## CURADURÍA URBANA PRIMERA DE SINCELEJO

Sucre - Colombia

# ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

## VIGENCIA 2025

*Basado en ISO/IEC 27005:2018 - Gestión de Riesgos de Seguridad de la Información y Guía de Gestión de Riesgos del MSPI - MinTIC*

www.curaduriaprimerasincelejo.com.co

Sincelejo, Enero 2025

# CONTROL DE VERSIONES

| VERSIÓN | FECHA | DESCRIPCIÓN | ELABORADO POR |
|---|---|---|---|
| 1.0 | [DD/MM/2025] | Versión inicial del Análisis de Riesgos | [Responsable] |

# TABLA DE CONTENIDO

# 1. INTRODUCCIÓN

El presente documento establece el Análisis de Riesgos de Seguridad de la Información de la Curaduría Urbana Primera de Sincelejo, como parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) y en cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC.

La gestión de riesgos permite identificar, analizar, evaluar y tratar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de los activos de información, permitiendo tomar decisiones informadas sobre los controles necesarios para proteger la información.

# 2. OBJETIVO

Identificar, analizar, evaluar y establecer el tratamiento de los riesgos de seguridad de la información que puedan afectar los activos de información de la Curaduría Urbana Primera de Sincelejo, con el fin de implementar controles que minimicen su probabilidad de ocurrencia y/o su impacto.

# 3. ALCANCE

Este análisis de riesgos aplica a todos los activos de información identificados en el Registro de Activos de Información de la Curaduría, incluyendo:

- Información en formato físico y digital.
- Sistemas de información y aplicaciones.
- Infraestructura tecnológica (hardware, redes, comunicaciones).
- Instalaciones físicas.
- Personal que procesa información.

# 4. METODOLOGÍA DE GESTIÓN DE RIESGOS

La metodología adoptada se basa en la norma ISO/IEC 27005:2018 y la Guía de Gestión de Riesgos del MSPI del MinTIC, siguiendo las siguientes fases:

## 4.1 Fases del Proceso

1. Establecimiento del contexto: Definir el alcance, criterios y metodología.
2. Identificación de riesgos: Identificar activos, amenazas, vulnerabilidades y controles existentes.
3. Análisis de riesgos: Estimar la probabilidad e impacto de cada riesgo.
4. Evaluación de riesgos: Comparar con criterios de aceptación y priorizar.
5. Tratamiento de riesgos: Seleccionar opciones y definir controles.
6. Monitoreo y revisión: Seguimiento continuo y actualización.

## 4.2 Criterios de Valoración - Probabilidad

| VALOR | NIVEL | DESCRIPCIÓN |
|---|---|---|
| **1** | Muy Baja | Puede ocurrir excepcionalmente (menos de 1 vez cada 5 años) |
| **2** | Baja | Puede ocurrir ocasionalmente (1 vez cada 2-5 años) |
| **3** | Media | Puede ocurrir en algún momento (1 vez al año) |
| **4** | Alta | Probablemente ocurra (varias veces al año) |
| **5** | Muy Alta | Se espera que ocurra frecuentemente (mensual o más) |

## 4.3 Criterios de Valoración - Impacto

| VALOR | NIVEL | DESCRIPCIÓN |
|---|---|---|
| **1** | Insignificante | No afecta la operación. Pérdida mínima o nula. |
| **2** | Menor | Afectación menor que se resuelve internamente sin impacto en usuarios. |
| **3** | Moderado | Interrupción parcial del servicio. Requiere esfuerzo para recuperación. |
| **4** | Mayor | Interrupción significativa. Afecta usuarios y puede generar sanciones. |
| **5** | Catastrófico | Interrupción total. Pérdida crítica de información. Sanciones graves. |

# 5. CONTEXTO ORGANIZACIONAL

## 5.1 Descripción de la Entidad

La Curaduría Urbana Primera de Sincelejo es un particular que ejerce función pública, encargada de estudiar, tramitar y expedir licencias urbanísticas en el municipio de Sincelejo, Sucre. Como sujeto obligado por la Ley 1712 de 2014, debe garantizar la transparencia, acceso a la información pública y protección de datos personales.

## 5.2 Procesos Críticos

- Radicación y gestión de solicitudes de licencias urbanísticas.
- Estudio técnico y jurídico de proyectos.
- Expedición de licencias (construcción, urbanización, subdivisión, parcelación).
- Notificación de actos administrativos.
- Gestión documental y archivo.
- Atención al ciudadano y PQRSD.

# 6. IDENTIFICACIÓN DE ACTIVOS

Los activos de información se clasifican según su tipo y criticidad:

| ID | TIPO | ACTIVO | CONF. | CRITIC. |
|---|---|---|---|---|
| A01 | Información | Expedientes de licencias urbanísticas | CLASIF. | ALTA |
| A02 | Información | Planos arquitectónicos y urbanísticos | CLASIF. | ALTA |
| A03 | Información | Base de datos de solicitantes | CLASIF. | ALTA |
| A04 | Sistema | Sitio web institucional | PÚBLICA | ALTA |
| A05 | Sistema | Correo electrónico institucional | CLASIF. | ALTA |
| A06 | Hardware | Servidor de archivos | N/A | CRÍTICA |
| A07 | Hardware | Equipos de cómputo (estaciones de trabajo) | N/A | MEDIA |
| A08 | Red | Conexión a Internet | N/A | ALTA |
| A09 | Instalaciones | Sede física de la Curaduría | N/A | ALTA |
| A10 | Personal | Personal técnico y administrativo | N/A | ALTA |

# 7. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

## 7.1 Catálogo de Amenazas

| ID | CATEGORÍA | AMENAZA | ACTIVOS AFECTADOS |
|---|---|---|---|
| AM01 | Malware | Infección por ransomware o virus | A04, A05, A06, A07 |
| AM02 | Acceso no autorizado | Intrusión a sistemas o redes | A04, A05, A06, A08 |
| AM03 | Ingeniería social | Phishing, suplantación de identidad | A05, A10 |
| AM04 | Falla técnica | Daño de hardware (disco duro, servidor) | A06, A07 |
| AM05 | Falla de servicios | Interrupción de energía eléctrica | A06, A07, A08, A09 |
| AM06 | Falla de servicios | Caída del servicio de internet | A04, A05, A08 |
| AM07 | Desastre natural | Inundación, terremoto, incendio | Todos los activos físicos |
| AM08 | Error humano | Eliminación accidental de información | A01, A02, A03 |
| AM09 | Fuga de información | Divulgación no autorizada de datos | A01, A02, A03 |
| AM10 | Ataque web | Defacement, DDoS, inyección SQL | A04 |

## 7.2 Vulnerabilidades Identificadas

| ID | VULNERABILIDAD | AMENAZA RELACIONADA |
|---|---|---|
| V01 | Falta de capacitación en seguridad al personal | AM03, AM08, AM09 |
| V02 | Contraseñas débiles o compartidas | AM02, AM03 |
| V03 | Software desactualizado (sin parches de seguridad) | AM01, AM02, AM10 |
| V04 | Ausencia de respaldos periódicos o sin verificar | AM01, AM04, AM07, AM08 |
| V05 | Falta de UPS o generador eléctrico | AM05 |
| V06 | Sin enlace de internet de respaldo | AM06 |
| V07 | Configuración insegura del sitio web | AM02, AM10 |
| V08 | Sin control de acceso físico adecuado | AM07, AM09 |

# 8. ANÁLISIS Y VALORACIÓN DE RIESGOS

## 8.1 Matriz de Calor - Niveles de Riesgo

El nivel de riesgo se calcula multiplicando la Probabilidad por el Impacto:

| PROB \ IMPACTO | 1-Insignif. | 2-Menor | 3-Moderado | 4-Mayor |
|---|---|---|---|---|
| **4-Alta** | **4** | **8** | **12** | **16** |
| **3-Media** | **3** | **6** | **9** | **12** |
| **2-Baja** | **2** | **4** | **6** | **8** |
| **1-Muy Baja** | **1** | **2** | **3** | **4** |

## 8.2 Criterios de Aceptación del Riesgo

| NIVEL | RANGO | TRATAMIENTO REQUERIDO |
|---|---|---|
| **BAJO** | 1 - 4 | Aceptar el riesgo. Monitoreo periódico. |
| **MEDIO** | 5 - 9 | Implementar controles. Revisar periódicamente. |
| **ALTO** | 10 - 12 | Acción inmediata requerida. Plan de tratamiento prioritario. |
| **CRÍTICO** | 13 - 20 | Acción urgente. Escalar a la dirección. Controles inmediatos. |

# 9. MATRIZ DE RIESGOS

| ID | RIESGO | ACTIVO | PROB | IMP | NIVEL | ZONA | TRATAMIENTO |
|---|---|---|---|---|---|---|---|
| **R01** | Pérdida de información por ransomware | Expedientes, servidor | 3 | 4 | **12** | **ALTO** | Mitigar |
| **R02** | Acceso no autorizado a expedientes | Expedientes, BD | 3 | 4 | **12** | **ALTO** | Mitigar |
| **R03** | Caída del sitio web institucional | Sitio web | 3 | 3 | **9** | **MEDIO** | Mitigar |
| **R04** | Robo de credenciales por phishing | Correo, personal | 4 | 3 | **12** | **ALTO** | Mitigar |
| **R05** | Pérdida de información por falla de disco | Servidor | 2 | 4 | **8** | **MEDIO** | Mitigar |
| **R06** | Interrupción por corte de energía | Equipos, servidor | 3 | 3 | **9** | **MEDIO** | Mitigar |
| **R07** | Fuga de datos personales | BD solicitantes | 2 | 4 | **8** | **MEDIO** | Mitigar |
| **R08** | Eliminación accidental de expedientes | Expedientes | 3 | 4 | **12** | **ALTO** | Mitigar |
| **R09** | Defacement del sitio web | Sitio web | 2 | 3 | **6** | **MEDIO** | Mitigar |
| **R10** | Daño físico por desastre natural | Instalaciones | 1 | 5 | **5** | **MEDIO** | Transferir |

# 10. PLAN DE TRATAMIENTO DE RIESGOS

| ID | RIESGO | CONTROL / ACCIÓN | RESPONSABLE | FECHA LÍMITE |
|---|---|---|---|---|
| **R01** | Ransomware | Implementar antivirus/antimalware, backups diarios, capacitación | Resp. Seguridad | Mar 2025 |
| **R02** | Acceso no autorizado | Control de acceso por roles, política de contraseñas, logs de auditoría | Resp. Seguridad | Feb 2025 |
| **R03** | Caída sitio web | Hosting con alta disponibilidad, monitoreo, backup del sitio | Webmaster | Feb 2025 |
| **R04** | Phishing | Capacitación al personal, filtros antispam, MFA en correo | Resp. Seguridad | Mar 2025 |
| **R05** | Falla de disco | Servidor con RAID, backups en nube, monitoreo de salud del disco | Soporte TI | Feb 2025 |
| **R06** | Corte de energía | UPS para equipos críticos, procedimiento de apagado seguro | Área Admin. | Abr 2025 |
| **R07** | Fuga de datos | Clasificación de información, política de datos, cifrado | Resp. Seguridad | May 2025 |
| **R08** | Eliminación accidental | Backups con versionado, papelera de reciclaje, permisos restrictivos | Soporte TI | Mar 2025 |
| **R09** | Defacement web | WAF, actualizaciones de CMS, hardening del servidor | Webmaster | Mar 2025 |
| **R10** | Desastre natural | Seguro contra siniestros, backup externo, BCP | Curador Urbano | Jun 2025 |

# 11. MONITOREO Y REVISIÓN

## 11.1 Frecuencia de Revisión

| ACTIVIDAD | FRECUENCIA | RESPONSABLE |
|---|---|---|
| Revisión de controles implementados | Trimestral | Responsable de Seguridad |
| Actualización de la matriz de riesgos | Semestral | Responsable de Seguridad |
| Análisis de nuevos riesgos | Ante cambios significativos | Responsable de Seguridad |
| Revisión completa del documento | Anual | Curador Urbano |
| Reporte de estado de riesgos | Trimestral | Responsable de Seguridad |

## 11.2 Indicadores de Gestión de Riesgos

| INDICADOR | FÓRMULA / MEDICIÓN | META |
|---|---|---|
| Riesgos en zona alta/crítica | Cantidad de riesgos con nivel ≥ 10 | ≤ 2 |
| Controles implementados | (Controles implementados / Controles planificados) × 100 | ≥ 90% |
| Incidentes de seguridad | Número de incidentes materializados | ≤ 2/año |
| Efectividad de controles | Incidentes prevenidos / Total incidentes detectados | ≥ 80% |

---

**URL de Publicación:** https://curaduriaprimerasincelejo.com.co/transparencia/seguridad-digital/analisis-riesgos