POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SOBRE LA BASE DISPOSICIONES LEGALES Y REGLAMENTOS VIGENTES

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

PERIODO 2025

Índice de contenidos

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SOBRE LA BASE DISPOSICIONES LEGALES Y REGLAMENTOS VIGENTES

1. ANTECEDENTES

La seguridad de la información en Ecuador ha evolucionado significativamente en los últimos años, impulsada por la necesidad de proteger datos sensibles frente a crecientes amenazas cibernéticas. A medida que las organizaciones, tanto públicas como privadas, han adoptado procesos digitales, la regulación en esta materia se ha vuelto fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información.

Uno de las primeras actividades del país en este ámbito ha sido la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), establecido mediante el Acuerdo Ministerial Nro. 025-2019 del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). Este esquema se ha convertido en un referente para la administración pública, exigiendo el cumplimiento de estándares basados en la norma internacional ISO/IEC 27001. En un contexto donde la protección de datos personales ha cobrado mayor relevancia, en mayo de 2021 se aprobó la Ley Orgánica de Protección de Datos Personales (LOPDP), normativa que entró en vigor en mayo de 2023 con el propósito de regular el tratamiento de información personal en el país, esta ley establece derechos y obligaciones para las entidades que manejan datos sensibles, alineando a Ecuador con estándares internacionales en privacidad y ciberseguridad.

Otro hito importante ha sido la creación de la Política Nacional de Ciberseguridad en 2021, que definió directrices para fortalecer la resiliencia digital del país. Esta política ha impulsado la formación de los Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT) estableciendo lineamientos para la prevención y gestión de riesgos cibernéticos en sectores estratégicos. Más recientemente, en 2024, Ecuador adoptó la versión más actualizada de la norma ISO/IEC 27001:2022 a través del Instituto Ecuatoriano de Normalización (INEN). Esta actualización refuerza la importancia de la gestión de riesgos y la implementación de controles de seguridad adaptados a las nuevas amenazas digitales. El marco regulatorio ecuatoriano continúa fortaleciéndose con la actualización de normativas y políticas internas en distintas instituciones.

2. GENERALIDADES

Las políticas de seguridad de la información son un conjunto de normas, directrices y procedimientos que establecen los lineamientos para la protección de los activos de información dentro de una organización. Su implementación es fundamental para prevenir riesgos asociados a accesos no autorizados, pérdida de datos, ataques cibernéticos y otras amenazas que puedan comprometer la integridad, confidencialidad y disponibilidad de la información.

En Ecuador, estas políticas están reguladas por normativas nacionales e internacionales, tales como la Ley Orgánica de Protección de Datos Personales (LOPDP), el Esquema Gubernamental de Seguridad de la Información (EGSI) y los estándares de la ISO/IEC 27001:2022, adoptados por el Instituto Ecuatoriano de Normalización (INEN). Estas regulaciones establecen las bases para la gestión de seguridad de la información en entidades públicas y privadas, promoviendo el cumplimiento de controles adecuados para minimizar riesgos y garantizar la protección de datos sensibles.

2.1. Descripción de las políticas de seguridad de la información

Las políticas de seguridad de la información en Ecuador están diseñadas para garantizar que los sistemas y datos sean gestionados de manera segura, conforme a los principios de confidencialidad, integridad y disponibilidad. Estas políticas se aplican a todas las organizaciones que manejan información sensible, estableciendo directrices sobre el acceso, uso, almacenamiento y protección de los datos.

En términos generales, las políticas de seguridad de la información incluyen los siguientes aspectos fundamentales:

- **Gestión de accesos y autenticación**: Define los controles para el acceso a sistemas y bases de datos, asegurando que solo usuarios autorizados puedan consultar o modificar información.
- **Clasificación y manejo de la información**: Establece criterios para identificar y categorizar los datos según su nivel de sensibilidad, determinando medidas específicas de protección.

- **Protección de datos personales**: En cumplimiento con la LOPDP, se establecen mecanismos para la recolección, almacenamiento, tratamiento y eliminación de datos personales, garantizando el respeto a los derechos de los titulares.
- **Control de incidentes de seguridad**: Define procedimientos para la detección, reporte y mitigación de eventos de seguridad, incluyendo ataques informáticos y accesos no autorizados.
- **Continuidad del negocio y recuperación ante desastres**: Implementa planes para garantizar la operatividad de los sistemas en caso de fallos, ataques cibernéticos o desastres naturales.
- **Normas de ciberseguridad**: Establece medidas de protección contra amenazas digitales, asegurando el uso seguro de redes, dispositivos y aplicaciones tecnológicas.
- **Concienciación y capacitación en seguridad**: Promueve la formación de empleados y usuarios en buenas prácticas de seguridad informática, reduciendo el riesgo de errores humanos.

Cada organización debe adaptar estas políticas a su contexto operativo, asegurando el cumplimiento de las normativas vigentes y la implementación de controles efectivos que reduzcan vulnerabilidades y riesgos asociados a la gestión de la información.

2.2. Objetivo

Establecer un marco normativo y operativo que garantice la protección de los activos de información dentro de las organizaciones, minimizando riesgos asociados a accesos no autorizados, pérdida de datos, ciberataques y cualquier otra amenaza que pueda comprometer la integridad, confidencialidad y disponibilidad de la información. Estas políticas buscan asegurar el cumplimiento de estándares internacionales y normativas ecuatorianas vigentes, como la Ley Orgánica de Protección de Datos Personales (LOPDP), el Esquema Gubernamental de Seguridad de la Información (EGSI) y la ISO/IEC 27001:2022, promoviendo la implementación de controles adecuados para prevenir vulnerabilidades y garantizar el resguardo de datos sensibles. Asimismo, establecen lineamientos para la gestión de accesos, la detección y mitigación de incidentes, la continuidad operativa ante posibles fallos y la capacitación del personal en buenas prácticas de ciberseguridad.

2.3. Ámbito De Aplicación

El presente instrumento regirá a todos los/las servidores/as, funcionarios/as de la Prefectura de Cotopaxi, incluyendo a proveedores externos vinculados a la institución mediante contratos, convenios o acuerdos. Su aplicación se enmarca en el cumplimiento del Esquema Gubernamental de Seguridad de la Información (EGSI) y demás normativas vigentes, garantizando que todas las personas con acceso a los activos de información de la institución cumplan con las medidas de seguridad establecidas. Asimismo, este instrumento se aplica con apego a la definición de roles y perfiles, asegurando una gestión responsable y segura de la información dentro del marco normativo nacional.

2.4. Conceptos y Definiciones

Para el correcto entendimiento e implementación de las Políticas de Seguridad de la Información en la Prefectura de Cotopaxi, se establecen los siguientes conceptos y definiciones, los cuales permiten una interpretación uniforme de los términos empleados en el presente documento:

a) Seguridad de la Información

Conjunto de medidas, políticas y procedimientos diseñados para garantizar la confidencialidad, integridad y disponibilidad de la información dentro de una organización, protegiéndola de accesos no autorizados, alteraciones o pérdidas.

b) Infraestructura Tecnológica

Conjunto de servidores, redes, sistemas de almacenamiento, bases de datos, software y hardware que conforman el entorno digital de una institución y que permiten la gestión, almacenamiento y procesamiento de la información.

c) Plan de Análisis, Identificación y Mitigación de Riesgos

Estrategia implementada para detectar, evaluar y minimizar los riesgos que puedan comprometer la infraestructura tecnológica, mediante la aplicación de medidas preventivas y correctivas que aseguren la continuidad operativa y la protección de los datos institucionales.

d) Respaldo de Bases de Datos

Procedimiento técnico mediante el cual se realizan copias de seguridad de la información almacenada en bases de datos institucionales, garantizando su recuperación en caso de fallos de hardware, ataques informáticos o errores humanos.

e) Acceso y Medidas de Control de Seguridad Física

Conjunto de mecanismos de protección que regulan el ingreso a áreas críticas donde se almacenan o procesan activos tecnológicos, incluyendo sistemas de identificación, videovigilancia, monitoreo de accesos y control de dispositivos.

f) Incidente de Seguridad

Evento o acción que compromete la confidencialidad, integridad o disponibilidad de la información y los sistemas tecnológicos, pudiendo ser causado por errores humanos, fallas técnicas, ataques cibernéticos o accesos no autorizados.

g) Informe Técnico de Seguridad

Documento que recopila información sobre análisis de riesgos, incidentes detectados, medidas de mitigación implementadas y cumplimiento de normativas, proporcionando una evaluación detallada del estado de la seguridad tecnológica en la institución.

h) Esquema Gubernamental de Seguridad de la Información (EGSI)

Marco normativo establecido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), que regula la seguridad de la información en instituciones públicas del Ecuador, asegurando la implementación de controles adecuados en la gestión digital.

i) Ley Orgánica de Protección de Datos Personales (LOPDP)

Normativa ecuatoriana que regula el tratamiento, almacenamiento y protección de los datos personales, estableciendo derechos y obligaciones para garantizar la privacidad y seguridad de la información de los ciudadanos.

j) ISO/IEC 27001:2022

Estándar internacional de gestión de seguridad de la información, que define requisitos y mejores prácticas para la protección de datos y sistemas tecnológicos, promoviendo la gestión de riesgos y el cumplimiento de controles de seguridad.

k) Monitoreo de Infraestructura Tecnológica

Proceso continuo de supervisión de redes, servidores y sistemas de información para detectar vulnerabilidades, prevenir incidentes y optimizar el desempeño tecnológico mediante herramientas especializadas de seguridad informática.

l) Políticas de Seguridad de la Información

Conjunto de directrices y normativas implementadas en una organización para proteger los activos digitales, regulando el acceso, tratamiento y resguardo de la información institucional.

m) Control de Acceso

Mecanismos implementados para garantizar que solo usuarios autorizados puedan acceder a recursos tecnológicos, mediante autenticación biométrica, contraseñas, tarjetas de proximidad o sistemas de doble factor.

n) Gestión de Riesgos Tecnológicos

Proceso de identificación, análisis y mitigación de amenazas que puedan afectar la seguridad de los sistemas y la infraestructura digital, permitiendo implementar medidas preventivas para minimizar impactos negativos.

o) Auditoría de Seguridad de la Información

Evaluación periódica de las medidas y controles de seguridad aplicados en una organización, con el fin de detectar fallos, optimizar procesos y asegurar el cumplimiento de normativas y estándares de ciberseguridad.

3. ACCESOS Y MEDIDAS DE CONTROL A LA SEGURIDAD FÍSICA SOBRE LOS RECURSOS INFORMÁTICOS.

La seguridad física de los recursos informáticos de la Prefectura de Cotopaxi es un pilar fundamental en la protección de la infraestructura tecnológica, garantizando la disponibilidad, integridad y confidencialidad de la información. Para ello, se establece un Plan de Acceso y Medidas de Control a la Seguridad Física, el cual debe ser ejecutado, monitoreado y evaluado de manera anual.

El propósito de este plan es minimizar los riesgos asociados a accesos no autorizados, sabotaje, daño intencional o accidental, desastres naturales y cualquier otra amenaza que pueda comprometer la operatividad de los sistemas informáticos. Su cumplimiento es obligatorio para todos los funcionarios, servidores, proveedores y terceros con acceso a la infraestructura tecnológica de la institución.

3.1. Control de Accesos y Restricciones

Para garantizar que solo personal autorizado tenga acceso a los recursos informáticos críticos, se establecen los siguientes mecanismos de control:

- **Identificación y autenticación de usuarios**: Se implementarán sistemas de acceso mediante tarjetas de proximidad, autenticación biométrica o códigos de seguridad, según el nivel de criticidad de cada área.
- **Zonificación de acceso**: Las instalaciones con infraestructura informática serán categorizadas en diferentes niveles de seguridad, restringiendo el acceso solo a personal autorizado según su función y necesidad operativa.
- **Protocolos de ingreso y egreso**: Toda persona que acceda a las salas de servidores, centros de datos o áreas con recursos tecnológicos críticos deberá registrarse en un control de acceso, detallando el motivo de su visita, la hora de entrada y salida.

3.2. Monitoreo y Vigilancia de Áreas Críticas

Para prevenir incidentes de seguridad y garantizar un control efectivo de accesos, se aplicarán las siguientes medidas de monitoreo:

- **Sistema de videovigilancia 24/7**: Se instalarán cámaras de seguridad en puntos estratégicos de acceso y dentro de las salas donde se resguarden los recursos informáticos. Las grabaciones serán almacenadas durante un período definido para su análisis en caso de incidentes.
- **Patrullaje y supervisión**: Se establecerá un esquema de inspecciones periódicas a cargo del personal de seguridad para verificar el cumplimiento de las medidas establecidas.

- **Alarmas y sensores de movimiento**: Se implementarán sistemas de detección temprana de accesos no autorizados, alertando a los responsables de seguridad en caso de intentos de ingreso no autorizados.

3.3. Protección Ambiental y Seguridad Física de los Equipos

Además del acceso restringido, es fundamental garantizar condiciones óptimas para el resguardo de los equipos informáticos, evitando daños por factores externos. Para ello, se aplicarán las siguientes medidas:

- **Sistemas de detección y extinción de incendios**: Instalación de sensores de humo y temperatura en áreas críticas, así como extintores específicos para equipos electrónicos.
- **Control de temperatura y humedad**: Implementación de sistemas de aire acondicionado y ventilación adecuados para mantener la operatividad de los servidores y equipos sensibles.
- **Protección contra cortes eléctricos**: Uso de sistemas de alimentación ininterrumpida (UPS) y generadores de respaldo para garantizar la continuidad operativa en caso de fallos en el suministro eléctrico.

3.4. Control De Dispositivos y Medios de Almacenamiento

Para prevenir la fuga o alteración de información, se establecerán normativas claras sobre el uso de dispositivos externos:

- **Restricción de dispositivos USB y almacenamiento externo**: Solo el personal autorizado podrá utilizar dispositivos de almacenamiento, previa aprobación de la administración de TI.
- **Cifrado de información confidencial**: Los datos almacenados en dispositivos externos deberán estar protegidos mediante cifrado, evitando accesos no autorizados en caso de extravío o robo.
- **Auditoría de dispositivos conectados**: Se registrará y supervisará el uso de discos duros externos, memorias USB y otros medios de almacenamiento para detectar posibles vulnerabilidades.

3.5. Procedimientos en Caso de Incidentes de Seguridad Física

Ante cualquier incidente que comprometa la seguridad física de los recursos informáticos, se seguirán los siguientes protocolos:

- **Reporte inmediato**: Todo evento sospechoso o intento de acceso no autorizado deberá ser reportado de inmediato al área de seguridad y tecnología de la información.
- **Evaluación del impacto**: Se analizará la magnitud del incidente y se aplicarán las medidas correctivas necesarias para evitar afectaciones en la infraestructura informática.
- **Registro de incidentes**: Se mantendrá un historial documentado de eventos de seguridad física, facilitando la identificación de patrones y la implementación de mejoras en las medidas de protección.

3.6. Auditoría y Evaluación Anual del Plan de Seguridad Física

Para asegurar la efectividad del Plan de Acceso y Medidas de Control a la Seguridad Física, se realizará una auditoría anual con los siguientes objetivos:

- **Evaluar el cumplimiento de los protocolos establecidos** y detectar posibles deficiencias en los controles de acceso y monitoreo.
- **Actualizar las medidas de seguridad física** en función de nuevas amenazas y necesidades operativas.
- **Capacitar al personal** en mejores prácticas de seguridad y gestión de incidentes, asegurando una correcta implementación de los procedimientos.

4. INFORME TÉCNICO EN EL ÁMBITO DE SU COMPETENCIA.

La gestión de la seguridad de la información en la Prefectura de Cotopaxi requiere una supervisión constante y un monitoreo efectivo de las actividades relacionadas con la protección de los recursos tecnológicos. Para ello, se establece la obligación de generar un Informe Técnico Diario Ordinario, en el cual se documentan los eventos, incidencias, controles y acciones realizadas en el ámbito de la seguridad de la información y la infraestructura tecnológica.

4.1. Objetivo Del Informe Técnico

Proporcionar un registro detallado de las actividades operativas, incidentes de seguridad, cumplimiento de protocolos y cualquier otra acción relevante que haya sido ejecutada en el día, permitiendo un análisis continuo de la seguridad y facilitando la toma de decisiones para la mejora de los procesos de protección de la información.

4.2. Contenido Del Informe Técnico

El informe deberá incluir la siguiente información:

4.2.1. Datos Generales

- Fecha y hora del informe.
- Responsable de la elaboración del informe.
- Área o departamento al que corresponde.

4.2.2. Registro de Actividades Realizadas

- Controles de acceso aplicados a sistemas y recursos informáticos.
- Actividades de mantenimiento preventivo o correctivo en infraestructura tecnológica.
- Monitoreo de redes, servidores y dispositivos de almacenamiento.
- Implementación de actualizaciones de seguridad en software y hardware.

4.2.3. Incidentes de Seguridad Detectados

- Descripción del incidente (intentos de acceso no autorizado, fallas en sistemas, alertas de ciberseguridad, etc.).
- Impacto y nivel de riesgo del incidente.
- Acciones correctivas implementadas.
- Recomendaciones para la prevención de incidentes similares.

4.2.4. Gestión de Usuarios y Accesos

- Creación, modificación o eliminación de cuentas de usuario en sistemas institucionales.
- Asignación de permisos y restricciones de acceso según los perfiles de usuario.
- Control de accesos físicos a infraestructuras críticas.

4.2.5. Verificación de Cumplimiento de Normativas

- Evaluación del cumplimiento de los protocolos establecidos en el Esquema Gubernamental de Seguridad de la Información (EGSI).
- Cumplimiento de los lineamientos de la Ley Orgánica de Protección de Datos Personales (LOPDP).
- Validación de las auditorías internas y externas.

4.2.6. Observaciones y Recomendaciones

- Identificación de áreas de mejora en la seguridad de la información.
- Propuestas para optimizar los procesos de gestión y monitoreo.
- Requerimientos adicionales en infraestructura o capacitación del personal.
- Firma y Aprobación
- Elaborado por: (Nombre y cargo del responsable del informe).
- Aprobado por: (Nombre y cargo del supervisor o autoridad competente).

4.3. Frecuencia Y Responsabilidad

Este informe deberá ser generado diariamente por el personal responsable de la gestión de la seguridad de la información en la Prefectura de Cotopaxi y remitido a las autoridades pertinentes para su revisión y archivo. Su correcta elaboración permitirá garantizar un control eficiente y documentado sobre la operatividad de la infraestructura tecnológica, facilitando la detección temprana de amenazas y la mejora continua de los procedimientos de seguridad.

5. PLAN DE ANÁLISIS, IDENTIFICACIÓN Y MITIGACIÓN DE RIESGOS DE INFRAESTRUCTURA TECNOLÓGICA.

La Prefectura de Cotopaxi implementa un Plan de Análisis, Identificación y Mitigación de Riesgos de Infraestructura Tecnológica, cuyo objetivo es garantizar la seguridad, estabilidad y continuidad operativa de los sistemas y recursos tecnológicos institucionales. Este plan se ejecuta con una periodicidad anual, permitiendo la evaluación de amenazas, vulnerabilidades y posibles incidentes que puedan comprometer la operatividad de la infraestructura digital.

5.1. Objetivo del Plan

El propósito principal de este plan es identificar, evaluar y mitigar los riesgos asociados a la infraestructura tecnológica de la institución, asegurando la implementación de controles

preventivos y correctivos que minimicen el impacto de incidentes de seguridad. Asimismo, busca alinear las estrategias de gestión de riesgos con las normativas vigentes, como el Esquema Gubernamental de Seguridad de la Información (EGSI), la Ley Orgánica de Protección de Datos Personales (LOPDP) y los estándares internacionales de seguridad como ISO/IEC 27001:2022.

5.2. Metodología de Análisis de Riesgos

El proceso de análisis y mitigación de riesgos se desarrolla en cuatro fases:

1. **Identificación de Activos Críticos**
   - Inventario de servidores, redes, bases de datos, aplicaciones y dispositivos tecnológicos.
   - Priorización de activos en función de su importancia para las operaciones institucionales.
2. **Evaluación de Riesgos y Vulnerabilidades**
   - Análisis de amenazas internas y externas, incluyendo ciberataques, fallas de hardware, desastres naturales y errores humanos.
   - Uso de herramientas de evaluación de vulnerabilidades en redes y sistemas.
   - Determinación del nivel de riesgo mediante matrices de impacto y probabilidad.
3. **Definición de Estrategias de Mitigación**
   - Implementación de controles técnicos, administrativos y físicos para reducir vulnerabilidades.
   - Aplicación de parches de seguridad, actualizaciones de software y refuerzo de protocolos de autenticación.
   - Respaldo y cifrado de datos para evitar pérdida o robo de información.
   - Planes de contingencia y recuperación ante desastres para asegurar la continuidad operativa.
4. **Monitoreo y Evaluación Continua**
   - Revisión anual del plan para actualizar estrategias según nuevas amenazas.
   - Auditorías de seguridad y pruebas de penetración en sistemas críticos.
   - Capacitación del personal en gestión de riesgos y seguridad de la información.

5. **Responsabilidad y Ejecución**

   - La ejecución de este plan es responsabilidad del área de Tecnologías de la Información de la Prefectura de Cotopaxi, en coordinación con las unidades administrativas pertinentes. La evaluación de riesgos y la implementación de medidas de mitigación deben ser documentadas anualmente en un informe técnico, asegurando el cumplimiento de los lineamientos establecidos y la mejora continua en la gestión de la seguridad tecnológica.

Este plan representa un instrumento fundamental para la protección de la infraestructura tecnológica de la institución, permitiendo la identificación proactiva de riesgos y la adopción de medidas preventivas que garanticen la estabilidad de los servicios digitales. La constante actualización y revisión de este plan contribuirán a fortalecer la resiliencia tecnológica de la Prefectura de Cotopaxi frente a amenazas emergentes.

6. RESPALDO DE LAS BASES DE DATOS.

Para garantizar la disponibilidad, integridad y recuperación de la información almacenada en los sistemas institucionales, la Prefectura de Cotopaxi establece un proceso operativo de respaldo de bases de datos, cuya ejecución y verificación se realizará de manera diaria y ordinaria. Este procedimiento es fundamental para proteger la información ante posibles fallos de hardware, ataques cibernéticos, corrupción de datos o errores humanos, asegurando la continuidad operativa de los servicios digitales de la institución.

6.1. Objetivo del Respaldo de Bases de Datos

El objetivo principal es realizar copias de seguridad periódicas que permitan restaurar la información en caso de incidentes, minimizando el impacto en las operaciones institucionales. Adicionalmente, este proceso garantiza el cumplimiento de normativas nacionales e internacionales de seguridad de la información, como el Esquema Gubernamental de Seguridad de la Información (EGSI) y la Ley Orgánica de Protección de Datos Personales (LOPDP), asegurando la protección y confidencialidad de los datos administrados por la institución.

6.2. Proceso de Respaldo y Almacenamiento

El respaldo de bases de datos seguirá las siguientes directrices:

6.3. Identificación de Bases de Datos a Resguardar

- Se priorizarán aquellas bases de datos que contengan información crítica para la operación de la institución.
- Se mantendrá un registro actualizado de las bases de datos activas, con sus respectivas configuraciones y tiempos de retención de copias.

6.4. Frecuencia y Tipos de Respaldo

- **Respaldos diarios completos**: Se realizará una copia íntegra de todas las bases de datos esenciales cada 24 horas.
- **Respaldos incrementales**: Se almacenarán únicamente los cambios realizados desde el último respaldo completo, optimizando espacio y tiempos de recuperación.
- **Respaldos en tiempo real (replicación de datos)**: Se establecerán configuraciones para mantener sincronizados los datos con servidores de respaldo en ubicaciones seguras.
- **Almacenamiento y Protección de Copias de Seguridad**
- **Ubicación del respaldo**: Se almacenarán copias en servidores locales y en repositorios externos seguros para evitar pérdidas por fallos físicos o ataques informáticos.
- **Cifrado y control de acceso**: Se implementará el cifrado de datos y la restricción de accesos a los respaldos, garantizando que solo personal autorizado pueda gestionarlos.
- **Retención y eliminación de copias antiguas**: Se establecerá una política de retención para almacenar respaldos durante un período definido y eliminar automáticamente aquellos que superen el tiempo estipulado.

6.5. Validación y Pruebas de Restauración

- Se realizarán pruebas periódicas de restauración de bases de datos para verificar la integridad de los respaldos y la eficiencia de los tiempos de recuperación.
- Cualquier error identificado en los respaldos será documentado y corregido de inmediato.

6.6. Reporte Diario de Respaldo

Cada respaldo de bases de datos deberá ser documentado en un reporte diario ordinario, el cual contendrá la siguiente información:

- Fecha y hora del respaldo.
- Nombre y tipo de bases de datos respaldadas.
- Tipo de respaldo realizado (completo, incremental, replicación en tiempo real).
- Ubicación del almacenamiento del respaldo.
- Estado del respaldo (exitoso o con fallas).
- Observaciones y medidas correctivas en caso de errores.

6.7. Responsabilidad y Supervisión

El proceso de respaldo es gestionado por el área de Tecnologías de la Información de la Prefectura de Cotopaxi, la cual es responsable de su correcta ejecución, almacenamiento seguro y documentación. Además, se deberán realizar auditorías periódicas para asegurar el cumplimiento de las mejores prácticas en gestión de respaldos y recuperación de bases de datos.

El cumplimiento estricto de este procedimiento garantizará la seguridad, continuidad y disponibilidad de la información institucional, permitiendo recuperar datos en caso de incidentes. La generación y validación del reporte diario de respaldo permitirá monitorear la efectividad del proceso y optimizar la gestión de la infraestructura tecnológica de la Prefectura de Cotopaxi.

7. INFORME DE CUMPLIMIENTO DEL PLAN DE ANÁLISIS, IDENTIFICACIÓN Y MITIGACIÓN DE RIESGOS DE INFRAESTRUCTURA TECNOLÓGICA.

Para garantizar la seguridad, estabilidad y operatividad continua de los sistemas tecnológicos de la Prefectura de Cotopaxi, se establece la obligación de generar un Informe Diario Ordinario que refleje el cumplimiento del Plan de Análisis, Identificación y Mitigación de Riesgos de Infraestructura Tecnológica. Este informe es un elemento fundamental dentro de la gestión de la seguridad de la información, ya que proporciona un registro detallado y actualizado de la evaluación de vulnerabilidades, incidentes de seguridad, medidas de mitigación implementadas y controles de prevención aplicados a la infraestructura tecnológica.

El propósito de este informe es documentar, de manera estructurada y periódica, los hallazgos obtenidos durante la inspección y análisis de los sistemas informáticos, redes, servidores,

bases de datos y demás activos tecnológicos que forman parte de la operatividad institucional. Además, permite detectar patrones en la ocurrencia de incidentes, facilitando la implementación de estrategias preventivas y correctivas para minimizar riesgos que puedan comprometer la disponibilidad, integridad y confidencialidad de la información.

Este proceso de monitoreo constante no solo fortalece la capacidad de respuesta ante posibles amenazas, sino que también asegura el cumplimiento de normativas vigentes, como el Esquema Gubernamental de Seguridad de la Información (EGSI), la Ley Orgánica de Protección de Datos Personales (LOPDP) y los estándares internacionales en gestión de seguridad de la información, como la ISO/IEC 27001:2022. La correcta implementación de este informe diario permitirá optimizar la gestión de riesgos tecnológicos, mejorar la toma de decisiones estratégicas y garantizar la continuidad operativa de los servicios digitales de la Prefectura de Cotopaxi, alineándose con las mejores prácticas en ciberseguridad y administración de infraestructura tecnológica.

7.1. Objetivo Del Informe

Proporcionar un registro detallado de los riesgos identificados en la infraestructura tecnológica, evaluando su impacto y estableciendo medidas de mitigación oportunas. Asimismo, busca asegurar el cumplimiento de normativas vigentes como el Esquema Gubernamental de Seguridad de la Información (EGSI), la Ley Orgánica de Protección de Datos Personales (LOPDP) y los estándares internacionales de seguridad, como la ISO/IEC 27001:2022.

7.2. Contenido del Informe Diario de Riesgos

El informe debe contener la siguiente información clave:

7.3. Datos Generales

- Fecha y hora del informe.
- Nombre del responsable de su elaboración.
- Área o sistema tecnológico evaluado.

7.4. Registro de Análisis de Riesgos

- Identificación de nuevos riesgos o vulnerabilidades detectadas.
- Evaluación del impacto de cada riesgo en la operatividad institucional.

- Probabilidad de ocurrencia del riesgo según criterios de análisis.

7.5. Medidas de Mitigación Implementadas

- Controles técnicos y administrativos aplicados para reducir vulnerabilidades.
- Implementación de parches de seguridad o actualización de software/hardware.
- Refuerzo de políticas de acceso y monitoreo de actividades sospechosas.

7.6. Incidentes Reportados y Gestión de Respuesta

- Descripción de incidentes de seguridad detectados.
- Medidas inmediatas tomadas para su contención.
- Evaluación de efectividad de las acciones correctivas.

7.7. Recomendaciones y Acciones Pendientes

- Identificación de mejoras en la infraestructura tecnológica.
- Revisión de políticas de seguridad y actualización de procedimientos.
- Plan de seguimiento para resolver vulnerabilidades críticas.

7.8. Validación y Aprobación

- Nombre y cargo del responsable del informe.
- Firma y visto bueno del supervisor o área encargada.

7.9. Frecuencia y Supervisión

Este informe deberá generarse diariamente, siendo responsabilidad del área de Tecnologías de la Información de la Prefectura de Cotopaxi. Se entregará a las autoridades competentes para su revisión y análisis, asegurando la mejora continua en la gestión de la seguridad de la infraestructura tecnológica.

La elaboración de este informe diario es una herramienta clave para la identificación y mitigación de riesgos en la infraestructura tecnológica institucional. Su aplicación rigurosa garantizará la protección de los sistemas, reduciendo la exposición a amenazas y asegurando la disponibilidad y estabilidad de los servicios digitales de la Prefectura de Cotopaxi.

REGISTRO DE ACCESOS A ÁREAS RESTRINGIDAS

Institución: Prefectura de Cotopaxi

Área Restringida: _____

Responsable del Área: _____

Fecha: _____

DATOS DEL ACCESO

Hora de Ingreso	Hora de Salida	Nombre Completo	Identificación	Cargo	Motivo de Ingreso	Firma del Visitante

NORMAS DE CONTROL

- Solo personal autorizado puede ingresar a áreas restringidas.
- Es obligatorio registrar el acceso en este documento.
- Se verificará la identidad mediante documento de identificación válido.
- El acceso debe estar autorizado por el responsable del área.
- En caso de incidentes, se debe reportar de inmediato al área de seguridad.

PLAN DE ANÁLISIS, IDENTIFICACIÓN Y MITIGACIÓN DE RIESGOS DE INFRAESTRUCTURA TECNOLÓGICA

Institución: Prefectura de Cotopaxi

Área Responsable: _____

Fecha de Elaboración: _____

Responsable del Plan: _____

Periodo de Revisión: ☑ Anual

---

1. PROPÓSITO DEL PLAN

El propósito de este plan es garantizar la seguridad y estabilidad de la infraestructura tecnológica de la Prefectura de Cotopaxi, minimizando riesgos asociados a ciberataques, fallos técnicos, accesos no autorizados y cualquier otra amenaza que pueda comprometer la operatividad institucional. Se establecen estrategias para la identificación, evaluación y mitigación de riesgos, asegurando la continuidad operativa y la protección de los datos institucionales.

---

2. IDENTIFICACIÓN DE ACTIVOS CRÍTICOS

ACTIVO TECNOLÓGICO	UBICACIÓN	RESPONSABLE	NIVEL DE RIESGO
SERVIDORES DE DATOS	Centro de Datos	Administrador de TI	Alto
BASE DE DATOS INSTITUCIONAL	Sala de Servidores	Jefe de Infraestructura	Alto
REDES Y COMUNICACIONES	Edificio Administrativo	Técnico de Redes	Medio
EQUIPOS DE USUARIO FINAL	Diferentes Oficinas	Encargado de Soporte	Bajo

---

3. IDENTIFICACIÓN Y CLASIFICACIÓN DE RIESGOS

RIESGO DETECTADO	ÁREA AFECTADA	PROBABILIDAD	IMPACTO	ESTADO
CIBERATAQUES	Servidores y bases de datos	Alta	Alto	Crítico
PÉRDIDA DE INFORMACIÓN	Bases de Datos	Media	Alto	Controlado
FALLOS DE ENERGÍA	Equipos de Red y Servidores	Alta	Medio	Mitigado
ACCESOS NO AUTORIZADOS	Áreas Restringidas	Media	Alto	Controlado

4. ACCIONES DE MITIGACIÓN Y PREVENCIÓN

RIESGO	ACCIÓN CORRECTIVA / PREVENTIVA	RESPONSABLE	PLAZO DE EJECUCIÓN
CIBERATAQUES	Implementación de Firewall y Monitoreo 24/7	Administrador de Seguridad TI	1 mes
PÉRDIDA DE INFORMACIÓN	Automatización de Respaldos de Datos	Jefe de Infraestructura	15 días
FALLOS DE ENERGÍA	Instalación de UPS y Generadores de Respaldo	Área de Mantenimiento	2 semanas
ACCESOS NO AUTORIZADOS	Refuerzo de Autenticación en Sistemas	Área de Seguridad	1 mes

5. PLAN DE RESPUESTA ANTE INCIDENTES

Etapa	Acción	Responsable
Detección	Identificación del incidente y análisis preliminar	Equipo de Monitoreo
Notificación	Informar a las áreas responsables y activar protocolos	Jefe de Seguridad TI
Contención	Aplicar medidas para minimizar daños	Administrador de Sistemas
Corrección	Implementar soluciones definitivas	Área Técnica
Evaluación	Análisis post-incidente y mejoras	Dirección de Tecnología

6. REVISIÓN Y VALIDACIÓN DEL PLAN

Revisión	Fecha	Responsable	Estado
Primera Evaluación		Director de Tecnología	Pendiente ☐ Completado ☐
Segunda Evaluación		Administrador de Seguridad	Pendiente ☐ Completado ☐
Auditoría Final		Jefe de Infraestructura	Pendiente ☐ Completado ☐

7. FIRMAS Y RESPONSABILIDADES

Elaborado por	Revisado por	Aprobado por
Firma: _____	Firma: _____	Firma: _____

8. NOTAS IMPORTANTES

✓ El plan debe ser revisado periódicamente y actualizado según nuevas amenazas.

✓ Las acciones correctivas deben ejecutarse dentro del plazo establecido.

✓ Todos los responsables deben validar y aprobar el plan en cada revisión.