**TABLA DE EVALUACIÓN CONTROLES ISO 27002:2022**

**Sistema de Control de Comparendos Policiales - Municipio de Palermo**

**Clasificación según ISO 27002:2022**

| **#** | **CONTROL** | **CATEGORÍA** | **TIPO** | **ESTADO** | **RAZÓN** |
| --- | --- | --- | --- | --- | --- |
| **5.1** | Políticas de seguridad de la información | Organizacional | Preventivo | NO IMPLEMENTADO | No se desarrollaron políticas formales de seguridad durante el proyecto |
| **5.2** | Roles y responsabilidades de seguridad de la información | Organizacional | Preventivo | PARCIALMENTE IMPLEMENTADO | Definimos roles básicos (coordinador, líder, desarrollador) sin responsabilidades específicas de seguridad |
| **5.3** | Segregación de funciones | Organizacional | Preventivo | NO IMPLEMENTADO | El equipo pequeño (3 personas) no permitió segregación efectiva de funciones |
| **5.4** | Responsabilidades de la dirección | Organizacional | Preventivo | NO IMPLEMENTADO | No se establecieron responsabilidades directivas específicas de seguridad |
| **5.5** | Contacto con las autoridades | Organizacional | Preventivo-Correctivo | NO IMPLEMENTADO | No establecimos procedimientos para contacto con autoridades en incidentes |
| **5.6** | Contacto con grupos de interés especial | Organizacional | Preventivo-Correctivo | NO IMPLEMENTADO | No identificamos grupos especializados en seguridad |
| **5.7** | Inteligencia de amenazas | Organizacional | Preventivo-Detectivo-Correctivo | NO IMPLEMENTADO | No implementamos sistema de inteligencia de amenazas |
| **5.8** | Seguridad de la información en la gestión de proyectos | Organizacional | Preventivo | NO IMPLEMENTADO | La gestión se centró en funcionalidades, no en aspectos de seguridad |
| **5.9** | Inventario de información y otros activos asociados | Organizacional | Preventivo | NO IMPLEMENTADO | No creamos inventario formal de activos de información |
| **5.10** | Uso aceptable de la información y otros activos asociados | Organizacional | Preventivo | NO IMPLEMENTADO | No establecimos políticas de uso aceptable |
| **5.11** | Devolución de activos | Organizacional | Preventivo | NO IMPLEMENTADO | No definimos procedimientos para devolución de activos |
| **5.12** | Clasificación de la información | Organizacional | Preventivo | PARCIALMENTE IMPLEMENTADO | Clasificamos básicamente como "datos personales" y "datos de pago" sin esquema formal |
| **5.13** | Etiquetado de la información | Organizacional | Preventivo | NO IMPLEMENTADO | No implementamos etiquetado sistemático de información |
| **5.14** | Transferencia de información | Organizacional | Preventivo | NO IMPLEMENTADO | No establecimos políticas para transferencia de información |
| **5.15** | Control de acceso | Organizacional | Preventivo | IMPLEMENTADO | Implementamos control basado en roles (ciudadanos vs administradores) |
| **5.16** | Gestión de identidad | Organizacional | Preventivo | PARCIALMENTE IMPLEMENTADO | Sistema de autenticación por cédula sin gestión formal de identidades |
| **5.17** | Información de autenticación | Organizacional | Preventivo | NO IMPLEMENTADO | No aplicable por método de autenticación elegido (solo cédula) |
| **5.18** | Derechos de acceso | Organizacional | Preventivo | IMPLEMENTADO | Los usuarios solo ven sus propias multas, acceso restringido por tipo de usuario |
| **5.19** | Seguridad de la información en las relaciones con los proveedores | Organizacional | Preventivo | NO IMPLEMENTADO | No trabajamos con proveedores externos |
| **5.20** | Abordar la seguridad de la información en los acuerdos con proveedores | Organizacional | Preventivo | NO IMPLEMENTADO | No establecimos acuerdos formales con proveedores |
| **5.21** | Gestión de la seguridad de la información en la cadena de suministro de las TIC | Organizacional | Preventivo | NO IMPLEMENTADO | No consideramos aspectos de cadena de suministro |
| **5.22** | Monitoreo, revisión y gestión de cambios de servicios de proveedores | Organizacional | Preventivo | NO IMPLEMENTADO | No implementamos monitoreo de servicios externos |
| **5.23** | Seguridad de la información para el uso de servicios en la nube | Organizacional | Preventivo | NO IMPLEMENTADO | No utilizamos servicios en la nube |
| **5.24** | Planificación y preparación de la gestión de incidentes de seguridad de la información | Organizacional | Correctivo | NO IMPLEMENTADO | No establecimos procedimientos de gestión de incidentes |
| **5.25** | Evaluación y decisión sobre eventos de seguridad de la información | Organizacional | Detectivo | NO IMPLEMENTADO | No implementamos evaluación de eventos de seguridad |
| **5.26** | Respuesta a incidentes de seguridad de la información | Organizacional | Correctivo | NO IMPLEMENTADO | No definimos procedimientos de respuesta a incidentes |
| **5.27** | Aprendizaje de los incidentes de seguridad de la información | Organizacional | Preventivo | NO IMPLEMENTADO | No establecimos procesos de lecciones aprendidas |
| **5.28** | Recopilación de evidencias | Organizacional | Correctivo | NO IMPLEMENTADO | No definimos procedimientos de recopilación de evidencia |
| **5.29** | Seguridad de la información durante la interrupción | Organizacional | Preventivo-Correctivo | NO IMPLEMENTADO | No consideramos seguridad durante interrupciones |
| **5.30** | Preparación de las TIC para la continuidad del negocio | Organizacional | Correctivo | NO IMPLEMENTADO | No desarrollamos plan de continuidad del negocio |
| **5.31** | Requisitos legales, estatutarios, reglamentarios y contractuales | Organizacional | Preventivo | IMPLEMENTADO | Sistema diseñado según Código de Policía de Colombia |
| **5.32** | Derechos de propiedad intelectual | Organizacional | Preventivo | NO IMPLEMENTADO | No establecimos políticas de propiedad intelectual |
| **5.33** | Protección de registros | Organizacional | Preventivo | NO IMPLEMENTADO | No implementamos protección específica de registros |
| **5.34** | Privacidad y protección de PII | Organizacional | Preventivo | IMPLEMENTADO | Implementamos protección básica de datos personales |
| **5.35** | Revisión independiente de la seguridad de la información | Organizacional | Preventivo-Correctivo | NO IMPLEMENTADO | No realizamos auditorías independientes |
| **5.36** | Cumplimiento de políticas, normas y estándares de seguridad de la información | Organizacional | Preventivo | NO IMPLEMENTADO | No establecimos verificación de cumplimiento |
| **5.37** | Procedimientos operativos documentados | Organizacional | Preventivo-Correctivo | NO IMPLEMENTADO | No documentamos procedimientos operativos formales |
| **6.1** | Reclutamiento (Screening) | Personas | Preventivo | NO IMPLEMENTADO | No realizamos verificaciones de antecedentes |
| **6.2** | Términos y condiciones del empleo | Personas | Preventivo | NO IMPLEMENTADO | Contratos sin cláusulas específicas de seguridad |
| **6.3** | Concientización, educación y capacitación en seguridad de la información | Personas | Preventivo | NO IMPLEMENTADO | No realizamos capacitación en seguridad |
| **6.4** | Proceso disciplinario | Personas | Preventivo-Correctivo | NO IMPLEMENTADO | No establecimos procesos disciplinarios por seguridad |
| **6.5** | Responsabilidades después de la terminación o cambio de empleo | Personas | Preventivo-Correctivo | NO IMPLEMENTADO | No definimos procedimientos de finalización de acceso |
| **6.6** | Acuerdos de confidencialidad o de no divulgación | Personas | Preventivo | NO IMPLEMENTADO | No firmamos acuerdos de confidencialidad |
| **6.7** | Teletrabajo (Trabajo a distancia) | Personas | Preventivo | NO IMPLEMENTADO | No establecimos políticas para trabajo remoto |
| **6.8** | Reporte de eventos de seguridad de la información | Personas | Detectivo | NO IMPLEMENTADO | No definimos canales de reporte de eventos |
| **7.1** | Perímetros de seguridad física | Físico | Preventivo | NO IMPLEMENTADO | No definimos perímetros de seguridad física |
| **7.2** | Entrada física | Físico | Preventivo | NO IMPLEMENTADO | No implementamos controles de acceso físico |
| **7.3** | Asegurar oficinas, salas e instalaciones | Físico | Preventivo | NO IMPLEMENTADO | No establecimos áreas de trabajo seguras |
| **7.4** | Monitoreo de la seguridad física | Físico | Preventivo-Detectivo | NO IMPLEMENTADO | No implementamos monitoreo físico |
| **7.5** | Protección contra amenazas físicas y ambientales | Físico | Preventivo | NO IMPLEMENTADO | No consideramos protección ambiental |
| **7.6** | Trabajo en áreas seguras | Físico | Preventivo | NO IMPLEMENTADO | No establecimos zonas de trabajo seguras |
| **7.7** | Escritorio limpio y pantalla limpia | Físico | Preventivo | NO IMPLEMENTADO | No implementamos políticas de escritorio limpio |
| **7.8** | Emplazamiento y protección de equipos | Físico | Preventivo | NO IMPLEMENTADO | No definimos ubicaciones seguras para equipos |
| **7.9** | Seguridad de los activos fuera de las instalaciones | Físico | Preventivo | NO IMPLEMENTADO | No establecimos políticas para equipos externos |
| **7.10** | Medios de almacenamiento | Físico | Preventivo | NO IMPLEMENTADO | No consideramos seguridad de medios de almacenamiento |
| **7.11** | Instalaciones de suministro | Físico | Preventivo-Detectivo | NO IMPLEMENTADO | No implementamos controles de suministro eléctrico |
| **7.12** | Seguridad del cableado | Físico | Preventivo | NO IMPLEMENTADO | No consideramos seguridad de cableado |
| **7.13** | Mantenimiento de los equipos | Físico | Preventivo | NO IMPLEMENTADO | No establecimos mantenimiento seguro |
| **7.14** | Eliminación o reutilización segura de equipos | Físico | Preventivo | NO IMPLEMENTADO | No definimos eliminación segura de equipos |
| **8.1** | Dispositivos de punto final de usuario | Tecnológico | Preventivo | NO IMPLEMENTADO | No establecimos controles para dispositivos de usuario |
| **8.2** | Gestión de privilegios de acceso | Tecnológico | Preventivo | NO IMPLEMENTADO | No implementamos gestión de privilegios administrativos |
| **8.3** | Restricción del acceso a la información | Tecnológico | Preventivo | IMPLEMENTADO | Usuarios solo acceden a sus propias multas |
| **8.4** | Acceso al código fuente | Tecnológico | Preventivo | NO IMPLEMENTADO | No implementamos controles de acceso al código |
| **8.5** | Autenticación segura | Tecnológico | Preventivo | PARCIALMENTE IMPLEMENTADO | Autenticación por cédula sin autenticación multifactor |
| **8.6** | Gestión de capacidad | Tecnológico | Preventivo-Detectivo | NO IMPLEMENTADO | No implementamos monitoreo de capacidad |
| **8.7** | Protección contra malware | Tecnológico | Preventivo-Detectivo-Correctivo | NO IMPLEMENTADO | No implementamos protección específica contra malware |
| **8.8** | Gestión de vulnerabilidades técnicas | Tecnológico | Preventivo | IMPLEMENTADO | Implementamos validaciones de entrada para prevenir vulnerabilidades |
| **8.9** | Gestión de la configuración | Tecnológico | Preventivo | NO IMPLEMENTADO | No establecimos gestión formal de configuración |
| **8.10** | Eliminación de información | Tecnológico | Preventivo | NO IMPLEMENTADO | No implementamos eliminación segura de información |
| **8.11** | Enmascaramiento de datos | Tecnológico | Preventivo | NO IMPLEMENTADO | No implementamos enmascaramiento de datos |
| **8.12** | Prevención de fuga de datos | Tecnológico | Preventivo-Detectivo | NO IMPLEMENTADO | No implementamos DLP (Data Loss Prevention) |
| **8.13** | Copias de seguridad de la información | Tecnológico | Correctivo | PARCIALMENTE IMPLEMENTADO | Base de datos con respaldos automáticos implícitos |
| **8.14** | Redundancia de las instalaciones de procesamiento de información | Tecnológico | Preventivo | NO IMPLEMENTADO | No implementamos redundancia de sistemas |
| **8.15** | Inicio sesión | Tecnológico | Detectivo | IMPLEMENTADO | Implementamos logs para intentos de acceso no autorizado |
| **8.16** | Monitoreo de actividades | Tecnológico | Detectivo-Correctivo | NO IMPLEMENTADO | No implementamos monitoreo continuo de actividades |
| **8.17** | Sincronización de reloj | Tecnológico | Detectivo | NO IMPLEMENTADO | No configuramos sincronización de tiempo |
| **8.18** | Uso de utilidades con privilegios del sistema | Tecnológico | Preventivo | NO IMPLEMENTADO | No establecimos controles para herramientas privilegiadas |
| **8.19** | Instalación de software en sistemas operativos | Tecnológico | Preventivo | NO IMPLEMENTADO | No establecimos restricciones de instalación |
| **8.20** | Seguridad en redes | Tecnológico | Preventivo-Detectivo | NO IMPLEMENTADO | No implementamos controles específicos de red |
| **8.21** | Seguridad de los servicios de red | Tecnológico | Preventivo | NO IMPLEMENTADO | No establecimos seguridad específica de servicios |
| **8.22** | Segregación de redes | Tecnológico | Preventivo | NO IMPLEMENTADO | No implementamos segregación de red |
| **8.23** | Filtrado web | Tecnológico | Preventivo | NO IMPLEMENTADO | No implementamos filtrado web |
| **8.24** | Uso de criptografía | Tecnológico | Preventivo | IMPLEMENTADO | Implementamos cifrado para datos personales y de pago |
| **8.25** | Política de desarrollo seguro | Tecnológico | Preventivo | IMPLEMENTADO | Aplicamos validaciones de entrada y manejo de errores |
| **8.26** | Requerimientos de seguridad en aplicaciones | Tecnológico | Preventivo | PARCIALMENTE IMPLEMENTADO | Especificamos algunos requisitos básicos sin formalización |
| **8.27** | Principios de arquitectura e ingeniería de sistemas seguros | Tecnológico | Preventivo | IMPLEMENTADO | Aplicamos principios básicos como validación y manejo de errores |
| **8.28** | Codificación segura | Tecnológico | Preventivo | PARCIALMENTE IMPLEMENTADO | Implementamos validaciones básicas sin estándares formales |
| **8.29** | Pruebas de seguridad en el desarrollo y la aceptación | Tecnológico | Preventivo | NO IMPLEMENTADO | No realizamos pruebas específicas de seguridad |
| **8.30** | Externalización del desarrollo de software | Tecnológico | Preventivo-Detectivo | NO IMPLEMENTADO | Todo el desarrollo fue interno |
| **8.31** | Separación de los entornos de desarrollo, prueba y producción | Tecnológico | Preventivo | NO IMPLEMENTADO | Desarrollamos en un solo entorno |
| **8.32** | Gestión del cambio | Tecnológico | Preventivo | NO IMPLEMENTADO | No establecimos gestión formal de cambios |
| **8.33** | Información de prueba | Tecnológico | Preventivo | NO IMPLEMENTADO | No establecimos protección de datos de prueba |
| **8.34** | Protección de los sistemas de información durante las pruebas de auditoría | Tecnológico | Preventivo | NO IMPLEMENTADO | No realizamos auditorías formales |