PLAN DE CONTINGENCIAS INFORMÁTICO

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

PERIODO 2025

Índice de contenidos

1. ANTECEDENTES

En la actualidad, la tecnología juega un papel fundamental en la gestión y operatividad de las instituciones públicas. La Prefectura de Latacunga, al igual que muchas entidades gubernamentales, depende de sus sistemas informáticos para la administración de servicios, la toma de decisiones y la atención a la ciudadanía. Sin embargo, la creciente dependencia de la infraestructura tecnológica también implica una mayor exposición a riesgos como fallos técnicos, ataques cibernéticos, desastres naturales, errores humanos o interrupciones en el suministro eléctrico, los cuales pueden comprometer la continuidad de los servicios y la integridad de la información institucional.

Ante esta realidad, es fundamental la implementación de un Plan de Contingencias Informático (PCI), que permita establecer estrategias y procedimientos para responder eficazmente ante incidentes que afecten la infraestructura tecnológica de la Prefectura. Este plan tiene como objetivo minimizar tiempos de inactividad, mitigar el impacto operativo y garantizar la rápida recuperación de los sistemas críticos, asegurando la prestación continua de los servicios públicos y el resguardo de la información institucional.

El desarrollo de un PCI debe basarse en normas y estándares internacionales de gestión de seguridad informática y continuidad operativa. Directrices como la ISO/IEC 27001 (Gestión de Seguridad de la Información), el NIST SP 800-34 (Guía para la Contingencia de Sistemas de Información) y las buenas prácticas de ITIL proporcionan lineamientos esenciales para establecer un plan efectivo de respuesta ante incidentes. Asimismo, en Ecuador, la Norma Técnica de Seguridad de la Información (NTCI) y la Ley Orgánica de Protección de Datos Personales (LOPDP) obligan a las instituciones públicas a adoptar medidas de seguridad y planes de contingencia que garanticen la protección de la información y la operatividad de los sistemas gubernamentales.

Considerando la importancia de la estabilidad operativa en la Prefectura de Latacunga y su compromiso con la eficiencia en la gestión pública, este documento establece un marco estratégico para el desarrollo e implementación de un Plan de Contingencias Informático, con el fin de fortalecer la capacidad de respuesta ante incidentes, minimizar riesgos y asegurar la continuidad de los servicios a la ciudadanía.

2. GENERALIDADES

El Plan de Contingencias Informático (PCI) de la Prefectura de Latacunga es un instrumento estratégico fundamental para la gestión de la seguridad y continuidad de los sistemas tecnológicos que sustentan la operatividad de la institución. Su propósito es garantizar la estabilidad y disponibilidad de los servicios informáticos, minimizando el impacto de posibles incidentes que puedan comprometer la funcionalidad de la infraestructura digital.

En un entorno donde las amenazas tecnológicas evolucionan constantemente, es crucial contar con un plan estructurado que permita no solo reaccionar ante emergencias, sino también anticiparse a ellas mediante medidas preventivas. Este plan establece un conjunto de lineamientos, procedimientos y estrategias diseñados para abordar cada fase del ciclo de contingencia: prevención, mitigación, respuesta y recuperación.

- **Prevención:** Implementación de controles y medidas de seguridad que reduzcan la probabilidad de incidentes informáticos.
- **Mitigación:** Acciones orientadas a minimizar los daños en caso de que se materialice una amenaza.
- **Respuesta:** Procedimientos operativos para actuar de manera rápida y efectiva ante un incidente, evitando la paralización prolongada de los sistemas.
- **Recuperación:** Estrategias para restablecer la operatividad de los sistemas afectados y normalizar los servicios en el menor tiempo posible.

El PCI abarca desde fallos en hardware y software hasta ataques cibernéticos, errores humanos y desastres naturales que puedan comprometer la infraestructura tecnológica de la institución. Su aplicación no solo protege los sistemas y datos críticos de la Prefectura de Latacunga, sino que también asegura la prestación eficiente de los servicios administrativos y operativos a la ciudadanía, evitando interrupciones que puedan afectar su normal funcionamiento.

2.1. Objetivo

Garantizar la continuidad operativa de los sistemas tecnológicos de la Prefectura de Latacunga a través de la implementación de estrategias integrales, procedimientos estructurados y medidas de respuesta eficientes que permitan mitigar los efectos de cualquier incidente

informático. Este plan tiene como finalidad reducir el impacto de interrupciones tecnológicas provocadas por fallos en la infraestructura, ataques cibernéticos, desastres naturales o errores humanos, asegurando que los servicios digitales permanezcan activos y funcionales.

Para ello, se establecen mecanismos de prevención, detección temprana y recuperación que permitan restablecer la operatividad de los sistemas en el menor tiempo posible, garantizando que la información institucional se mantenga protegida contra accesos no autorizados, pérdidas o alteraciones. Además, el plan busca fortalecer la capacidad de respuesta de la Prefectura mediante la capacitación del personal, la adopción de tecnologías de respaldo y la mejora continua de los protocolos de seguridad, asegurando la resiliencia digital y la prestación eficiente de los servicios a la ciudadanía.

2.2. Conceptos y Definiciones

La Prefectura de Cotopaxi, en su compromiso con la modernización y seguridad de sus sistemas tecnológicos, ha desarrollado un Plan de Contingencias Informático (PCI) que establece estrategias y procedimientos para garantizar la continuidad operativa de sus servicios digitales. Este plan es fundamental para minimizar el impacto de posibles incidentes que puedan comprometer la infraestructura tecnológica, ya sean fallas técnicas, ataques cibernéticos, desastres naturales o errores humanos.

Plan de Contingencias Informático (PCI)

Conjunto de estrategias, procedimientos y medidas diseñadas para garantizar la continuidad operativa de los sistemas tecnológicos ante incidentes imprevistos. Su objetivo es minimizar tiempos de inactividad y proteger la integridad de la información institucional.

Seguridad Física en Infraestructura Tecnológica

Conjunto de controles y mecanismos implementados para proteger los recursos informáticos de la organización contra accesos no autorizados, desastres naturales y sabotajes. Incluye medidas como control de accesos, videovigilancia y monitoreo ambiental.

Medidas de Control de Acceso

Normas y procedimientos que regulan la entrada y manipulación de equipos tecnológicos en áreas sensibles. Pueden incluir autenticación biométrica, tarjetas de acceso, supervisión de visitantes y monitoreo en tiempo real.

Gestión de Riesgos Tecnológicos

Proceso mediante el cual se identifican, evalúan y mitigan amenazas potenciales que pueden afectar la infraestructura informática. Permite anticiparse a fallas y minimizar el impacto de eventos adversos.

Infraestructura Tecnológica

Conjunto de servidores, redes, sistemas de almacenamiento, software y hardware que soportan la operatividad de una institución. Su administración eficiente es clave para garantizar estabilidad y disponibilidad.

Plan de Análisis, Identificación y Mitigación de Riesgos

Documento que establece un enfoque metodológico para detectar vulnerabilidades en la infraestructura tecnológica, clasificarlas por impacto y aplicar estrategias para su reducción.

Matriz de Riesgos

Herramienta utilizada para clasificar y priorizar los riesgos tecnológicos en función de su impacto y probabilidad de ocurrencia, facilitando la toma de decisiones en la mitigación de amenazas.

Seguridad Perimetral y Digital

Conjunto de medidas implementadas para proteger la infraestructura informática contra amenazas cibernéticas, incluyendo firewalls, sistemas de detección de intrusos (IDS/IPS) y cifrado de datos.

Respaldo y Recuperación de Datos

Proceso de copia y almacenamiento seguro de información crítica con el fin de garantizar su recuperación en caso de incidentes como fallos de hardware, ataques cibernéticos o errores humanos.

Auditorías de Seguridad Tecnológica

Revisión periódica de la infraestructura y procedimientos de seguridad informática para evaluar su nivel de protección, detectar vulnerabilidades y proponer mejoras en los controles implementados.

Simulación de Incidentes

Ejercicio práctico en el que se recrean escenarios de fallas tecnológicas para medir la capacidad de respuesta, evaluar protocolos de recuperación y optimizar tiempos de reacción ante emergencias.

Evaluación de Impacto en Infraestructura Tecnológica

Análisis que permite determinar el nivel de afectación que puede generar un incidente sobre los sistemas informáticos y las operaciones institucionales, estableciendo criterios de criticidad.

Continuidad Operativa

Capacidad de una institución para mantener la prestación de sus servicios esenciales a pesar de incidentes o fallos en su infraestructura tecnológica, gracias a la aplicación de planes de contingencia.

Seguridad Informática

Disciplina que abarca la protección de sistemas, redes y datos contra amenazas, garantizando su integridad, disponibilidad y confidencialidad mediante la implementación de medidas técnicas y administrativas.

Actualización y Mejora Continua del PCI

Proceso de revisión y optimización del **Plan de Contingencias Informático**, basado en auditorías, análisis de incidentes previos y avances tecnológicos, con el fin de mantener su efectividad frente a nuevas amenazas.

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

La seguridad física de los recursos informáticos es un componente esencial dentro de la gestión de la seguridad de la información en la Prefectura de Latacunga. Asegurar la protección de la infraestructura tecnológica minimiza riesgos asociados a accesos no autorizados, manipulación indebida de los equipos, fallas ambientales y sabotajes.

El presente documento establece un Plan de Acceso y Medidas de Control de Seguridad Física, el cual detalla los mecanismos y protocolos a implementar para garantizar la protección integral de los recursos informáticos. Este plan tiene un carácter operativo y de actualización

anual, lo que permite su constante revisión y mejora con base en nuevas amenazas y necesidades tecnológicas.

3.1. PLAN DE ACCESO A LOS RECURSOS INFORMÁTICOS

El acceso a los centros de datos, salas de servidores, oficinas de TI y cualquier área con infraestructura crítica debe estar debidamente regulado para evitar incidentes de seguridad. Para ello, se implementan las siguientes medidas de control:

3.1.1. Control de Identificación y Registro

- **Autenticación biométrica y tarjetas de acceso:** Se asignan credenciales personalizadas al personal autorizado, permitiendo su ingreso solo a las áreas asignadas.
- **Registro de ingreso y salida:** Todas las personas que accedan a áreas restringidas deben firmar un registro detallado, indicando hora de entrada, motivo de la visita y persona responsable de su acceso.
- **Acceso basado en perfiles de usuario:** Se asignan permisos de entrada según los roles y funciones de cada colaborador. El acceso a servidores y dispositivos críticos está restringido únicamente al personal de TI autorizado.
- **Supervisión de visitantes:** Toda persona ajena a la institución que requiera acceder a áreas restringidas deberá estar acompañada por un funcionario del área de tecnología.

3.1.2. Protección de Áreas Restringidas

- **Zonificación de acceso:** Se establecen diferentes niveles de acceso dentro de las instalaciones para evitar que personal no autorizado ingrese a áreas de alto riesgo.
- **Implementación de cerraduras electrónicas y códigos de acceso:** Se restringe el acceso a salas de servidores y racks de comunicaciones mediante mecanismos de autenticación avanzados.
- **Bloqueo automático de puertas:** Las áreas con acceso restringido cuentan con un sistema de cierre automático para evitar ingresos accidentales o no autorizados.
- **Póliza de acceso fuera de horario:** Solo personal autorizado podrá acceder a los recursos informáticos fuera del horario laboral, previo registro y autorización formal.

3.2. MEDIDAS DE CONTROL A LA SEGURIDAD FÍSICA

Además de regular el acceso, se implementan controles físicos y ambientales para garantizar la seguridad y el correcto funcionamiento de los equipos informáticos. Estas medidas incluyen:

3.2.1. Monitoreo y Vigilancia

- **Cámaras de videovigilancia (CCTV):** Instalación de cámaras en todas las áreas críticas con grabación las 24 horas y almacenamiento de registros por un período mínimo de 90 días.
- **Sensores de movimiento y alarmas:** Detección de actividad inusual dentro de los espacios protegidos, generando alertas en tiempo real al equipo de seguridad.
- **Supervisión del personal de seguridad:** Rondas de inspección periódicas para verificar la seguridad de las instalaciones.

3.2.2. Protección de Equipos Tecnológicos

- **Uso de gabinetes de seguridad y racks cerrados:** Todo equipo de red (servidores, routers, switches) debe estar protegido dentro de estructuras metálicas con cerraduras de alta seguridad.
- **Control de dispositivos extraíbles:** Restricción del uso de unidades USB, discos duros externos y otros dispositivos de almacenamiento para prevenir filtraciones o ataques malintencionados.
- **Etiquetado y registro de activos tecnológicos:** Cada equipo cuenta con un código de identificación único, permitiendo su rastreo y control en caso de robo o extravío.

3.2.3. Control de Condiciones Ambientales

- **Sistema de climatización para servidores:** Monitoreo constante de temperatura y humedad en salas de equipos críticos para evitar sobrecalentamientos y fallos por condiciones adversas.
- **Sensores de humo y alarmas contra incendios:** Instalación de detectores de incendio con sistemas de extinción automáticos en áreas sensibles.

- **Protección ante fallos eléctricos:** Uso de sistemas de alimentación ininterrumpida (UPS) y plantas eléctricas de respaldo para garantizar el suministro de energía ante cortes inesperados.

3.3. EVALUACIÓN Y ACTUALIZACIÓN DEL PLAN DE SEGURIDAD FÍSICA

Este plan es evaluado y actualizado anualmente, permitiendo adaptarse a nuevas necesidades, amenazas y cambios en la infraestructura tecnológica. Para ello, se realizan las siguientes actividades:

- **Auditorías de seguridad:** Inspecciones periódicas para detectar vulnerabilidades y definir acciones correctivas.
- **Simulacros de incidentes:** Ejercicios prácticos para evaluar la capacidad de respuesta ante emergencias.
- **Capacitación del personal:** Formación continua sobre protocolos de seguridad y concienciación sobre el manejo adecuado de los recursos tecnológicos.
- **Actualización de normativas internas:** Revisión y ajuste de las políticas de acceso y control físico conforme a los cambios en la legislación y estándares internacionales de seguridad.

Con estas acciones, la Prefectura de Latacunga refuerza su compromiso con la seguridad informática y la continuidad operativa, asegurando que su infraestructura tecnológica se mantenga protegida frente a amenazas físicas y digitales.

4. INFORME TÉCNICO EN EL ÁMBITO DE SU COMPETENCIA

El presente Informe Técnico tiene como objetivo documentar de manera detallada las actividades ejecutadas dentro del ámbito de gestión tecnológica e informática en la Prefectura de Latacunga. Su propósito es registrar de forma sistemática las incidencias detectadas, las acciones correctivas y preventivas aplicadas, así como las medidas implementadas para garantizar el correcto funcionamiento de los sistemas y la continuidad operativa de los servicios institucionales.

Dado que el informe tiene una frecuencia diaria y de carácter ordinario, se convierte en un instrumento clave para la toma de decisiones estratégicas, la optimización de procesos y la prevención de incidentes que puedan afectar el desempeño tecnológico de la entidad.

Este documento es elaborado por el equipo de gestión informática y es revisado por las instancias responsables con el fin de evaluar la evolución de los indicadores de rendimiento tecnológico, detectar patrones de fallos recurrentes y establecer planes de mejora en la administración de los recursos digitales.

4.1. ALCANCE

El presente informe cubre las siguientes áreas dentro del ámbito tecnológico de la Prefectura de Latacunga:

- **Gestión de infraestructura tecnológica:** Administración y monitoreo de servidores, almacenamiento y sistemas de respaldo.
- **Soporte técnico y atención a usuarios:** Resolución de incidencias relacionadas con equipos de cómputo, software y accesos a sistemas.
- **Administración de redes y conectividad:** Gestión de redes LAN, Wi-Fi y servicios de telecomunicaciones.
- **Seguridad informática:** Control de accesos, gestión de riesgos cibernéticos y aplicación de protocolos de protección de datos.
- **Mantenimiento preventivo y correctivo:** Revisión, actualización y reparación de equipos y sistemas de información.
- **Monitoreo y optimización de plataformas digitales:** Evaluación del rendimiento de aplicaciones institucionales y sistemas operativos.

El informe abarca actividades realizadas tanto en el ámbito interno, relacionado con la infraestructura y sistemas de la Prefectura, como en el ámbito externo, cuando se requiera soporte o coordinación con proveedores tecnológicos o entidades gubernamentales.

4.2. CONTENIDO DEL INFORME TÉCNICO

El informe se estructura en los siguientes apartados:

4.2.1. Actividades Realizadas

Se describen las tareas ejecutadas durante la jornada, clasificadas según su naturaleza:

- **Atención y soporte técnico:**

- ✓ Registro y resolución de solicitudes de asistencia de los diferentes departamentos.
- ✓ Diagnóstico y solución de problemas de hardware y software en estaciones de trabajo.
- ✓ Configuración de equipos y periféricos para su correcta operatividad.
- ✓ Restauración de sistemas y recuperación de información en caso de incidentes menores.

- **Administración de sistemas y servidores:**
  - ✓ Supervisión del estado de los servidores y análisis de métricas de rendimiento.
  - ✓ Implementación de parches y actualizaciones de seguridad.
  - ✓ Gestión de bases de datos, respaldo y optimización del almacenamiento.
  - ✓ Monitoreo de procesos en ejecución y carga de trabajo en servidores críticos.
- **Gestión de redes y telecomunicaciones:**
  - ✓ Revisión de conectividad en la red interna y detección de fallos de comunicación.
  - ✓ Configuración de routers, switches y puntos de acceso Wi-Fi.
  - ✓ Evaluación del tráfico de datos y mitigación de cuellos de botella en la infraestructura de red.
- **Seguridad informática:**
  - ✓ Aplicación de controles de acceso y auditoría de actividad en los sistemas informáticos.
  - ✓ Verificación de integridad de archivos y detección de posibles amenazas cibernéticas.
  - ✓ Monitoreo de registros de eventos para identificar comportamientos sospechosos.
  - ✓ Aplicación de protocolos de cifrado y resguardo de información confidencial.
- **Mantenimiento preventivo y correctivo:**

- ✓ Diagnóstico de estado de equipos y planificación de mantenimientos rutinarios.
- ✓ Reemplazo o reparación de componentes de hardware defectuosos.
- ✓ Limpieza física y lógica de equipos de cómputo y dispositivos periféricos.

4.3. INCIDENCIAS Y PROBLEMAS DETECTADOS

Se detallan las incidencias registradas, clasificándolas según su impacto en la operatividad de la institución:

- **Incidentes menores:** Problemas que no afectan la continuidad de los servicios y son resueltos de manera inmediata.
- **Incidentes críticos:** Fallas que generan interrupciones en los sistemas institucionales, requiriendo una respuesta prioritaria.
- **Vulnerabilidades detectadas:** Posibles brechas de seguridad que deben ser mitigadas para evitar futuros incidentes.

Para cada incidencia se documenta:

- **Descripción del problema** (sistemas afectados, tipo de error, impacto en los usuarios).
- **Análisis de causa raíz** (posibles razones del fallo y factores que contribuyeron al incidente).
- **Acciones correctivas implementadas** (medidas tomadas para solucionar la falla y evitar su repetición).
- **Tiempo de resolución** y nivel de efectividad de la solución aplicada.

4.4. MEDIDAS IMPLEMENTADAS

Se detallan las estrategias y soluciones aplicadas para mejorar la seguridad y estabilidad de los sistemas. Estas incluyen:

- **Mejoras en la infraestructura tecnológica:** Implementación de nuevos equipos o reconfiguración de servidores.
- **Refuerzo de políticas de seguridad:** Aplicación de medidas más estrictas en el control de accesos y autenticación de usuarios.

- **Optimización de redes y sistemas:** Configuración avanzada para mejorar el rendimiento de los servicios tecnológicos.
- **Respaldo y recuperación de datos:** Implementación de copias de seguridad y pruebas de restauración de información crítica.
- **Actualización de software y licencias:** Revisión y renovación de aplicaciones para garantizar compatibilidad y estabilidad operativa.

4.5. ANÁLISIS DE RIESGOS Y RECOMENDACIONES

Se realiza un análisis de riesgos potenciales basado en las observaciones registradas durante la jornada. Se identifican amenazas internas y externas que podrían afectar la infraestructura tecnológica y se proponen recomendaciones para su mitigación.

4.5.1. Ejemplos de riesgos detectados:

- Fallas recurrentes en equipos obsoletos que requieren reemplazo.
- Intentos de acceso no autorizado a la red institucional.
- Deficiencias en los procedimientos de respaldo y recuperación de datos.
- Uso inadecuado de software no autorizado por parte de los usuarios.

4.5.2. Recomendaciones:

- Adquirir y renovar hardware crítico para evitar fallos operativos.
- Implementar autenticación multifactor en accesos a sistemas sensibles.
- Optimizar la gestión de copias de seguridad con soluciones automatizadas.
- Capacitar al personal en buenas prácticas de ciberseguridad y manejo de la infraestructura informática.

El informe técnico diario permite documentar de manera precisa las actividades realizadas en el área de tecnología, proporcionando una visión detallada del estado de la infraestructura informática y de los posibles riesgos a mitigar. Gracias a este registro continuo, la Prefectura de Latacunga podrá tomar decisiones fundamentadas para fortalecer su capacidad de respuesta ante incidentes, mejorar la eficiencia de sus procesos tecnológicos y garantizar la disponibilidad de los servicios digitales que ofrece a la ciudadanía.

La información recopilada en estos informes servirá como base para la planificación estratégica en materia de TI, asegurando una gestión proactiva en la administración de los recursos informáticos.

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

La infraestructura tecnológica de la Prefectura de Latacunga es el pilar sobre el cual se soportan sus servicios digitales, sistemas de información, redes de comunicación y almacenamiento de datos. Sin una adecuada gestión de riesgos, estos activos pueden verse comprometidos por fallas técnicas, ciberataques, desastres naturales o errores humanos, afectando la continuidad operativa de la institución.

Ante este panorama, es fundamental contar con un Plan de Análisis, Identificación y Mitigación de Riesgos de Infraestructura Tecnológica, el cual tiene como objetivo establecer un marco metodológico para detectar, evaluar y mitigar posibles amenazas que puedan afectar la estabilidad y seguridad de los sistemas informáticos.

Este plan es de carácter operativo y se actualiza anualmente, permitiendo a la Prefectura de Latacunga fortalecer su capacidad de prevención y respuesta ante incidentes, garantizando la disponibilidad de sus servicios tecnológicos y la integridad de la información institucional.

5.1. ALCANCE

Este plan abarca la identificación y gestión de riesgos en los siguientes componentes de la infraestructura tecnológica:

- **Infraestructura de servidores y almacenamiento:** Riesgos asociados a fallas en servidores físicos, virtualización y sistemas de respaldo de datos.
- **Redes y telecomunicaciones:** Evaluación de vulnerabilidades en redes cableadas, inalámbricas y enlaces con proveedores de servicios.
- **Sistemas de seguridad informática:** Protección ante ataques cibernéticos, accesos no autorizados y brechas de seguridad en la red.
- **Equipos de usuario y estaciones de trabajo:** Mantenimiento y control sobre los equipos informáticos utilizados por el personal.

- **Sistemas de respaldo y recuperación de datos:** Evaluación de planes de contingencia y estrategias de restauración ante incidentes.
- **Factores ambientales y físicos:** Identificación de riesgos por incendios, cortes eléctricos, temperatura y humedad que puedan afectar los equipos.

5.2. METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS

Para garantizar una evaluación efectiva, se adopta una metodología basada en cuatro fases fundamentales:

5.2.1. Identificación de Riesgos

Se realiza un levantamiento de información para detectar posibles amenazas que puedan afectar la infraestructura tecnológica, clasificándolas en:

- **Riesgos físicos:** Desastres naturales, incendios, fallas eléctricas, humedad excesiva.
- **Riesgos técnicos:** Fallas en hardware, obsolescencia de equipos, incompatibilidades de software.
- **Riesgos humanos:** Errores operativos, accesos no autorizados, falta de capacitación en seguridad informática.
- **Riesgos cibernéticos:** Malware, ransomware, intentos de intrusión en la red, filtración de datos.

5.2.2. Evaluación y Clasificación de Riesgos

Cada riesgo identificado es evaluado en función de su probabilidad de ocurrencia y el impacto que podría generar en la institución. Se utilizan matrices de riesgo para clasificar y priorizar los eventos más críticos:

Tabla 1

Evaluación y Clasificación de Riesgos

Riesgo	Impacto (Bajo, Medio, Alto)	Probabilidad (Baja, Media, Alta)	Prioridad
Falla en servidores críticos	Alto	Alta	Urgente
Ataques de ransomware	Alto	Media	Crítico

Interrupción de red institucional	Medio	Alta	Importante
Accesos no autorizados	Alto	Baja	Moderado

5.2.3. Estrategias de Mitigación de Riesgos

Para cada riesgo identificado, se establecen medidas preventivas y correctivas que permitan minimizar su impacto:

- **Seguridad perimetral y digital:** Implementación de firewalls, sistemas de detección de intrusos (IDS/IPS) y monitoreo en tiempo real.
- **Mantenimiento preventivo de infraestructura:** Renovación y actualización de hardware y software para reducir el riesgo de fallas técnicas.
- **Gestión de respaldos y recuperación de datos:** Implementación de copias de seguridad automatizadas y pruebas de restauración periódicas.
- **Capacitación y sensibilización del personal:** Formación en buenas prácticas de ciberseguridad y procedimientos ante incidentes tecnológicos.
- **Refuerzo de medidas de seguridad física:** Protección de servidores y equipos críticos mediante controles de acceso biométricos, vigilancia CCTV y sensores ambientales.
- **Simulacros y pruebas de continuidad operativa:** Ejecución de ejercicios para medir tiempos de respuesta y validar la efectividad de los planes de contingencia.

5.2.4. Plan de Respuesta ante Riesgos Críticos

Para los riesgos de **mayor impacto**, se definen protocolos específicos de respuesta, los cuales incluyen:

a) **Detección y notificación del incidente** al equipo de TI y autoridades responsables.

b) **Activación de medidas de contención** para evitar la propagación del problema.

c) **Ejecución de procedimientos de recuperación** para restablecer los servicios en el menor tiempo posible.

d) **Análisis post-incidente y documentación** para fortalecer estrategias de prevención futura.

5.3. EVALUACIÓN Y ACTUALIZACIÓN DEL PLAN

El presente plan se revisa y actualiza **anualmente**, garantizando su alineación con las mejores prácticas en seguridad informática y gestión de riesgos. Como parte de este proceso, se realizan:

- **Auditorías internas de seguridad tecnológica** para evaluar la efectividad de las estrategias de mitigación.
- **Revisión de incidentes ocurridos en el período anterior**, identificando patrones y oportunidades de mejora.
- **Ejercicios de simulación y análisis de impacto**, evaluando tiempos de respuesta ante eventos críticos.
- **Actualización de protocolos y herramientas de seguridad**, incorporando soluciones tecnológicas innovadoras.

El Plan de Análisis, Identificación y Mitigación de Riesgos de Infraestructura Tecnológica es un instrumento clave para la gestión de la seguridad tecnológica en la Prefectura de Latacunga. Su correcta aplicación permite anticipar amenazas, minimizar vulnerabilidades y garantizar la continuidad operativa de los sistemas informáticos.

A través de este plan, la institución fortalece su capacidad de respuesta ante incidentes, asegurando que sus plataformas digitales y redes operen bajo altos estándares de seguridad y disponibilidad, protegiendo la información institucional y los servicios ofrecidos a la ciudadanía.

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

La infraestructura tecnológica de la Prefectura de Latacunga es un componente crítico para la operatividad de sus sistemas y servicios. Sin una adecuada gestión de riesgos, la estabilidad, disponibilidad y seguridad de los recursos tecnológicos pueden verse comprometidas por amenazas internas y externas.

El presente Plan de Análisis, Identificación y Mitigación de Riesgos de Infraestructura Tecnológica tiene como propósito establecer un marco estructurado para detectar, evaluar y

mitigar posibles amenazas que puedan afectar la infraestructura tecnológica institucional. Este plan es de carácter operativo y se actualiza anualmente, garantizando su alineación con las mejores prácticas de seguridad informática y continuidad operativa.

6.1. ALCANCE

Este plan abarca el análisis y gestión de riesgos en las siguientes áreas de infraestructura tecnológica:

- **Infraestructura de servidores y almacenamiento:** Gestión de riesgos en servidores físicos, virtuales y sistemas de almacenamiento de datos.
- **Redes y telecomunicaciones:** Evaluación de vulnerabilidades en redes LAN, Wi-Fi, conexiones de fibra óptica y enlaces con proveedores de servicio.
- **Sistemas de seguridad informática:** Protección contra ataques cibernéticos, accesos no autorizados y fuga de información.
- **Equipos de usuario y estaciones de trabajo:** Mantenimiento de equipos de cómputo, dispositivos móviles y terminales de acceso.
- **Sistemas de respaldo y recuperación de datos:** Evaluación de estrategias de respaldo y tiempo de restauración en caso de incidentes.
- **Factores ambientales y físicos:** Identificación de riesgos por incendios, cortes eléctricos, humedad, temperatura y desastres naturales.

6.2. METODOLOGÍA DE ANÁLISIS DE RIESGOS

El análisis de riesgos en infraestructura tecnológica se lleva a cabo en **cuatro fases fundamentales:**

6.2.1. Identificación de Riesgos

Se realiza un diagnóstico exhaustivo para detectar amenazas potenciales que puedan afectar los sistemas tecnológicos. Las categorías de riesgos incluyen:

- **Riesgos físicos:** Incendios, inundaciones, cortes eléctricos, sabotajes.
- **Riesgos técnicos:** Fallos en servidores, sobrecargas de red, vulnerabilidades de software, obsolescencia de hardware.

- **Riesgos humanos:** Errores operativos, accesos no autorizados, negligencia en el manejo de datos.
- **Riesgos cibernéticos:** Ataques de malware, ransomware, intrusiones en la red, robo de credenciales.

6.2.2. Evaluación y Clasificación de Riesgos

Cada riesgo identificado es evaluado y clasificado según su nivel de impacto y probabilidad de ocurrencia. Se utilizan matrices de riesgo para priorizar los riesgos más críticos y enfocar esfuerzos en su mitigación.

Tabla 2

Evaluación y Clasificación de Riesgos

Riesgo	Impacto (Bajo, Medio, Alto)	Probabilidad (Baja, Media, Alta)	Clasificación de Prioridad
Falla en servidores críticos	Alto	Alta	Urgente
Ataques de ransomware	Alto	Media	Crítico
Interrupción de red	Medio	Alta	Importante
Accesos no autorizados	Alto	Baja	Moderado

6.2.3. Estrategias de Mitigación de Riesgos

Con base en la clasificación de los riesgos, se definen estrategias específicas para su mitigación, entre ellas:

- **Fortalecimiento de la seguridad perimetral y digital** mediante la implementación de firewalls, IDS/IPS y monitoreo en tiempo real.
- **Actualización y mantenimiento preventivo** de hardware y software para reducir el riesgo de fallos técnicos y vulnerabilidades.
- **Respaldo y redundancia de información** a través de copias de seguridad periódicas almacenadas en ubicaciones seguras.
- **Capacitación del personal** en buenas prácticas de ciberseguridad y protocolos de respuesta ante incidentes.

- **Mejoras en infraestructura física**, incluyendo sistemas de climatización para servidores, protección contra incendios y estabilizadores eléctricos.
- **Simulacros de recuperación ante desastres** para evaluar tiempos de respuesta y garantizar la efectividad de los planes de contingencia.

6.2.4. Plan de Respuesta ante Riesgos Críticos

Para los riesgos de mayor impacto, se establecen protocolos de respuesta que incluyen:

- **Acciones inmediatas** en caso de incidentes tecnológicos graves.
- **Procedimientos de contención y mitigación** para evitar la propagación del problema.
- **Activación de planes de contingencia** para mantener la operatividad institucional.
- **Evaluación post-incidente** para mejorar la respuesta en futuros eventos similares.

6.3. EVALUACIÓN Y ACTUALIZACIÓN DEL PLAN

Este plan es revisado anualmente para garantizar su efectividad y alineación con los avances tecnológicos y nuevas amenazas emergentes. Para ello, se realizan las siguientes actividades:

- **Auditorías de seguridad y revisiones técnicas** de la infraestructura informática.
- **Análisis de incidentes previos**, identificando patrones y áreas de mejora.
- **Simulaciones de ataques y fallas técnicas** para evaluar la capacidad de respuesta.
- **Ajuste de estrategias de mitigación** según las lecciones aprendidas.

El Plan de Análisis, Identificación y Mitigación de Riesgos de Infraestructura Tecnológica es una herramienta esencial para proteger la infraestructura digital de la Prefectura de Latacunga. Su correcta implementación permite anticipar amenazas, reducir vulnerabilidades y garantizar la continuidad operativa de los sistemas institucionales, minimizando los impactos en la prestación de servicios a la ciudadanía.

Este plan refuerza la resiliencia tecnológica de la institución, asegurando que sus plataformas digitales operen con altos estándares de seguridad y disponibilidad, alineándose con las mejores prácticas de gestión de riesgos y ciberseguridad.