| | UNIVERSIDAD SURCOLOMBIANA<br>GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN<br>SEGURIDAD Y PRIVACIDAD DE LA INFORMACION EN LA GESTION DE PROYECTOS | | | | | | |
|---|---|---|---|---|---|---|---|
| **CÓDIGO** | **ES-GSPI-FO-06** | **VERSIÓN** | **1** | **VIGENCIA** | **2026** | **PAGINA** | **1 DE** |

| **1. IDENTIFICACIÓN Y CARACTERIZACIÓN DEL PROYECTO** | | | | | |
|---|---|---|---|---|---|
| **Nombre del proyecto** | | | **Código del proyecto** | | |
| **Proceso / dependencia responsable** | | | **Líder del proyecto** | | |
| **Responsable técnico** | | | **Responsable del proyecto** | | |
| **Responsable de Seguridad y Privacidad** | | | **Tipo de proyecto** | | |
| **Fecha de inicio** | | | **Fecha prevista de finalización** | | |
| **Estado del proyecto** | | | **¿Implica desarrollo de software?** | ☐ Si | ☐ No |
| **¿Implica infraestructura tecnológica?** | ☐ Si | ☐ No | **¿Implica servicios en la nube?** | ☐ Si | ☐ No |
| **¿Implica intercambio de información?** | ☐ Si | ☐ No | **¿Involucra terceros?** | ☐ Si | ☐ No |

| **2. CLASIFICACIÓN Y CARACTERIÍSTICAS DE LA INFORMACIÓN** | | | |
|---|---|---|---|
| **Tipo de información** | **Sí** | **No** | **Observaciones** |
| ¿Involucra datos personales? | ☐ | ☐ | |
| ¿Involucra datos personales sensibles? | ☐ | ☐ | |
| ¿Involucra información institucional reservada? | ☐ | ☐ | |
| ¿Involucra información académica? | ☐ | ☐ | |
| ¿Involucra información financiera? | ☐ | ☐ | |
| ¿Involucra información de estudiantes? | ☐ | ☐ | |
| ¿Involucra información de funcionarios/docentes? | ☐ | ☐ | |
| ¿Involucra información de contratistas? | ☐ | ☐ | |

**3. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**
**(Escala: C = Cumple | CP = Cumple parcialmente | NC = No cumple | NA = No aplica)**

| **N.º** | **Aspecto a validar** | **C** | **CP** | **NC** | **NA** | **Evidencia / observación** |
|---|---|---|---|---|---|---|
| 1 | Se identificaron los activos de información involucrados en el proyecto. | ☐ | ☐ | ☐ | ☐ | |
| 2 | Se identificaron los responsables de los activos de información. | ☐ | ☐ | ☐ | ☐ | |
| 2 | Se realizó la clasificación de la información. | ☐ | ☐ | ☐ | ☐ | |
| 3 | Se identificaron los riesgos de seguridad de la información. | ☐ | ☐ | ☐ | ☐ | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | Se identificaron los riesgos relacionados con privacidad y datos personales. | ☐ | ☐ | ☐ | ☐ | |
| 5 | Se definieron controles para mitigar los riesgos identificados. | ☐ | ☐ | ☐ | ☐ | |
| 6 | Se definieron perfiles y permisos de acceso. | ☐ | ☐ | ☐ | ☐ | |
| 7 | El acceso a la información se limita según las funciones del usuario. | ☐ | ☐ | ☐ | ☐ | |
| 8 | Se implementa autenticación adecuada para los usuarios. | ☐ | ☐ | ☐ | ☐ | |
| 9 | Se controla la creación, modificación y eliminación de usuarios. | ☐ | ☐ | ☐ | ☐ | |
| 10 | Se cuenta con mecanismos de trazabilidad y registro de actividades. | ☐ | ☐ | ☐ | ☐ | |
| 11 | Se protege la información durante su transmisión. | ☐ | ☐ | ☐ | ☐ | |
| 12 | Se protege la información almacenada. | ☐ | ☐ | ☐ | ☐ | |
| 13 | Se realizan copias de seguridad cuando corresponde. | ☐ | ☐ | ☐ | ☐ | |
| 14 | Se ha definido el procedimiento para recuperación de información. | ☐ | ☐ | ☐ | ☐ | |
| 15 | Se han definido mecanismos para prevenir pérdida o alteración de información. | ☐ | ☐ | ☐ | ☐ | |
| 16 | Se aplican controles contra software malicioso. | ☐ | ☐ | ☐ | ☐ | |
| 17 | Se han establecido mecanismos de actualización y gestión de vulnerabilidades. | ☐ | ☐ | ☐ | ☐ | |
| 18 | Se realizaron pruebas de seguridad antes de la puesta en producción. | ☐ | ☐ | ☐ | ☐ | |
| 19 | Se corrigieron o gestionaron las vulnerabilidades identificadas durante las pruebas. | ☐ | ☐ | ☐ | ☐ | |
| 20 | Se definieron controles para ambientes de desarrollo, pruebas y producción, cuando aplique | ☐ | ☐ | ☐ | ☐ | |
| 21 | Se cuenta con un procedimiento para gestionar, aprobar y registrar cambios del proyecto y sus componentes. | ☐ | ☐ | ☐ | ☐ | |
| 22 | Se mantiene identificada y controlada la configuración de los componentes tecnológicos involucrados, cuando aplica. | ☐ | ☐ | ☐ | ☐ | |
| 23 | Se controlan las cuentas con privilegios administrativos. | ☐ | ☐ | ☐ | ☐ | |
| 24 | Se realizan revisiones de permisos de acceso, especialmente para usuarios privilegiados, cuando aplica. | ☐ | ☐ | ☐ | ☐ | |

## 4. PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

**(Escala: C = Cumple | CP = Cumple parcialmente | NC = No cumple | NA = No aplica)**

| N.º | Aspecto a validar | C | CP | NC | NA | Evidencia / observación |
|---|---|---|---|---|---|---|
| 1 | Se identificaron los datos personales tratados por el proyecto. | ☐ | ☐ | ☐ | ☐ | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | Se identificó la finalidad del tratamiento de los datos personales. | ☐ | ☐ | ☐ | ☐ | |
| 3 | La finalidad del tratamiento se encuentra definida y documentada. | ☐ | ☐ | ☐ | ☐ | |
| 4 | Los datos personales recolectados son adecuados, pertinentes y limitados a lo necesario para las finalidades definidas. | ☐ | ☐ | ☐ | ☐ | |
| 5 | Se verificó la base jurídica que permite el tratamiento de los datos. | ☐ | ☐ | ☐ | ☐ | |
| 6 | Se informa al titular sobre el tratamiento de sus datos cuando corresponde. | ☐ | ☐ | ☐ | ☐ | |
| 7 | Se implementan controles para proteger los datos personales. | ☐ | ☐ | ☐ | ☐ | |
| 8 | Se controla quién puede consultar los datos personales. | ☐ | ☐ | ☐ | ☐ | |
| 9 | Se controla quién puede modificar o eliminar datos personales. | ☐ | ☐ | ☐ | ☐ | |
| 10 | Se evita almacenar datos personales que no sean necesarios. | ☐ | ☐ | ☐ | ☐ | |
| 11 | Se han definido tiempos de conservación y/o eliminación. | ☐ | ☐ | ☐ | ☐ | |
| 12 | Se contemplan mecanismos para atender solicitudes de los titulares. | ☐ | ☐ | ☐ | ☐ | |
| 13 | Se han identificado terceros que puedan tratar información personal. | ☐ | ☐ | ☐ | ☐ | |
| 14 | Se identificaron transferencias y/o transmisiones de datos personales, cuando corresponde. | ☐ | ☐ | ☐ | ☐ | |
| 15 | Se identificaron los terceros que actúan como encargados del tratamiento, cuando corresponde. | ☐ | ☐ | ☐ | ☐ | |
| 16 | Se han establecido obligaciones de seguridad y privacidad con terceros, cuando aplica. | ☐ | ☐ | ☐ | ☐ | |
| 17 | Se ha contemplado el manejo de incidentes que involucren datos personales. | ☐ | ☐ | ☐ | ☐ | |

## 5. SEGURIDAD Y PRIVACIDAD DESDE EL DISEÑO

**(Escala: C = Cumple | CP = Cumple parcialmente | NC = No cumple | NA = No aplica)**

| N.º | Aspecto a validar | C | CP | NC | NA | Evidencia / observación |
|---|---|---|---|---|---|---|
| 1 | Se identificaron los requisitos de seguridad desde la etapa de diseño. | ☐ | ☐ | ☐ | ☐ | |
| 2 | Se identificaron los requisitos de privacidad desde la etapa de diseño, cuando aplica. | ☐ | ☐ | ☐ | ☐ | |
| 3 | Se evaluaron los riesgos derivados de nuevas funcionalidades, integraciones o cambios. | ☐ | ☐ | ☐ | ☐ | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | Se definieron controles de seguridad y privacidad antes de la implementación. | ☐ | ☐ | ☐ | ☐ | |
| 5 | Se aplicaron principios de minimización de datos cuando se tratan datos personales. | ☐ | ☐ | ☐ | ☐ | |
| 6 | Se definieron requisitos de seguridad para proveedores, componentes y servicios de terceros. | ☐ | ☐ | ☐ | ☐ | |

**6. SEGURIDAD DURANTE EL DESARROLLO DEL PROYECTO**
**(Escala: C = Cumple | CP = Cumple parcialmente | NC = No cumple | NA = No aplica)**

| N.º | Aspecto a validar | C | CP | NC | NA | Evidencia / observación |
|---|---|---|---|---|---|---|
| 1 | El código fuente se encuentra bajo control de versiones. | ☐ | ☐ | ☐ | ☐ | |
| 2 | Se controla el acceso al repositorio del proyecto. | ☐ | ☐ | ☐ | ☐ | |
| 3 | No se almacenan contraseñas directamente en el código fuente. | ☐ | ☐ | ☐ | ☐ | |
| 4 | No se almacenan claves, tokens o secretos en repositorios públicos. | ☐ | ☐ | ☐ | ☐ | |
| 5 | Se validan las entradas suministradas por los usuarios. | ☐ | ☐ | ☐ | ☐ | |
| 6 | Se aplican controles contra inyección SQL. | ☐ | ☐ | ☐ | ☐ | |
| 7 | Se aplican controles contra XSS. | ☐ | ☐ | ☐ | ☐ | |
| 8 | Se aplican controles adecuados de autenticación y autorización. | ☐ | ☐ | ☐ | ☐ | |
| 9 | Se gestionan adecuadamente las sesiones. | ☐ | ☐ | ☐ | ☐ | |
| 10 | Se manejan adecuadamente los errores sin revelar información sensible. | ☐ | ☐ | ☐ | ☐ | |
| 11 | Se utilizan componentes y librerías actualizados. | ☐ | ☐ | ☐ | ☐ | |
| 12 | Se identifican y gestionan las dependencias de terceros utilizadas por la aplicación. | ☐ | ☐ | ☐ | ☐ | |
| 13 | Se realizó análisis automatizado de calidad y seguridad del código fuente, cuando aplica. | ☐ | ☐ | ☐ | ☐ | |
| 14 | Los hallazgos de análisis de código fueron evaluados y tratados de acuerdo con su criticidad. | ☐ | ☐ | ☐ | ☐ | |
| 15 | Se realizaron pruebas de vulnerabilidades. | ☐ | ☐ | ☐ | ☐ | |
| 16 | Se documentaron las correcciones realizadas. | ☐ | ☐ | ☐ | ☐ | |

**7. INFRAESTRUCTURA Y OPERACIÓN**
**(Escala: C = Cumple | CP = Cumple parcialmente | NC = No cumple | NA = No aplica)**

| N.º | Aspecto a validar | C | CP | NC | NA | Evidencia / observación |
|---|---|---|---|---|---|---|

| | UNIVERSIDAD SURCOLOMBIANA<br>GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN<br>SEGURIDAD Y PRIVACIDAD DE LA INFORMACION EN LA GESTION DE PROYECTOS | | | | | |
|---|---|---|---|---|---|---|
| **CÓDIGO** | **ES-GSPI-FO-06** | **VERSIÓN** | **1** | **VIGENCIA** | **2026** | **PAGINA** **1 DE** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | Los servidores cuentan con configuración segura. | ☐ | ☐ | ☐ | ☐ | |
| 2 | Se aplican actualizaciones de seguridad. | ☐ | ☐ | ☐ | ☐ | |
| 3 | Se restringen los puertos y servicios innecesarios. | ☐ | ☐ | ☐ | ☐ | |
| 4 | Se aplicaron configuraciones de endurecimiento (hardening), de acuerdo con las capacidades de la plataforma. | ☐ | ☐ | ☐ | ☐ | |
| 5 | Se aplicaron configuraciones de endurecimiento (hardening), de acuerdo con las capacidades de la plataforma. | ☐ | ☐ | ☐ | ☐ | |
| 6 | Se implementan mecanismos de protección perimetral cuando aplica. | ☐ | ☐ | ☐ | ☐ | |
| 7 | Se cuenta con monitoreo y registro de eventos. | ☐ | ☐ | ☐ | ☐ | |
| 8 | Se cuenta con respaldo de las bases de datos. | ☐ | ☐ | ☐ | ☐ | |
| 9 | Se ha probado la restauración de las copias de seguridad. | ☐ | ☐ | ☐ | ☐ | |
| 10 | Se cuenta con mecanismos de continuidad y recuperación. | ☐ | ☐ | ☐ | ☐ | |
| 11 | Se controla el acceso administrativo a servidores y bases de datos. | ☐ | ☐ | ☐ | ☐ | |

## 8. GESTIÓN DE TERCEROS
**(Escala: C = Cumple | CP = Cumple parcialmente | NC = No cumple | NA = No aplica)**

| ¿El proyecto involucra proveedores, contratistas, servicios en la nube o terceros? | | ☐ Si | ☐ No | | | |
|---|---|---|---|---|---|---|
| **N.º** | **Aspecto a validar** | **C** | **CP** | **NC** | **NA** | **Evidencia / observación** |
| 1 | Se identificaron los terceros involucrados. | ☐ | ☐ | ☐ | ☐ | |
| 2 | Se evaluaron los riesgos asociados al tercero. | ☐ | ☐ | ☐ | ☐ | |
| 3 | Se establecieron obligaciones de seguridad. | ☐ | ☐ | ☐ | ☐ | |
| 4 | Se establecieron obligaciones de privacidad, cuando aplica. | ☐ | ☐ | ☐ | ☐ | |
| 5 | Se definieron responsabilidades sobre la información. | ☐ | ☐ | ☐ | ☐ | |
| 6 | Se definieron controles para el acceso remoto del tercero, cuando aplica. | ☐ | ☐ | ☐ | ☐ | |
| 7 | Se establecieron mecanismos para finalizar el acceso del tercero. | ☐ | ☐ | ☐ | ☐ | |
| 8 | Se establecieron mecanismos para la devolución, eliminación o disposición de la información al finalizar el servicio, cuando corresponde. | ☐ | ☐ | ☐ | ☐ | |

## 9. GESTIÓN DE RIESGOS - PLAN DE TRATAMIENTO DE HALLAZGOS

Si el proyecto permite identificar riesgos u oportunidades remitase a ES-GSPI-DA-05 METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## 10. EVIDENCIAS REQUERIDAS

| | Evidencia | Aplica | | Observaciones |
|---|---|---|---|---|
| 1 | Documento de arquitectura | ☐ Si | ☐ No | |
| 2 | Diagrama de infraestructura | ☐ Si | ☐ No | |
| 3 | Diagrama de flujo de información | ☐ Si | ☐ No | |
| 4 | Matriz de riesgos | ☐ Si | ☐ No | |
| 5 | Matriz de permisos | ☐ Si | ☐ No | |
| 6 | Política / aviso de tratamiento de datos personales | ☐ Si | ☐ No | |
| 7 | Resultado de pruebas de seguridad | ☐ Si | ☐ No | |
| 8 | Resultado de análisis de vulnerabilidades | ☐ Si | ☐ No | |
| 9 | Evidencia de copias de seguridad | ☐ Si | ☐ No | |
| 10 | Evidencia de pruebas de restauración | ☐ Si | ☐ No | |
| 11 | Contrato / acuerdo con terceros | ☐ Si | ☐ No | |
| 12 | Manual o documentación técnica | ☐ Si | ☐ No | |
| 13 | Código fuente / repositorio | ☐ Si | ☐ No | |
| 14 | Otra | ☐ Si | ☐ No | |

## 11. CONCEPTO DE SEGURIDAD Y PRIVACIDAD

Observaciones del líder de Seguridad y Privacidad de la información:

## 12. APROBACIÓN

| Rol | Nombre | Firma | Fecha |
|---|---|---|---|
| Líder del proyecto | | | |
| Responsable técnico | | | |
| Responsable del proceso | | | |
| Líder de Seguridad y Privacidad de la Información | | | |