**Proyecto:**

**Lava Rápido Vehicular**

**Documento:**

Política de Seguridad de la información

**Versión:**  
📄 **1.0**

**Fecha de Emisión:**

**10 de octubre de 2025**

**Elaborado por:**

Santiago Gordo Pérez

José Stiven Perdomo Martínez

# Declaración de Aplicabilidad (SoA) – Lava Rápido Vehicular

|  |  |  |
| --- | --- | --- |
| ID | Control | Estado |
| 5.1 | Política de seguridad de la información | Falta implementar |
| 5.2 | Roles y responsabilidades de seguridad | Falta implementar |
| 5.3 | Segregación de deberes | No aplica |
| 5.4 | Responsabilidades de gestión | Falta implementar |
| 5.5 | Contacto con autoridades | No aplica |
| 5.6 | Contacto con grupos de interés especial | Falta implementar |
| 5.7 | Inteligencia de amenazas | Falta implementar |
| 5.8 | Seguridad en la gestión de proyectos | Implementado |
| 5.9 | Inventario de información y activos | Falta implementar |
| 5.10 | Uso aceptable de activos | Falta implementar |
| 5.11 | Devolución de activos | Falta implementar |
| 5.12 | Clasificación de la información | Falta implementar |
| 5.13 | Etiquetado de información | Falta implementar |
| 5.14 | Transferencia de información | Falta implementar |
| 5.15 | Control de acceso | Implementado |
| 5.16 | Gestión de identidades | Implementado |
| 5.17 | Información de autenticación | Implementado |
| 5.18 | Derechos de acceso | Falta implementar |
| 5.19 | Seguridad en relaciones con proveedores | Falta implementar |
| 5.20 | Seguridad en acuerdos con proveedores | Falta implementar |
| 5.21 | Seguridad en la cadena de suministro TIC | Falta implementar |
| 5.22 | Gestión de servicios de proveedores | Falta implementar |
| 5.23 | Seguridad en servicios en la nube | Falta implementar |
| 5.24 | Preparación de gestión de incidentes | Falta implementar |
| 5.25 | Evaluación de eventos de seguridad | Falta implementar |
| 5.26 | Respuesta a incidentes | Falta implementar |
| 5.27 | Lecciones aprendidas de incidentes | Falta implementar |
| 5.28 | Recolección de evidencia | Falta implementar |
| 5.29 | Seguridad durante interrupciones | Falta implementar |
| 5.30 | Continuidad de TIC | Falta implementar |
| 5.31 | Requisitos legales y contractuales | Falta implementar |
| 5.32 | Derechos de propiedad intelectual | Falta implementar |
| 5.33 | Protección de registros | Falta implementar |
| 5.34 | Privacidad y protección de datos personales | Falta implementar |
| 5.35 | Revisión independiente de seguridad | Falta implementar |
| 5.36 | Cumplimiento de políticas y normas | Falta implementar |
| 5.37 | Procedimientos documentados | Falta implementar |
| 6.1 | Verificación de antecedentes | No aplica |
| 6.2 | Términos y condiciones de empleo | Falta implementar |
| 6.3 | Capacitación en seguridad | Falta implementar |
| 6.4 | Proceso disciplinario | Falta implementar |
| 6.5 | Responsabilidades post-empleo | No aplica |
| 6.6 | Acuerdos de confidencialidad | Falta implementar |
| 6.7 | Trabajo remoto | Implementado |
| 6.8 | Reporte de incidentes de seguridad | Falta implementar |
| 7.1 | Perímetros físicos de seguridad | No aplica |
| 7.2 | Control de acceso físico | No aplica |
| 7.3 | Seguridad en oficinas e instalaciones | No aplica |
| 7.4 | Monitoreo físico | No aplica |
| 7.5 | Protección contra amenazas ambientales | No aplica |
| 7.6 | Áreas seguras | No aplica |
| 7.7 | Escritorio y pantalla despejada | Falta implementar |
| 7.8 | Protección de equipos | Falta implementar |
| 7.9 | Seguridad fuera de las instalaciones | Falta implementar |
| 7.10 | Medios de almacenamiento | Implementado |
| 7.11 | Utilities de apoyo | No aplica |
| 7.12 | Seguridad del cableado | No aplica |
| 7.13 | Mantenimiento de equipos | No aplica |
| 7.14 | Eliminación segura de equipos | Falta implementar |
| 8.1 | Procedimientos operativos | Falta implementar |
| 8.2 | Seguridad en desarrollo de software | Implementado |
| 8.3 | Copias de seguridad | Falta implementar |
| 8.4 | Gestión de vulnerabilidades y parches | Falta implementar |
| 8.5 | Registro de actividades (logs) | Falta implementar |
| 8.6 | Protección contra malware | Falta implementar |
| 8.7 | Criptografía | Implementado |
| 8.8 | Seguridad en redes | Falta implementar |
| 8.9 | Separación de entornos (dev/prod) | Falta implementar |
| 8.10 | Gestión de configuraciones | Falta implementar |
| 8.11 | Control de acceso a red | Falta implementar |
| 8.12 | Seguridad de endpoints | Falta implementar |
| 8.13 | Gestión de privilegios | Falta implementar |
| 8.14 | Autenticación multifactor | Falta implementar |
| 8.15 | Protección de datos en tránsito | Implementado |
| 8.16 | Protección de datos en reposo | Implementado |
| 8.17 | Seguridad en APIs | Falta implementar |
| 8.18 | Seguridad en bases de datos | Implementado |
| 8.19 | Seguridad en contenedores/virtualización | No aplica |
| 8.20 | Registro y gestión de accesos a sistemas críticos | Falta implementar |
| 8.21 | Seguridad en ciclo de vida del software | Falta implementar |
| 8.22 | Pruebas de seguridad / pentesting | Falta implementar |
| 8.23 | Gestión de claves | Falta implementar |
| 8.24 | Protección contra DoS | Falta implementar |
| 8.25 | Seguridad en pasarela de pagos | Implementado |
| 8.26 | Monitorización de integridad de archivos | Falta implementar |
| 8.27 | Gestión de sesión / timeout | Falta implementar |
| 8.28 | Protección en interfaces de terceros | Falta implementar |
| 8.29 | Copias fuera de sitio y restauración | Falta implementar |
| 8.30 | Segmentación de infraestructura | Falta implementar |
| 8.31 | Seguridad por diseño | Falta implementar |
| 8.32 | Control de versiones | Implementado |
| 8.33 | Protección contra fuga de datos | Falta implementar |
| 8.34 | Telemetría y alertas de seguridad | Falta implementar |

**Política de Seguridad de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece la **Política de Seguridad de la Información** del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.1 de la ISO/IEC 27001:2022.

El objetivo es definir el marco de referencia para la gestión de la seguridad de la información, garantizando la **confidencialidad, integridad y disponibilidad** de los datos manejados por el sistema, incluyendo información de clientes, servicios contratados y transacciones de pago.

**2. Alcance**

Esta política aplica a toda la información generada, procesada o almacenada en el proyecto, incluyendo:

* Datos personales de clientes (nombres, teléfonos, correos).
* Información de reservas y pagos de servicios.
* Código fuente, base de datos y configuraciones del sistema.
* Documentación técnica, políticas y manuales de uso.

Está dirigida a todo el personal involucrado en el desarrollo, operación y administración del sistema, así como a los proveedores externos que participen en su gestión.

**3. Principios de Seguridad**

* **Confidencialidad:** Solo usuarios autorizados pueden acceder a la información.
* **Integridad:** La información debe mantenerse correcta y libre de modificaciones no autorizadas.
* **Disponibilidad:** Los sistemas estarán disponibles para los usuarios cuando se necesiten.
* **Cumplimiento:** Toda la información se gestionará conforme a la legislación vigente y requisitos contractuales.

**4. Responsabilidades**

* **Dirección del proyecto:** Aprobar la política y garantizar los recursos para su cumplimiento.
* **Administrador del sistema:** Implementar los controles de seguridad necesarios (accesos, copias de seguridad, monitoreo).
* **Usuarios del sistema:** Cumplir con las normas establecidas, proteger sus credenciales y reportar incidentes de seguridad.

**5. Reglas de Manejo**

* El acceso al sistema debe realizarse con credenciales únicas y seguras.
* Se utilizarán mecanismos de cifrado para proteger datos sensibles (contraseñas, pagos).
* Todo incidente de seguridad debe ser reportado al administrador del sistema.
* Se deben realizar copias de seguridad periódicas y verificar su restauración.
* La política será revisada al menos una vez al año o tras cambios significativos en el sistema.

**6. Revisión y Actualización**

Esta política será revisada:

* Cada 12 meses.
* Cuando se incorporen nuevos servicios o tecnologías en el sistema.
* Tras incidentes de seguridad relevantes.

**Roles y Responsabilidades de Seguridad de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece los **roles y responsabilidades en materia de seguridad de la información** dentro del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.2 de la ISO/IEC 27001:2022.

Su objetivo es garantizar que cada integrante conozca y asuma las tareas relacionadas con la **protección de la información**, reduciendo riesgos de uso indebido o pérdida de datos.

**2. Alcance**

Aplica a:

* Todo el personal involucrado en el desarrollo, operación y administración del sistema.
* Proveedores de servicios externos que tengan acceso a datos o infraestructura del proyecto.

**3. Roles y Responsabilidades**

| **Rol** | **Responsabilidades de Seguridad** |
| --- | --- |
| **Dirección del Proyecto** | - Aprobar políticas y procedimientos de seguridad. - Asignar recursos para implementar controles. - Dar seguimiento al cumplimiento de la ISO 27001. |
| **Administrador del Sistema** | - Configurar y gestionar accesos a la base de datos y aplicación. - Implementar copias de seguridad y recuperación. - Monitorear logs e incidentes de seguridad. - Coordinar pruebas de seguridad. |
| **Desarrolladores** | - Implementar código siguiendo prácticas de “seguridad por diseño”. - Aplicar controles de autenticación, cifrado y gestión de errores. - Documentar cambios y mantener la seguridad en APIs. |
| **Usuarios Autorizados** | - Usar credenciales seguras y mantener su confidencialidad. - Reportar incidentes o actividades sospechosas. - Respetar las políticas de uso aceptable. |
| **Proveedores Externos** | - Cumplir con las cláusulas de seguridad en contratos. - Asegurar la protección de los datos bajo su responsabilidad. - Informar incidentes de seguridad relacionados con los servicios prestados. |

**4. Reglas de Cumplimiento**

* Cada miembro del equipo es responsable de la información que maneja.
* Ningún usuario podrá compartir credenciales o accesos sin autorización.
* El incumplimiento de estas responsabilidades puede dar lugar a medidas disciplinarias o la terminación de la relación contractual.

**5. Revisión y Actualización**

Este documento será revisado:

* Cada 12 meses.
* Cuando se incorporen nuevos roles, servicios o proveedores.

**Responsabilidades de Gestión en Seguridad de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define las **responsabilidades de la dirección y del equipo de gestión** en materia de seguridad de la información, en cumplimiento del control A.5.4 de la ISO/IEC 27001:2022.

El objetivo es asegurar el compromiso de la alta dirección en el establecimiento, implementación y mejora continua de la seguridad de la información dentro del sistema *Lava Rápido Vehicular*.

**2. Alcance**

Esta política aplica a:

* La dirección del proyecto.
* El administrador del sistema.
* Los responsables de procesos clave (desarrollo, base de datos, pagos en línea).

**3. Responsabilidades de la Dirección**

La Dirección del Proyecto debe:

* Aprobar la política de seguridad de la información (control 5.1).
* Asegurar que se establezcan **objetivos de seguridad medibles** (ej. % de incidentes resueltos, % de respaldos verificados).
* Asignar los recursos necesarios para implementar controles técnicos y documentales.
* Definir un **canal oficial de reporte de incidentes** de seguridad.
* Realizar revisiones periódicas al cumplimiento de la ISO 27001.

**4. Responsabilidades de Gestión del Sistema**

El Administrador y responsables designados deben:

* Implementar y mantener los controles de seguridad aprobados.
* Supervisar el cumplimiento de roles y responsabilidades (control 5.2).
* Revisar periódicamente los accesos a la base de datos y la aplicación.
* Monitorear la ejecución de copias de seguridad y pruebas de restauración.
* Asegurar que se gestionen y documenten los incidentes de seguridad.

**5. Reglas de Cumplimiento**

* Las decisiones de gestión deben priorizar siempre la **confidencialidad, integridad y disponibilidad** de la información.
* Cualquier cambio en la infraestructura, procesos o proveedores debe ser aprobado por la dirección y documentado.
* El incumplimiento de estas responsabilidades será reportado a la dirección y puede derivar en sanciones disciplinarias.

**6. Revisión y Actualización**

Este documento se revisará:

* Anualmente.
* Cuando haya cambios en el equipo directivo o en los procesos críticos.

**Contacto con Grupos de Interés Especial**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las pautas para mantener **contacto con grupos de interés especial en seguridad de la información**, en cumplimiento del control A.5.6 de la ISO/IEC 27001:2022.

El objetivo es asegurar que el proyecto *Lava Rápido Vehicular* esté actualizado frente a **nuevas amenazas, vulnerabilidades, mejores prácticas y requisitos normativos**, mediante el vínculo con asociaciones, comunidades y autoridades relevantes.

**2. Alcance**

Este procedimiento aplica a:

* La dirección del proyecto y al administrador del sistema.
* Todos los contactos y relaciones con grupos externos relacionados con seguridad, regulaciones o normativas de protección de datos.

**3. Grupos de Interés Especial**

Los grupos con los que se debe mantener contacto incluyen, pero no se limitan a:

* **Autoridades nacionales de protección de datos** (ej. Superintendencia de Industria y Comercio en Colombia).
* **Entidades certificadoras y normalizadoras** (ej. ISO, ICONTEC).
* **Asociaciones y comunidades de ciberseguridad** (ej. OWASP, ISACA, foros locales).
* **Proveedores de servicios tecnológicos** (hosting, pasarela de pagos, nube).

**4. Responsabilidades**

* **Dirección del Proyecto:** Aprobar la participación en asociaciones y asegurar los recursos para mantener estas relaciones.
* **Administrador del Sistema:** Mantener comunicación técnica con proveedores y comunidades de seguridad (parches, alertas, buenas prácticas).
* **Usuarios Autorizados:** Reportar al administrador cualquier alerta recibida por comunidades externas.

**5. Reglas de Cumplimiento**

* Toda la información recibida de estos grupos debe evaluarse y, si es relevante, incorporarse en el SGSI.
* Se debe mantener un **registro actualizado de contactos clave** (autoridades, proveedores, asociaciones).
* La participación en actividades externas (capacitaciones, foros, conferencias) debe documentarse y compartirse con el equipo.

**6. Revisión y Actualización**

* El listado de grupos de interés debe revisarse **cada 12 meses**.
* En caso de cambio de proveedor o autoridad regulatoria, la información debe actualizarse inmediatamente.

**Inteligencia de Amenazas**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece el proceso de **inteligencia de amenazas de seguridad de la información**, en cumplimiento del control A.5.7 de la ISO/IEC 27001:2022.

El objetivo es garantizar que el proyecto *Lava Rápido Vehicular* pueda **anticiparse, identificar y responder a amenazas emergentes** (ciberataques, malware, vulnerabilidades, incidentes en proveedores, etc.) que puedan afectar la confidencialidad, integridad o disponibilidad de la información.

**2. Alcance**

Aplica a todos los activos de información del proyecto:

* Aplicación web y móvil.
* Servidores, base de datos y servicios en la nube.
* Integraciones con pasarelas de pago y proveedores externos.
* Información personal y financiera de los clientes.

**3. Fuentes de Inteligencia de Amenazas**

La organización debe recopilar y analizar información de:

* **Reportes de vulnerabilidades** de fabricantes de software (Microsoft, Linux, bases de datos).
* **Alertas de ciberseguridad** emitidas por autoridades nacionales (ej. ColCERT en Colombia).
* **Comunidades y foros especializados** (OWASP, CERT, ISACA).
* **Proveedores de servicios en la nube y pasarelas de pago**.

**4. Responsabilidades**

* **Administrador del Sistema:**
  + Monitorear alertas y reportes de seguridad.
  + Evaluar impacto en los sistemas del proyecto.
  + Aplicar parches y actualizaciones cuando corresponda.
* **Dirección del Proyecto:**
  + Aprobar la implementación de medidas preventivas y correctivas.
  + Revisar informes periódicos sobre amenazas detectadas.
* **Usuarios Autorizados:**
  + Reportar comportamientos sospechosos o incidentes inusuales.

**5. Reglas de Cumplimiento**

* Se debe mantener un **registro de amenazas analizadas** y las medidas aplicadas.
* Las vulnerabilidades críticas deben resolverse en un plazo máximo de **72 horas** tras su notificación.
* El análisis de inteligencia de amenazas debe integrarse en la **gestión de incidentes** (controles 5.24–5.27).
* El sistema debe contar con mecanismos de actualización de seguridad periódicos.

**6. Revisión y Actualización**

* La información de amenazas debe revisarse al menos **mensualmente**.
* El procedimiento será actualizado cuando se detecten nuevas fuentes de inteligencia relevantes o cambios tecnológicos en el sistema.

**Inventario de Información y Activos**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece el proceso de **identificación, registro y gestión de activos de información y tecnológicos**, en cumplimiento del control A.5.9 de la ISO/IEC 27001:2022.

El objetivo es mantener un **inventario actualizado** que permita proteger de manera adecuada la información, los sistemas y los equipos que soportan el proyecto *Lava Rápido Vehicular*.

**2. Alcance**

Este procedimiento aplica a todos los activos de información y tecnología usados en el proyecto, incluyendo:

* Información de clientes (datos personales, historial de servicios, pagos).
* Aplicación web y móvil.
* Base de datos y servidores en la nube.
* Equipos de cómputo utilizados por el personal autorizado.
* Documentación técnica, políticas y manuales de usuario.
* Licencias de software y herramientas utilizadas en el desarrollo.

**3. Tipos de Activos**

Los activos se clasifican en las siguientes categorías:

* **Información:** Datos personales de clientes, transacciones de pago, reportes de servicios.
* **Software:** Código fuente, aplicaciones desarrolladas, sistemas de terceros.
* **Hardware:** Servidores, laptops, dispositivos móviles autorizados.
* **Servicios:** Plataforma en la nube, pasarela de pagos, proveedores externos.
* **Documentación:** Manuales, políticas, procedimientos y contratos.

**4. Responsabilidades**

* **Administrador del Sistema:**
  + Crear y mantener actualizado el inventario.
  + Clasificar activos según su nivel de criticidad y confidencialidad.
  + Reportar a la dirección sobre cambios en el inventario.
* **Dirección del Proyecto:**
  + Aprobar la clasificación de activos críticos.
  + Asignar recursos para la protección de activos esenciales.
* **Usuarios Autorizados:**
  + Usar los activos conforme a la política de uso aceptable.
  + Reportar pérdida, daño o uso indebido de un activo.

**5. Reglas de Cumplimiento**

* Todo activo debe estar registrado en el inventario con su propietario asignado.
* Los activos críticos (ej. base de datos de clientes) deben contar con medidas adicionales de protección (cifrado, backups).
* No se permite el uso de activos sin estar previamente autorizados e incluidos en el inventario.
* El inventario debe revisarse y actualizarse **al menos cada 6 meses**.

**6. Revisión y Actualización**

* La información del inventario será revisada trimestralmente.
* El procedimiento será actualizado cuando se adquieran, modifiquen o eliminen activos del sistema.

**Uso Aceptable de Activos**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define las **reglas para el uso aceptable de los activos de información y tecnológicos** del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.10 de la ISO/IEC 27001:2022.

El objetivo es garantizar que todos los recursos del sistema (equipos, software, datos y servicios en la nube) sean utilizados **de forma segura, ética y conforme a las políticas de la organización**.

**2. Alcance**

Esta política aplica a todos los miembros del proyecto, empleados, contratistas y proveedores que:

* Accedan al sistema o base de datos del proyecto.
* Utilicen dispositivos, software o información propiedad del proyecto.
* Manejen datos personales o sensibles de los clientes.

**3. Activos Cubiertos**

Los activos incluidos en esta política son:

* **Hardware:** Computadores, dispositivos móviles, servidores, periféricos.
* **Software:** Aplicaciones, licencias, herramientas de desarrollo y bases de datos.
* **Datos:** Información de clientes, registros de servicios, información financiera.
* **Servicios:** Almacenamiento en la nube, correo electrónico y pasarela de pagos.

**4. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar esta política y asegurar su difusión a todo el personal.
  + Supervisar el cumplimiento del uso adecuado de los activos.
* **Administrador del Sistema:**
  + Configurar controles de acceso, cifrado y copias de seguridad.
  + Detectar y registrar cualquier uso indebido o no autorizado.
* **Usuarios Autorizados:**
  + Utilizar los activos únicamente para fines relacionados con el proyecto.
  + Mantener la confidencialidad de credenciales y datos.
  + Reportar inmediatamente incidentes o comportamientos sospechosos.

**5. Reglas de Uso Aceptable**

* Está **prohibido instalar software no autorizado** en equipos del proyecto.
* No se permite compartir contraseñas ni accesos a cuentas del sistema.
* El uso de activos personales para acceder al sistema requiere autorización previa.
* La información sensible (clientes, pagos) **no debe compartirse por medios no seguros**.
* El uso de servicios en la nube debe cumplir con las políticas de seguridad aprobadas.
* Los activos deben mantenerse protegidos mediante contraseñas seguras, cifrado y antivirus actualizado.

**6. Revisión y Actualización**

* Esta política será revisada **anualmente** o cuando se incorporen nuevos activos tecnológicos.
* Las violaciones a esta política serán tratadas como incidentes de seguridad y evaluadas por la dirección.

**Devolución de Activos**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las **directrices para la devolución de activos de información y tecnológicos** utilizados en el proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.11 de la ISO/IEC 27001:2022.

El objetivo es garantizar que, cuando un colaborador, contratista o proveedor finalice su relación con el proyecto, todos los activos asignados sean **devueltos y asegurados adecuadamente**, evitando la pérdida, daño o uso indebido de la información.

**2. Alcance**

Esta política aplica a:

* Todos los empleados, contratistas, desarrolladores o proveedores externos con acceso a los sistemas o información del proyecto.
* Todos los activos asignados temporalmente o de forma permanente, incluyendo hardware, software, credenciales y documentos.

**3. Activos Sujeto a Devolución**

* **Equipos físicos:** Laptops, memorias USB, discos duros, celulares o periféricos asignados.
* **Activos digitales:** Cuentas de usuario, credenciales de acceso, repositorios de código, correo institucional, software licenciado.
* **Información y documentación:** Archivos, respaldos, políticas o datos relacionados con el sistema o clientes.

**4. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar la baja o desvinculación de personal.
  + Supervisar que el proceso de devolución se realice correctamente.
* **Administrador del Sistema:**
  + Revocar accesos y credenciales del usuario saliente.
  + Verificar la devolución física y digital de todos los activos.
  + Actualizar el inventario de activos (ver control 5.9).
* **Usuario o Colaborador Saliente:**
  + Entregar todos los activos asignados en buen estado.
  + Eliminar información confidencial del proyecto de sus dispositivos personales.
  + Firmar el formato de entrega y conformidad.

**5. Procedimiento de Devolución**

1. El usuario notifica su salida o finalización de contrato.
2. El administrador de sistemas realiza la **revocación de accesos** (bases de datos, nube, repositorios, correo).
3. El colaborador entrega los equipos y activos físicos asignados.
4. Se realiza la **verificación y registro de devolución** en el inventario de activos.
5. La dirección aprueba y archiva el **formato de devolución firmado**.

**6. Reglas de Cumplimiento**

* Ningún usuario puede conservar copias de información del proyecto tras su salida.
* La falta de devolución de activos puede conllevar sanciones contractuales.
* Todo el proceso debe documentarse y mantenerse en los registros del proyecto.

**7. Revisión y Actualización**

* Esta política será revisada anualmente o cuando cambien los procedimientos de contratación o desvinculación.
* Cualquier incidente relacionado con pérdida o falta de devolución será analizado como incidente de seguridad.

**Clasificación de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define el **proceso de clasificación de la información** gestionada por el proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.12 de la ISO/IEC 27001:2022.

El objetivo es garantizar que toda la información se proteja según su nivel de sensibilidad, reduciendo los riesgos de acceso no autorizado, divulgación o pérdida de datos.

**2. Alcance**

Aplica a toda la información creada, recibida, procesada o almacenada por el sistema, incluyendo:

* Datos personales de clientes (nombre, teléfono, correo, historial de servicios).
* Registros de pagos y facturación.
* Información interna del sistema (configuraciones, contraseñas, logs).
* Documentación del proyecto (políticas, manuales, reportes técnicos).

**3. Criterios de Clasificación**

La información será clasificada según su nivel de confidencialidad y el impacto que tendría su divulgación o alteración:

| **Nivel de Clasificación** | **Descripción** | **Ejemplos** |
| --- | --- | --- |
| **Confidencial** | Información sensible que podría causar daño si se divulga. | Contraseñas, datos de clientes, copias de seguridad, claves de API. |
| **Interna** | Información de uso limitado dentro del equipo de trabajo. | Documentación técnica, manuales internos, informes de mantenimiento. |
| **Pública** | Información que puede divulgarse sin restricción. | Publicaciones web, material publicitario, información general del servicio. |

**4. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar los niveles de clasificación.
  + Asegurar que la política de clasificación sea comunicada y aplicada.
* **Administrador del Sistema:**
  + Etiquetar digitalmente la información según su nivel.
  + Controlar los accesos a información confidencial.
  + Realizar copias de seguridad con las medidas de seguridad apropiadas.
* **Usuarios Autorizados:**
  + Respetar las etiquetas de clasificación asignadas.
  + No divulgar información confidencial sin autorización.

**5. Reglas de Clasificación**

* Toda información debe clasificarse en el momento de su creación o recepción.
* La información “Confidencial” debe almacenarse en entornos protegidos mediante cifrado.
* Los documentos “Internos” no deben compartirse fuera del equipo del proyecto.
* Cualquier cambio en la clasificación de la información debe ser autorizado por la dirección.

**6. Revisión y Actualización**

* La política de clasificación será revisada anualmente o cuando se modifiquen los tipos de datos manejados.
* Cualquier incidente que involucre información mal clasificada será tratado como **incidente de seguridad**.

**Etiquetado de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las directrices para el **etiquetado de la información** manejada dentro del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.13 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que cada tipo de información sea **claramente identificada y protegida según su nivel de confidencialidad**, asegurando un manejo adecuado durante su almacenamiento, transmisión, copia o eliminación.

**2. Alcance**

Aplica a toda la información creada, procesada o almacenada por el sistema, tanto en formato físico como digital:

* Datos personales y financieros de los clientes.
* Información operativa, técnica y administrativa.
* Documentación interna del proyecto y reportes de seguridad.
* Copias de seguridad, registros de actividad y configuraciones del sistema.

**3. Niveles de Etiquetado**

Toda la información debe llevar una etiqueta o marca visible (digital o física) que indique su nivel de confidencialidad.

| **Nivel de Etiqueta** | **Descripción** | **Ejemplo de Marcado** |
| --- | --- | --- |
| **Confidencial** | Información sensible con acceso restringido. | “🔒 CONFIDENCIAL – Solo personal autorizado” |
| **Interna** | Información de uso interno del equipo de trabajo. | “INFORMACIÓN INTERNA – No divulgar externamente” |
| **Pública** | Información que puede compartirse libremente. | “INFORMACIÓN PÚBLICA” |

**4. Requisitos de Etiquetado**

* Los **archivos digitales** deben incluir la etiqueta en el **nombre del archivo, encabezado o metadatos**.  
  Ejemplo: ListaClientes\_CONFIDENCIAL.xlsx
* Los **documentos físicos** deben llevar la etiqueta visible en la parte superior de cada página.
* Las **copias de seguridad** deben marcarse con su nivel de confidencialidad antes del almacenamiento.
* La etiqueta asignada debe mantenerse durante **todo el ciclo de vida** de la información.
* Cualquier cambio en la clasificación o etiqueta debe estar **autorizado por la dirección del proyecto**.

**5. Responsabilidades**

* **Administrador del Sistema:**
  + Asegurar que la información almacenada esté etiquetada correctamente.
  + Verificar la coherencia entre la clasificación (ver control 5.12) y el etiquetado aplicado.
  + Capacitar al personal sobre el uso correcto de etiquetas.
* **Dirección del Proyecto:**
  + Aprobar el procedimiento y verificar su cumplimiento.
* **Usuarios Autorizados:**
  + Respetar las etiquetas y no modificar ni eliminar marcas de seguridad sin autorización.

**6. Revisión y Actualización**

* El procedimiento de etiquetado se revisará **anualmente** o cuando cambie la clasificación de los datos manejados.
* Las etiquetas podrán actualizarse para adaptarse a nuevas necesidades de confidencialidad o regulaciones.

**Transferencia de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las directrices para la **transferencia segura de información**, tanto dentro como fuera del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.14 de la ISO/IEC 27001:2022.

El objetivo es garantizar que toda la información transmitida por medios electrónicos, físicos o mediante terceros esté **protegida contra acceso no autorizado, pérdida o alteración** durante su transferencia.

**2. Alcance**

Esta política aplica a todas las transferencias de información que involucren:

* Datos personales y financieros de clientes.
* Información interna y técnica del sistema.
* Comunicaciones entre el servidor, base de datos y pasarela de pagos.
* Intercambio de información con proveedores o autoridades.

Incluye medios como:

* Correos electrónicos.
* Plataformas en la nube.
* APIs, servicios web y conexiones seguras.
* Dispositivos de almacenamiento físico (USB, discos externos).

**3. Medidas de Seguridad para la Transferencia**

* Toda transferencia de información sensible debe realizarse a través de **canales cifrados (TLS, HTTPS, SFTP, VPN)**.
* Los correos con información confidencial deben cifrarse y enviarse solo a destinatarios autorizados.
* Está **prohibido usar servicios no aprobados** (por ejemplo, nubes personales o mensajerías no seguras) para enviar datos del proyecto.
* Los documentos físicos con información sensible deben transportarse en sobres sellados o bajo control directo del personal autorizado.
* Toda información compartida con terceros debe estar amparada por **acuerdos de confidencialidad (NDA)** o cláusulas contractuales.

**4. Responsabilidades**

* **Administrador del Sistema:**
  + Configurar y mantener canales seguros de transferencia.
  + Controlar permisos de acceso a la información que se transmite.
  + Monitorear y registrar las transferencias críticas.
* **Dirección del Proyecto:**
  + Aprobar transferencias de información fuera de la organización.
  + Validar acuerdos de confidencialidad con terceros.
* **Usuarios Autorizados:**
  + Cumplir las reglas de envío seguro.
  + Notificar incidentes o errores durante una transferencia.

**5. Reglas de Cumplimiento**

* Ningún usuario puede enviar información confidencial a direcciones o sistemas no autorizados.
* Toda transferencia de datos personales deberá cumplir con la legislación vigente (Ley de Protección de Datos Personales).
* Las transferencias que involucren información crítica deberán **registrarse en un log o bitácora de actividad**.
* La información transferida deberá eliminarse de medios temporales una vez confirmada su recepción.

**6. Revisión y Actualización**

* Este procedimiento se revisará **anualmente** o cuando cambien los medios de transferencia utilizados.
* Los incidentes detectados durante la transferencia deberán ser analizados y documentados como parte del proceso de gestión de incidentes (controles 5.24–5.27).

**Control de Acceso**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define las políticas y procedimientos de **control de acceso a la información y sistemas** del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.15 de la ISO/IEC 27001:2022.

El objetivo es asegurar que únicamente las personas **autorizadas y autenticadas** puedan acceder a los activos de información, minimizando el riesgo de accesos indebidos, pérdida o alteración de datos.

**2. Alcance**

Esta política aplica a todos los recursos tecnológicos del proyecto:

* Aplicación web y base de datos.
* Servidores, sistemas de autenticación y almacenamiento en la nube.
* Repositorios de código fuente y documentación interna.
* Cuentas de usuario, contraseñas y credenciales de acceso.

**3. Principios de Control de Acceso**

1. **Necesidad de saber:** El acceso se otorga solo a quienes lo requieren para su función.
2. **Mínimo privilegio:** Cada usuario tiene los permisos estrictamente necesarios.
3. **Autenticación segura:** Todos los accesos requieren credenciales válidas.
4. **Registro y auditoría:** Toda actividad de acceso se registra para su seguimiento.
5. **Revisión periódica:** Los accesos se revisan y ajustan regularmente.

**4. Roles de Acceso**

| **Rol** | **Descripción** | **Permisos principales** |
| --- | --- | --- |
| **Administrador del Sistema** | Gestiona la infraestructura, bases de datos y usuarios. | Acceso completo a configuración y monitoreo. |
| **Desarrollador** | Mantiene y actualiza el código del sistema. | Acceso al repositorio y entorno de pruebas. |
| **Usuario Operativo** | Utiliza el sistema para registrar servicios y clientes. | Acceso limitado a módulos asignados. |
| **Cliente/Usuario final** | Interactúa con la aplicación web o móvil. | Acceso a su cuenta personal y servicios. |

**5. Reglas de Acceso**

* Cada usuario debe tener una **cuenta individual** y no compartida.
* Las contraseñas deben cumplir con los criterios de seguridad definidos (mínimo 8 caracteres, combinación de letras, números y símbolos).
* Las sesiones deben **cerrarse automáticamente** tras un periodo de inactividad (ver control 8.27).
* Los accesos de usuarios inactivos o desvinculados deben **revocarse inmediatamente**.
* Los permisos deben revisarse trimestralmente.
* Todo acceso remoto o administrativo debe estar protegido con **autenticación multifactor (MFA)**.

**6. Responsabilidades**

* **Administrador del Sistema:**
  + Crear, modificar o eliminar cuentas de usuario según autorización.
  + Monitorear los registros de acceso y detectar intentos fallidos o sospechosos.
  + Aplicar mecanismos de cifrado en las credenciales y conexiones.
* **Dirección del Proyecto:**
  + Aprobar las políticas de acceso y asignar roles según responsabilidades.
* **Usuarios Autorizados:**
  + Mantener la confidencialidad de sus credenciales.
  + No compartir cuentas ni contraseñas con terceros.

**7. Revisión y Actualización**

* Las políticas de acceso se revisarán **cada 6 meses** o ante cambios en los sistemas o personal.
* Los registros de auditoría se conservarán por un periodo mínimo de **12 meses**.

**Gestión de Identidades**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define el proceso de **gestión de identidades y cuentas de usuario** del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.16 de la ISO/IEC 27001:2022.

El objetivo es asegurar que todas las identidades digitales creadas, utilizadas y eliminadas en los sistemas del proyecto estén **autenticadas, autorizadas y gestionadas adecuadamente**, garantizando la trazabilidad y el principio del mínimo privilegio.

**2. Alcance**

Esta política aplica a todos los sistemas, servicios y aplicaciones que gestionen identidades de usuarios, incluyendo:

* Plataforma web y base de datos del proyecto.
* Repositorios de código y sistemas de control de versiones.
* Cuentas en la nube o servicios de terceros.
* Usuarios internos (equipo del proyecto) y externos (clientes).

**3. Principios de Gestión de Identidades**

1. **Unicidad:** Cada usuario tendrá una identidad única en el sistema.
2. **Autenticidad:** Toda identidad deberá ser verificada antes de otorgar acceso.
3. **Ciclo de vida controlado:** Las identidades deben crearse, modificarse y eliminarse siguiendo un proceso autorizado.
4. **Mínimo privilegio:** Cada identidad tendrá solo los permisos necesarios para su función.
5. **Trazabilidad:** Toda acción de creación, acceso o eliminación debe registrarse.

**4. Ciclo de Vida de la Identidad**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Creación** | Solicitud formal de cuenta, revisión y aprobación por la dirección. | Administrador del Sistema |
| **Modificación** | Cambios de permisos o rol por cambio de función. | Dirección / Administrador |
| **Revisión** | Auditoría periódica de accesos activos. | Administrador |
| **Eliminación** | Revocación inmediata de acceso cuando el usuario deja de participar. | Administrador / Dirección |

**5. Requisitos de Seguridad**

* Toda identidad debe vincularse con una persona real o función específica.
* Las credenciales deben almacenarse **cifradas y protegidas** (hash seguro con sal).
* Los accesos privilegiados (administradores, desarrolladores) deben estar **limitados y monitoreados**.
* La creación de usuarios sin autorización escrita o digital está prohibida.
* Los usuarios inactivos por más de **90 días** deben ser bloqueados o eliminados.
* El sistema debe registrar los eventos de inicio y cierre de sesión, intentos fallidos y cambios de privilegios.

**6. Responsabilidades**

* **Administrador del Sistema:**
  + Gestionar la creación, modificación y eliminación de identidades.
  + Garantizar la protección de las credenciales.
  + Revisar periódicamente las identidades y permisos.
* **Dirección del Proyecto:**
  + Aprobar la creación de usuarios con roles especiales.
  + Definir los criterios de acceso según responsabilidades.
* **Usuarios Autorizados:**
  + Mantener la confidencialidad de sus credenciales.
  + Notificar inmediatamente si detectan uso indebido o acceso no autorizado.

**7. Revisión y Actualización**

* El proceso de gestión de identidades se revisará **cada 6 meses** o cuando se cambie la infraestructura o modelo de roles.
* Los incidentes relacionados con identidades (accesos indebidos, duplicados, suplantaciones) se tratarán según el procedimiento de gestión de incidentes (controles 5.24–5.27).

**Información de Autenticación**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las políticas y medidas de seguridad para la **protección, creación, uso y gestión de la información de autenticación** en el proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.17 de la norma ISO/IEC 27001:2022.

El propósito es garantizar que las credenciales utilizadas para acceder al sistema sean **únicas, seguras, confidenciales y gestionadas adecuadamente**, previniendo el acceso no autorizado a los activos de información.

**2. Alcance**

Aplica a todas las formas de autenticación empleadas dentro del proyecto, incluyendo:

* Contraseñas de usuarios (internos y externos).
* Claves de API y tokens de acceso.
* Certificados digitales o credenciales emitidas por servicios externos.
* Códigos temporales o factores adicionales de autenticación (MFA).

**3. Requisitos de Seguridad de Autenticación**

* Las contraseñas deben tener **mínimo 8 caracteres**, incluir letras mayúsculas, minúsculas, números y símbolos.
* Las credenciales deben almacenarse mediante **algoritmos de hash seguros**.
* El sistema debe implementar **autenticación multifactor (MFA)** para usuarios administradores o con acceso privilegiado.
* Se deben bloquear las cuentas tras **5 intentos fallidos de autenticación**.
* Las claves de API y tokens deben tener **fecha de expiración definida** y ser rotados periódicamente.
* No se permite el uso de contraseñas por defecto ni el intercambio de credenciales entre usuarios.
* El sistema debe mantener **registros de inicio y cierre de sesión**, intentos fallidos y cambios de credenciales.

**4. Responsabilidades**

* **Administrador del Sistema:**
  + Implementar mecanismos de autenticación segura y protección de credenciales.
  + Monitorear intentos de acceso no autorizados.
  + Administrar la rotación de claves y contraseñas.
* **Dirección del Proyecto:**
  + Aprobar políticas de autenticación y asegurar su cumplimiento.
  + Revisar incidentes de seguridad relacionados con credenciales comprometidas.
* **Usuarios Autorizados:**
  + Mantener la confidencialidad de sus contraseñas y credenciales.
  + No guardar contraseñas en archivos o navegadores sin cifrado.
  + Reportar de inmediato si sospechan que su cuenta ha sido comprometida.

**5. Reglas de Cumplimiento**

* Está **prohibido compartir o reutilizar contraseñas** en diferentes sistemas del proyecto.
* Las credenciales deben transmitirse únicamente por **canales cifrados (HTTPS, SSH, TLS)**.
* Las credenciales de servicio (APIs o integraciones) deben almacenarse en entornos seguros, como cofres de contraseñas o variables de entorno cifradas.
* La autenticación de usuarios debe estar integrada con la **gestión de identidades** (ver control 5.16).

**6. Revisión y Actualización**

* Esta política será revisada **cada 12 meses** o cuando cambien los métodos de autenticación utilizados.
* Los incidentes relacionados con la autenticación serán gestionados conforme al procedimiento de incidentes (controles 5.24–5.27).

**Derechos de Acceso**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece los lineamientos para la **gestión, asignación, revisión y revocación de los derechos de acceso** a la información y recursos del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.18 de la ISO/IEC 27001:2022.

El objetivo es garantizar que los usuarios tengan únicamente los permisos necesarios para desempeñar sus funciones, evitando accesos indebidos o privilegios excesivos que comprometan la seguridad del sistema.

**2. Alcance**

Esta política aplica a todos los sistemas, aplicaciones, bases de datos y servicios en la nube utilizados en el proyecto, incluyendo:

* Plataforma web y Backend del sistema.
* Repositorios de código y almacenamiento de datos.
* Entornos de desarrollo, pruebas y producción.
* Cuentas de usuarios internos, proveedores y clientes.

**3. Principios de Asignación de Accesos**

1. **Principio de mínimo privilegio:** cada usuario tendrá el acceso estrictamente necesario para realizar su trabajo.
2. **Separación de funciones:** las tareas críticas estarán divididas entre diferentes usuarios para evitar conflictos de interés.
3. **Autorización previa:** ningún acceso podrá otorgarse sin aprobación de la dirección o del responsable designado.
4. **Revisión periódica:** los permisos se revisarán regularmente para detectar accesos innecesarios.
5. **Revocación inmediata:** los accesos se eliminarán de forma inmediata al finalizar la relación con el proyecto.

**4. Roles y Tipos de Acceso**

| **Rol** | **Tipo de Acceso** | **Ejemplo de Funciones Autorizadas** |
| --- | --- | --- |
| **Administrador del Sistema** | Acceso total | Configuración, monitoreo, gestión de usuarios. |
| **Desarrollador** | Acceso parcial controlado | Mantenimiento del código, entorno de pruebas. |
| **Usuario Operativo** | Acceso funcional limitado | Registro de servicios, consulta de datos de clientes. |
| **Cliente** | Acceso personal | Visualización de su información y reservas. |

**5. Procedimiento para Asignación y Revocación**

1. **Solicitud de acceso:** el usuario solicita acceso indicando su rol y funciones.
2. **Aprobación:** la dirección valida la necesidad y aprueba el nivel de acceso.
3. **Creación:** el administrador del sistema asigna los permisos en la aplicación o base de datos.
4. **Revisión periódica:** se auditan los accesos cada **3 meses**.
5. **Revocación:** los accesos se eliminan inmediatamente cuando un usuario cambia de rol o deja el proyecto.

**6. Reglas de Cumplimiento**

* Los accesos privilegiados deben estar **restringidos y monitoreados**.
* Está prohibido compartir credenciales o utilizar cuentas genéricas.
* Toda modificación en los permisos deberá registrarse en la bitácora de seguridad.
* Las credenciales y accesos deben alinearse con los controles de **Gestión de Identidades (5.16)** y **Autenticación (5.17)**.
* El incumplimiento de estas normas puede derivar en sanciones o suspensión del acceso al sistema.

**7. Responsabilidades**

* **Administrador del Sistema:**
  + Crear, modificar o revocar los accesos.
  + Registrar toda actividad de gestión de permisos.
* **Dirección del Proyecto:**
  + Aprobar accesos especiales o privilegiados.
  + Supervisar auditorías de acceso.
* **Usuarios Autorizados:**
  + Usar solo los accesos asignados y reportar cualquier acceso indebido detectado.

**8. Revisión y Actualización**

* Este procedimiento será revisado **anualmente** o tras incidentes de seguridad relacionados con accesos.
* Los resultados de auditorías de accesos serán documentados y analizados para aplicar mejoras.

**Seguridad en las Relaciones con Proveedores**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define los lineamientos para garantizar la **seguridad de la información compartida, procesada o accedida por proveedores y terceros** dentro del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.19 de la ISO/IEC 27001:2022.

El objetivo es establecer un marco seguro de relación con los proveedores que manejan activos, datos o servicios del proyecto, minimizando los riesgos de pérdida, filtración o mal uso de la información.

**2. Alcance**

Esta política aplica a todos los **proveedores externos, contratistas y aliados tecnológicos** que tengan acceso directo o indirecto a los activos de información del proyecto, incluyendo:

* Servicios en la nube o alojamiento web.
* Pasarelas de pago y plataformas de facturación.
* Proveedores de software o mantenimiento técnico.
* Consultores o terceros con acceso temporal al sistema o datos.

**3. Requisitos de Seguridad para Proveedores**

* Los proveedores deben cumplir con las políticas de seguridad de la información definidas por el proyecto.
* Antes de contratar cualquier servicio, se debe realizar una **evaluación de riesgos** sobre la información que será compartida.
* Los acuerdos con proveedores deben incluir cláusulas de **confidencialidad, protección de datos y cumplimiento normativo**.
* Los proveedores con acceso a información confidencial deben implementar **controles de autenticación y cifrado**.
* Se deben definir los procedimientos de notificación y respuesta ante incidentes de seguridad que involucren a terceros.
* Todo acceso otorgado a proveedores debe ser **temporal, controlado y registrado**.

**4. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar la contratación de proveedores con base en la evaluación de seguridad.
  + Asegurar que los contratos incluyan los requisitos de seguridad aplicables.
  + Supervisar el cumplimiento de las cláusulas de confidencialidad.
* **Administrador del Sistema:**
  + Gestionar los accesos y permisos otorgados a proveedores.
  + Monitorear las actividades realizadas por terceros dentro de los sistemas.
  + Revocar accesos al finalizar el contrato o servicio.
* **Proveedores:**
  + Cumplir con las normas y políticas de seguridad acordadas.
  + Notificar cualquier incidente o vulnerabilidad detectada en los servicios prestados.

**5. Reglas de Cumplimiento**

* Ningún proveedor podrá manipular información del proyecto sin autorización expresa y contractual.
* Los accesos otorgados deben tener una **fecha de expiración o límite temporal**.
* Los proveedores deben proteger la información según los mismos niveles de seguridad que utiliza el proyecto.
* En caso de incumplimiento, el contrato podrá suspenderse o rescindirse por razones de seguridad.

**6. Revisión y Seguimiento**

* Los contratos con proveedores serán revisados **anualmente** o cuando se renueven servicios.
* La dirección y el administrador del sistema deben realizar auditorías o revisiones de cumplimiento.
* Los incidentes de seguridad reportados por proveedores deben registrarse y analizarse para prevenir recurrencias.

**Seguridad en los Acuerdos con Proveedores**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece los **requisitos de seguridad que deben incluirse en los acuerdos, contratos o convenios con proveedores** del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.20 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que todos los proveedores que accedan a la información, sistemas o servicios del proyecto cumplan con las políticas de seguridad y protejan los datos conforme a la legislación vigente.

**2. Alcance**

Aplica a todos los proveedores y terceros que mantengan acuerdos contractuales con el proyecto, incluyendo:

* Servicios en la nube y alojamiento web.
* Plataformas de pago y gestión financiera.
* Consultores técnicos, desarrolladores externos o empresas de soporte.
* Proveedores de hardware, software y mantenimiento.

**3. Contenido de los Acuerdos con Proveedores**

Todo contrato o acuerdo debe contener, como mínimo, las siguientes **cláusulas de seguridad**:

| **Tipo de Cláusula** | **Descripción** |
| --- | --- |
| **Confidencialidad** | El proveedor debe proteger la información a la que accede y no divulgarla sin autorización. |
| **Protección de Datos Personales** | Cumplimiento con la legislación aplicable (Ley de Protección de Datos Personales y normas ISO). |
| **Propiedad Intelectual** | El proyecto conserva la titularidad de la información, software y documentación entregada al proveedor. |
| **Seguridad Técnica** | El proveedor debe aplicar medidas de cifrado, control de acceso y autenticación segura. |
| **Gestión de Incidentes** | Obligación del proveedor de informar cualquier incidente de seguridad detectado. |
| **Derecho de Auditoría** | El proyecto podrá auditar o revisar el cumplimiento de las cláusulas de seguridad. |
| **Finalización del Contrato** | El proveedor deberá eliminar o devolver toda la información del proyecto al finalizar la relación. |

**4. Responsabilidades**

* **Dirección del Proyecto:**
  + Supervisar que todos los acuerdos incluyan las cláusulas de seguridad requeridas.
  + Revisar los contratos antes de su firma y validar su cumplimiento.
* **Administrador del Sistema:**
  + Controlar los accesos otorgados a proveedores y garantizar su revocación al finalizar el contrato.
  + Verificar que los proveedores cumplan con los controles técnicos establecidos.
* **Proveedor:**
  + Cumplir las obligaciones contractuales y legales de seguridad.
  + Notificar cualquier evento que pueda afectar la seguridad del proyecto.

**5. Reglas de Cumplimiento**

* No se debe firmar ningún contrato sin la inclusión de las cláusulas de seguridad indicadas.
* Los acuerdos deben revisarse **anualmente o con cada renovación de servicio**.
* Los proveedores deberán conservar evidencias de cumplimiento de las políticas acordadas.
* En caso de incumplimiento o incidente grave, la organización podrá **suspender o terminar el contrato** por motivos de seguridad.

**6. Revisión y Actualización**

* Este procedimiento se revisará **cada 12 meses** o cuando se establezcan nuevos acuerdos con proveedores.
* Los cambios en la legislación o en los servicios contratados deberán reflejarse en la próxima versión del documento.

**Seguridad en la Cadena de Suministro TIC**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define las medidas de **seguridad de la información aplicables a la cadena de suministro de Tecnologías de la Información y la Comunicación (TIC)** del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.21 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que todos los proveedores, socios y componentes tecnológicos externos cumplan con los requisitos de seguridad necesarios para proteger la confidencialidad, integridad y disponibilidad de la información gestionada por el sistema.

**2. Alcance**

Esta política aplica a todos los **componentes, servicios y dependencias TIC externas** que apoyan el funcionamiento del sistema, incluyendo:

* Infraestructura en la nube (hosting, bases de datos, almacenamiento).
* Plataformas de pago y pasarelas financieras.
* Servicios de autenticación externa o APIs integradas.
* Proveedores de software, hardware y soporte técnico.
* Librerías y frameworks utilizados en el desarrollo del sistema.

**3. Requisitos de Seguridad en la Cadena de Suministro**

* Los proveedores de TIC deben cumplir con las políticas de seguridad del proyecto y las normas internacionales aplicables.
* Antes de integrar cualquier servicio o tecnología externa, se debe realizar una **evaluación de riesgos** y validación técnica.
* Los contratos con proveedores deben incluir cláusulas de **protección de datos, confidencialidad y notificación de incidentes**.
* Todo componente de software externo debe ser **verificado y mantenido actualizado** para evitar vulnerabilidades conocidas.
* Los accesos concedidos a servicios o personal de terceros deben ser **controlados, temporales y documentados**.
* Los datos compartidos con proveedores deben ser transmitidos mediante **canales cifrados (HTTPS, SFTP, VPN)**.
* El proyecto debe mantener un **registro actualizado de proveedores TIC** y los servicios que ofrecen.

**4. Responsabilidades**

* **Dirección del Proyecto:**
  + Asegurar que las relaciones dentro de la cadena de suministro cumplan con los estándares de seguridad requeridos.
  + Revisar periódicamente los contratos y evaluaciones de proveedores TIC.
* **Administrador del Sistema:**
  + Controlar la integración y mantenimiento de componentes externos.
  + Validar la seguridad de APIs, librerías y dependencias utilizadas.
  + Monitorear el cumplimiento de las políticas por parte de los proveedores tecnológicos.
* **Proveedores TIC:**
  + Mantener sus sistemas protegidos y actualizados.
  + Notificar cualquier incidente o brecha de seguridad que pueda afectar al proyecto.

**5. Reglas de Cumplimiento**

* No se debe incorporar ningún componente o proveedor TIC sin la evaluación previa de seguridad.
* Todo software o librería externa debe provenir de **fuentes oficiales y verificadas**.
* Las actualizaciones y parches deben aplicarse de forma oportuna.
* Los incidentes en la cadena de suministro deben gestionarse según el procedimiento de incidentes (controles 5.24–5.27).
* El incumplimiento de estas normas puede resultar en la suspensión o reemplazo del proveedor.

**6. Revisión y Actualización**

* Este documento se revisará **anualmente** o cuando se integren nuevos servicios o componentes tecnológicos.
* Se documentará cada evaluación de proveedor TIC como evidencia de cumplimiento del SGSI.

**Gestión de Servicios de Proveedores**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define los procesos y responsabilidades para la **gestión de los servicios prestados por proveedores** en el proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.22 de la norma ISO/IEC 27001:2022.

El objetivo es asegurar que los proveedores cumplan de forma continua con los **requisitos de seguridad, calidad y desempeño**, y que sus servicios se mantengan alineados con las políticas del Sistema de Gestión de Seguridad de la Información (SGSI).

**2. Alcance**

Esta política aplica a todos los **servicios contratados a terceros**, incluyendo:

* Hosting y servicios en la nube.
* Pasarelas de pago y facturación electrónica.
* Soporte técnico, mantenimiento o consultoría.
* Servicios de software de terceros integrados al sistema.

**3. Principios de Gestión de Servicios**

1. **Evaluación inicial:** todo proveedor debe ser evaluado antes de la contratación, considerando su capacidad técnica, cumplimiento normativo y seguridad.
2. **Acuerdos documentados:** cada servicio debe estar formalizado mediante un contrato o acuerdo de nivel de servicio (SLA).
3. **Supervisión continua:** los servicios deben monitorearse regularmente para verificar su cumplimiento.
4. **Comunicación activa:** los proveedores deben mantener canales de comunicación abiertos ante cambios o incidentes.
5. **Revisión periódica:** los servicios se revisarán al menos una vez al año para evaluar su desempeño y seguridad.

**4. Criterios de Evaluación y Seguimiento**

| **Criterio** | **Descripción** | **Frecuencia de Revisión** |
| --- | --- | --- |
| **Cumplimiento del SLA** | Verificar tiempos de respuesta, disponibilidad y soporte acordados. | Trimestral |
| **Seguridad de la Información** | Confirmar aplicación de controles de seguridad, cifrado y gestión de incidentes. | Semestral |
| **Confidencialidad de Datos** | Comprobar el cumplimiento de las cláusulas de protección de datos. | Semestral |
| **Actualización del Servicio** | Evaluar mejoras, parches o nuevas versiones aplicadas. | Anual |
| **Riesgos Asociados** | Analizar riesgos derivados del servicio y sus posibles impactos. | Continuo |

**5. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar los contratos y supervisar el cumplimiento de los SLA.
  + Evaluar el desempeño de los proveedores y tomar decisiones de renovación o sustitución.
* **Administrador del Sistema:**
  + Monitorear los servicios activos y registrar incidencias.
  + Verificar que los proveedores apliquen las medidas de seguridad acordadas.
* **Proveedor:**
  + Cumplir con los compromisos de calidad y seguridad establecidos en el contrato.
  + Notificar de inmediato cualquier cambio, interrupción o incidente.

**6. Reglas de Cumplimiento**

* Todo servicio debe estar respaldado por un **acuerdo formal (SLA)** que especifique responsabilidades y niveles mínimos de servicio.
* Los proveedores deben proporcionar **evidencias de cumplimiento** cuando sean requeridas.
* Si un proveedor incumple repetidamente los niveles de servicio o medidas de seguridad, se procederá a **evaluar su reemplazo**.
* Los incidentes con proveedores se documentarán en el sistema de gestión de incidentes del SGSI.

**7. Revisión y Actualización**

* Esta política se revisará **anualmente** o tras modificaciones significativas en los servicios o contratos vigentes.
* Los resultados de las revisiones servirán como base para los reportes de cumplimiento del SGSI.

**Gestión de Incidentes de Seguridad de la Información y Comunicación**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las políticas y procedimientos para la **gestión, notificación, respuesta y comunicación de incidentes de seguridad de la información** en el proyecto *Lava Rápido Vehicular*, conforme al control A.5.23 de la ISO/IEC 27001:2022.

El objetivo es garantizar que todos los incidentes reales o potenciales se identifiquen, reporten y gestionen de manera oportuna para minimizar su impacto en la confidencialidad, integridad y disponibilidad de la información.

**2. Alcance**

Esta política aplica a todo el personal, contratistas y proveedores que participen en el proyecto, y a cualquier sistema, equipo o información que pueda verse afectado por un incidente, incluyendo:

* Aplicación web, bases de datos y servicios en la nube.
* Dispositivos de almacenamiento y comunicación.
* Plataformas de terceros conectadas al sistema (por ejemplo, pasarela de pagos).

**3. Definición de Incidente de Seguridad**

Se considera incidente de seguridad cualquier evento que:

* Comprometa la **confidencialidad, integridad o disponibilidad** de la información.
* Ocurra por **error humano, fallo técnico o acción deliberada**.
* Requiera una respuesta inmediata o una investigación posterior.

Ejemplos:

* Accesos no autorizados a la base de datos.
* Pérdida o robo de información sensible.
* Fuga de credenciales o contraseñas.
* Infección por malware o ataques de denegación de servicio (DoS).
* Fallos en las copias de seguridad o restauración de datos.

**4. Proceso de Gestión de Incidentes**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación** | Detección del incidente a través de reportes o monitoreo. | Cualquier usuario / Administrador |
| **Notificación** | Comunicación inmediata al responsable de seguridad. | Usuario que detecta el evento |
| **Análisis** | Evaluación del tipo, origen y alcance del incidente. | Administrador / Dirección |
| **Contención y Mitigación** | Acciones para limitar el impacto y restaurar servicios. | Equipo Técnico |
| **Registro** | Documentación del incidente en el registro de seguridad. | Responsable de Seguridad |
| **Revisión y Lecciones Aprendidas** | Evaluación final y mejora de controles. | Dirección / SGSI |

**5. Canales de Comunicación**

* Los incidentes deben reportarse de inmediato al correo institucional: **seguridad@lavarapido.com** (o canal definido).
* En caso de emergencia, se debe comunicar directamente con el **responsable de seguridad** o la **dirección del proyecto**.
* Los proveedores deberán notificar cualquier incidente que involucre información del proyecto **dentro de las primeras 24 horas** de detección.

**6. Registro de Incidentes**

Cada incidente debe documentarse incluyendo:

* Fecha y hora del evento.
* Persona que lo detectó y medio de notificación.
* Descripción del incidente y sistemas afectados.
* Acciones correctivas aplicadas.
* Resultado final y medidas preventivas futuras.

**7. Responsabilidades**

* **Responsable de Seguridad / Administrador del Sistema:**
  + Recibir y gestionar los reportes de incidentes.
  + Aplicar medidas de contención y registrar la evidencia.
  + Coordinar con el equipo técnico la recuperación del sistema.
* **Dirección del Proyecto:**
  + Aprobar las decisiones críticas y reportar al cliente o autoridad competente si es necesario.
  + Supervisar la revisión post-incidente y las mejoras del SGSI.
* **Usuarios y Proveedores:**
  + Reportar cualquier evento sospechoso de manera inmediata.

**8. Revisión y Actualización**

* Este procedimiento será revisado **anualmente** o después de un incidente significativo.
* Se utilizarán los resultados de cada evento para mejorar la detección y respuesta ante futuros incidentes.

**Notificación de Incidentes de Seguridad de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define el proceso y los canales oficiales para la **notificación o reporte de incidentes de seguridad de la información** dentro del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.24 de la norma ISO/IEC 27001:2022.

El objetivo es asegurar que todos los incidentes, sospechas o vulnerabilidades sean **reportados inmediatamente**, para permitir una respuesta rápida y efectiva que minimice el impacto sobre los activos de información.

**2. Alcance**

Aplica a todo el personal, colaboradores, contratistas y proveedores del proyecto que detecten o sospechen la ocurrencia de un incidente de seguridad relacionado con:

* Datos de clientes, usuarios o del sistema.
* Accesos no autorizados o intentos de intrusión.
* Pérdida, robo o divulgación de información.
* Fallos de disponibilidad o integridad en los servicios.

**3. Principios de Notificación**

1. **Inmediatez:** Los incidentes deben reportarse tan pronto sean detectados.
2. **Exactitud:** El reporte debe incluir información clara, verificable y detallada.
3. **Trazabilidad:** Todo incidente reportado debe registrarse oficialmente.
4. **No represalias:** Ningún empleado o colaborador será sancionado por reportar un incidente de buena fe.
5. **Confidencialidad:** La información del incidente será manejada de forma segura y restringida.

**4. Procedimiento de Notificación**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Detección** | Identificación de un evento anómalo o incidente. | Cualquier usuario / proveedor |
| **Reporte Inicial** | Envío del reporte por los canales oficiales. | Usuario / empleado |
| **Registro Formal** | Creación de un registro en la bitácora de incidentes. | Administrador del Sistema |
| **Evaluación** | Análisis preliminar del tipo y severidad del incidente. | Responsable de Seguridad |
| **Escalamiento** | Si el incidente es grave, se comunica a la Dirección del Proyecto. | Responsable de Seguridad |

**5. Canales de Notificación**

* **Formulario web interno:** Portal SGSI → “Reportar Incidente”
* **Línea directa:** [Número interno de contacto de seguridad]
* **Notificación a terceros:** Los proveedores deben notificar incidentes dentro de las **24 horas posteriores a la detección**.

**6. Contenido Mínimo del Reporte**

Cada notificación debe incluir:

* Fecha y hora de detección.
* Descripción del evento y su impacto aparente.
* Activos o sistemas afectados.
* Evidencias o capturas de pantalla (si aplica).

**7. Responsabilidades**

* **Usuarios y Proveedores:**
  + Reportar inmediatamente cualquier incidente o sospecha.
* **Administrador del Sistema:**
  + Registrar y clasificar los incidentes notificados.
  + Comunicar los reportes a la dirección y al responsable de seguridad.
* **Dirección del Proyecto:**
  + Evaluar la necesidad de activar el plan de respuesta o notificar a las autoridades.

**8. Revisión y Seguimiento**

* Todos los incidentes notificados deben ser **analizados y documentados** hasta su cierre.
* Los reportes y resultados se revisarán **mensualmente** como parte del control de seguridad continua.
* Las lecciones aprendidas se utilizarán para fortalecer los controles y procedimientos del SGSI.

**Evaluación y Decisión sobre Incidentes de Seguridad de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece el proceso formal de **evaluación, clasificación y toma de decisiones ante incidentes de seguridad de la información**, en cumplimiento del control A.5.25 de la norma ISO/IEC 27001:2022.

El objetivo es asegurar que cada incidente sea analizado de forma sistemática para determinar su gravedad, origen, impacto y las acciones correctivas necesarias, permitiendo una respuesta proporcional y eficiente.

**2. Alcance**

Este procedimiento aplica a todos los incidentes de seguridad detectados o reportados dentro del proyecto *Lava Rápido Vehicular*, incluyendo:

* Accesos no autorizados a datos o sistemas.
* Pérdida o exposición de información confidencial.
* Fallos de disponibilidad en los servicios tecnológicos.
* Vulnerabilidades explotadas o brechas de seguridad.

Aplica también a los incidentes notificados por **proveedores o terceros** que afecten los servicios o datos del proyecto.

**3. Principios de Evaluación**

1. **Objetividad:** El análisis se basa en hechos verificables y evidencias.
2. **Trazabilidad:** Cada incidente debe documentarse completamente.
3. **Priorización:** Los incidentes se clasifican por nivel de impacto y urgencia.
4. **Acción Correctiva:** Toda decisión debe incluir una medida preventiva o de mitigación.
5. **Lecciones Aprendidas:** Los resultados deben alimentar la mejora continua del SGSI.

**4. Proceso de Evaluación y Decisión**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Recepción del Incidente** | Se recibe el reporte formal del incidente (ver control 5.24). | Administrador / Responsable de Seguridad |
| **Clasificación** | Se determina la categoría del incidente (baja, media, alta, crítica). | Responsable de Seguridad |
| **Análisis de Causa y Efecto** | Se identifican los sistemas afectados, causa raíz y alcance. | Equipo Técnico |
| **Evaluación del Impacto** | Se evalúa el efecto en la confidencialidad, integridad y disponibilidad. | Dirección / Responsable de Seguridad |
| **Decisión de Respuesta** | Se decide si aplicar contención, recuperación o escalamiento. | Dirección del Proyecto |
| **Documentación** | Se registran los resultados y decisiones adoptadas. | Responsable de Seguridad |

**5. Criterios de Clasificación de Incidentes**

| **Nivel** | **Descripción** | **Acción Requerida** |
| --- | --- | --- |
| **Bajo** | Impacto mínimo, sin afectación al servicio o datos. | Registro y cierre. |
| **Medio** | Afectación parcial o temporal de un sistema. | Contención y revisión. |
| **Alto** | Compromiso de información sensible o indisponibilidad significativa. | Activación del plan de respuesta. |
| **Crítico** | Brecha de seguridad grave o pérdida masiva de datos. | Notificación a dirección y autoridades, mitigación urgente. |

**6. Responsabilidades**

* **Administrador del Sistema:**
  + Recopilar y preservar evidencias del incidente.
  + Ejecutar acciones técnicas de contención o restauración.
* **Responsable de Seguridad:**
  + Clasificar el incidente y coordinar la evaluación.
  + Emitir el informe de evaluación con las decisiones adoptadas.
* **Dirección del Proyecto:**
  + Aprobar decisiones de escalamiento y notificación externa.
  + Validar el cierre formal del incidente.

**7. Registro y Seguimiento**

Cada incidente evaluado debe registrarse en la **bitácora de seguridad**, incluyendo:

* Fecha y hora de la detección y cierre.
* Clasificación asignada.
* Causa raíz y medidas tomadas.
* Impacto real y acciones preventivas implementadas.

**8. Revisión y Actualización**

* Este procedimiento será revisado **anualmente** o después de incidentes críticos.
* Las lecciones aprendidas se incorporarán a los controles y políticas futuras.

**Respuesta a Incidentes de Seguridad de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define las **acciones, procedimientos y responsabilidades para responder a incidentes de seguridad de la información**, en cumplimiento del control A.5.26 de la ISO/IEC 27001:2022.

El objetivo es establecer un proceso estructurado que permita **contener, mitigar y recuperar los servicios afectados**, minimizando los daños y evitando recurrencias.

**2. Alcance**

Este procedimiento aplica a todos los incidentes de seguridad que afecten:

* Los sistemas, datos o servicios del proyecto *Lava Rápido Vehicular*.
* Los activos tecnológicos de proveedores o aliados integrados al sistema.
* Cualquier infraestructura crítica relacionada con la operación o almacenamiento de información.

Incluye tanto incidentes confirmados como sospechosos que puedan comprometer la confidencialidad, integridad o disponibilidad de la información.

**3. Principios de Respuesta**

1. **Rapidez:** Actuar de forma inmediata para reducir el impacto.
2. **Coordinación:** Las acciones deben ser ejecutadas por roles claramente definidos.
3. **Documentación:** Todas las medidas adoptadas deben registrarse.
4. **Recuperación controlada:** Los sistemas deben restaurarse bajo supervisión.
5. **Aprendizaje continuo:** Cada incidente debe servir para fortalecer la seguridad futura.

**4. Fases del Proceso de Respuesta**

| **Fase** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Contención Inicial** | Aislar los sistemas o cuentas afectadas para evitar propagación. | Administrador / Equipo Técnico |
| **Mitigación** | Aplicar medidas inmediatas para detener el ataque o eliminar la amenaza. | Administrador / Responsable de Seguridad |
| **Erradicación** | Identificar y eliminar la causa raíz del incidente (malware, error, brecha). | Equipo Técnico |
| **Recuperación** | Restaurar sistemas, servicios y datos a su estado normal operativo. | Administrador / Dirección |
| **Verificación** | Confirmar que el sistema es seguro y funcional antes de reactivarlo. | Responsable de Seguridad |
| **Informe Final** | Documentar las acciones realizadas y las lecciones aprendidas. | Responsable de Seguridad / Dirección |

**5. Acciones Inmediatas ante un Incidente**

* Desconectar sistemas comprometidos o afectados de la red.
* Bloquear cuentas o accesos involucrados.
* Notificar inmediatamente al responsable de seguridad y a la dirección del proyecto.
* Conservar evidencia digital (registros, logs, archivos) sin alterarla.
* Activar los planes de respaldo o recuperación si hay pérdida de información.

**6. Coordinación y Comunicación**

* El **responsable de seguridad** coordinará las acciones con el equipo técnico y dirección.
* Las comunicaciones externas (clientes, autoridades, proveedores) deben realizarse **solo con aprobación de la dirección del proyecto**.
* Se mantendrá un **registro cronológico de las acciones ejecutadas** durante todo el proceso.

**7. Responsabilidades**

* **Administrador del Sistema:**
  + Implementar medidas de contención y restauración.
  + Asegurar la integridad de la evidencia digital.
* **Responsable de Seguridad:**
  + Coordinar la respuesta, evaluar el impacto y elaborar el informe final.
* **Dirección del Proyecto:**
  + Autorizar decisiones críticas y la reanudación de los servicios afectados.

**8. Revisión y Actualización**

* Este procedimiento será revisado **anualmente** o tras un incidente relevante.
* Se actualizarán los planes de respuesta con base en las lecciones aprendidas.
* Los resultados se documentarán como parte del proceso de mejora continua del SGSI.

**Aprendizaje a partir de Incidentes de Seguridad de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las directrices para **analizar y aprovechar la información obtenida de los incidentes de seguridad** ocurridos en el proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.27 de la norma ISO/IEC 27001:2022.

El propósito es identificar las causas raíz, mejorar los controles de seguridad, prevenir recurrencias y fortalecer el **Sistema de Gestión de Seguridad de la Información (SGSI)** mediante el aprendizaje continuo.

**2. Alcance**

Aplica a todos los incidentes de seguridad registrados, tanto internos como externos, y a los que afecten:

* Datos personales y operativos del sistema.
* Servicios tecnológicos del proyecto (web, base de datos, nube).
* Proveedores o terceros vinculados al procesamiento de información.

También aplica a los **eventos de seguridad potenciales**, incluso si no se materializan, con el fin de aprender de situaciones cercanas a incidentes.

**3. Principios de Aprendizaje**

1. **Documentación:** Todo incidente debe registrar causas, acciones y resultados.
2. **Evaluación crítica:** Analizar qué controles fallaron o fueron insuficientes.
3. **Prevención:** Implementar medidas que eviten recurrencias.
4. **Difusión controlada:** Compartir las lecciones aprendidas solo con el personal autorizado.
5. **Mejora continua:** Incorporar las lecciones en políticas, procesos y formación del personal.

**4. Proceso de Aprendizaje Post-Incidente**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Recolección de Evidencias** | Se consolidan registros, informes e información técnica del incidente. | Administrador / Responsable de Seguridad |
| **Análisis de Causa Raíz** | Se identifican las causas directas e indirectas del incidente. | Responsable de Seguridad / Equipo Técnico |
| **Evaluación de Controles** | Se revisa si los controles existentes fueron adecuados o fallaron. | Responsable de Seguridad |
| **Definición de Acciones Correctivas** | Se establecen nuevas medidas para evitar la repetición del evento. | Dirección del Proyecto |
| **Difusión de Lecciones Aprendidas** | Se comunica el aprendizaje al personal relevante del proyecto. | Responsable de Seguridad |
| **Actualización de Procedimientos** | Se revisan políticas o procesos afectados. | Dirección / SGSI |

**5. Tipos de Acciones Derivadas**

* **Técnicas:** Aplicación de nuevos parches, mejoras en autenticación o cifrado.
* **Procedimentales:** Modificación de protocolos de comunicación o control de acceso.
* **Formativas:** Capacitación al personal en buenas prácticas de seguridad.
* **Contractuales:** Actualización de cláusulas con proveedores o aliados tecnológicos.

**6. Registro y Seguimiento**

Cada incidente debe generar un **Informe de Lecciones Aprendidas**, que incluya:

* Descripción del incidente.
* Causa raíz y factores contribuyentes.
* Medidas correctivas adoptadas.
* Eficacia de la respuesta.
* Recomendaciones futuras.

Los informes se almacenarán en el **repositorio del SGSI** y serán revisados en las reuniones de seguridad trimestrales.

**7. Responsabilidades**

* **Responsable de Seguridad:**
  + Liderar el análisis post-incidente.
  + Documentar y comunicar las lecciones aprendidas.
* **Administrador del Sistema:**
  + Apoyar con la evidencia técnica y evaluación de controles.
* **Dirección del Proyecto:**
  + Validar las acciones correctivas y su implementación en el SGSI.

**8. Revisión y Actualización**

* Este procedimiento se revisará **anualmente** o tras cada incidente relevante.
* Las lecciones aprendidas se integrarán en los controles 5.23–5.26 y en los planes de capacitación del personal.

**Evaluación de la Eficacia de la Seguridad de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 02 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define el proceso mediante el cual el proyecto *Lava Rápido Vehicular* **evalúa la eficacia de sus controles y políticas de seguridad de la información**, en cumplimiento del control A.5.28 de la norma ISO/IEC 27001:2022.

El objetivo es determinar si los controles implementados funcionan adecuadamente, identificar deficiencias y establecer acciones de mejora continua dentro del **Sistema de Gestión de Seguridad de la Información (SGSI)**.

**2. Alcance**

Esta política aplica a todos los procesos, activos y controles relacionados con la seguridad de la información, incluyendo:

* Controles técnicos (acceso, cifrado, autenticación, respaldos).
* Controles administrativos (políticas, procedimientos, revisiones).
* Controles físicos y organizacionales.
* Actividades realizadas por empleados, proveedores y terceros que impacten la seguridad.

**3. Objetivos de la Evaluación**

1. Verificar que los controles implementados cumplen con los requisitos definidos.
2. Medir la eficacia de los controles mediante indicadores y resultados tangibles.
3. Detectar desviaciones, vulnerabilidades o brechas en los procedimientos.
4. Proporcionar información para la mejora continua del SGSI.

**4. Metodología de Evaluación**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Planificación** | Definir qué controles serán evaluados, cuándo y cómo. | Responsable de Seguridad / Dirección |
| **Recolección de Evidencias** | Obtener registros, reportes, métricas o entrevistas. | Administrador del Sistema / Equipo Técnico |
| **Evaluación** | Comparar los resultados con los objetivos definidos en el SGSI. | Responsable de Seguridad |
| **Análisis de Desempeño** | Identificar fortalezas, debilidades y áreas de mejora. | Dirección del Proyecto |
| **Informe de Resultados** | Elaborar un informe con hallazgos y recomendaciones. | Responsable de Seguridad |
| **Seguimiento** | Monitorear la implementación de las mejoras propuestas. | Dirección / SGSI |

**5. Indicadores de Eficacia**

Algunos ejemplos de indicadores utilizados en la evaluación son:

* Porcentaje de incidentes gestionados en el tiempo establecido.
* Cumplimiento de políticas de acceso y autenticación.
* Disponibilidad del sistema y continuidad del servicio.
* Resultados de auditorías internas o revisiones.
* Cumplimiento de acuerdos de confidencialidad y manejo de datos.

**6. Responsabilidades**

* **Responsable de Seguridad:**
  + Coordinar la evaluación de controles y recopilar evidencias.
  + Emitir el informe de resultados y proponer acciones correctivas.
* **Administrador del Sistema:**
  + Suministrar los registros técnicos y reportes de desempeño.
* **Dirección del Proyecto:**
  + Aprobar las acciones de mejora y asignar recursos para su implementación.

**7. Frecuencia de Evaluación**

* Las evaluaciones se realizarán **al menos una vez al año** o cuando:
  + Se introduzcan nuevos sistemas o controles.
  + Ocurran incidentes significativos.
  + Se detecten desviaciones en auditorías internas.

**8. Revisión y Mejora Continua**

* Los resultados de cada evaluación se utilizarán para **actualizar los procedimientos, políticas y controles** del SGSI.
* Las deficiencias detectadas deberán ser tratadas mediante planes de acción documentados.
* Las mejoras se verificarán en la siguiente evaluación o auditoría interna.

**Revisión y Aprobación de Políticas de Seguridad de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 03 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece el procedimiento para la **revisión, actualización y aprobación de las políticas de seguridad de la información**, conforme al control A.5.29 de la norma ISO/IEC 27001:2022.

El objetivo es asegurar que todas las políticas del proyecto *Lava Rápido Vehicular* se mantengan **actualizadas, alineadas con los objetivos del negocio y efectivas ante los cambios tecnológicos o normativos**.

**2. Alcance**

Aplica a todas las políticas, normas y procedimientos relacionados con la seguridad de la información dentro del proyecto, incluyendo:

* Políticas de acceso, autenticación y gestión de identidades.
* Políticas de respaldo, continuidad y manejo de incidentes.
* Políticas de proveedores, privacidad y protección de datos.
* Documentos del Sistema de Gestión de Seguridad de la Información (SGSI).

**3. Principios de Revisión**

1. **Periodicidad:** Las políticas deben revisarse al menos **una vez al año**.
2. **Pertinencia:** Toda revisión debe considerar cambios tecnológicos, regulatorios o organizacionales.
3. **Participación:** La revisión debe involucrar a las áreas técnica, directiva y de seguridad.
4. **Trazabilidad:** Todas las versiones deben registrarse, conservarse y controlarse.
5. **Aprobación formal:** Ninguna política entra en vigor sin la aprobación de la dirección.

**4. Procedimiento de Revisión y Aprobación**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación de Políticas a Revisar** | Se define qué documentos requieren actualización. | Responsable de Seguridad |
| **Revisión de Contenido** | Se analiza la vigencia y coherencia con los objetivos del proyecto. | Equipo de Seguridad / Dirección |
| **Actualización** | Se introducen los cambios necesarios (mejoras, ajustes normativos, etc.). | Responsable de Seguridad |
| **Validación Técnica y Legal** | Se verifica el cumplimiento con los requisitos legales y técnicos. | Dirección del Proyecto |
| **Aprobación Final** | La dirección aprueba la versión actualizada del documento. | Dirección / Comité del SGSI |
| **Publicación y Comunicación** | La política aprobada se distribuye a todos los involucrados. | Responsable de Seguridad |

**5. Criterios de Revisión**

* Cambios en las operaciones del sistema o servicios del proyecto.
* Nuevas amenazas o vulnerabilidades detectadas.
* Modificaciones en la legislación o normativa aplicable.
* Resultados de auditorías internas o externas.
* Retroalimentación de usuarios o lecciones aprendidas.

**6. Control de Versiones**

Cada política debe incluir en su portada:

* Código o número de control.
* Fecha de emisión y versión.
* Autor y revisor.
* Fecha de aprobación y firma del responsable.
* Historial de cambios realizados.

**7. Responsabilidades**

* **Responsable de Seguridad:**
  + Coordinar la revisión y actualización de las políticas.
  + Garantizar su almacenamiento y distribución controlada.
* **Dirección del Proyecto:**
  + Aprobar las versiones finales.
  + Comunicar los cambios relevantes al personal.
* **Equipo Técnico:**
  + Aportar información sobre la efectividad y aplicabilidad de las políticas.

**8. Revisión y Actualización**

* Este procedimiento será revisado **anualmente o tras un cambio significativo** en el entorno del proyecto.
* Se mantendrá un registro actualizado de todas las versiones aprobadas.

**Documentación del Sistema de Gestión de Seguridad de la Información (SGSI)**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 03 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define las directrices y requisitos para la **elaboración, control, mantenimiento y protección de la documentación del SGSI**, en cumplimiento del control A.5.30 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que toda la información relacionada con la seguridad esté **claramente documentada, actualizada, disponible y protegida contra accesos no autorizados o pérdida**.

**2. Alcance**

Aplica a todos los documentos que componen el **Sistema de Gestión de Seguridad de la Información** del proyecto *Lava Rápido Vehicular*, incluyendo:

* Políticas y procedimientos de seguridad.
* Registros, formularios y bitácoras.
* Planes de respuesta, continuidad y recuperación.
* Documentos de evaluación de riesgos y auditorías.
* Declaraciones de aplicabilidad (SoA) y planes de acción.

**3. Principios de Gestión Documental**

1. **Estandarización:** Todos los documentos deben seguir una estructura y formato uniforme.
2. **Control de versiones:** Cada documento debe tener código, fecha, versión y responsable.
3. **Accesibilidad:** Los documentos deben estar disponibles para el personal autorizado.
4. **Confidencialidad:** Solo se otorgará acceso según los roles definidos en el SGSI.
5. **Conservación:** La documentación se mantendrá actualizada y almacenada en entornos seguros.
6. **Trazabilidad:** Todos los cambios deben ser registrados y auditables.

**4. Estructura del SGSI Documentado**

| **Tipo de Documento** | **Ejemplo o Descripción** | **Responsable** |
| --- | --- | --- |
| **Políticas** | Políticas de acceso, respaldo, proveedores, etc. | Dirección / Seguridad |
| **Procedimientos** | Procedimientos de incidentes, auditoría, evaluación, etc. | Responsable de Seguridad |
| **Registros** | Logs, bitácoras, formularios de control, auditorías. | Administrador / SGSI |
| **Informes** | Resultados de evaluaciones o revisiones. | Seguridad / Dirección |
| **Manuales y Planes** | Manual del SGSI, Plan de continuidad, Plan de respuesta. | Seguridad / Dirección |

**5. Control de Documentos**

* Todos los documentos deben tener un **identificador único (código SGSI-XXX)**.
* Las versiones obsoletas deben **archivarse y marcarse como “NO VIGENTES”**.
* La modificación de documentos requiere aprobación de la **Dirección del Proyecto**.
* Se debe llevar un **registro de control de versiones** que indique autor, fecha, cambios y motivo.
* Los documentos confidenciales se almacenarán en ubicaciones seguras (repositorio con acceso controlado o nube cifrada).

**6. Creación y Revisión**

1. **Creación:** Elaboración inicial del documento por parte del responsable designado.
2. **Revisión:** Validación técnica y legal antes de su aprobación.
3. **Aprobación:** Firma o autorización de la dirección.
4. **Difusión:** Comunicación a los usuarios relevantes y publicación en el repositorio oficial.
5. **Revisión periódica:** Cada documento debe revisarse **al menos una vez al año** o cuando se produzcan cambios significativos.

**7. Responsabilidades**

* **Responsable de Seguridad:**
  + Elaborar, mantener y proteger la documentación del SGSI.
  + Controlar versiones y acceso.
* **Administrador del Sistema:**
  + Garantizar el respaldo y disponibilidad digital de los documentos.
* **Dirección del Proyecto:**
  + Aprobar los documentos y asegurar su cumplimiento.

**8. Revisión y Actualización**

* Este procedimiento será revisado **anualmente** o tras auditorías internas o externas.
* Toda actualización se registrará en la tabla de control de versiones con su motivo y fecha.

**Identificación de Requisitos Legales, Reglamentarios y Contractuales**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 03 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define el proceso de **identificación, evaluación y cumplimiento de los requisitos legales, reglamentarios y contractuales** relacionados con la seguridad de la información en el proyecto *Lava Rápido Vehicular*, conforme al control A.5.31 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que el proyecto cumpla con todas las leyes y compromisos aplicables, protegiendo los datos personales, los derechos de los usuarios y las obligaciones establecidas con terceros.

**2. Alcance**

Este procedimiento aplica a todas las actividades, contratos, servicios y operaciones que involucren el manejo, almacenamiento o procesamiento de información dentro del proyecto, incluyendo:

* Tratamiento de datos personales de clientes y empleados.
* Contratos con proveedores, aliados y pasarelas de pago.
* Licencias de software, uso de herramientas y servicios en la nube.
* Requisitos normativos nacionales e internacionales aplicables.

**3. Requisitos Legales y Normativos Relevantes**

| **Tipo de Requisito** | **Descripción** | **Entidad / Fuente Legal** |
| --- | --- | --- |
| **Protección de Datos Personales** | Cumplimiento de la Ley 1581 de 2012 (Colombia) y sus decretos reglamentarios. | Superintendencia de Industria y Comercio (SIC) |
| **Comercio Electrónico** | Cumplimiento de la Ley 527 de 1999 sobre mensajes de datos y comercio electrónico. | Ministerio TIC |
| **Derechos del Consumidor** | Aplicación de la Ley 1480 de 2011 (Estatuto del Consumidor). | Superintendencia de Industria y Comercio |
| **Seguridad Digital** | Cumplimiento de la Política Nacional de Seguridad Digital y lineamientos del MinTIC. | Gobierno Nacional / MinTIC |
| **Propiedad Intelectual y Software** | Uso legal de licencias de software y respeto por derechos de autor. | Dirección Nacional de Derechos de Autor |
| **Contratos con Proveedores** | Inclusión de cláusulas de confidencialidad y seguridad de la información. | Contratos del Proyecto |
| **Normas Internacionales** | Referencia a estándares ISO/IEC 27001, 27002 y 27701 para gestión de seguridad y privacidad. | ISO / IEC |

**4. Procedimiento de Identificación y Cumplimiento**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación** | Se listan todas las leyes y regulaciones aplicables al proyecto. | Responsable de Seguridad / Dirección |
| **Evaluación** | Se analiza el impacto de cada requisito sobre las operaciones. | Dirección / Jurídico |
| **Implementación** | Se definen controles o políticas para cumplir los requisitos. | Responsable de Seguridad |
| **Monitoreo** | Se revisa el cumplimiento de forma continua o ante cambios normativos. | Dirección / SGSI |
| **Actualización** | Se ajusta la lista de requisitos cuando se promulguen nuevas leyes. | Responsable de Seguridad |

**5. Mecanismos de Cumplimiento**

* Incorporar los requisitos legales en las políticas y contratos del proyecto.
* Mantener evidencia documental del cumplimiento (acuerdos, avisos de privacidad, consentimientos).
* Revisar periódicamente las obligaciones vigentes con el apoyo de asesoría legal.
* Aplicar medidas técnicas y organizacionales para cumplir con los principios de seguridad y confidencialidad.

**6. Responsabilidades**

* **Dirección del Proyecto:**
  + Garantizar el cumplimiento legal y la asignación de recursos.
  + Aprobar las actualizaciones de la lista de requisitos.
* **Responsable de Seguridad:**
  + Monitorear los cambios normativos y mantener actualizado el registro.
  + Coordinar la implementación de medidas de cumplimiento.
* **Administrador del Sistema:**
  + Garantizar que los sistemas cumplan con requisitos técnicos de seguridad y privacidad.

**7. Revisión y Actualización**

* Este procedimiento se revisará **anualmente** o cuando se produzcan cambios normativos o contractuales relevantes.
* Toda actualización deberá documentarse en la **Matriz de Cumplimiento Legal del SGSI**.

**Propiedad Intelectual**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 03 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define las directrices para la **protección, uso y respeto de los derechos de propiedad intelectual** en el proyecto *Lava Rápido Vehicular*, conforme al control A.5.32 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que el proyecto cumpla con las leyes nacionales e internacionales relacionadas con **derechos de autor, licencias de software, marcas y contenido digital**, previniendo el uso indebido de materiales protegidos y asegurando la titularidad sobre los activos propios.

**2. Alcance**

Aplica a todos los activos y materiales del proyecto, incluyendo:

* Software desarrollado internamente.
* Códigos fuente, bases de datos y documentación técnica.
* Material gráfico, logotipos, interfaces y contenido audiovisual.
* Herramientas, librerías o recursos de terceros utilizados en el sistema.
* Contratos o acuerdos con proveedores o colaboradores que generen propiedad intelectual.

**3. Principios de Propiedad Intelectual**

1. **Respeto:** Se prohíbe el uso no autorizado de software, imágenes o contenidos protegidos.
2. **Autenticidad:** Todo software o recurso debe provenir de una fuente legítima y contar con licencia válida.
3. **Titularidad:** Los desarrollos, diseños y documentos producidos en el marco del proyecto son propiedad del *Lava Rápido Vehicular*.
4. **Reconocimiento:** Los derechos de autor y licencias de terceros deben mantenerse visibles en los productos que así lo exijan.
5. **Conservación:** Los contratos y licencias deben archivarse como evidencia de cumplimiento legal.

**4. Procedimiento de Gestión de Propiedad Intelectual**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación** | Se listan todos los activos y materiales sujetos a derechos de autor o licencias. | Responsable de Seguridad / Desarrollo |
| **Verificación** | Se comprueba la existencia de licencias válidas y el cumplimiento de sus términos. | Dirección / Administrador |
| **Registro** | Los activos desarrollados internamente se documentan en el inventario de propiedad intelectual. | Responsable de Seguridad |
| **Control de Uso** | Se supervisa que las herramientas y contenidos usados sean legítimos. | Administrador del Sistema |
| **Protección Legal** | Se incluyen cláusulas de propiedad intelectual en los contratos con proveedores o colaboradores. | Dirección del Proyecto |

**5. Políticas de Uso de Software y Contenido**

* Está prohibida la instalación o uso de **software sin licencia o pirata**.
* Las herramientas de código abierto deben cumplir sus términos de licencia (GPL, MIT, Apache, etc.).
* Todo contenido multimedia (imágenes, íconos, videos, música) debe ser de **propiedad del proyecto o tener autorización de uso**.
* Los documentos, diseños y desarrollos creados por el equipo son **propiedad intelectual exclusiva del proyecto**.
* Los derechos de terceros deben respetarse según los contratos y condiciones de uso aplicables.

**6. Responsabilidades**

* **Dirección del Proyecto:**
  + Garantizar el cumplimiento de las normas de propiedad intelectual.
  + Incluir cláusulas de propiedad intelectual en todos los acuerdos y contratos.
* **Responsable de Seguridad:**
  + Mantener el inventario de activos intelectuales y licencias.
  + Verificar la legitimidad del software y contenido utilizado.
* **Equipo de Desarrollo / Diseño:**
  + Utilizar únicamente herramientas y materiales autorizados.
  + Registrar adecuadamente la autoría y procedencia de los materiales creados.

**7. Revisión y Actualización**

* Este procedimiento será revisado **anualmente** o ante cambios en el uso de software, herramientas o acuerdos de licencia.
* Los activos creados o modificados deben actualizarse en el **Inventario de Propiedad Intelectual del SGSI**.

**8. Evidencias y Documentación**

* Contratos de cesión o uso de derechos de autor.
* Licencias de software (comerciales o libres).
* Registros de marcas o logotipos.
* Inventario de activos de propiedad intelectual.

**Protección de los Registros**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 03 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece los lineamientos para la **gestión, protección y conservación de los registros** generados por el proyecto *Lava Rápido Vehicular*, conforme al control A.5.33 de la norma ISO/IEC 27001:2022.

El objetivo es asegurar que todos los registros que contienen información crítica o evidencia de actividades del SGSI sean **precisos, íntegros, accesibles y protegidos contra pérdida, alteración o destrucción no autorizada**.

**2. Alcance**

Aplica a todos los **registros físicos y digitales** generados durante la operación del proyecto, incluyendo:

* Bitácoras de acceso, errores y auditorías del sistema.
* Registros de incidentes de seguridad y reportes técnicos.
* Documentación de usuarios, mantenimiento y respaldos.
* Contratos, consentimientos y acuerdos con terceros.
* Copias de seguridad, registros de pruebas y revisiones del SGSI.

**3. Principios de Protección de Registros**

1. **Integridad:** Los registros deben mantenerse sin alteraciones.
2. **Disponibilidad:** Deben estar accesibles para usuarios autorizados cuando se requieran.
3. **Confidencialidad:** Solo el personal autorizado podrá acceder a los registros sensibles.
4. **Autenticidad:** Los registros deben poder verificarse y ser trazables a su origen.
5. **Retención:** Los registros deben conservarse durante el tiempo establecido por la política del proyecto o la ley.

**4. Procedimiento de Gestión de Registros**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Creación y Captura** | Se generan y almacenan registros como evidencia de actividades del sistema o SGSI. | Administrador / Equipo Técnico |
| **Clasificación** | Se determina el tipo de registro y su nivel de confidencialidad. | Responsable de Seguridad |
| **Almacenamiento Seguro** | Los registros digitales se guardan en servidores o nubes seguras, con respaldo periódico. | Administrador del Sistema |
| **Acceso Controlado** | Solo usuarios con permisos asignados pueden consultar los registros. | Responsable de Seguridad |
| **Retención y Eliminación** | Los registros se conservan durante el periodo establecido y se eliminan de forma segura. | Dirección / SGSI |

**5. Requisitos de Seguridad para Registros**

* Los registros de seguridad (logs) deben **protegerse contra alteraciones o borrados no autorizados**.
* Los registros físicos deben almacenarse en **archivadores cerrados y áreas restringidas**.
* Los registros digitales deben tener **copias de seguridad cifradas** y almacenadas en ubicaciones diferentes.
* Los registros deben conservarse por al menos **dos (2) años** o según lo exija la normativa aplicable.
* El acceso a los registros debe auditarse y registrarse.

**6. Responsabilidades**

* **Responsable de Seguridad:**
  + Supervisar el cumplimiento de las políticas de protección y retención de registros.
  + Clasificar los registros según su nivel de sensibilidad.
* **Administrador del Sistema:**
  + Implementar controles técnicos de respaldo y acceso seguro.
  + Garantizar la integridad y disponibilidad de los registros digitales.
* **Dirección del Proyecto:**
  + Aprobar los periodos de retención y los métodos de eliminación segura.

**7. Revisión y Actualización**

* Este procedimiento se revisará **anualmente** o cuando cambien los requisitos legales o tecnológicos.
* Cualquier modificación debe documentarse en el **registro de control de versiones del SGSI**.

**8. Evidencias y Soportes**

* Bitácoras de auditoría y logs del sistema.
* Formularios de control de acceso a registros.
* Registros de respaldo y restauración.
* Actas de eliminación segura de documentos.

**Privacidad y Protección de la Información Personal Identificable (PII)**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 03 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las políticas y procedimientos para la **protección y tratamiento adecuado de la información personal identificable (PII)** de clientes, empleados y terceros, conforme al control A.5.34 de la norma ISO/IEC 27001:2022 y las disposiciones de la Ley 1581 de 2012 (Colombia).

El objetivo es garantizar que todos los datos personales tratados por el proyecto *Lava Rápido Vehicular* sean gestionados de manera **lícita, transparente y segura**, respetando los derechos de los titulares.

**2. Alcance**

Esta política aplica a todas las actividades del proyecto que involucren la recolección, almacenamiento, uso, transmisión o eliminación de información personal, incluyendo:

* Datos de clientes y usuarios registrados en la plataforma.
* Información de empleados y contratistas.
* Datos compartidos con proveedores, pasarelas de pago y terceros.
* Registros de acceso, formularios web, consentimientos y comunicaciones electrónicas.

**3. Principios de Protección de Datos Personales**

1. **Legalidad:** Todo tratamiento debe realizarse conforme a la ley.
2. **Finalidad:** Los datos solo se utilizarán para los fines informados al titular.
3. **Consentimiento:** El tratamiento requiere autorización previa, expresa e informada.
4. **Seguridad:** Los datos deben protegerse mediante medidas técnicas y organizativas adecuadas.
5. **Transparencia:** Los titulares pueden acceder, actualizar o eliminar su información.
6. **Minimización:** Solo se recolectarán los datos estrictamente necesarios.
7. **Responsabilidad Proactiva:** El proyecto debe demostrar cumplimiento con la normativa.

**4. Categorías de Información Personal**

| **Tipo de Dato** | **Ejemplo** | **Medida de Protección Aplicada** |
| --- | --- | --- |
| **Datos Básicos** | Nombre, correo, teléfono, dirección. | Cifrado en base de datos y autenticación segura. |
| **Datos Financieros** | Información de pago y facturación. | Envío cifrado (TLS), almacenamiento restringido. |
| **Datos Laborales** | Información del personal interno. | Acceso controlado y archivo seguro. |
| **Datos Contractuales** | Acuerdos o formularios de clientes. | Conservación bajo políticas de confidencialidad. |

**5. Procedimiento para el Tratamiento de PII**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Recolección** | Obtención de datos mediante formularios o sistemas digitales. | Área de Atención / Sistema Web |
| **Registro y Consentimiento** | Registro del consentimiento del titular y finalidad del uso. | Responsable de Seguridad / Legal |
| **Almacenamiento** | Cifrado y custodia en bases de datos seguras. | Administrador del Sistema |
| **Uso y Acceso** | Solo usuarios autorizados pueden acceder a la PII. | Responsable de Seguridad |
| **Eliminación o Anonimización** | Borrado seguro o anonimización tras finalizar el propósito. | Administrador / Dirección |

**6. Derechos de los Titulares**

Los titulares de la información tienen derecho a:

* Acceder a su información personal.
* Solicitar corrección o eliminación de datos.
* Revocar la autorización para el tratamiento.
* Conocer el uso que se ha dado a su información.

Las solicitudes se gestionarán a través del canal oficial:  
📧 **protecciondatos@lavarapido.com**

**7. Medidas de Seguridad**

* Cifrado de datos sensibles en tránsito y almacenamiento.
* Autenticación multifactor para usuarios con acceso a PII.
* Control de accesos basado en roles (principio del mínimo privilegio).
* Registro y auditoría de accesos a información personal.
* Políticas de respaldo y eliminación segura de información.

**8. Responsabilidades**

* **Dirección del Proyecto:**
  + Garantizar el cumplimiento de la ley y esta política.
  + Aprobar las medidas de protección implementadas.
* **Responsable de Seguridad:**
  + Supervisar el cumplimiento de las políticas de privacidad.
  + Gestionar incidentes que involucren PII.
* **Administrador del Sistema:**
  + Implementar controles técnicos de cifrado y acceso.
* **Usuarios del Sistema:**
  + Cumplir las políticas y reportar cualquier incidente o filtración.

**9. Revisión y Actualización**

* Este procedimiento será revisado **anualmente** o cuando cambien las regulaciones sobre protección de datos.
* Los cambios deberán reflejarse en la **Política de Privacidad y Tratamiento de Datos Personales** publicada por el proyecto.

**Eliminación de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 03 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece los lineamientos para la **eliminación segura de la información** dentro del proyecto *Lava Rápido Vehicular*, conforme al control A.5.35 de la norma ISO/IEC 27001:2022.

El objetivo es asegurar que toda información —tanto digital como física— sea **eliminada de forma segura, controlada y verificable** cuando haya cumplido su propósito o haya expirado su periodo de retención, evitando accesos no autorizados o recuperaciones indebidas.

**2. Alcance**

Esta política aplica a todos los **datos, documentos y registros** manejados por el proyecto, incluyendo:

* Archivos digitales en servidores, bases de datos o sistemas en la nube.
* Documentación física (contratos, consentimientos, reportes).
* Dispositivos de almacenamiento (discos duros, memorias USB, backups).
* Datos personales o confidenciales que deban eliminarse tras finalizar su tratamiento.

**3. Principios de Eliminación Segura**

1. **Confidencialidad:** La eliminación debe garantizar que la información no pueda recuperarse.
2. **Integridad:** La eliminación no debe afectar otros datos activos.
3. **Trazabilidad:** Todas las eliminaciones deben registrarse y ser verificables.
4. **Legalidad:** La eliminación debe realizarse conforme a los plazos legales o contractuales.
5. **Responsabilidad:** Solo personal autorizado puede ejecutar la eliminación.

**4. Procedimiento de Eliminación**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación** | Determinar la información o medio que será eliminado. | Responsable de Seguridad / Administrador |
| **Verificación de Retención** | Confirmar que se haya cumplido el periodo de conservación. | Dirección / Seguridad |
| **Método de Eliminación** | Aplicar el método adecuado según el tipo de soporte (digital o físico). | Administrador del Sistema |
| **Registro del Proceso** | Documentar fecha, método y responsable de la eliminación. | Responsable de Seguridad |
| **Validación Final** | Confirmar que la información no pueda ser recuperada. | Dirección / Auditor Interno |

**5. Métodos de Eliminación**

| **Tipo de Soporte** | **Método Recomendado** |
| --- | --- |
| **Archivos Digitales** | Eliminación mediante sobrescritura segura o software de borrado certificado (ej. DBAN, Eraser). |
| **Bases de Datos** | Eliminación mediante comandos de purga y verificación del respaldo. |
| **Documentos Físicos** | Triturado, incineración o destrucción controlada. |
| **Discos Duros o USB** | Desmagnetización o destrucción física del medio. |
| **Backups** | Eliminación segura al término del ciclo de vida o reemplazo por nuevas copias. |

**6. Registro de Eliminación**

Se mantendrá un **“Registro de Eliminación de Información”** que contenga:

* Código del documento o archivo.
* Tipo de información.
* Fecha de eliminación.
* Método aplicado.
* Responsable y aprobación de la dirección.

**7. Responsabilidades**

* **Responsable de Seguridad:**
  + Supervisar el cumplimiento de esta política y mantener los registros.
  + Autorizar las solicitudes de eliminación.
* **Administrador del Sistema:**
  + Ejecutar la eliminación de medios digitales y respaldos.
  + Garantizar la imposibilidad de recuperación posterior.
* **Dirección del Proyecto:**
  + Aprobar los procesos de eliminación masiva o sensibles.
  + Revisar los reportes anuales de eliminación.

**8. Revisión y Actualización**

* Este procedimiento será revisado **anualmente** o cuando se introduzcan nuevos tipos de almacenamiento o medios digitales.
* Cualquier cambio debe reflejarse en la **Política de Retención y Eliminación de la Información** del SGSI.

**9. Evidencias y Soportes**

* Registro de eliminación de información.
* Reportes de software de borrado seguro.
* Actas de destrucción de documentos físicos.
* Auditorías internas de cumplimiento.

**Clasificación de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 04 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las directrices para la **clasificación de la información** del proyecto *Lava Rápido Vehicular*, conforme al control A.5.36 de la norma ISO/IEC 27001:2022.

El objetivo es asegurar que toda la información sea **clasificada según su nivel de sensibilidad, valor, impacto y requisitos legales o contractuales**, garantizando que se apliquen los controles de seguridad adecuados para cada tipo de dato.

**2. Alcance**

Esta política aplica a toda la información manejada en el proyecto, independientemente de su formato o soporte, incluyendo:

* Archivos digitales (bases de datos, documentos, registros).
* Documentos físicos (contratos, formularios, informes).
* Comunicaciones electrónicas, reportes y respaldos.
* Datos personales, financieros o operativos.

**3. Principios de Clasificación**

1. **Relevancia:** La clasificación depende del valor e impacto que tendría su pérdida, alteración o divulgación.
2. **Consistencia:** Todas las áreas deben aplicar los mismos criterios de clasificación.
3. **Actualización:** Las clasificaciones deben revisarse cuando cambie el contexto o valor de la información.
4. **Protección proporcional:** Cuanto más sensible sea la información, mayor debe ser el nivel de protección.
5. **Responsabilidad:** Cada propietario de la información debe asegurar su correcta clasificación y manejo.

**4. Niveles de Clasificación**

| **Nivel** | **Descripción** | **Ejemplos** | **Medidas de Protección** |
| --- | --- | --- | --- |
| **Pública** | Información que puede ser divulgada sin causar perjuicio. | Material promocional, información en redes. | Sin restricciones, pero revisión previa a publicación. |
| **Interna** | Uso interno del proyecto, sin autorización para divulgación externa. | Manuales, reportes técnicos, políticas internas. | Acceso restringido a empleados. |
| **Confidencial** | Su divulgación podría afectar operaciones o competitividad. | Datos de clientes, proveedores, bases de datos. | Cifrado, control de acceso, respaldo seguro. |
| **Restringida** | Información crítica cuya exposición causaría graves daños o incumplimientos legales. | Contraseñas, claves API, datos financieros sensibles. | Cifrado avanzado, autenticación multifactor, acceso limitado. |

**5. Procedimiento de Clasificación**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación** | Reconocer la información generada o recibida por el proyecto. | Responsable de Seguridad / Usuarios |
| **Evaluación de Sensibilidad** | Determinar el nivel de confidencialidad según su impacto potencial. | Responsable de Seguridad |
| **Asignación de Clasificación** | Etiquetar o marcar la información con su nivel correspondiente. | Administrador / Propietario del Activo |
| **Aplicación de Controles** | Implementar medidas de protección de acuerdo al nivel asignado. | Administrador del Sistema |
| **Revisión Periódica** | Evaluar si la clasificación sigue siendo válida. | Dirección / SGSI |

**6. Etiquetado y Manejo de la Información**

* Todo documento o archivo deberá incluir su **nivel de clasificación visible** (por ejemplo: “CONFIDENCIAL”).
* Las carpetas digitales deben tener permisos definidos conforme al nivel asignado.
* La información física debe almacenarse en lugares seguros con acceso controlado.
* Está prohibida la divulgación de información confidencial o restringida sin autorización escrita.
* Las transferencias de información sensible deben realizarse por canales cifrados (TLS, VPN).

**7. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar los criterios de clasificación y revisar su aplicación.
* **Responsable de Seguridad:**
  + Definir las políticas de clasificación y verificar su cumplimiento.
  + Capacitar al personal sobre el manejo adecuado de la información.
* **Usuarios del Sistema:**
  + Clasificar la información que generen o gestionen.
  + Proteger los datos según su nivel asignado.

**8. Revisión y Actualización**

* Esta política será revisada **anualmente** o cuando se produzcan cambios en los activos de información o requerimientos legales.
* Las actualizaciones deberán reflejarse en el **Inventario de Activos de Información del SGSI**.

**9. Evidencias y Soportes**

* Inventario y clasificación de activos de información.
* Etiquetas de clasificación visibles en documentos y sistemas.
* Registros de revisión de clasificaciones.
* Capacitación del personal en manejo de información clasificada.

**Etiquetado de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 04 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece los lineamientos para el **etiquetado, identificación y manejo adecuado de la información** de acuerdo con su nivel de clasificación, conforme al control A.5.37 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que toda la información del proyecto *Lava Rápido Vehicular* sea **correctamente identificada y protegida**, evitando su divulgación o uso indebido mediante el uso de **etiquetas visuales, metadatos o marcas electrónicas** que indiquen su sensibilidad.

**2. Alcance**

Esta política aplica a toda la información generada, recibida o almacenada por el proyecto, sin importar su soporte o formato, incluyendo:

* Documentos digitales (archivos, reportes, bases de datos, correos electrónicos).
* Documentos físicos (contratos, formularios, bitácoras, reportes).
* Información transmitida o compartida entre empleados, clientes o terceros.

**3. Principios de Etiquetado**

1. **Coherencia:** El etiquetado debe corresponder al nivel de clasificación definido (ver control A.5.36).
2. **Claridad:** Las etiquetas deben ser fácilmente visibles y comprensibles.
3. **Seguridad:** Las etiquetas no deben exponer información sensible innecesaria.
4. **Obligatoriedad:** Todo documento clasificado debe estar etiquetado antes de su distribución.
5. **Actualización:** Las etiquetas deben revisarse y actualizarse cuando cambie la clasificación del documento.

**4. Tipos de Etiquetas**

| **Nivel de Clasificación** | **Etiqueta Requerida** | **Color o Formato Sugerido** | **Ejemplo de Marcado** |
| --- | --- | --- | --- |
| **Pública** | “PÚBLICO” | Verde / Texto plano | [PÚBLICO] Manual de usuario.pdf |
| **Interna** | “USO INTERNO” | Azul | [INTERNO] Reporte mensual.docx |
| **Confidencial** | “CONFIDENCIAL” | Amarillo / Negrita | [CONFIDENCIAL] BaseClientes.xlsx |
| **Restringida** | “RESTRINGIDO” | Rojo / Mayúsculas | [RESTRINGIDO] ClavesSistema.txt |

**5. Procedimiento de Etiquetado**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación** | Determinar el nivel de clasificación del documento o archivo. | Responsable de Seguridad / Usuario creador |
| **Asignación de Etiqueta** | Colocar la etiqueta correspondiente de manera visible en el encabezado, pie o nombre del archivo. | Usuario / Administrador |
| **Registro** | Documentar los archivos etiquetados en el inventario de activos de información. | Responsable de Seguridad |
| **Revisión y Actualización** | Revisar etiquetas cuando se cambie el nivel de clasificación. | Dirección / SGSI |

**6. Lineamientos Específicos**

* Los documentos digitales deben incluir la etiqueta en el **nombre del archivo**, así como en el **encabezado o pie de página**.
* Los correos electrónicos con información sensible deben indicar el nivel de confidencialidad en el **asunto o cuerpo del mensaje**.
* Los documentos físicos deben tener una **marca visible** en la primera página o portada.
* Está prohibida la eliminación o alteración de etiquetas sin autorización.
* La información etiquetada como “Confidencial” o “Restringida” debe **cifrarse antes de enviarse electrónicamente**.

**7. Ejemplos de Aplicación**

| **Tipo de Documento** | **Nivel** | **Ejemplo de Etiqueta** |
| --- | --- | --- |
| Política de seguridad | Interna | [USO INTERNO] PolíticaSeguridad.docx |
| Base de datos de clientes | Confidencial | [CONFIDENCIAL] Clientes2025.sql |
| Manual de usuario público | Pública | [PÚBLICO] ManualWebApp.pdf |
| Contratos financieros | Restringida | [RESTRINGIDO] ContratoBanco.pdf |

**8. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar los criterios y formatos de etiquetado.
* **Responsable de Seguridad:**
  + Definir y supervisar la correcta aplicación de etiquetas.
  + Mantener el inventario de información clasificada.
* **Usuarios del Sistema:**
  + Etiquetar adecuadamente los documentos que generen.
  + Reportar errores o inconsistencias en el etiquetado.

**9. Revisión y Actualización**

* Esta política será revisada **anualmente** o cuando se modifique la política de clasificación.
* Los cambios deben reflejarse en el **Inventario de Clasificación y Etiquetado de Información del SGSI**.

**10. Evidencias y Soportes**

* Ejemplos de documentos etiquetados correctamente.
* Registros del inventario de información clasificada.
* Auditorías de cumplimiento del etiquetado.

**Transferencia de la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 04 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define las políticas y procedimientos para la **transferencia segura de la información**, conforme al control A.5.38 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que toda la información que se intercambie **dentro o fuera del proyecto *Lava Rápido Vehicular*** esté **protegida contra accesos no autorizados, pérdida o alteración**, ya sea durante su transmisión por medios digitales o físicos.

**2. Alcance**

Esta política aplica a todos los medios y canales utilizados para la transferencia de información, incluyendo:

* Correo electrónico, mensajería instantánea o plataformas de colaboración.
* Servicios en la nube, FTP, API o sistemas internos.
* Transferencia de documentos físicos (contratos, formularios).
* Comunicación con proveedores, clientes y terceros.

**3. Principios de Transferencia Segura**

1. **Confidencialidad:** Toda información transmitida debe protegerse contra accesos no autorizados.
2. **Integridad:** Los datos deben llegar completos y sin alteraciones.
3. **Autenticidad:** Se debe verificar la identidad de los remitentes y destinatarios.
4. **Trazabilidad:** Toda transferencia debe poder auditarse y registrarse.
5. **Legalidad:** Las transferencias deben cumplir con la legislación aplicable (Ley 1581/2012 y contratos vigentes).

**4. Procedimiento de Transferencia**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación de la Información** | Se determina el tipo de datos a transferir y su nivel de confidencialidad. | Responsable de Seguridad / Usuario |
| **Selección del Canal Seguro** | Se elige el medio de transmisión apropiado (TLS, VPN, cifrado, etc.). | Administrador del Sistema |
| **Autorización** | Se valida si la transferencia requiere aprobación de la dirección o responsable. | Dirección / Seguridad |
| **Ejecución** | Se realiza la transferencia aplicando las medidas de seguridad definidas. | Usuario / Administrador |
| **Registro y Evidencia** | Se documenta la transferencia (fecha, destino, método y responsable). | Responsable de Seguridad |

**5. Medidas de Seguridad Requeridas**

* Utilizar **canales cifrados** (HTTPS, SFTP, VPN) para la transferencia digital.
* **No enviar información confidencial** mediante correos o plataformas no corporativas.
* **Verificar la identidad** de los destinatarios antes de enviar datos sensibles.
* Los archivos **confidenciales o restringidos deben cifrarse** y protegerse con contraseña.
* En transferencias físicas, los documentos deben enviarse en **sobres sellados o por mensajería segura**.
* Todo envío debe registrarse en el **Registro de Transferencias de Información del SGSI**.

**6. Tipos de Transferencia y Nivel de Control**

| **Tipo de Transferencia** | **Ejemplo** | **Medida de Seguridad Aplicable** |
| --- | --- | --- |
| Interna (entre empleados) | Envío de reportes internos | Canal cifrado / Correo institucional |
| Externa (proveedores) | Envío de base de datos a aliado | Cifrado + Contraseña separada |
| Automática (sistema a sistema) | Comunicación entre API y servidor | Certificados SSL / Tokens seguros |
| Física | Entrega de contrato impreso | Envío en sobre sellado y registro de entrega |

**7. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar transferencias externas de información sensible.
* **Responsable de Seguridad:**
  + Definir y supervisar las medidas de transferencia segura.
  + Mantener registros y evidencias de los intercambios.
* **Administrador del Sistema:**
  + Configurar los canales cifrados y gestionar credenciales.
* **Usuarios:**
  + Cumplir los procedimientos establecidos y reportar incidentes.

**8. Revisión y Actualización**

* Este procedimiento será revisado **anualmente** o cuando se implementen nuevos medios de comunicación o proveedores.
* Cualquier cambio se reflejará en la **Política de Transferencia y Comunicación de la Información del SGSI**.

**9. Evidencias y Soportes**

* Registro de transferencias de información.
* Logs de sistemas y comprobantes de envío.
* Reportes de cifrado o firma digital.
* Contratos con cláusulas de confidencialidad.

**Manejo de los Activos de Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 04 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las directrices para la **gestión, uso, protección y control de los activos de información** del proyecto *Lava Rápido Vehicular*, conforme al control A.5.39 de la norma ISO/IEC 27001:2022.

El objetivo es asegurar que todos los activos que soportan la información —ya sean físicos, digitales o humanos— sean **identificados, registrados, protegidos y utilizados adecuadamente** a lo largo de su ciclo de vida.

**2. Alcance**

Esta política aplica a todos los **activos de información** del proyecto, incluyendo:

* Equipos tecnológicos (servidores, computadoras, dispositivos móviles).
* Software, licencias, bases de datos y aplicaciones del sistema.
* Información en cualquier formato (digital o físico).
* Instalaciones y redes.
* Personal con acceso a la información del proyecto.

**3. Principios de Gestión de Activos**

1. **Identificación:** Todo activo debe ser reconocido y registrado en el inventario del SGSI.
2. **Propiedad:** Cada activo debe tener un responsable claramente asignado.
3. **Protección:** Los activos deben mantenerse seguros frente a pérdida, acceso no autorizado o mal uso.
4. **Ciclo de Vida:** Se debe definir el manejo del activo desde su adquisición hasta su eliminación.
5. **Valor:** La protección del activo debe ser proporcional a su importancia para el proyecto.

**4. Inventario de Activos**

El **Inventario de Activos de Información** incluirá como mínimo:

* Código de identificación.
* Tipo de activo (hardware, software, información, personas, servicios).
* Descripción y ubicación.
* Propietario o responsable.
* Clasificación de seguridad (ver control 5.36).
* Estado (activo, en mantenimiento, retirado).
* Fecha de alta o baja.

Este inventario será administrado por el **Responsable de Seguridad** y revisado semestralmente.

**5. Procedimiento de Gestión de Activos**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación** | Registrar nuevos activos adquiridos o desarrollados. | Responsable de Seguridad / Dirección |
| **Asignación de Propiedad** | Designar a una persona o área responsable del activo. | Dirección del Proyecto |
| **Clasificación** | Determinar el nivel de confidencialidad o criticidad. | Responsable de Seguridad |
| **Uso y Mantenimiento** | Garantizar el uso correcto, respaldos y soporte técnico. | Administrador / Usuario |
| **Eliminación o Baja** | Aplicar el proceso de eliminación segura (ver control 5.35). | Responsable de Seguridad |

**6. Control de Activos**

* Todo activo debe estar **etiquetado o identificado** físicamente o en sistema.
* Los activos **no deben ser utilizados para fines personales** o no autorizados.
* Está prohibida la **instalación de software no autorizado** en equipos del proyecto.
* Los equipos portátiles deben **mantener medidas de seguridad adicionales** (contraseña, cifrado, bloqueo automático).
* Las pérdidas, daños o robos deben **reportarse inmediatamente** al Responsable de Seguridad.

**7. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar la adquisición y baja de activos.
  + Asignar los recursos necesarios para su protección.
* **Responsable de Seguridad:**
  + Mantener el inventario actualizado.
  + Definir medidas de protección según el nivel de riesgo.
* **Administrador del Sistema:**
  + Implementar controles técnicos (acceso, respaldo, mantenimiento).
* **Usuarios:**
  + Utilizar los activos conforme a las políticas y reportar incidentes o daños.

**8. Revisión y Actualización**

* Este procedimiento se revisará **anualmente** o cuando se introduzcan nuevos activos relevantes.
* Las actualizaciones se reflejarán en el **Inventario de Activos y Políticas de Uso** del SGSI.

**9. Evidencias y Soportes**

* Inventario actualizado de activos de información.
* Registros de mantenimiento y asignación.
* Formularios de entrega y devolución de equipos.
* Actas de baja o eliminación segura de activos.

**Uso Aceptable de los Activos**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 04 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las normas para el **uso responsable y seguro de los activos de información** del proyecto *Lava Rápido Vehicular*, conforme al control A.5.40 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que todos los empleados, colaboradores y contratistas hagan un **uso adecuado, ético y seguro** de los recursos tecnológicos y de información, reduciendo los riesgos de mal uso, pérdida o exposición no autorizada.

**2. Alcance**

Esta política aplica a **todas las personas que utilicen activos del proyecto**, incluyendo personal interno, desarrolladores, proveedores o terceros con acceso a:

* Equipos informáticos (computadores, portátiles, celulares).
* Software y sistemas de información.
* Redes internas y servicios en la nube.
* Información en cualquier formato (digital o físico).

**3. Principios del Uso Aceptable**

1. **Responsabilidad:** Cada usuario es responsable del uso de los activos asignados.
2. **Seguridad:** Los activos deben usarse conforme a las políticas de seguridad establecidas.
3. **Legalidad:** Está prohibido utilizar los activos para actividades ilícitas o no autorizadas.
4. **Privacidad:** Se deben respetar los datos personales y la confidencialidad de la información.
5. **Eficiencia:** Los activos deben emplearse únicamente para fines laborales o institucionales.

**4. Reglas Generales de Uso**

| **Activo** | **Uso Aceptable** | **Uso No Aceptable** |
| --- | --- | --- |
| **Equipos de cómputo** | Uso para tareas del proyecto, acceso a sistemas corporativos, comunicación interna. | Instalar software no autorizado, alterar configuraciones, uso personal prolongado. |
| **Internet y correo electrónico** | Comunicación laboral, acceso a sitios de soporte o documentación técnica. | Acceso a sitios inapropiados, descarga de software ilegal, envío de datos sin cifrar. |
| **Sistemas y aplicaciones** | Ingreso con credenciales propias, cumplimiento de políticas de acceso. | Compartir contraseñas, alterar registros o acceder a áreas restringidas. |
| **Información** | Consulta y uso solo de datos necesarios para la función asignada. | Copiar, divulgar o eliminar información sin autorización. |
| **Dispositivos móviles** | Acceso controlado con contraseña o huella. | Transferir información sin medidas de seguridad. |

**5. Uso de Contraseñas y Credenciales**

* Las contraseñas deben ser **únicas, seguras y personales** (mínimo 10 caracteres, con mayúsculas, minúsculas, número y símbolo).
* Está **prohibido compartir contraseñas** o anotarlas en lugares visibles.
* Las credenciales de acceso se deben cambiar al menos cada **90 días**.
* En caso de sospecha de compromiso, el usuario debe **reportarlo de inmediato** al Responsable de Seguridad.

**6. Monitoreo y Cumplimiento**

* El uso de los sistemas y redes puede ser **monitoreado** para garantizar el cumplimiento de esta política.
* Cualquier uso indebido será considerado una **falta disciplinaria o contractual**, pudiendo implicar sanciones.
* Los usuarios deben firmar el **Compromiso de Uso Aceptable de Activos** antes de recibir acceso a los sistemas.

**7. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar esta política y supervisar su cumplimiento.
* **Responsable de Seguridad:**
  + Capacitar al personal y mantener los registros de aceptación.
  + Detectar y gestionar incidentes por mal uso de activos.
* **Usuarios y Colaboradores:**
  + Cumplir las reglas establecidas y reportar cualquier uso indebido.

**8. Revisión y Actualización**

* Esta política se revisará **anualmente** o cuando se introduzcan nuevos activos o sistemas.
* Las actualizaciones deberán comunicarse a todos los usuarios antes de su aplicación.

**9. Evidencias y Soportes**

* Registros de capacitación y compromisos firmados.
* Reportes de auditoría o monitoreo de uso.
* Actas de sanciones o medidas disciplinarias.

**Devolución de los Activos**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 04 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece el procedimiento para la **devolución y control de los activos de información** al finalizar la relación laboral, contractual o de colaboración con el proyecto *Lava Rápido Vehicular*, conforme al control A.5.41 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que todos los **activos físicos, digitales y de información** sean devueltos y protegidos adecuadamente, evitando pérdida, retención o divulgación no autorizada de datos o recursos del proyecto.

**2. Alcance**

Aplica a todo el personal interno, contratistas y proveedores que hayan recibido o utilizado activos del proyecto, tales como:

* Equipos informáticos, dispositivos móviles o periféricos.
* Credenciales de acceso, tarjetas, llaves o identificaciones.
* Software, licencias o configuraciones de sistemas.
* Información en cualquier formato (digital o físico).
* Cuentas o permisos en plataformas corporativas.

**3. Principios de la Devolución de Activos**

1. **Responsabilidad:** Cada usuario es responsable de los activos asignados durante su permanencia.
2. **Trazabilidad:** Toda devolución debe registrarse formalmente.
3. **Confidencialidad:** Se deben revocar accesos y eliminar credenciales al cierre de la relación.
4. **Seguridad:** Los activos devueltos deben revisarse antes de su reutilización o eliminación.
5. **Cumplimiento:** Ningún colaborador debe conservar copias o información del proyecto una vez finalizado su vínculo.

**4. Procedimiento de Devolución**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Notificación de Finalización** | Se comunica la terminación de la relación contractual o de colaboración. | Dirección / RRHH |
| **Inventario de Activos Asignados** | Se revisa la lista de activos entregados al usuario. | Responsable de Seguridad |
| **Devolución Física y Digital** | Se entregan los equipos, dispositivos, credenciales y documentos. | Usuario / Supervisor |
| **Verificación Técnica** | Se inspeccionan los equipos devueltos y se eliminan accesos o datos. | Administrador del Sistema |
| **Registro y Firma de Entrega** | Se documenta la devolución mediante un acta firmada. | Responsable de Seguridad / Usuario |

**5. Controles Específicos**

* Las **cuentas de usuario y accesos** deben desactivarse inmediatamente después de la desvinculación.
* Los equipos devueltos deben someterse a un proceso de **revisión, formateo y reinstalación segura**.
* Se debe garantizar la **eliminación de toda información del proyecto** almacenada en dispositivos personales o externos.
* Los usuarios deben firmar el **Acta de Devolución de Activos** como evidencia del cumplimiento.
* En caso de pérdida o daño, se debe **registrar el incidente** y aplicar las sanciones correspondientes.

**6. Acta de Devolución (Formato Base)**

| **Código: DA-SGSI-001** | **Versión: 1.0** | **Fecha: 04/10/2025** |
| --- | --- | --- |
| **Nombre del Usuario:** |  |  |
| **Cargo o Rol:** |  |  |
| **Activos Devueltos:** |  |  |
| **Estado de los Activos:** |  |  |
| **Observaciones:** |  |  |
| **Firma del Usuario:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |  |
| **Firma del responsable de Seguridad:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |  |

**7. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar el proceso de devolución y verificar el cumplimiento.
* **Responsable de Seguridad:**
  + Controlar y registrar la devolución de activos.
  + Garantizar la eliminación de accesos y datos.
* **Administrador del Sistema:**
  + Revocar permisos en sistemas y plataformas.
  + Validar la integridad de los activos devueltos.
* **Usuarios o Colaboradores:**
  + Devolver todos los activos asignados y firmar el acta correspondiente.

**8. Revisión y Actualización**

* Este procedimiento se revisará **anualmente** o cuando cambie el proceso de asignación de activos.
* Las modificaciones deben actualizarse en el **Inventario y Registro de Devolución de Activos del SGSI**.

**9. Evidencias y Soportes**

* Actas de devolución firmadas.
* Registros de desactivación de cuentas.
* Reportes técnicos de inspección y formateo.
* Auditorías de control de activos devueltos.

**Clasificación de la Información y Gestión de Medios de Almacenamiento**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define las políticas y procedimientos para la **gestión, control y protección de los medios de almacenamiento** que contienen información del proyecto *Lava Rápido Vehicular*, conforme al control A.5.42 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que todos los dispositivos y soportes de información sean **clasificados, almacenados, transportados y eliminados de manera segura**, de acuerdo con su nivel de sensibilidad.

**2. Alcance**

Aplica a todos los medios físicos y digitales que contengan información del proyecto, incluyendo:

* Discos duros, memorias USB, CD/DVD, tarjetas SD.
* Servidores, respaldos, copias de seguridad y nubes corporativas.
* Documentos físicos impresos, formularios y registros.
* Equipos portátiles que contengan información del proyecto.

**3. Principios de Gestión de Medios**

1. **Confidencialidad:** Los medios deben protegerse según la sensibilidad de los datos que contengan.
2. **Control:** Todo medio de almacenamiento debe ser inventariado y gestionado.
3. **Responsabilidad:** Cada medio tendrá un responsable asignado.
4. **Protección física y digital:** Se deben aplicar controles técnicos y físicos de seguridad.
5. **Eliminación segura:** Los medios deben destruirse o limpiarse adecuadamente al final de su ciclo de vida.

**4. Clasificación de Medios de Almacenamiento**

| **Categoría** | **Ejemplo de Medio** | **Clasificación de Información** | **Medida de Protección** |
| --- | --- | --- | --- |
| **Baja Sensibilidad** | Manuales, documentos públicos. | Pública / Interna | Almacenamiento sin restricciones especiales. |
| **Media Sensibilidad** | Reportes operativos, registros técnicos. | Interna / Confidencial | Acceso restringido, control de usuarios. |
| **Alta Sensibilidad** | Bases de datos de clientes, contraseñas, respaldos. | Confidencial / Restringida | Cifrado, custodia segura, control de salida y destrucción segura. |

**5. Procedimiento de Gestión de Medios**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Inventario de Medios** | Registrar todos los medios de almacenamiento del proyecto. | Responsable de Seguridad |
| **Clasificación** | Evaluar el nivel de confidencialidad de los datos almacenados. | Responsable de Seguridad |
| **Almacenamiento** | Guardar los medios en lugares seguros o repositorios cifrados. | Administrador del Sistema |
| **Transporte** | Usar contenedores seguros o cifrado en transferencias digitales. | Usuario / Responsable designado |
| **Eliminación** | Aplicar el proceso de eliminación segura al finalizar su uso. | Administrador / Seguridad |

**6. Controles de Seguridad Requeridos**

* Los medios digitales deben almacenarse **encriptados o con acceso restringido**.
* Está **prohibido usar medios personales** (USB, discos externos) sin autorización del responsable de seguridad.
* Los medios físicos deben guardarse en **archivadores cerrados o salas seguras**.
* Se debe mantener un **registro de préstamo, transporte o eliminación de medios**.
* Los respaldos deben **probarse periódicamente** para asegurar su integridad.

**7. Transporte de Medios**

* Los medios que contengan información confidencial solo podrán transportarse **en contenedores sellados** o mediante **transmisión cifrada (VPN, TLS)**.
* El transporte debe documentarse con fecha, destino, responsable y propósito.
* En caso de pérdida durante el transporte, se debe **reportar inmediatamente** al Responsable de Seguridad como incidente de información.

**8. Eliminación de Medios**

* Los medios reutilizables deben **limpiarse completamente (wipe o desmagnetización)** antes de ser reasignados.
* Los medios no reutilizables deben **destruirse físicamente o triturarse**.
* La eliminación debe registrarse en el **Acta de Destrucción de Medios** con firma de aprobación.

**9. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar las políticas de gestión y destrucción de medios.
* **Responsable de Seguridad:**
  + Mantener el inventario y supervisar el cumplimiento de los procedimientos.
  + Autorizar el uso, traslado o eliminación de medios.
* **Administrador del Sistema:**
  + Implementar controles técnicos de cifrado, respaldo y borrado seguro.
* **Usuarios:**
  + Cumplir con las políticas de uso, transporte y devolución de medios.

**10. Revisión y Actualización**

* Este procedimiento será revisado **anualmente** o ante cambios en la infraestructura tecnológica o medios utilizados.
* Las modificaciones deberán reflejarse en el **Inventario y Registro de Gestión de Medios del SGSI**.

**11. Evidencias y Soportes**

* Inventario actualizado de medios de almacenamiento.
* Registros de préstamo, transporte y eliminación.
* Actas de destrucción de medios.
* Auditorías de cumplimiento.

**Eliminación Segura o Reutilización de Medios**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define los lineamientos y procedimientos para la **eliminación segura o reutilización controlada de los medios de almacenamiento**, conforme al control A.5.43 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que toda la información almacenada en medios digitales o físicos del proyecto *Lava Rápido Vehicular* sea **eliminada de forma irrecuperable o reutilizada de manera segura**, protegiendo la confidencialidad y evitando fugas de datos.

**2. Alcance**

Aplica a todos los medios de almacenamiento utilizados por el proyecto, incluyendo:

* Discos duros, SSD, memorias USB, CD/DVD y tarjetas SD.
* Equipos informáticos, servidores y dispositivos móviles.
* Copias de respaldo, cintas o medios ópticos.
* Documentos físicos o formularios impresos.

**3. Principios de Eliminación y Reutilización**

1. **Confidencialidad:** La información debe eliminarse sin posibilidad de recuperación.
2. **Control:** Toda eliminación o reutilización debe ser registrada y aprobada.
3. **Legalidad:** El proceso debe cumplir con los requisitos legales y contractuales de retención.
4. **Integridad:** La eliminación no debe afectar otros sistemas o datos activos.
5. **Responsabilidad:** Solo personal autorizado puede ejecutar o supervisar la eliminación.

**4. Procedimiento General**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación del Medio** | Se determina el tipo de medio a eliminar o reutilizar. | Responsable de Seguridad / Administrador |
| **Verificación de Retención** | Se confirma que la información haya cumplido su periodo de conservación. | Dirección / Seguridad |
| **Selección del Método de Eliminación** | Se elige el método adecuado según el tipo de medio. | Administrador del Sistema |
| **Ejecución Controlada** | Se aplica la técnica de eliminación o limpieza. | Administrador / Técnico Autorizado |
| **Registro y Validación** | Se documenta el proceso y se valida su correcta ejecución. | Responsable de Seguridad |

**5. Métodos de Eliminación o Reutilización**

| **Tipo de Medio** | **Método de Eliminación Segura** | **Alternativa de Reutilización Segura** |
| --- | --- | --- |
| **Discos Duros / SSD** | Sobrescritura múltiple (wipe) o desmagnetización. | Formateo completo + reinstalación limpia del sistema. |
| **Memorias USB / SD** | Borrado mediante software de destrucción de datos. | Limpieza total + validación de espacio y contenido. |
| **Cintas de Respaldo / CD / DVD** | Trituración física o incineración. | No aplicable. |
| **Equipos Computacionales** | Eliminación de discos o destrucción de componentes. | Reasignación con instalación nueva y validación. |
| **Documentos Físicos** | Triturado o incineración bajo supervisión. | No aplicable. |

**6. Requisitos de Seguridad**

* Toda eliminación debe ser **verificada y registrada** en el **Acta de Destrucción o Reutilización de Medios**.
* Los medios con información confidencial o restringida deben **destruirse físicamente**, sin opción de reutilización.
* No se permitirá la eliminación de medios **sin supervisión o evidencia documental**.
* Las empresas externas que realicen la destrucción deben contar con **certificados de eliminación segura**.
* La reutilización solo se autoriza cuando se garantice la **borradura total** de los datos anteriores.

**7. Formato de Registro**

**Acta de Eliminación o Reutilización de Medios (Código: EM-SGSI-001)**

| **Fecha** | **Medio** | **Método Aplicado** | **Tipo (Eliminación/Reutilización)** | **Responsable** | **Aprobación Dirección** |
| --- | --- | --- | --- | --- | --- |

*(El acta debe conservarse como evidencia dentro del SGSI.)*

**8. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar la eliminación o reutilización de medios sensibles.
  + Asegurar el cumplimiento de las normas de protección de datos.
* **Responsable de Seguridad:**
  + Supervisar los procesos y conservar las actas de eliminación.
  + Validar los certificados emitidos por proveedores externos.
* **Administrador del Sistema:**
  + Ejecutar el proceso técnico de eliminación o limpieza.
  + Reportar cualquier anomalía o recuperación fallida.

**9. Revisión y Actualización**

* Este procedimiento se revisará **anualmente** o cuando se adopten nuevos medios de almacenamiento o tecnologías.
* Toda actualización se reflejará en el **Registro de Eliminación y Reutilización de Medios del SGSI**.

**10. Evidencias y Soportes**

* Actas de eliminación y reutilización firmadas.
* Certificados de destrucción emitidos por terceros.
* Reportes de software de eliminación segura.
* Auditorías internas del proceso.

**Protección de los Datos en Tránsito**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece los lineamientos y medidas para la **protección de los datos durante su transmisión** entre sistemas, dispositivos o personas, conforme al control A.5.44 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que toda la información intercambiada por el proyecto *Lava Rápido Vehicular* se transmita **de forma segura, confidencial e íntegra**, evitando accesos no autorizados, interceptaciones o alteraciones de datos.

**2. Alcance**

Esta política aplica a todos los tipos de transmisión de información, tanto **interna como externa**, incluyendo:

* Comunicaciones entre sistemas, servicios y bases de datos.
* Envío de correos electrónicos, archivos y formularios digitales.
* Acceso remoto a los sistemas del proyecto.
* Comunicaciones con proveedores, clientes o pasarelas de pago.
* Intercambio de información en redes inalámbricas o móviles.

**3. Principios de Protección en Tránsito**

1. **Confidencialidad:** La información debe protegerse para evitar su exposición o lectura por terceros.
2. **Integridad:** Los datos no deben alterarse durante la transmisión.
3. **Autenticidad:** Se debe garantizar la identidad de los emisores y receptores.
4. **Trazabilidad:** Toda transmisión importante debe poder auditarse.
5. **Cumplimiento:** La transmisión debe cumplir las normas legales y contractuales aplicables.

**4. Medidas de Seguridad Obligatorias**

| **Tipo de Comunicación** | **Medida de Protección Requerida** | **Herramienta / Ejemplo** |
| --- | --- | --- |
| **Transmisión Web / API** | Cifrado TLS 1.2 o superior. | HTTPS, certificados SSL, OAuth. |
| **Correos Electrónicos** | Cifrado de contenido y autenticación. | S/MIME, cifrado PGP, autenticación SMTP. |
| **Redes Internas y VPN** | Cifrado extremo a extremo y control de acceso. | VPN corporativa, IPSec. |
| **Transferencia de Archivos** | Cifrado durante transferencia y almacenamiento temporal. | SFTP, FTPS, OneDrive Empresarial. |
| **Comunicación Móvil o Wi-Fi** | Autenticación segura y cifrado WPA2/WPA3. | VPN o acceso mediante túneles seguros. |

**5. Procedimiento para la Transmisión Segura**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación del Tipo de Dato** | Determinar si la información es pública, interna o confidencial. | Usuario / Responsable de Seguridad |
| **Selección del Canal Seguro** | Elegir el medio de transmisión apropiado (VPN, TLS, SFTP, etc.). | Administrador del Sistema |
| **Autenticación de las Partes** | Verificar identidad de emisor y receptor mediante credenciales o certificados. | Responsable de Seguridad |
| **Transmisión Controlada** | Enviar la información aplicando los protocolos y cifrados definidos. | Usuario / Sistema |
| **Registro y Evidencia** | Documentar transferencias relevantes y almacenar logs. | Administrador del Sistema |

**6. Controles Complementarios**

* Prohibido enviar información sensible por **redes públicas sin cifrado**.
* Los usuarios deben **verificar la autenticidad** de los sitios web y certificados antes de ingresar credenciales.
* Los sistemas del proyecto deben **bloquear conexiones inseguras (HTTP, FTP, Telnet)**.
* Las claves de cifrado deben ser **únicas, seguras y almacenadas bajo control restringido**.
* Se debe **auditar periódicamente** la seguridad de los canales de comunicación.

**7. Gestión de Incidentes**

* Si se detecta una posible interceptación, pérdida o manipulación de datos en tránsito, se deberá:
  1. Suspender la transferencia de inmediato.
  2. Notificar al **Responsable de Seguridad**.
  3. Registrar el incidente y aplicar el **Procedimiento de Gestión de Incidentes (Control 5.24)**.
  4. Revisar y reforzar las medidas técnicas del canal afectado.

**8. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar los protocolos de comunicación y herramientas utilizadas.
* **Responsable de Seguridad:**
  + Verificar el cumplimiento de las políticas de transmisión segura.
  + Coordinar auditorías de comunicaciones cifradas.
* **Administrador del Sistema:**
  + Configurar y mantener certificados, VPN y cifrados.
* **Usuarios:**
  + Usar únicamente los canales aprobados y reportar anomalías.

**9. Revisión y Actualización**

* Esta política será revisada **anualmente** o ante cambios en los mecanismos de comunicación.
* Cualquier modificación deberá documentarse en el **Registro de Controles de Transmisión Segura del SGSI**.

**Separación de Redes**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las políticas y medidas para la **separación y segmentación de redes** del proyecto *Lava Rápido Vehicular*, en cumplimiento del control A.5.45 de la norma ISO/IEC 27001:2022.

El objetivo es **reducir los riesgos de acceso no autorizado, propagación de amenazas o interferencias** entre sistemas, garantizando que cada componente de la infraestructura opere en entornos seguros y controlados.

**2. Alcance**

Esta política aplica a toda la **infraestructura tecnológica del proyecto**, incluyendo:

* Servidores y bases de datos del sistema.
* Estaciones de trabajo del personal administrativo y operativo.
* Dispositivos de red (routers, switches, firewalls).
* Conexiones inalámbricas y redes de invitados.
* Servicios en la nube y entornos de desarrollo remoto.

**3. Principios de Separación de Redes**

1. **Aislamiento lógico:** Las diferentes funciones de red deben separarse mediante VLAN, subredes o firewalls.
2. **Control de acceso:** Solo se permite la comunicación entre redes si existe una necesidad funcional.
3. **Protección por capas:** Cada red debe contar con controles propios de seguridad.
4. **Monitoreo y trazabilidad:** Toda conexión entre redes debe registrarse y auditarse.
5. **Seguridad adaptativa:** La segmentación debe revisarse regularmente frente a nuevas amenazas.

**4. Estructura de Red del Proyecto (Ejemplo)**

| **Red / Segmento** | **Descripción** | **Tipo de Acceso** | **Medidas de Seguridad** |
| --- | --- | --- | --- |
| **Red Administrativa (LAN-A)** | Equipos del personal, gestión interna del sistema. | Interno restringido | Firewall, VLAN dedicada, acceso autenticado. |
| **Red de Servidores (LAN-S)** | Hospeda base de datos, servicios web y copias de respaldo. | Interno seguro | Segmento aislado, acceso por VPN, reglas específicas en firewall. |
| **Red de Clientes (LAN-C)** | Usuarios del sistema o clientes externos. | Externo controlado | HTTPS, proxy inverso, IDS/IPS activo. |
| **Red de Desarrollo (LAN-D)** | Entorno de pruebas y despliegue. | Interno limitado | Separada de producción, permisos restringidos. |
| **Red de Invitados / Wi-Fi** | Acceso a internet para visitantes o proveedores. | Público aislado | Red separada sin acceso a otros recursos. |

**5. Procedimiento para la Segmentación**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación de Componentes Críticos** | Determinar los activos que requieren separación. | Responsable de Seguridad / Administrador |
| **Diseño de Segmentación** | Definir VLAN, subredes y reglas de firewall. | Administrador del Sistema |
| **Implementación Técnica** | Configurar equipos y dispositivos de red. | Administrador / Técnico Autorizado |
| **Pruebas de Aislamiento** | Verificar que las redes estén correctamente separadas. | Responsable de Seguridad |
| **Documentación y Control** | Registrar configuraciones, IPs y diagramas de red. | Administrador del Sistema |

**6. Controles Técnicos Obligatorios**

* Implementar **firewalls o routers con control de tráfico** entre redes segmentadas.
* Aplicar **VLAN o subredes independientes** para usuarios, servidores y visitantes.
* Limitar las conexiones **solo a los puertos y protocolos necesarios**.
* Usar **VPN seguras** para conexiones remotas.
* Activar **sistemas de detección de intrusos (IDS/IPS)** entre segmentos críticos.
* Registrar y auditar todas las conexiones entre redes.

**7. Reglas de Comunicación entre Redes**

* El tráfico entre redes debe pasar por dispositivos de **inspección y filtrado**.
* Se deben aplicar políticas de “**mínimo privilegio**”: solo habilitar lo estrictamente necesario.
* Las redes de invitados o externas **no pueden tener acceso directo** a servidores internos.
* Toda modificación en la estructura de red debe **documentarse y ser aprobada** por el Responsable de Seguridad.

**8. Gestión y Monitoreo**

* Los **logs de red y firewall** deben conservarse por al menos 6 meses.
* Se realizarán **pruebas trimestrales de conectividad** entre redes para verificar el aislamiento.
* Las configuraciones deben **respaldarse regularmente** y almacenarse en repositorios seguros.

**9. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar el diseño y las políticas de segmentación.
* **Responsable de Seguridad:**
  + Verificar la correcta separación y monitoreo continuo de las redes.
* **Administrador del Sistema:**
  + Configurar y mantener las VLAN, firewalls y reglas de acceso.
* **Usuarios:**
  + Cumplir con las políticas de conexión y no modificar configuraciones sin autorización.

**10. Revisión y Actualización**

* Este documento se revisará **anualmente** o cuando se implementen nuevas infraestructuras o servicios en red.
* Las modificaciones deben reflejarse en el **Diagrama de Red y Registro de Segmentación del SGSI**.

**11. Evidencias y Soportes**

* Diagrama de red actualizado.
* Configuraciones de VLAN y firewall.
* Logs de conexión y auditorías de red.
* Resultados de pruebas de aislamiento.

**Filtrado de Red**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define las políticas, procedimientos y responsabilidades para la **implementación del filtrado de red**, conforme al control A.5.46 de la norma ISO/IEC 27001:2022.

El objetivo es asegurar que todo el tráfico que entra o sale de la red del proyecto *Lava Rápido Vehicular* esté **controlado, monitoreado y limitado** únicamente a las comunicaciones autorizadas, reduciendo riesgos de intrusión, malware o fuga de información.

**2. Alcance**

Aplica a toda la infraestructura de red y comunicación del proyecto, incluyendo:

* Servidores y sistemas del sistema de gestión.
* Equipos de red (routers, firewalls, switches).
* Conexiones VPN y accesos remotos.
* Servicios externos, proveedores y pasarelas de pago.
* Tráfico interno y externo (entrante y saliente).

**3. Principios del Filtrado de Red**

1. **Control Total del Tráfico:** Todo flujo de datos debe pasar por mecanismos de control (firewalls, routers).
2. **Política de Mínimo Privilegio:** Solo se permitirá el tráfico estrictamente necesario.
3. **Seguridad por Defecto:** El tráfico no autorizado debe ser bloqueado.
4. **Monitoreo Activo:** Todo tráfico relevante debe registrarse y analizarse.
5. **Actualización Continua:** Las reglas deben revisarse y actualizarse según las necesidades del sistema.

**4. Tipos de Filtrado**

| **Tipo de Filtrado** | **Descripción** | **Ejemplo de Aplicación** |
| --- | --- | --- |
| **Filtrado por Dirección IP** | Permite o bloquea tráfico según origen o destino. | Permitir solo IP del servidor web. |
| **Filtrado por Puerto / Protocolo** | Controla el uso de puertos y protocolos autorizados. | Permitir HTTP/HTTPS (80/443) y bloquear Telnet. |
| **Filtrado por Aplicación** | Identifica y gestiona tráfico según la aplicación. | Bloquear redes sociales o apps no laborales. |
| **Filtrado por Contenido** | Analiza datos en tránsito para detectar amenazas o información sensible. | Inspección profunda de paquetes (DPI). |
| **Filtrado por Usuario / Rol** | Asocia políticas de acceso según el perfil del usuario. | Solo administradores acceden a SSH. |

**5. Procedimiento de Filtrado**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación del Tráfico Autorizado** | Definir qué servicios, puertos y direcciones IP deben tener acceso. | Administrador de Red |
| **Configuración de Reglas de Firewall** | Establecer reglas de entrada y salida según políticas de seguridad. | Administrador del Sistema |
| **Aplicación de Políticas de Bloqueo** | Bloquear cualquier tráfico no autorizado por defecto. | Responsable de Seguridad |
| **Monitoreo y Alertas** | Supervisar los logs y generar alertas ante anomalías. | Seguridad / Auditoría |
| **Revisión Periódica** | Revisar y actualizar las reglas al menos una vez por trimestre. | Responsable de Seguridad |

**6. Políticas Específicas**

* Todo tráfico entrante desde internet debe pasar por un **firewall principal** configurado con política *deny all* (bloquear todo, permitir solo lo necesario).
* Las **bases de datos** solo aceptarán conexiones desde la aplicación interna autorizada.
* Las conexiones **SSH o RDP** estarán restringidas a direcciones IP conocidas o por VPN.
* El **tráfico saliente** será filtrado para evitar conexiones a sitios o servicios maliciosos.
* Se debe activar **registro (logging)** de todo acceso o intento de conexión bloqueado.

**7. Mecanismos de Protección Adicional**

* Uso de **IDS/IPS (Sistemas de Detección y Prevención de Intrusos)** para analizar tráfico sospechoso.
* Implementación de **Web Application Firewall (WAF)** para proteger servicios web.
* Activación de **filtrado de DNS seguro (DNS Filtering)** para evitar dominios maliciosos.
* Actualización constante de **firmware y listas de bloqueo** en firewalls.
* Auditorías trimestrales de configuración de red.

**8. Gestión de Incidentes**

En caso de detectar actividad sospechosa o bloqueo de tráfico legítimo:

1. Notificar inmediatamente al **Responsable de Seguridad**.
2. Analizar los registros (logs) para identificar la causa.
3. Tomar acciones correctivas (bloqueo adicional, ajuste de regla, restauración temporal).
4. Documentar el incidente en el **Registro de Eventos y Alertas de Red**.

**9. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar las políticas de filtrado y adquisición de equipos de seguridad.
* **Responsable de Seguridad:**
  + Diseñar y validar las políticas de filtrado.
  + Supervisar los informes de logs y auditorías.
* **Administrador del Sistema / Red:**
  + Configurar y mantener las reglas de filtrado.
  + Actualizar listas de bloqueo y certificados.
* **Usuarios:**
  + No alterar ni intentar evadir los mecanismos de control de red.

**10. Revisión y Actualización**

* Las reglas de filtrado se revisarán **trimestralmente** o ante cualquier cambio en la infraestructura.
* Toda modificación debe documentarse en el **Registro de Políticas de Filtrado del SGSI**.

**11. Evidencias y Soportes**

* Configuraciones del firewall y políticas activas.
* Logs de red y reportes de bloqueo.
* Informes de auditoría de tráfico.
* Registros de incidentes y acciones correctivas.

**Seguridad de los Servicios de Red**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las políticas y procedimientos para garantizar la **seguridad, disponibilidad y confiabilidad de los servicios de red**, conforme al control A.5.47 de la norma ISO/IEC 27001:2022.

El objetivo es asegurar que todos los servicios de red del proyecto *Lava Rápido Vehicular* operen bajo condiciones seguras, minimizando los riesgos de ataques, interrupciones o accesos no autorizados.

**2. Alcance**

Aplica a todos los **servicios de red internos y externos** utilizados por el proyecto, incluyendo:

* Servidores web y de bases de datos.
* Redes VPN y conexiones remotas.
* Servicios en la nube (hosting, almacenamiento, APIs).
* Sistemas de autenticación y correo electrónico.
* Redes inalámbricas y cableadas.

**3. Principios de Seguridad de Servicios de Red**

1. **Disponibilidad:** Los servicios deben estar accesibles cuando se necesiten, con mecanismos de respaldo y alta disponibilidad.
2. **Confidencialidad:** La información transmitida debe protegerse mediante cifrado y control de acceso.
3. **Integridad:** Los datos deben mantenerse exactos y libres de modificaciones no autorizadas.
4. **Autenticación:** Los usuarios y sistemas deben verificarse antes de permitir el acceso.
5. **Supervisión Continua:** Los servicios de red deben monitorearse constantemente.

**4. Tipos de Servicios y Controles Aplicados**

| **Servicio de Red** | **Riesgo Asociado** | **Control de Seguridad Aplicado** |
| --- | --- | --- |
| **Servidor Web** | Ataques externos, inyección SQL, denegación de servicio. | Firewall perimetral, WAF, actualizaciones, cifrado TLS. |
| **Servidor de Base de Datos** | Accesos no autorizados o robo de información. | Segmentación de red, autenticación de usuario, backups cifrados. |
| **VPN Corporativa** | Acceso remoto inseguro o suplantación. | Autenticación multifactor (MFA), cifrado IPSec, monitoreo de sesiones. |
| **Correo Electrónico** | Phishing, malware, pérdida de datos. | Filtros antispam, DMARC/SPF, cifrado de mensajes. |
| **Wi-Fi Interna** | Conexiones no autorizadas o espionaje. | WPA3, filtrado MAC, contraseñas rotatorias, red invitada separada. |

**5. Procedimiento para Asegurar los Servicios de Red**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación de Servicios Críticos** | Determinar los servicios de red esenciales para las operaciones del sistema. | Responsable de Seguridad |
| **Evaluación de Riesgos** | Analizar amenazas, vulnerabilidades y nivel de exposición. | Seguridad / Administración |
| **Implementación de Controles** | Aplicar las medidas técnicas y organizativas necesarias. | Administrador de Red |
| **Monitoreo y Auditoría** | Supervisar el estado, logs y accesos a los servicios. | Seguridad / TI |
| **Mantenimiento y Actualización** | Aplicar parches, configuraciones y revisiones periódicas. | Administrador del Sistema |

**6. Controles Específicos**

* Los **servidores de red** deben tener configuraciones seguras y actualizadas.
* Se deben utilizar **protocolos cifrados** (HTTPS, SSH, SFTP) para todas las comunicaciones.
* El **acceso remoto** solo será permitido mediante VPN y autenticación multifactor.
* Los **logs de servicios críticos** deben conservarse y revisarse periódicamente.
* Los **servicios en la nube** deben contar con acuerdos que garanticen seguridad y cumplimiento (SLA).
* Todo **nuevo servicio de red** deberá ser revisado antes de su integración al entorno productivo.

**7. Supervisión y Monitoreo**

* Implementar **sistemas de detección de intrusiones (IDS/IPS)** para vigilar la actividad de red.
* Utilizar **herramientas de monitoreo continuo** (como Zabbix o Nagios) para medir disponibilidad y alertas.
* Establecer alertas automáticas para intentos fallidos de acceso o comportamiento anómalo.
* Conservar registros de monitoreo por un periodo mínimo de **6 meses**.

**8. Gestión de Incidentes de Red**

En caso de detectar una anomalía o interrupción de servicio:

1. Reportar inmediatamente al **Responsable de Seguridad**.
2. Registrar el incidente en el **Sistema de Gestión de Incidentes (Control 5.24)**.
3. Analizar la causa raíz y aplicar medidas de contención.
4. Documentar la resolución y actualizaciones de control.

**9. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar la adquisición e implementación de servicios de red.
* **Responsable de Seguridad:**
  + Validar las configuraciones y cumplimiento de políticas.
  + Coordinar pruebas de vulnerabilidad y auditorías.
* **Administrador del Sistema / Red:**
  + Configurar, monitorear y mantener los servicios activos.
  + Garantizar disponibilidad y protección de los servidores.
* **Usuarios:**
  + Utilizar los servicios conforme a las políticas de seguridad establecidas.

**10. Revisión y Actualización**

* Este procedimiento se revisará **anualmente** o cuando se agreguen, eliminen o modifiquen servicios de red.
* Toda actualización debe registrarse en el **Inventario y Registro de Servicios de Red del SGSI**.

**11. Evidencias y Soportes**

* Diagramas y configuraciones de red.
* Logs de monitoreo y auditorías.
* Registros de parches y actualizaciones.
* Reportes de incidentes y acciones correctivas.

**Segregación de Redes Inalámbricas y Cableadas**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las políticas y lineamientos para la **segregación segura de redes inalámbricas (Wi-Fi) y cableadas (LAN)** dentro de la infraestructura del proyecto *Lava Rápido Vehicular*, conforme al control A.5.48 de la norma ISO/IEC 27001:2022.

El objetivo es garantizar que las redes utilizadas para la operación, administración y servicios al cliente se mantengan **aisladas entre sí**, evitando accesos no autorizados, fugas de información y propagación de amenazas entre los diferentes entornos.

**2. Alcance**

Aplica a todas las redes físicas e inalámbricas del proyecto, incluyendo:

* Red LAN interna de la oficina o centro de operaciones.
* Red Wi-Fi del personal administrativo y operativo.
* Red Wi-Fi para clientes o visitantes.
* Conexiones VPN y accesos remotos.
* Equipos de red (routers, switches, puntos de acceso inalámbricos).

**3. Principios de Segregación**

1. **Aislamiento por Propósito:** Cada red debe cumplir una función específica y estar separada de las demás.
2. **Control de Acceso:** Solo los usuarios autorizados pueden conectarse a redes internas.
3. **Protección de Datos:** El tráfico sensible no debe cruzar por redes públicas o de invitados.
4. **Monitoreo:** Toda conexión entre redes debe ser registrada y supervisada.
5. **Cumplimiento:** Las configuraciones deben cumplir los estándares de seguridad establecidos en el SGSI.

**4. Clasificación de Redes**

| **Tipo de Red** | **Descripción** | **Nivel de Seguridad** | **Medidas Específicas** |
| --- | --- | --- | --- |
| **LAN Interna** | Red cableada para servidores, sistemas administrativos y bases de datos. | Muy Alto | VLAN exclusiva, acceso por credenciales, firewall interno. |
| **Wi-Fi del Personal** | Red inalámbrica para dispositivos del equipo operativo. | Alto | WPA3, autenticación por usuario, contraseña rotatoria. |
| **Wi-Fi de Invitados / Clientes** | Red abierta con acceso a internet limitado. | Bajo | Aislamiento de la LAN, sin acceso a sistemas internos. |
| **VPN / Acceso Remoto** | Conexión segura a la red interna desde ubicaciones externas. | Muy Alto | Cifrado IPSec, autenticación multifactor (MFA). |

**5. Controles Técnicos Implementados**

* Uso de **VLAN (Redes Virtuales)** para separar el tráfico entre departamentos o funciones.
* Configuración de **firewalls internos** para limitar la comunicación entre redes cableadas e inalámbricas.
* Aplicación de **políticas de routing** que impidan el acceso desde redes públicas a sistemas internos.
* Implementación de **red Wi-Fi de invitados aislada (sin bridge a la LAN)**.
* Activación de **autenticación multifactor (MFA)** en conexiones VPN o administrativas.
* Desactivación de **SSID ocultos** para redes internas críticas.
* Supervisión continua del tráfico de red mediante herramientas IDS/IPS.

**6. Procedimiento de Segregación**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Identificación de Redes Existentes** | Levantar inventario de todas las redes activas (LAN/Wi-Fi). | Administrador de Red |
| **Diseño de Segmentación** | Definir subredes, VLAN y niveles de acceso. | Responsable de Seguridad |
| **Configuración Técnica** | Implementar firewalls, autenticaciones y políticas de aislamiento. | Administrador del Sistema |
| **Pruebas de Conectividad y Aislamiento** | Verificar que las redes estén correctamente separadas. | Seguridad / QA |
| **Monitoreo y Mantenimiento** | Supervisar el tráfico y detectar intentos de conexión cruzada. | Responsable de Seguridad |

**7. Políticas de Acceso**

* Los **usuarios administrativos** solo podrán conectarse desde la **LAN interna o VPN segura**.
* Los **clientes y visitantes** solo tendrán acceso a internet a través de la **red de invitados**, sin visibilidad de sistemas internos.
* Está prohibido conectar **dispositivos personales** a la red interna sin autorización previa.
* Todo **punto de acceso inalámbrico** debe estar configurado y controlado por el Administrador de Red.
* Las contraseñas Wi-Fi deben **cambiarse trimestralmente** y cumplir requisitos mínimos de seguridad.

**8. Gestión de Incidentes**

En caso de detectar un acceso no autorizado o intento de conexión entre redes:

1. Bloquear inmediatamente la conexión sospechosa.
2. Notificar al **Responsable de Seguridad**.
3. Registrar el incidente en el **Sistema de Gestión de Incidentes (Control 5.24)**.
4. Revisar las configuraciones de red y reforzar los controles de autenticación.

**9. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar los recursos técnicos necesarios para la segregación.
* **Responsable de Seguridad:**
  + Diseñar y supervisar la correcta segmentación de redes.
  + Coordinar pruebas de auditoría y revisión de acceso.
* **Administrador del Sistema / Red:**
  + Implementar y mantener las configuraciones VLAN, firewalls y puntos de acceso.
* **Usuarios:**
  + Cumplir con las políticas de conexión y uso de redes asignadas.

**10. Revisión y Actualización**

* Este procedimiento se revisará **anualmente** o cuando se incorporen nuevas redes o equipos.
* Toda modificación deberá registrarse en el **Mapa de Segmentación y Accesos de Red del SGSI**.

**11. Evidencias y Soportes**

* Diagramas de segmentación de red (LAN/Wi-Fi).
* Configuraciones de routers, switches y firewalls.
* Registros de accesos y conexiones.
* Informes de auditorías de seguridad de red.

**Seguridad de los Servicios en la Nube**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define las políticas, lineamientos y controles para garantizar la **seguridad de los servicios en la nube (cloud computing)** utilizados por el proyecto *Lava Rápido Vehicular*, conforme al control A.5.49 de la norma ISO/IEC 27001:2022.

El objetivo es proteger la **confidencialidad, integridad y disponibilidad de la información** almacenada, procesada o transmitida a través de plataformas y servicios en la nube, asegurando el cumplimiento de las políticas del SGSI.

**2. Alcance**

Aplica a todos los servicios en la nube utilizados por el proyecto, incluyendo:

* Plataformas de alojamiento de aplicaciones y bases de datos (PaaS / IaaS).
* Servicios de almacenamiento y respaldo en la nube.
* Herramientas de correo electrónico, colaboración o gestión de archivos.
* APIs y servicios externos integrados.
* Cualquier sistema contratado o mantenido por un proveedor cloud.

**3. Principios de Seguridad en la Nube**

1. **Responsabilidad Compartida:** El proveedor gestiona la infraestructura, y el proyecto administra la configuración y acceso seguro.
2. **Control de Acceso:** Solo usuarios autorizados pueden acceder a servicios en la nube.
3. **Cifrado:** Toda la información debe cifrarse en tránsito y en reposo.
4. **Auditoría y Monitoreo:** Todas las acciones deben registrarse y ser rastreables.
5. **Cumplimiento:** Los servicios deben cumplir con los requisitos legales y normativos del SGSI.

**4. Clasificación de Servicios en la Nube**

| **Tipo de Servicio** | **Ejemplo en el Proyecto** | **Riesgo Asociado** | **Medidas de Seguridad Aplicadas** |
| --- | --- | --- | --- |
| **IaaS (Infraestructura como Servicio)** | Hosting de servidores y bases de datos. | Pérdida o acceso no autorizado a recursos. | Cifrado, autenticación MFA, gestión de roles. |
| **PaaS (Plataforma como Servicio)** | Entorno de desarrollo web. | Falla en configuraciones o brechas en APIs. | Control de versiones, auditorías y backups. |
| **SaaS (Software como Servicio)** | Almacenamiento, correo o gestión documental. | Exposición de datos o pérdida de acceso. | Políticas de acceso, revisión de permisos y respaldo. |

**5. Procedimiento de Gestión de Seguridad Cloud**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Evaluación del Proveedor Cloud** | Verificar cumplimiento con ISO 27001, SLA y cláusulas de seguridad. | Responsable de Seguridad |
| **Configuración Segura del Servicio** | Implementar controles de acceso, cifrado y políticas de respaldo. | Administrador del Sistema |
| **Monitoreo Continuo** | Supervisar accesos, logs y actividad inusual. | Seguridad / TI |
| **Gestión de Incidentes** | Responder ante fallas o brechas reportadas por el proveedor. | Responsable de Seguridad |
| **Revisión Periódica** | Validar contratos, configuraciones y rendimiento del servicio. | Dirección / Seguridad |

**6. Controles Específicos**

* Todo acceso a servicios cloud deberá requerir **autenticación multifactor (MFA)**.
* Los datos sensibles deben almacenarse **encriptados con algoritmos AES-256 o equivalentes**.
* Los servicios deben contar con **acuerdos de nivel de servicio (SLA)** que incluyan cláusulas de disponibilidad y seguridad.
* Los **logs de auditoría** deben mantenerse por un mínimo de **6 meses**.
* Está **prohibido el uso de servicios cloud personales** para información del proyecto.
* Se debe realizar un **backup local o alterno** de la información almacenada en la nube.

**7. Gestión de Proveedores Cloud**

* Todo proveedor debe demostrar cumplimiento con estándares internacionales (ISO/IEC 27001, SOC 2, GDPR si aplica).
* Los contratos deben incluir cláusulas de:
  + **Confidencialidad y protección de datos.**
  + **Ubicación geográfica de los servidores.**
  + **Derecho de auditoría.**
  + **Notificación de incidentes de seguridad.**
* El proveedor debe ofrecer **reportes de cumplimiento** o auditorías de terceros.

**8. Mantenimiento y Revisión**

* Se revisarán **trimestralmente los accesos activos** y configuraciones de seguridad.
* Los servicios obsoletos o sin uso deberán **desactivarse y eliminarse** de manera segura.
* Se realizarán **pruebas de recuperación** para validar los backups en la nube.

**9. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar el uso de servicios cloud y revisar contratos.
* **Responsable de Seguridad:**
  + Evaluar y auditar la seguridad de los proveedores.
  + Gestionar los incidentes relacionados con servicios cloud.
* **Administrador del Sistema:**
  + Configurar, monitorear y mantener los accesos y políticas.
* **Usuarios:**
  + Usar los servicios cloud únicamente bajo las directrices del SGSI.

**10. Revisión y Actualización**

* Este documento será revisado **anualmente** o cuando se integre un nuevo proveedor o servicio cloud.
* Los cambios deberán registrarse en el **Inventario de Servicios Cloud del SGSI**.

**11. Evidencias y Soportes**

* Contratos y SLA firmados con proveedores cloud.
* Configuraciones de acceso y cifrado.
* Logs de auditoría y actividad de usuarios.
* Registros de incidentes y reportes de seguridad.

**Protección de la Información en los Entornos de Desarrollo y Pruebas**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento define los lineamientos y controles para garantizar la **protección de la información en los entornos de desarrollo y pruebas** del proyecto *Lava Rápido Vehicular*, conforme al control A.5.50 de la norma ISO/IEC 27001:2022.

El objetivo es prevenir el **uso indebido, pérdida o exposición de información confidencial** durante el desarrollo, prueba o despliegue de nuevas funciones, componentes o actualizaciones del sistema.

**2. Alcance**

Aplica a todos los entornos técnicos del proyecto, incluyendo:

* Entornos de desarrollo (locales o en la nube).
* Entornos de pruebas (testing, QA, staging).
* Repositorios de código y control de versiones (Git, GitHub, GitLab, etc.).
* Copias de bases de datos utilizadas para pruebas.
* Equipos y servidores dedicados al desarrollo del sistema.

**3. Principios de Protección**

1. **Separación de Entornos:** Los entornos de desarrollo, pruebas y producción deben estar completamente aislados.
2. **Protección de Datos Reales:** Está prohibido usar datos reales de clientes en entornos de prueba o desarrollo.
3. **Acceso Restringido:** Solo personal autorizado puede acceder a los entornos de desarrollo o pruebas.
4. **Control de Versiones:** Todo cambio de código o configuración debe estar documentado.
5. **Eliminación Segura:** Los datos temporales generados en pruebas deben eliminarse una vez finalizadas.

**4. Clasificación de Entornos**

| **Entorno** | **Descripción** | **Tipo de Información** | **Nivel de Seguridad** |
| --- | --- | --- | --- |
| **Desarrollo** | Entorno donde los programadores crean y prueban nuevas funciones. | Datos simulados o anonimizados. | Medio |
| **Pruebas / QA** | Ambiente donde se validan los módulos antes del despliegue. | Datos de prueba o copias anonimizadas. | Alto |
| **Producción** | Sistema en operación con datos reales de clientes. | Información confidencial. | Muy Alto |

**5. Procedimiento de Protección**

| **Etapa** | **Descripción** | **Responsable** |
| --- | --- | --- |
| **Diseño del Entorno** | Crear entornos separados con configuraciones seguras. | Administrador del Sistema |
| **Control de Acceso** | Asignar permisos específicos según roles. | Responsable de Seguridad |
| **Uso de Datos de Prueba** | Utilizar datos anonimizados o sintéticos para pruebas. | Desarrolladores / QA |
| **Monitoreo y Auditoría** | Supervisar accesos, cambios y despliegues. | Seguridad / QA |
| **Eliminación y Limpieza** | Borrar datos temporales al finalizar las pruebas. | Administrador del Sistema |

**6. Controles de Seguridad**

* Todos los **entornos deben contar con autenticación individual y control de acceso por rol**.
* Se deben usar **datos ficticios o enmascarados** para validar procesos.
* Está prohibido **conectar entornos de desarrollo directamente con producción**.
* Las conexiones a bases de datos reales deben estar **restringidas y monitoreadas**.
* Se deben aplicar **actualizaciones de seguridad** en entornos de prueba antes de realizar despliegues.
* Los **repositorios de código** deben mantenerse **privados** y con políticas de commit seguro (sin contraseñas ni datos sensibles).

**7. Gestión de Cambios**

* Todos los cambios deben seguir un **proceso de control de versiones (GitFlow o similar)**.
* Cada modificación al código o configuración debe estar documentada y aprobada.
* Los entornos de prueba deben replicar el entorno de producción sin incluir información sensible.
* Los **despliegues a producción** deben ser autorizados por el **Responsable de Seguridad o Dirección del Proyecto**.

**8. Monitoreo y Registro**

* Mantener **registros de acceso, cambios y despliegues** en los entornos.
* Utilizar herramientas de monitoreo (por ejemplo: Jenkins, GitLab CI/CD, SonarQube).
* Revisar logs semanalmente para identificar errores o accesos indebidos.
* Los incidentes detectados deberán registrarse según el **Procedimiento de Gestión de Incidentes (Control 5.24)**.

**9. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar la infraestructura de desarrollo y pruebas.
* **Responsable de Seguridad:**
  + Supervisar la implementación de controles de seguridad.
  + Autorizar el uso de datos de prueba o copias anonimizadas.
* **Administrador del Sistema:**
  + Configurar y mantener los entornos.
  + Aplicar medidas de aislamiento y limpieza.
* **Desarrolladores / QA:**
  + Respetar las políticas de acceso, pruebas y manejo de información.

**10. Revisión y Actualización**

* Este procedimiento se revisará **anualmente** o al modificar entornos, herramientas o metodologías de desarrollo.
* Las actualizaciones deben reflejarse en el **Registro de Configuraciones del SGSI**.

**11. Evidencias y Soportes**

* Diagramas y configuraciones de entornos.
* Registros de acceso y despliegues.
* Informes de pruebas y auditorías.
* Actas de revisión y aprobación de cambios.

**Controles de Seguridad de las Aplicaciones**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Este documento establece las políticas, medidas y procedimientos para implementar **controles de seguridad en las aplicaciones** desarrolladas o utilizadas dentro del proyecto *Lava Rápido Vehicular*, conforme al control A.5.51 de la norma ISO/IEC 27001:2022.

El objetivo es asegurar que todas las aplicaciones y sistemas sean **diseñados, desarrollados y mantenidos de manera segura**, minimizando vulnerabilidades, accesos indebidos o pérdida de información.

**2. Alcance**

Aplica a todas las aplicaciones propias o de terceros que forman parte del proyecto, incluyendo:

* Sistema de gestión de clientes y servicios del Lava Rápido.
* Aplicaciones móviles o web utilizadas por clientes o personal.
* APIs y servicios externos integrados.
* Módulos administrativos, de facturación y reportes.
* Cualquier software desarrollado o modificado por el equipo del proyecto.

**3. Principios de Seguridad en Aplicaciones**

1. **Seguridad por Diseño:** La seguridad debe considerarse desde la fase inicial de desarrollo.
2. **Validación de Entradas:** Toda información ingresada por el usuario debe validarse.
3. **Gestión de Acceso:** Aplicar autenticación y autorización basadas en roles.
4. **Cifrado:** Proteger datos sensibles en tránsito y en reposo.
5. **Gestión de Vulnerabilidades:** Identificar y corregir errores o fallos de seguridad.
6. **Actualizaciones Seguras:** Controlar versiones, parches y despliegues.

**4. Controles de Seguridad por Etapa del Ciclo de Vida**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| **Diseño** | Identificar requisitos de seguridad y riesgos. | Responsable de Seguridad / Desarrollador Líder |
| **Desarrollo** | Implementar control de acceso, validación de entradas y cifrado. | Equipo de Desarrollo |
| **Pruebas** | Realizar pruebas de seguridad y análisis de código. | QA / Seguridad |
| **Despliegue** | Revisar configuración y credenciales antes de publicar. | Administrador del Sistema |
| **Mantenimiento** | Aplicar parches, monitorear vulnerabilidades y auditar código. | Seguridad / Desarrolladores |

**5. Controles Técnicos Obligatorios**

* Uso de **HTTPS (TLS 1.2 o superior)** para todas las comunicaciones.
* Cifrado de contraseñas mediante algoritmos seguros (bcrypt, SHA-256 o superior).
* Implementación de **autenticación multifactor (MFA)** para usuarios administrativos.
* Políticas de **timeout de sesión** e inactividad.
* Prevención de ataques comunes (SQL Injection, XSS, CSRF).
* Control de acceso basado en **roles y privilegios mínimos**.
* Registro y monitoreo de errores mediante herramientas seguras (no mostrar errores al usuario final).

**6. Validación y Pruebas de Seguridad**

* Realizar **pruebas de penetración o vulnerabilidad** antes de cada despliegue importante.
* Implementar análisis de código estático (SAST) y dinámico (DAST).
* Revisar dependencias y librerías externas para detectar riesgos.
* Utilizar entornos de prueba separados del entorno de producción.
* Documentar los resultados y acciones correctivas en el **Informe de Validación de Seguridad de Aplicaciones**.

**7. Protección de Datos dentro de las Aplicaciones**

* Los datos sensibles (como contraseñas, documentos o información de clientes) deben almacenarse **cifrados y con control de acceso restringido**.
* Se prohíbe el almacenamiento local no cifrado de información en dispositivos móviles.
* Las sesiones de usuario deben cerrarse automáticamente después de un periodo de inactividad.
* Las copias de seguridad de aplicaciones deben almacenarse en entornos seguros.

**8. Gestión de Vulnerabilidades**

* Las vulnerabilidades detectadas deben **reportarse de inmediato** al Responsable de Seguridad.
* Se deben **clasificar según su severidad (alta, media, baja)** y corregirse en un plazo máximo de:
  + Alta: 48 horas
  + Media: 5 días
  + Baja: 10 días
* Las actualizaciones deben registrarse en el **Historial de Cambios y Parches de Seguridad**.

**9. Responsabilidades**

* **Dirección del Proyecto:**
  + Aprobar las políticas de desarrollo seguro.
* **Responsable de Seguridad:**
  + Coordinar revisiones y pruebas de seguridad.
  + Mantener los registros de auditoría.
* **Desarrolladores:**
  + Aplicar las prácticas seguras definidas en este documento.
* **QA / Pruebas:**
  + Verificar que los controles de seguridad funcionen correctamente.
* **Administrador del Sistema:**
  + Asegurar configuraciones seguras en servidores y bases de datos.

**10. Revisión y Actualización**

* Este documento será revisado **cada seis meses** o cuando se realicen cambios significativos en la aplicación.
* Las actualizaciones deben reflejarse en el **Manual de Seguridad de Aplicaciones del SGSI**.

**11. Evidencias y Soportes**

* Reportes de pruebas de vulnerabilidad.
* Bitácora de despliegues y actualizaciones.
* Registro de cambios en el código fuente (control de versiones).
* Informes de auditoría interna o externa.

**Documento: Seguridad de Dispositivos de Usuario Final**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Establecer lineamientos y controles de seguridad para los dispositivos de usuario final (computadores, móviles, tablets) que acceden al sistema *Lava Rápido Vehicular*, conforme al control **A.8.1** de la norma ISO/IEC 27001:2022.  
El objetivo es garantizar que los dispositivos utilizados por clientes, operadores y administradores se mantengan protegidos contra accesos no autorizados, pérdida de datos o malware.

**2. Alcance**

Aplica a todos los dispositivos utilizados por:

* **Clientes:** al acceder desde la aplicación móvil o web.
* **Operadores:** que gestionan asignaciones de servicios.
* **Administradores:** que acceden al panel de gestión de clientes, pagos y reportes.
* **Equipo de desarrollo:** que utilice dispositivos en actividades de programación o pruebas.

**3. Principios de Seguridad en Dispositivos**

1. Solo se permitirá acceso desde dispositivos autorizados.
2. Debe aplicarse **bloqueo automático** tras un tiempo de inactividad.
3. Los dispositivos deben contar con **antivirus y actualizaciones de seguridad** instaladas.
4. Todo almacenamiento local debe estar **cifrado** en dispositivos móviles.
5. Debe existir **separación de entornos laborales y personales** (BYOD).

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Configuración | Instalación de antivirus, cifrado y políticas de bloqueo | Administrador del Sistema |
| Operación | Uso conforme a las políticas, no instalar apps no seguras | Usuarios / Operadores |
| Soporte | Revisión de actualizaciones y parches de seguridad | Equipo de TI |
| Baja del equipo | Eliminación segura de datos y restauración de fábrica | TI / Seguridad |

**5. Controles Técnicos Obligatorios**

* Antivirus actualizado en todo dispositivo.
* Bloqueo automático tras 5 minutos de inactividad.
* Cifrado de disco en dispositivos móviles.
* Prohibido almacenar credenciales sin cifrado.

**6. Validación y Pruebas de Seguridad**

* Auditorías semestrales de dispositivos corporativos.
* Escaneo de vulnerabilidades en equipos conectados a la aplicación.
* Pruebas de borrado seguro al retirar dispositivos.

**7. Protección de Datos**

* No almacenar datos sensibles (contraseñas, información de pagos) en memoria local.
* Uso obligatorio de VPN en accesos remotos de administradores.
* Eliminación segura antes de dar de baja dispositivos.

**8. Gestión de Vulnerabilidades**

* Dispositivos comprometidos deben reportarse en máximo **2 horas**.
* Aplicación de parches críticos en máximo **48 horas**.

**9. Responsabilidades**

* **Dirección del Proyecto:** aprobar lineamientos de seguridad en dispositivos.
* **Administrador del Sistema:** configurar y supervisar dispositivos.
* **Usuarios:** cumplir normas de seguridad y uso responsable.
* **Responsable de Seguridad:** coordinar revisiones periódicas.

**10. Revisión y Actualización**

Este documento será revisado anualmente o cuando existan cambios en la infraestructura tecnológica.

**11. Evidencias y Soportes**

* Informes de auditoría de dispositivos.
* Bitácoras de antivirus y actualizaciones.
* Registros de bajas y eliminaciones seguras.

**📄 Documento: Gestión de Acceso Privilegiado**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Establecer medidas para controlar y limitar el uso de accesos privilegiados en el sistema *Lava Rápido Vehicular*, conforme al control **A.8.2** de ISO/IEC 27001:2022.  
El objetivo es garantizar que las cuentas con privilegios especiales (administradores de sistemas, desarrolladores, gestores de base de datos) estén debidamente protegidas y monitoreadas.

**2. Alcance**

Aplica a:

* **Administradores del sistema:** con acceso a servidores y bases de datos.
* **Usuarios con rol administrador:** que gestionan servicios, clientes y pagos.
* **Equipo de desarrollo:** cuando requiera privilegios para despliegue o pruebas.

**3. Principios de Seguridad**

1. Aplicar el principio de **privilegios mínimos**.
2. Prohibido el uso de cuentas compartidas.
3. Implementación de **autenticación multifactor (MFA)**.
4. **Registro de todas las actividades** realizadas con cuentas privilegiadas.

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Diseño | Definir roles en la aplicación (cliente, operador, admin). | Equipo de Desarrollo |
| Desarrollo | Implementar control de acceso basado en roles. | Desarrolladores |
| Despliegue | Configurar MFA en panel administrativo y base de datos. | Administrador del Sistema |
| Operación | Revisar logs de accesos privilegiados periódicamente. | Responsable de Seguridad |
| Mantenimiento | Rotar contraseñas de cuentas privilegiadas cada 90 días. | TI / Seguridad |

**5. Controles Técnicos Obligatorios**

* MFA en accesos de administrador.
* Timeout por inactividad en cuentas privilegiadas.
* Registro detallado de cambios en el sistema.
* Rotación periódica de contraseñas (máx. 90 días).

**6. Validación y Pruebas de Seguridad**

* Auditorías trimestrales de accesos de administrador.
* Intentos de acceso indebido desde cuentas estándar como prueba.
* Revisiones de logs de accesos privilegiados.

**7. Protección de Datos**

* Cifrado de credenciales y llaves de acceso.
* Restricción de acceso a la base de datos de usuarios y pagos solo a administradores autorizados.
* Separación de funciones entre administradores de sistema y de negocio.

**8. Gestión de Vulnerabilidades**

* Bloqueo automático de cuentas tras 3 intentos fallidos.
* Reportar intentos de acceso sospechosos en máximo **2 horas**.
* Aplicar parches de seguridad a los servicios de autenticación.

**9. Responsabilidades**

* **Dirección del Proyecto:** aprobar políticas de acceso privilegiado.
* **Responsable de Seguridad:** supervisar revisiones de privilegios.
* **Administrador del Sistema:** gestionar cuentas privilegiadas.
* **Desarrolladores:** aplicar roles en software.

**10. Revisión y Actualización**

Revisar este documento cada 6 meses o cuando cambie la estructura de roles en la aplicación.

**11. Evidencias y Soportes**

* Logs de accesos de administradores.
* Informes de auditoría de privilegios.
* Registro de cambios y rotación de credenciales.

**Restricción de Acceso a la Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Establecer lineamientos y medidas para restringir el acceso a la información y recursos del sistema *Lava Rápido Vehicular*, conforme al control **A.8.3** de ISO/IEC 27001:2022.  
El objetivo es asegurar que solo los usuarios autorizados accedan a la información necesaria según su rol, evitando accesos indebidos a datos de clientes, pagos o historial de servicios.

**2. Alcance**

Aplica a:

* **Clientes:** acceso limitado a su propia información, historial y pagos.
* **Operadores:** acceso a los servicios asignados y datos necesarios para prestar el servicio.
* **Administradores:** acceso a reportes, facturación y gestión global.
* **Equipo de desarrollo y pruebas:** acceso restringido a entornos de test, nunca a datos reales en producción.

**3. Principios de Seguridad**

1. **Necesidad de saber:** cada usuario solo accede a lo que requiere para su función.
2. **Segregación de funciones:** diferenciar claramente clientes, operadores y administradores.
3. **Control dinámico:** acceso basado en roles y permisos configurables.
4. **Revisión periódica de permisos:** eliminación de accesos obsoletos.

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Diseño | Definir roles y perfiles de usuario. | Equipo de Desarrollo |
| Desarrollo | Implementar control de acceso a nivel de aplicación y BD. | Desarrolladores |
| Despliegue | Configurar perfiles en el panel administrativo. | Administrador del Sistema |
| Operación | Revisar logs de accesos y modificar permisos según cambios de rol. | Responsable de Seguridad |
| Mantenimiento | Retirar accesos de usuarios desvinculados. | TI / Seguridad |

**5. Controles Técnicos Obligatorios**

* Control de acceso basado en roles (RBAC).
* Restricción de acceso a endpoints sensibles en la API.
* Limitación de vistas en la aplicación según el rol.
* Sesiones con tiempo máximo de inactividad.

**6. Validación y Pruebas de Seguridad**

* Pruebas de acceso indebido (intento de ver datos de otros clientes).
* Auditorías semestrales de permisos activos.
* Verificación de logs de accesos.

**7. Protección de Datos**

* Información de clientes visible solo para ellos.
* Datos de pagos protegidos con cifrado en tránsito y en reposo.
* Eliminación de privilegios al momento de desvinculación de empleados.

**8. Gestión de Vulnerabilidades**

* Reportar accesos indebidos inmediatamente.
* Corrección de configuraciones incorrectas en máximo **48h**.

**9. Responsabilidades**

* **Dirección del Proyecto:** aprobar políticas de acceso.
* **Equipo de Desarrollo:** implementar RBAC en el sistema.
* **Administrador del Sistema:** gestionar roles y permisos.
* **Responsable de Seguridad:** auditar y ajustar accesos.

**10. Revisión y Actualización**

Revisar cada 6 meses o cuando se modifique la estructura de roles.

**11. Evidencias y Soportes**

* Informes de permisos.
* Logs de accesos.
* Bitácoras de revisiones de cuentas.

**Acceso al Código Fuente**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Proteger la integridad y confidencialidad del código fuente del sistema *Lava Rápido Vehicular*, conforme al control **A.8.4** de ISO/IEC 27001:2022.  
El objetivo es asegurar que solo personal autorizado tenga acceso al repositorio de código, evitando modificaciones indebidas o pérdida de trazabilidad.

**2. Alcance**

Aplica a:

* **Desarrolladores internos:** con acceso controlado al repositorio.
* **Proveedores externos (si aplica):** con permisos limitados y contratos de confidencialidad.
* **Administradores de repositorio:** responsables de gestionar ramas y revisiones.

**3. Principios de Seguridad**

1. **Acceso restringido:** solo personal autorizado puede acceder al repositorio.
2. **Control de versiones:** todo cambio debe estar registrado en un sistema de control (Git).
3. **Revisión obligatoria:** todo merge requiere aprobación por pares.
4. **Protección de ramas críticas:** no se permite commit directo en ramas de producción.

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Diseño | Definir estructura de ramas y roles en repositorio. | Equipo de Desarrollo |
| Desarrollo | Revisión de código por pares en cada pull request. | Desarrolladores |
| Despliegue | Bloqueo de ramas de producción. | Administrador de Repositorio |
| Operación | Monitoreo de commits y actividad en repositorios. | Responsable de Seguridad |
| Mantenimiento | Rotación de credenciales y eliminación de accesos inactivos. | TI / Seguridad |

**5. Controles Técnicos Obligatorios**

* Autenticación multifactor en GitHub/GitLab.
* Restricción de commits directos en main y prod.
* Revisión automática de dependencias vulnerables.
* Logs de auditoría de commits.

**6. Validación y Pruebas de Seguridad**

* Revisión mensual de repositorios.
* Simulación de intento de acceso indebido.
* Auditoría de dependencias externas usadas.

**7. Protección de Datos**

* El código fuente no debe incluir credenciales ni llaves.
* Variables sensibles se almacenan en archivos de configuración cifrados.
* Acceso diferenciado entre entornos (dev/test/prod).

**8. Gestión de Vulnerabilidades**

* Vulnerabilidades en dependencias externas deben corregirse en máximo **72h**.
* Reportar intentos de acceso indebido inmediatamente.

**9. Responsabilidades**

* **Dirección del Proyecto:** aprobar políticas de acceso a repositorios.
* **Administrador de Repositorio:** gestionar ramas y permisos.
* **Desarrolladores:** cumplir prácticas seguras de codificación.
* **Responsable de Seguridad:** auditar repositorios.

**10. Revisión y Actualización**

Cada 6 meses o cuando cambien los procesos de desarrollo.

**11. Evidencias y Soportes**

* Logs de commits y merges.
* Bitácora de revisiones de repositorios.
* Reportes de auditorías de dependencias.

**Protección contra Malware**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Establecer controles y medidas para prevenir, detectar y responder a amenazas de software malicioso (malware, virus, troyanos, ransomware) que puedan afectar al sistema *Lava Rápido Vehicular*, conforme al control **A.8.7** de ISO/IEC 27001:2022.

**2. Alcance**

Aplica a:

* **Servidores y bases de datos** del sistema.
* **Aplicación web y móvil** utilizada por clientes y operadores.
* **Dispositivos de usuario final** que se conecten al sistema.

**3. Principios de Seguridad**

1. Todos los dispositivos deben contar con **antimalware actualizado**.
2. El sistema debe filtrar y escanear **archivos y adjuntos cargados por clientes**.
3. El acceso web debe estar protegido contra **descargas maliciosas y scripts no autorizados**.
4. Los incidentes de malware deben registrarse y tratarse de inmediato.

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Diseño | Incluir filtros de archivos y sanitización de entradas. | Equipo de Desarrollo |
| Desarrollo | Aplicar librerías seguras contra XSS/SQL Injection. | Desarrolladores |
| Despliegue | Configurar antivirus en servidores y endpoints. | Administrador del Sistema |
| Operación | Monitorear eventos de malware y reportar incidentes. | Responsable de Seguridad |
| Mantenimiento | Actualizar motores de antimalware semanalmente. | TI / Seguridad |

**5. Controles Técnicos Obligatorios**

* Antivirus en servidores y dispositivos.
* Escaneo automático de archivos cargados por clientes.
* Bloqueo de macros y scripts desconocidos.
* Restricción de ejecución de software no autorizado.

**6. Validación y Pruebas**

* Escaneos semanales de servidores.
* Pruebas de subida de archivos infectados simulados.
* Auditorías de eventos de seguridad.

**7. Protección de Datos**

* Datos sensibles protegidos ante ransomware mediante backups cifrados.
* Copias de seguridad aisladas de entornos de producción.

**8. Gestión de Vulnerabilidades**

* Reportar detecciones de malware en máximo **2 horas**.
* Parches aplicados en máximo **48 horas**.

**9. Responsabilidades**

* **Dirección del Proyecto:** aprobar lineamientos.
* **TI / Seguridad:** instalar y monitorear herramientas antimalware.
* **Usuarios:** no instalar software no autorizado.

**10. Revisión**

Revisión semestral o tras incidentes relevantes.

**11. Evidencias**

* Logs de antivirus.
* Reportes de incidentes de malware.
* Bitácora de actualizaciones.

**Gestión de Vulnerabilidades Técnicas**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Definir procedimientos para identificar, evaluar y corregir vulnerabilidades técnicas en el sistema *Lava Rápido Vehicular*, conforme al control **A.8.8** de ISO/IEC 27001:2022.

**2. Alcance**

Aplica a:

* **Aplicación web y móvil.**
* **APIs y servicios externos integrados.**
* **Servidores y bases de datos del proyecto.**

**3. Principios**

1. Escaneo regular de vulnerabilidades.
2. Priorización según criticidad (alta, media, baja).
3. Aplicación de parches y correcciones en plazos definidos.
4. Documentación y seguimiento de vulnerabilidades.

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Diseño | Evaluación de riesgos técnicos. | Responsable de Seguridad |
| Desarrollo | Uso de librerías seguras y actualizadas. | Desarrolladores |
| Despliegue | Ejecución de escaneo de vulnerabilidades. | Administrador del Sistema |
| Operación | Monitoreo de nuevas amenazas y actualización de parches. | TI / Seguridad |
| Mantenimiento | Corrección documentada de vulnerabilidades detectadas. | Equipo de Desarrollo |

**5. Controles Técnicos Obligatorios**

* Escaneo mensual con herramientas (ej. OWASP ZAP, Nessus).
* Parches críticos en máximo **48h**.
* Registro en bitácora de vulnerabilidades.

**6. Validación y Pruebas**

* Escaneos antes de cada despliegue mayor.
* Pentesting anual de la aplicación.
* Revisión de dependencias externas.

**7. Protección de Datos**

* Evitar fugas de información mediante corrección de vulnerabilidades.
* Cifrado en tránsito y en reposo para datos sensibles.

**8. Gestión de Vulnerabilidades**

* Clasificación: alta (48h), media (5 días), baja (10 días).
* Escalamiento inmediato si no se cumple plazo.

**9. Responsabilidades**

* **Responsable de Seguridad:** coordinar procesos de revisión.
* **Desarrolladores:** corregir vulnerabilidades.
* **Administrador de Sistema:** aplicar parches.

**10. Revisión**

Cada 6 meses o cuando se detecte nueva amenaza crítica.

**11. Evidencias**

* Reportes de escaneo.
* Informes de pentesting.
* Historial de parches aplicados.

**Gestión de Configuraciones**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Definir políticas de configuración segura (hardening) para todos los sistemas del proyecto *Lava Rápido Vehicular*, conforme al control **A.8.9** de ISO/IEC 27001:2022.

**2. Alcance**

Incluye:

* Configuración de **servidores, bases de datos y aplicaciones web/móviles**.
* Configuración de **API y servicios externos**.
* Estaciones de trabajo utilizadas por el equipo.

**3. Principios**

1. Uso de configuraciones seguras por defecto.
2. Eliminación de servicios innecesarios.
3. Documentación de configuraciones aplicadas.
4. Monitoreo continuo de cambios no autorizados.

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Diseño | Definir configuraciones seguras para servidores y BD. | Equipo de Desarrollo |
| Despliegue | Aplicar plantillas de hardening en servidores. | Administrador del Sistema |
| Operación | Monitorear configuraciones activas. | Responsable de Seguridad |
| Mantenimiento | Revisar configuraciones tras actualizaciones. | TI / Seguridad |

**5. Controles Técnicos Obligatorios**

* Plantillas estándar de configuración (OWASP, CIS).
* Deshabilitación de puertos y servicios no utilizados.
* Uso de firewalls y listas de control de acceso.

**6. Validación y Pruebas**

* Auditorías semestrales de configuración.
* Comparación contra baseline de seguridad.

**7. Protección de Datos**

* Configuraciones que aseguren cifrado y acceso controlado a datos sensibles.
* Bloqueo de usuarios no autorizados.

**8. Gestión de Vulnerabilidades**

* Corrección de configuraciones débiles detectadas en máximo **72h**.

**9. Responsabilidades**

* **Equipo de Desarrollo:** definir parámetros seguros.
* **Administrador del Sistema:** aplicar configuraciones.
* **Responsable de Seguridad:** auditar configuraciones.

**10. Revisión**

Revisión anual o tras despliegues críticos.

**11. Evidencias**

* Bitácora de configuraciones aplicadas.
* Informes de auditoría de hardening.
* Logs de cambios en configuraciones.

**Eliminación de Información**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Establecer las directrices para la eliminación segura de información y soportes electrónicos en el sistema *Lava Rápido Vehicular*, conforme al control **A.8.10** de ISO/IEC 27001:2022.  
El objetivo es garantizar que los datos sensibles de clientes, pagos y servicios no puedan ser recuperados tras su eliminación.

**2. Alcance**

Incluye:

* **Bases de datos de clientes, servicios y facturación.**
* **Copias de seguridad temporales.**
* **Dispositivos de almacenamiento y servidores obsoletos.**

**3. Principios**

1. La información debe eliminarse de forma **irrecuperable** cuando ya no sea necesaria.
2. Se prohíbe la eliminación manual no controlada.
3. Los medios de almacenamiento deben ser **destruidos o borrados de forma certificada**.

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Diseño | Definir procesos de retención y eliminación. | Responsable de Seguridad |
| Operación | Aplicar borrado seguro en registros obsoletos. | Administrador del Sistema |
| Mantenimiento | Destruir medios de almacenamiento retirados. | TI / Seguridad |

**5. Controles Técnicos Obligatorios**

* Uso de herramientas de borrado seguro (ej. DB Shredder).
* Eliminación de archivos temporales tras procesamiento.
* Destrucción física de discos fuera de uso.

**6. Validación y Pruebas**

* Pruebas de no recuperación de datos tras eliminación.
* Certificación de eliminación segura.

**7. Protección de Datos**

* Datos de clientes y pagos eliminados conforme a normativa.
* No mantener registros fuera de los plazos definidos.

**8. Gestión de Vulnerabilidades**

* Detectar archivos residuales no eliminados y corregirlos en máximo **48h**.

**9. Responsabilidades**

* **Dirección:** aprobar políticas de retención y eliminación.
* **TI:** ejecutar borrado seguro.
* **Seguridad:** auditar procesos de eliminación.

**10. Revisión**

Cada 12 meses o tras cambios en políticas legales.

**11. Evidencias**

* Reportes de eliminación de datos.
* Certificados de destrucción de medios.

**Enmascaramiento de Datos**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Definir políticas para proteger información sensible mediante técnicas de enmascaramiento y anonimización en el sistema *Lava Rápido Vehicular*, conforme al control **A.8.11** de ISO/IEC 27001:2022.

**2. Alcance**

Aplica a:

* **Bases de datos utilizadas en entornos de prueba.**
* **Datos sensibles de clientes (ej. teléfono, datos de pago).**
* **Módulos de facturación y reportes.**

**3. Principios**

1. No se deben usar datos reales en entornos de prueba.
2. Los datos deben ser **anonimizados o enmascarados** antes de su uso fuera de producción.
3. El enmascaramiento debe ser irreversible.

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Diseño | Definir qué datos requieren enmascaramiento. | Responsable de Seguridad |
| Desarrollo | Implementar funciones de enmascaramiento. | Desarrolladores |
| Pruebas | Usar solo datos anonimizados en entornos de QA. | QA / Seguridad |

**5. Controles Técnicos Obligatorios**

* Enmascaramiento de números de teléfono y correos.
* Sustitución de información sensible en reportes de prueba.
* Uso de datos sintéticos para simulaciones.

**6. Validación y Pruebas**

* Verificar que en entornos de prueba no existan datos reales.
* Auditorías semestrales de bases de datos de QA.

**7. Protección de Datos**

* La información sensible solo puede estar en producción.
* Los datos de clientes deben cifrarse y nunca replicarse sin protección.

**8. Gestión de Vulnerabilidades**

* Cualquier exposición de datos reales en pruebas debe corregirse en **24h**.

**9. Responsabilidades**

* **Desarrolladores:** aplicar enmascaramiento en bases de datos de prueba.
* **QA:** validar que las pruebas no contengan información real.
* **Seguridad:** auditar entornos de prueba.

**10. Revisión**

Cada 12 meses o al modificar procesos de QA.

**11. Evidencias**

* Bitácoras de enmascaramiento.
* Reportes de auditoría en QA.

**Prevención de Fuga de Datos (DLP)**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Implementar controles para evitar fugas o pérdidas de información sensible del proyecto *Lava Rápido Vehicular*, conforme al control **A.8.12** de ISO/IEC 27001:2022.

**2. Alcance**

Incluye:

* **Datos de clientes y servicios.**
* **Registros de pagos y facturación.**
* **Información administrativa y operativa.**

**3. Principios**

1. Controlar la transferencia de datos sensibles.
2. Prohibir el uso de medios removibles no autorizados.
3. Monitorear la salida de información hacia internet o dispositivos externos.

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Diseño | Definir clasificación de información sensible. | Responsable de Seguridad |
| Desarrollo | Aplicar restricciones en API para exportar datos. | Desarrolladores |
| Operación | Configurar DLP en correo y endpoints. | TI / Seguridad |
| Mantenimiento | Revisar logs de transferencias de datos. | Responsable de Seguridad |

**5. Controles Técnicos Obligatorios**

* Bloqueo de uso de USB sin autorización.
* Monitoreo de envíos de datos sensibles por correo.
* Restricción de exportaciones masivas desde la aplicación.

**6. Validación y Pruebas**

* Pruebas de intento de copia de datos a dispositivos externos.
* Simulación de fuga de información vía correo electrónico.

**7. Protección de Datos**

* Cifrado de información en tránsito hacia servicios externos.
* Control de acceso a reportes sensibles.

**8. Gestión de Vulnerabilidades**

* Reportar intentos de fuga en máximo **2h**.
* Correcciones de configuración en **48h**.

**9. Responsabilidades**

* **Dirección del Proyecto:** aprobar política de protección de datos.
* **TI:** configurar DLP y restricciones de acceso.
* **Seguridad:** monitorear y auditar transferencias.

**10. Revisión**

Cada 6 meses o tras un incidente de fuga de información.

**11. Evidencias**

* Logs de intentos de fuga de información.
* Reportes de auditoría de DLP.
* Bitácora de incidentes.

**Copias de Seguridad**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Establecer políticas y procedimientos para garantizar la creación, almacenamiento y recuperación de copias de seguridad de la información crítica del *Lava Rápido Vehicular*, conforme al control **A.8.13** de ISO/IEC 27001:2022.

**2. Alcance**

Incluye:

* **Bases de datos** de clientes, servicios y facturación.
* **Configuraciones de servidores y API.**
* **Módulos de la aplicación web y móvil.**

**3. Principios**

1. Copias de seguridad deben realizarse de manera **periódica y automática**.
2. Las copias deben estar **cifradas** en tránsito y en reposo.
3. Debe existir al menos **una copia externa o en la nube**.
4. Verificación regular de la integridad y recuperación de las copias.

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Planificación | Definir frecuencia y datos críticos a respaldar. | Responsable de Seguridad |
| Ejecución | Generar backups automáticos de BD y configuraciones. | Administrador del Sistema |
| Almacenamiento | Guardar copias cifradas en nube y almacenamiento local. | Administrador del Sistema |
| Verificación | Probar restauración periódica de copias. | QA / Seguridad |

**5. Controles Técnicos Obligatorios**

* Backup diario de la base de datos.
* Backup semanal completo de servidores.
* Almacenamiento en nube con cifrado AES-256.
* Retención mínima de 30 días.

**6. Validación y Pruebas**

* Restauración de prueba cada trimestre.
* Verificación de checksums de integridad.

**7. Protección de Datos**

* Copias cifradas en todo momento.
* Acceso restringido solo a personal autorizado.

**8. Gestión de Vulnerabilidades**

* Incidentes de pérdida de datos deben resolverse en máximo **24h**.
* Fallos de backup deben reportarse en el mismo día.

**9. Responsabilidades**

* **Dirección:** aprobar políticas de backup.
* **TI:** ejecutar copias y pruebas de restauración.
* **Seguridad:** auditar copias y restauraciones.

**10. Revisión**

Cada 6 meses o tras cambios en la infraestructura.

**11. Evidencias**

* Informes de copias generadas.
* Registros de pruebas de restauración.
* Bitácora de fallos de backup.

**Redundancia de Sistemas**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Asegurar la disponibilidad del sistema *Lava Rápido Vehicular* mediante mecanismos de redundancia en la infraestructura tecnológica, conforme al control **A.8.14** de ISO/IEC 27001:2022.

**2. Alcance**

Incluye:

* **Servidores de aplicación web y móvil.**
* **Base de datos central del sistema.**
* **Servicios en la nube y red de comunicaciones.**

**3. Principios**

1. El sistema debe mantenerse **disponible ante fallos** de hardware o software.
2. Las bases de datos críticas deben estar **replicadas**.
3. La infraestructura debe contar con **balanceo de carga**.
4. Las comunicaciones deben tener **rutas alternativas**.

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Diseño | Definir arquitectura con redundancia. | Equipo de Desarrollo |
| Despliegue | Configurar servidores en clúster. | Administrador del Sistema |
| Operación | Monitorear alta disponibilidad y conmutación. | Responsable de Seguridad |
| Mantenimiento | Revisar logs de replicación y fallos. | TI / Seguridad |

**5. Controles Técnicos Obligatorios**

* Servidores en alta disponibilidad (HA).
* Replicación en tiempo real de la base de datos.
* Balanceadores de carga configurados.
* UPS y redundancia eléctrica.

**6. Validación y Pruebas**

* Prueba de conmutación cada 6 meses.
* Simulación de caída de un nodo.

**7. Protección de Datos**

* Replicación cifrada entre servidores.
* Garantía de consistencia de datos replicados.

**8. Gestión de Vulnerabilidades**

* Reportar fallos de replicación inmediatamente.
* Ajustes en configuraciones críticas en **48h**.

**9. Responsabilidades**

* **Dirección:** aprobar inversión en infraestructura redundante.
* **TI:** implementar redundancia.
* **Seguridad:** validar alta disponibilidad.

**10. Revisión**

Cada 12 meses o tras incidentes de caída.

**11. Evidencias**

* Logs de replicación.
* Informes de pruebas de failover.

**Sincronización de Reloj**

**Proyecto Lava Rápido Vehicular**  
**Fecha de Emisión:** 05 de octubre de 2025  
**Versión:** 1.0

**1. Propósito**

Mantener sincronizados los relojes de todos los sistemas y dispositivos del *Lava Rápido Vehicular*, conforme al control **A.8.17** de ISO/IEC 27001:2022.  
El objetivo es asegurar que los registros y auditorías de seguridad tengan coherencia temporal.

**2. Alcance**

Aplica a:

* **Servidores y bases de datos.**
* **Aplicación web y móvil.**
* **Sistemas de seguridad y monitoreo.**

**3. Principios**

1. Todos los equipos deben sincronizar su reloj con un servidor confiable.
2. No se permiten ajustes manuales sin autorización.
3. Los registros deben tener marcas de tiempo consistentes.

**4. Controles de Seguridad por Etapa**

| **Etapa** | **Medida de Seguridad Aplicada** | **Responsable** |
| --- | --- | --- |
| Diseño | Incluir sincronización de reloj como requisito. | Equipo de Desarrollo |
| Despliegue | Configurar NTP en servidores y bases de datos. | Administrador del Sistema |
| Operación | Monitorear desfase de tiempo. | Responsable de Seguridad |
| Mantenimiento | Verificar logs con consistencia horaria. | TI / Seguridad |

**5. Controles Técnicos Obligatorios**

* Uso de servidores NTP confiables.
* Sincronización automática cada hora.
* Alertas en caso de desfase mayor a 5 segundos.

**6. Validación y Pruebas**

* Verificación de sincronía semanal.
* Prueba de auditoría con logs de diferentes sistemas.

**7. Protección de Datos**

* Garantía de trazabilidad confiable en incidentes de seguridad.

**8. Gestión de Vulnerabilidades**

* Reportar desfases críticos de tiempo en máximo **2h**.

**9. Responsabilidades**

* **TI:** configurar NTP en servidores.
* **Seguridad:** auditar consistencia horaria.
* **Desarrolladores:** registrar logs con timestamps sincronizados.

**10. Revisión**

Cada 6 meses o tras fallos detectados.

**11. Evidencias**

* Logs de sincronización NTP.
* Reportes de auditoría de tiempo.

El presente documento ha sido revisado y aprobado por los responsables designados del proyecto Lava Rápido Vehicular. Con su firma, se confirma el compromiso con el cumplimiento de los lineamientos aquí establecidos y la implementación de buenas prácticas de seguridad de la información conforme a la norma ISO/IEC 27001:2022.

**Firma del responsable de Seguridad de la Información:**

[Nombre del responsable]  
Fecha: 05/10/2025

**Firma de los Integrantes del Proyecto:**

[Nombres de los integrantes o espacio para firmas]

**Firma del responsable del Proyecto:**

[Nombre del responsable del proyecto]  
Fecha: 05/10/2025