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.