POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Sistema ServiCiudadConectada

---

1. INFORMACIÓN GENERAL

1.1 Propósito

Esta política establece el marco de seguridad de la información para el sistema ServiCiudadConectada, garantizando la confidencialidad, integridad y disponibilidad de los datos ciudadanos y servicios municipales.

1.2 Alcance

Aplica a todos los componentes del sistema ServiCiudadConectada, incluyendo:

- Plataforma digital de servicios ciudadanos
- Bases de datos de información personal y municipal
- Sistemas de autenticación y autorización
- Interfaces de comunicación con entidades externas
- Personal técnico y administrativo

1.3 Objetivos

- Proteger la información personal de los ciudadanos
- Garantizar la continuidad de los servicios municipales
- Cumplir con normativas de protección de datos
- Establecer controles de acceso efectivos
- Implementar medidas de prevención y respuesta a incidentes

---

2. MARCO NORMATIVO

2.1 Normativas Aplicables

- Ley 1581 de 2012 (Protección de Datos Personales - Colombia)
- Decreto 1377 de 2013 (Reglamentario de la Ley 1581)
- ISO/IEC 27001:2013 (Sistemas de Gestión de Seguridad de la Información)
- NIST Cybersecurity Framework
- Ley de Gobierno Digital (Decreto 1008 de 2018)

2.2 Principios de Seguridad

- **Confidencialidad**: Acceso restringido a información autorizada
- **Integridad**: Protección contra modificaciones no autorizadas
- **Disponibilidad**: Acceso oportuno a servicios e información
- **Autenticidad**: Verificación de identidad de usuarios y sistemas
- **No repudio**: Garantía de acciones realizadas en el sistema

---

3. CLASIFICACIÓN DE LA INFORMACIÓN

3.1 Niveles de Clasificación

3.1.1 CRÍTICA

- Datos biométricos de ciudadanos
- Información financiera y tributaria
- Datos de seguridad nacional
- **Controles**: Cifrado AES-256, acceso multifactor, auditoría completa

3.1.2 SENSIBLE

- Información personal identificable (PII)
- Datos de salud y educación
- Información de servicios sociales
- **Controles**: Cifrado en tránsito y reposo, logs de acceso, autorización por roles

3.1.3 INTERNA

- Información operativa municipal
- Datos estadísticos anonimizados
- Configuraciones de sistema
- **Controles**: Autenticación básica, controles de acceso por departamento

3.1.4 PÚBLICA

- Información de servicios municipales
- Noticias y comunicados oficiales
- Datos abiertos gubernamentales
- **Controles**: Validación de integridad, control de modificaciones

---

4. CONTROLES DE ACCESO

4.1 Gestión de Identidades

- Registro único de usuarios con validación de identidad
- Asignación de roles basada en principio de menor privilegio
- Revisión periódica de cuentas de usuario (trimestral)
- Desactivación automática de cuentas inactivas (90 días)

4.2 Autenticación

- **Ciudadanos**: Autenticación multifactor (SMS/App + contraseña)
- **Funcionarios**: Autenticación biométrica + tarjeta inteligente
- **Administradores**: Autenticación multifactor + certificados digitales
- Políticas de contraseñas robustas (mínimo 12 caracteres, caracteres especiales)

4.3 Autorización

- Modelo de control de acceso basado en roles (RBAC)
- Segregación de funciones críticas
- Aprobación dual para operaciones sensibles
- Registro de todas las actividades de acceso

---

5. SEGURIDAD TÉCNICA

5.1 Protección de Datos

- Cifrado AES-256 para datos en reposo
- TLS 1.3 para datos en tránsito
- Tokenización de datos sensibles
- Anonimización para análisis estadísticos

5.2 Seguridad de Red

- Firewall de nueva generación con inspección profunda
- Segmentación de red por zonas de seguridad
- Sistema de detección y prevención de intrusiones (IDS/IPS)
- VPN para acceso remoto administrativo

5.3 Seguridad de Aplicaciones

- Desarrollo seguro siguiendo OWASP Top 10
- Pruebas de penetración semestrales
- Análisis estático y dinámico de código
- Gestión segura de APIs con OAuth 2.0/OpenID Connect

5.4 Respaldo y Recuperación

- Respaldos automatizados diarios con cifrado
- Respaldos geográficamente distribuidos
- Pruebas de recuperación trimestrales
- RTO (Recovery Time Objective): 4 horas
- RPO (Recovery Point Objective): 1 hora

---

6. GESTIÓN DE INCIDENTES

6.1 Clasificación de Incidentes

- **Crítico**: Compromiso de datos personales, caída total del sistema
- **Alto**: Acceso no autorizado, compromiso parcial de servicios
- **Medio**: Intentos de intrusión, anomalías de rendimiento
- **Bajo**: Violaciones menores de política, eventos informativos

6.2 Procedimientos de Respuesta

1. **Detección y Análisis** (0-1 hora)
2. **Contención y Erradicación** (1-4 horas)
3. **Recuperación** (4-24 horas)
4. **Lecciones Aprendidas** (48 horas)

6.3 Notificaciones

- Incidentes críticos: Notificación inmediata a autoridades de protección de datos
- Comunicación a ciudadanos afectados dentro de 72 horas
- Reporte post-incidente a la alta dirección

---

7. AUDITORÍA Y MONITOREO

7.1 Monitoreo Continuo

- SIEM (Security Information and Event Management) 24/7
- Monitoreo de integridad de archivos críticos
- Análisis de comportamiento de usuarios (UBA)
- Correlación de eventos de seguridad

7.2 Auditorías

- Auditoría interna trimestral
- Auditoría externa anual por terceros certificados
- Revisión de cumplimiento normativo semestral
- Pruebas de controles de seguridad

7.3 Métricas de Seguridad

- Tiempo medio de detección (MTTD)
- Tiempo medio de respuesta (MTTR)
- Índice de vulnerabilidades críticas
- Porcentaje de cumplimiento de políticas

---

8. CAPACITACIÓN Y CONCIENCIACIÓN

8.1 Programa de Capacitación

- Inducción en seguridad para nuevos empleados
- Capacitación anual obligatoria en seguridad de la información
- Simulacros de phishing trimestrales
- Talleres especializados por rol y responsabilidad

8.2 Concienciación Ciudadana

- Campañas educativas sobre uso seguro de servicios digitales
- Guías de buenas prácticas en el portal web
- Notificaciones proactivas sobre amenazas de seguridad

---

9. GESTIÓN DE PROVEEDORES

9.1 Evaluación de Seguridad

- Due diligence de seguridad previa a contratación
- Cláusulas de seguridad en contratos
- Auditorías periódicas a proveedores críticos
- Gestión de accesos de terceros

9.2 Transferencia de Datos

- Acuerdos de procesamiento de datos (DPA)
- Evaluación de adecuación para transferencias internacionales
- Controles de seguridad específicos por tipo de proveedor

---

10. CUMPLIMIENTO Y SANCIONES

10.1 Responsabilidades

- **Alta Dirección**: Aprobación y recursos para la política
- **CISO**: Implementación y supervisión de controles
- **Administradores de Sistema**: Aplicación técnica de controles
- **Usuarios**: Cumplimiento de procedimientos establecidos

10.2 Sanciones

- Violaciones menores: Capacitación adicional
- Violaciones graves: Medidas disciplinarias
- Violaciones críticas: Terminación de contrato/acceso

---

11. REVISIÓN Y ACTUALIZACIÓN

11.1 Frecuencia de Revisión

- Revisión anual completa de la política
- Actualizaciones por cambios normativos (inmediato)
- Revisión post-incidente crítico
- Evaluación por cambios tecnológicos significativos

11.2 Proceso de Aprobación

- Propuesta por el equipo de seguridad
- Revisión por comité de seguridad
- Aprobación por alta dirección
- Comunicación a todos los stakeholders

---

12. CONTACTOS Y REFERENCIAS

12.1 Equipo de Seguridad

- **CISO**: [Nombre y contacto]
- **Equipo de Respuesta a Incidentes**: [Contacto 24/7]
- **Oficial de Protección de Datos**: [Nombre y contacto]

12.2 Autoridades Competentes

- Superintendencia de Industria y Comercio (SIC)
- COLCERT (Equipo de Respuesta a Emergencias Cibernéticas)
- Ministerio de Tecnologías de la Información y las Comunicaciones