INFORMES DE IMPLEMENTACIÓN ADMINISTRACIÓN Y CONTROL DE ACCESOS A SISTEMAS Y APLICACIONES ABARCANDO LA GESTIÓN DE ALTAS Y BAJAS MODIFICACIONES SOBRE LOS PERMISOS DE ACCESO Y GESTIÓN DE USUARIOS.

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

PERIODO 2025

Índice de contenidos

INFORMES DE IMPLEMENTACIÓN ADMINISTRACIÓN Y CONTROL DE ACCESOS A SISTEMAS Y APLICACIONES ABARCANDO LA GESTIÓN DE ALTAS Y BAJAS MODIFICACIONES SOBRE LOS PERMISOS DE ACCESO Y GESTIÓN DE USUARIOS.

1. ANTECEDENTES

El control de accesos a los sistemas informáticos constituye una de las funciones estratégicas dentro de la gestión de tecnologías de la información en las entidades públicas. Su correcta implementación permite salvaguardar la integridad, confidencialidad y disponibilidad de los recursos digitales institucionales, así como prevenir accesos no autorizados, pérdidas de información o vulneraciones a los sistemas críticos.

En cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP), el Esquema Gubernamental de Seguridad de la Información (EGSI), y en concordancia con los estándares internacionales como la ISO/IEC 27001:2022, la Prefectura de Cotopaxi ha venido fortaleciendo sus procesos de administración de accesos, estableciendo procedimientos formales para la gestión de altas, bajas y modificaciones de usuarios y permisos en los sistemas y aplicaciones institucionales.

Durante el último período, las áreas técnicas responsables han desarrollado e implementado mecanismos para mejorar el control de credenciales, la asignación de perfiles por rol, la trazabilidad de actividades de usuarios, y la automatización parcial de los procesos de habilitación y eliminación de cuentas de acceso. Este esfuerzo responde a la necesidad de fortalecer la seguridad lógica y de alinear los sistemas de información a los principios de legalidad, proporcionalidad y minimización en el tratamiento de datos personales.

El presente informe tiene como propósito documentar las acciones realizadas en torno a la implementación, administración y control de accesos a sistemas y aplicaciones, consolidando las medidas aplicadas para el registro, seguimiento y auditoría de los usuarios institucionales, y estableciendo buenas prácticas para asegurar la eficiencia operativa y la protección del entorno digital de la Prefectura de Cotopaxi.

2. GENERALIDADES

La administración de accesos a los sistemas y aplicaciones institucionales constituye una función crítica dentro de la gestión de la seguridad de la información, ya que permite controlar

quién accede a qué recursos, bajo qué condiciones, y con qué privilegios. Este proceso no solo garantiza la protección de la infraestructura tecnológica y de los datos que en ella se gestionan, sino que además asegura el cumplimiento de los principios de legalidad, proporcionalidad y responsabilidad en el tratamiento de la información pública.

En el contexto ecuatoriano, la correcta implementación de controles de acceso responde a disposiciones establecidas en normativas 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 los lineamientos técnicos de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). Estas regulaciones exigen que las instituciones públicas adopten políticas claras sobre el ciclo de vida de los usuarios, incluyendo la creación (alta), modificación, suspensión y eliminación (baja) de accesos a los sistemas informáticos, conforme al rol funcional de cada servidor.

Adicionalmente, se fomenta la adopción de estándares internacionales como la ISO/IEC 27001:2022, homologados por el Instituto Ecuatoriano de Normalización (INEN), los cuales establecen prácticas de referencia para la implementación de controles de acceso, monitoreo de actividades, registro de eventos y revisión periódica de privilegios asignados.

Para la Prefectura de Cotopaxi, la gestión de accesos representa un eje estratégico en el fortalecimiento de la seguridad institucional y en la garantía del uso legítimo de los recursos tecnológicos. La administración ordenada de usuarios, perfiles y permisos no solo permite minimizar riesgos operativos, sino que también refuerza la trazabilidad de las acciones ejecutadas dentro de los sistemas, facilita los procesos de auditoría interna y externa, y contribuye al cumplimiento efectivo de los principios de transparencia, eficiencia y protección de datos personales que rigen el quehacer público.

3. OBJETIVO

Establecer un marco técnico y operativo que garantice la adecuada implementación, administración y control de accesos a los sistemas y aplicaciones institucionales de la Prefectura de Cotopaxi, asegurando que la asignación, modificación y revocación de permisos se realicen de forma ordenada, segura y conforme al rol funcional de cada usuario. Este lineamiento busca cumplir con las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP), el Esquema Gubernamental de Seguridad de la Información (EGSI) y los

estándares internacionales como la ISO/IEC 27001:2022, promoviendo buenas prácticas en la gestión del ciclo de vida de los accesos, el monitoreo de actividades, la trazabilidad de acciones, la protección de información sensible y la prevención de accesos indebidos. Asimismo, establece directrices claras para la gestión centralizada de usuarios, la aplicación de principios de privilegios mínimos, la revisión periódica de accesos, y la generación de informes técnicos que respalden la seguridad y eficiencia en el uso de los sistemas tecnológicos institucionales.

3.1. Ámbito De Aplicación

El presente instrumento es de aplicación obligatoria para todos los servidores, servidoras, funcionarios y funcionarias de la Prefectura de Cotopaxi, así como para proveedores externos, consultores o personal técnico que, por razón de su función o contrato, tengan acceso total o parcial a los sistemas, plataformas o aplicaciones institucionales.

Su alcance comprende todas las acciones vinculadas a la gestión de accesos, incluyendo la creación (alta), modificación, suspensión temporal y eliminación (baja) de usuarios, así como la asignación, revisión y control de permisos y privilegios asociados a roles funcionales en los distintos entornos tecnológicos utilizados por la institución.

Este lineamiento abarca tanto sistemas locales como plataformas en la nube, sistemas administrativos, aplicativos internos, bases de datos, entornos virtualizados, y cualquier otro recurso informático institucional que requiera autenticación y autorización para su uso. Su aplicación se enmarca en el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP), el Esquema Gubernamental de Seguridad de la Información (EGSI) y demás normativas técnicas y legales vigentes en el Ecuador.

Todos los usuarios institucionales, sin excepción, deberán actuar conforme a los roles, perfiles y responsabilidades asignadas, cumpliendo con los procedimientos establecidos para el acceso, uso y gestión de credenciales, en concordancia con los principios de legalidad, proporcionalidad, necesidad, trazabilidad y seguridad de la información.

3.2. 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.

4. INFORME TÉCNICO EN EL ÁMBITO DE SU COMPETENCIA.

El informe técnico en el ámbito de su competencia es un instrumento formal que permite a las unidades técnicas responsables de la administración de sistemas y accesos documentar las actividades realizadas, los cambios aplicados, los incidentes gestionados y las recomendaciones emitidas en relación con la gestión de usuarios, permisos y seguridad lógica de los sistemas institucionales.

Esta herramienta es fundamental para garantizar la trazabilidad de las acciones ejecutadas sobre plataformas críticas, fortalecer el control interno, facilitar auditorías, dar cumplimiento a los requerimientos de los organismos de control y respaldar decisiones institucionales sobre el manejo de accesos y privilegios.

4.1. OBJETIVO

Establecer un mecanismo sistemático de registro técnico que documente la gestión diaria de usuarios, permisos y accesos en los sistemas institucionales, permitiendo la verificación, evaluación y seguimiento de las acciones ejecutadas por los responsables de seguridad informática y administración de plataformas en la Prefectura de Cotopaxi.

4.2. CONTENIDO MÍNIMO DEL INFORME TÉCNICO

Todo informe técnico generado en el ámbito de la gestión de accesos debe contener:

- Fecha de elaboración
- Nombre del responsable y unidad
- Sistema o aplicación intervenida
- Tipo de acción realizada (alta, baja, modificación, auditoría)
- Detalle técnico de la acción
- Justificación (requerimiento, auditoría, incidente, rotación de personal)
- Evidencias adjuntas (capturas, logs, autorizaciones)
- Observaciones o recomendaciones
- Firma o validación de la jefatura inmediata

4.3. PLAN OPERATIVO DE INFORMES TÉCNICOS SOBRE ACCESOS

Actividad	Frecuencia	Responsable	Finalidad
Registro de altas, bajas y modificaciones	Diario ordinario	Técnico de sistemas o administrador de accesos	Documentar cada cambio realizado en usuarios o permisos
Consolidación de informes por sistema o área	Semanal	Unidad de TIC o Coordinación de Seguridad	Facilitar seguimiento centralizado y control de cambios
Revisión y validación de informes	Semanal	Jefatura de TI o Dirección Técnica	Asegurar cumplimiento de protocolos y coherencia con registros
Archivo y trazabilidad de informes	Permanente	Gestión Documental y Soporte TI	Mantener respaldo institucional en repositorio seguro
Reporte a dirección o entes de control	Trimestral o bajo requerimiento	Coordinación Técnica	Servir como evidencia en procesos de auditoría, control o fiscalización

4.4. TABLA DE RESPONSABILIDADES

Rol institucional	Función asignada
Técnico responsable de accesos	Elaboración y entrega del informe técnico diario
Jefatura inmediata	Revisión, validación y firma del informe
Unidad de Tecnologías de la Información	Consolidación, seguimiento y custodia documental
Gestión Documental	Respaldo digital y archivo físico
Auditoría Interna	Evaluación periódica de cumplimiento, coherencia y trazabilidad
Dirección Administrativa	Toma de decisiones correctivas o estratégicas basadas en informes

4.5. INDICADORES DE CUMPLIMIENTO

Indicador	Meta
Porcentaje de informes diarios entregados a tiempo	100%
Porcentaje de informes con evidencia documental completa	≥ 95%
Tiempo promedio de validación por jefatura	≤ 2 días
Incidentes sin respaldo de informe técnico	0
Porcentaje de informes auditados con observaciones corregidas	100%

4.6. DOCUMENTACIÓN OBLIGATORIA

- Formato institucional de informe técnico
- Bitácoras de cambios de usuarios y permisos
- Logs del sistema con marcas de auditoría

- Actas de aprobación o autorización de cambios críticos
- Registros de incidentes relacionados con accesos
- Evidencias digitales (capturas de pantalla, correos, reportes automáticos)
- Consolidado mensual de reportes por sistema o unidad

4.7. ESTRATEGIA DE SEGUIMIENTO Y MEJORA CONTINUA

- **Validación cruzada** entre informes técnicos, bitácoras de sistemas y autorizaciones emitidas.
- **Revisión periódica** de los informes por parte de Auditoría Interna para detectar inconsistencias o posibles negligencias.
- **Capacitación continua** del personal responsable de elaborar informes para asegurar calidad y uniformidad en el registro técnico.
- **Retroalimentación trimestral** desde la Dirección de TIC hacia las áreas responsables sobre el cumplimiento y calidad de los informes generados.
- **Integración futura** con sistemas de gestión documental automatizada para agilizar validación y archivo.

PREFECTURA DE COTOPAXI

INFORME TÉCNICO EN EL ÁMBITO DE SU COMPETENCIA

Gestión de Accesos a Sistemas y Aplicaciones

Unidad: _____

Fecha: ____ / ____ / 20__

- **1. Datos Generales**
- **Nombre del responsable: _____**
- **Cargo: _____**
- **Sistema o aplicación intervenida: _____**
- **Tipo de acción realizada:**

( ) Alta de usuario ( ) Baja de usuario ( ) Modificación de permisos ( ) Auditoría ( ) Revisión de accesos

---

- **2. Descripción de la Actividad Técnica**

Detalle de la acción realizada:

(Describir de forma clara la acción técnica ejecutada: a qué usuario se dio de alta, baja, cambios realizados, perfil aplicado, módulos habilitados, entre otros.)

Motivo o justificación:

(Indicar si fue por ingreso de nuevo personal, rotación de funciones, requerimiento institucional, auditoría, incidente, etc.)

Usuarios afectados (si aplica):

- **3. Resultados / Observaciones**

(Registrar resultados obtenidos, condiciones encontradas, alertas técnicas, limitaciones del sistema o riesgos identificados.)

- **4. Recomendaciones (si aplica)**

(Sugerencias técnicas, medidas preventivas, mejoras o solicitudes adicionales.)

- **5. Evidencias adjuntas**

(Marcar lo que se adjunta y especificar si corresponde)
[ ] Captura de pantalla [ ] Registro del sistema [ ] Autorización de jefatura [ ] Log técnico
[ ] Otro: _____

- **6. Validación**
- **Firma del responsable técnico:** _____
- **Revisado por (jefatura inmediata):** _____
- **Fecha de validación:** ____ / ____ / 20__

Nota: Este informe debe remitirse a la Unidad de Tecnologías de la Información y quedar archivado en el repositorio de seguridad digital correspondiente.