTIÓN DE INFORMES TÉCNICOS

a) Elaboración del informe:

Cada responsable documenta en un formato estandarizado todas las actividades, incidentes y observaciones del día.

b) Validación interna:

Antes de registrar el informe, se valida que la información sea completa, clara y respaldada.

c) Archivo y resguardo:

El informe se guarda en el repositorio digital institucional bajo la carpeta correspondiente a la fecha.

d) Consolidación semanal:

Los informes diarios son revisados semanalmente para extraer datos relevantes de desempeño y generar reportes ejecutivos si se requiere.

8.7. DOCUMENTACIÓN OBLIGATORIA

- Formato estándar de informe técnico diario.
- Base de datos o repositorio digital de informes técnicos.
- Evidencias de respaldo asociadas a cada informe (capturas, bitácoras, registros de tickets).
- Consolidaciones semanales y reportes de análisis de desempeño mensual.

8.8. INDICADORES DE ÉXITO

Tabla 18

Indicadores éxito

Indicador	Meta
% de informes técnicos presentados a tiempo	100% de los días laborables
% de actividades documentadas en informes	≥ 98%

Tiempo promedio de entrega del informe diario	Antes de las 17h00 de cada jornada
Número de incidencias críticas identificadas y tratadas oportunamente	100% tratadas en menos de 24 horas
Nivel de cumplimiento en calidad de la documentación	≥ 95% conforme a auditorías internas

9. CONCLUSIÓN

La implementación de una infraestructura tecnológica robusta y eficiente en la Prefectura de Cotopaxi constituye un pilar esencial para el fortalecimiento de la gestión institucional, la optimización de los procesos administrativos y la mejora en la prestación de servicios a la ciudadanía. A través de políticas claras y planes estratégicos específicos en las áreas de administración de proyectos informáticos, configuración de software base, gestión de comunicaciones, seguridad de la información, capacitación de usuarios y elaboración de informes técnicos, se establece un marco operativo sólido que garantiza la sostenibilidad y el éxito de la transformación digital emprendida. La correcta administración de proyectos tecnológicos asegura que las iniciativas institucionales se ejecuten en tiempo, forma y calidad; la adecuada configuración y mantenimiento del software base permite el funcionamiento estable de todos los sistemas; la gestión eficiente de las comunicaciones garantiza la disponibilidad de los servicios críticos; y el fortalecimiento de la seguridad informática protege la información y los activos tecnológicos ante amenazas internas y externas.

Asimismo, la capacitación permanente de los usuarios y el soporte técnico continuo impulsan una cultura de adopción tecnológica responsable, mientras que la elaboración sistemática de informes técnicos diarios proporciona herramientas efectivas para la toma de decisiones estratégicas y la mejora continua. De este modo, la Prefectura de Cotopaxi no solo responde a las exigencias normativas nacionales como la Ley Orgánica de Protección de Datos Personales (LOPDP) y el Esquema Gubernamental de Seguridad de la Información (EGSI), sino que también se proyecta como una institución moderna, innovadora y comprometida con la excelencia en la gestión pública, sentando las bases para su crecimiento tecnológico futuro y fortaleciendo su rol como referente en la administración pública ecuatoriana.