



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA RECREACIÓN Y DEPORTE
Instituto Distrital de las Artes

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

GUIA PRACTICA PARA EL DESARROLLO SEGURO DE SISTEMAS DE INFORMACION Y APLICATIVOS

GTI-G-10

V.1

02/10/2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN	2
2. OBJETIVOS	2
2.1. Objetivo principal	2
2.2. Objetivos específicos	2
3. ALCANCE	3
4. PRINCIPIOS DE APLICACIÓN	4
5. RESPONSABLES Y RESPONSABILIDADES	4
6. DEFINICIONES	4
7. FLUJO MÍNIMO DE DESARROLLO SEGURO	7
7.1. ¿Cuándo hacer análisis de amenazas?	7
8. CONTROLES MÍNIMOS OBLIGATORIOS	8
9. VERIFICACIONES OWASP SIMPLIFICADAS	9
9.1. Si el desarrollo expone o consume APIs	10
10. INTEGRACIÓN CON SCRUM	10
11. DEFINICIÓN DE TERMINADO (DoD) MÍNIMA	10
12. CLASIFICACIÓN PRÁCTICA DEL CAMBIO	10
13. GESTIÓN DE HALLAZGOS Y CRITERIOS DE LIBERACIÓN	11
14. MANTENIMIENTO Y OPERACIÓN SEGURA	11
15. CONTRIBUCIÓN PRÁCTICA AL MSPI	12
16. HERRAMIENTAS SUGERIDAS (NO OBLIGATORIAS)	12
17. GESTIÓN DE AMBIENTES Y DATOS DE PRUEBA	12
18. GESTIÓN DE CAMBIOS, RESPALDO Y RECUPERACIÓN	13
19. USO DE ASISTENTES DE INTELIGENCIA ARTIFICIAL Y COMPONENTES DE TERCEROS	14
20. TRAZABILIDAD CON EL ANEXO A DE LA NORMA ISO/IEC 27001:2022	15
21. CRIPTOGRAFÍA MÍNIMA ACEPTADA	16
Anexo A.	17
Anexo B.	19
Anexo C.	20
Anexo D.	21

TABLA DE TABLAS

TABLA 1. PRINCIPIOS DE APLICACIÓN	4
TABLA 2. RESPONSABLES Y RESPONSABILIDADES	5
TABLA 3. FLUJO MÍNIMO DE DESARROLLO SEGURO	8
TABLA 4. CONTROLES OBLIGATORIOS A IMPLEMENTAR	8
TABLA 5. VERIFICACIONES OWASP	10
TABLA 6. OWASP SI EL DESARROLLO EXPONE O CONSUME APIS	10
TABLA 7. INTEGRACIÓN CON SCRUM	10
TABLA 8. CLASIFICACIÓN DE PRÁCTICA DEL CAMBIO	11
TABLA 9. GESTIÓN DE HALLAZGOS Y CRITERIOS DE LIBERACIÓN	11
TABLA 10. MANTENIMIENTO Y OPERACIÓN SEGURA	12
TABLA 11. INTERRELACIÓN CON EL MSPI	12
TABLA 12. HERRAMIENTAS SUGERIDAS	13
TABLA 13. USOS PERMITIDOS POR AMBIENTES	13
TABLA 14. TIPOS DE CAMBIO, APROBACIÓN Y REVERSIÓN	14
TABLA 15. REGLAS PARA INTELIGENCIA ARTIFICIAL Y COMPONENTES DE TERCEROS	14
TABLA 16. TRAZABILIDAD DE LOS CONTROLES DE LA GUÍA CON ISO/IEC 27001:2022	15
TABLA 17. CRIPTOGRAFÍA MÍNIMA	16

1. INTRODUCCIÓN

El desarrollo de software constituye un componente fundamental para la transformación digital y el fortalecimiento de la gestión institucional. En este contexto, la seguridad de la información debe incorporarse de manera transversal durante todo el ciclo de vida de las aplicaciones y sistemas de información, de forma que los riesgos asociados al diseño, construcción, implementación y mantenimiento puedan ser identificados y tratados oportunamente.

La presente guía, establece lineamientos básicos y de fácil aplicación para integrar buenas prácticas de seguridad dentro de las actividades habituales de los equipos de desarrollo de software del Instituto Distrital de las Artes - Idartes. Su enfoque busca facilitar la adopción progresiva de controles de seguridad, sin generar cargas operativas innecesarias, especialmente en equipos pequeños que trabajan bajo metodologías ágiles y esquemas de desarrollo iterativo.

La guía articula prácticas de desarrollo seguro, principios del ciclo de vida de desarrollo de software seguro -SSDLC-, enfoques DevSecOps y criterios derivados de OWASP, incorporándolos en actividades como la definición de requisitos, diseño, desarrollo, revisión de código, pruebas, despliegue, mantenimiento y gestión de vulnerabilidades. Asimismo, promueve principios como seguridad desde el diseño, mínimo privilegio, protección de credenciales, validación de entradas, gestión adecuada de dependencias, trazabilidad de eventos, revisión de accesos y tratamiento oportuno de hallazgos.

Su aplicación contribuye al fortalecimiento de los controles técnicos y operativos requeridos para la gestión de la seguridad digital y apoya el cumplimiento de los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información -MSPI, mediante la generación de evidencias verificables y la incorporación de controles mínimos dentro del proceso institucional de desarrollo de software.

En consecuencia, este documento se concibe como una herramienta práctica de consulta y aplicación para desarrolladores, líderes técnicos, responsables funcionales, personal de pruebas y demás actores involucrados en el ciclo de vida del software, permitiendo que la seguridad sea gestionada como parte natural del desarrollo y no únicamente como una actividad posterior a la construcción o previa a la puesta en producción.

2. OBJETIVOS

2.1. Objetivo principal

Establecer un conjunto básico, verificable y de fácil aplicación de prácticas de desarrollo seguro para que los equipos de software de IDARTES incorporen seguridad desde el análisis de requerimientos hasta el mantenimiento, manteniendo trazabilidad suficiente para demostrar su aplicación y apoyar el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI).

2.2. Objetivos específicos

- Establecer controles mínimos de seguridad que puedan ser incorporados de manera sencilla durante las fases de análisis, diseño, desarrollo, pruebas, implementación y mantenimiento de los sistemas de información y aplicativos.
- Integrar prácticas básicas de desarrollo seguro en la metodología de trabajo de los equipos de gestión de software, promoviendo la seguridad desde el diseño, la revisión de código, la gestión segura de accesos, dependencias y vulnerabilidades.

- Definir criterios de verificación y evidencias mínimas que permitan demostrar la aplicación de buenas prácticas de desarrollo seguro y contribuir al cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI.

3. ALCANCE

La presente guía aplica a los proyectos de desarrollo, actualización, mantenimiento o mejora de sistemas de información y aplicaciones de software, desarrollados y/o gestionados por el Instituto Distrital de las Artes - Idartes, incluyendo todos aquellos desarrollados internamente o mediante terceros, cuando su alcance involucre construcción o modificación de componentes de software.

Su alcance inicia desde la identificación y definición de los requerimientos funcionales y no funcionales de una nueva solución, módulo, funcionalidad o modificación de software, momento en el cual deberán identificarse los requisitos básicos de seguridad, los riesgos asociados al cambio y los controles que resulten aplicables de acuerdo con las características de la solución.

A partir de este punto, la guía comprende las actividades de diseño, desarrollo, gestión del código fuente, revisión de código, control de dependencias y secretos, ejecución de pruebas funcionales y de seguridad, tratamiento de vulnerabilidades, preparación del despliegue, configuración segura y liberación de la solución en el ambiente correspondiente.

Para ajustes menores que no afecten autenticación, autorización, datos, integraciones, infraestructura o lógica crítica, se permite una aplicación simplificada. Para cambios significativos, datos sensibles, servicios expuestos a internet o funcionalidades críticas, se deben aplicar controles reforzados.

El alcance finaliza con la implementación de la solución en ambiente productivo, la validación de los controles mínimos de seguridad definidos para la liberación y el registro de las evidencias correspondientes. Posteriormente, durante la etapa de mantenimiento, deberán mantenerse los controles relacionados con actualización de componentes, gestión de vulnerabilidades, revisión de accesos, monitoreo y tratamiento de incidentes que resulten aplicables durante la vida útil del sistema de información y/o aplicativo.

La guía no pretende sustituir las actividades específicas de gestión de cambios, infraestructura tecnológica, gestión de incidentes, continuidad, protección de datos personales o gestión de vulnerabilidades, sino establecer los criterios básicos de desarrollo seguro que deben articularse con dichas actividades, para contribuir al cumplimiento del Modelo de Seguridad y Privacidad de la Información – MSPI.

4. PRINCIPIOS DE APLICACIÓN

Tabla 1. Principios de aplicación

Principio	Aplicación sencilla
Seguridad desde el diseño	Los requisitos de seguridad se definen desde el backlog y no al final del desarrollo.
Mínimo privilegio	Usuarios, servicios, tokens y repositorios reciben únicamente los permisos necesarios.
Defensa en profundidad	No se depende de un solo control; se combinan validaciones, autorización, configuración y monitoreo.
Predeterminado seguro	Ante error, ausencia de permiso o configuración incompleta, el sistema debe

Principio	Aplicación sencilla
	denegar o fallar de forma segura.
Trazabilidad simple	Cada control debe dejar una evidencia mínima: ticket, PR, reporte, captura, log o acta.
Proporcionalidad	El esfuerzo de seguridad se ajusta al riesgo, criticidad y alcance del cambio.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

5. RESPONSABLES Y RESPONSABILIDADES

Tabla 2. Responsables y responsabilidades

Rol	Responsabilidad mínima
Product Owner / líder funcional	Define alcance, datos involucrados, criticidad y acepta criterios funcionales y de seguridad.
Líder técnico / desarrollador responsable	Implementa controles, revisa arquitectura, gestiona dependencias, secretos y correcciones.
Segundo desarrollador / revisor	Realiza revisión de código y valida controles básicos antes del merge.
QA o responsable de pruebas	Ejecuta casos negativos, pruebas funcionales y verificaciones OWASP aplicables.
Seguridad / infraestructura	Apoya cambios de alto riesgo, configuraciones, vulnerabilidades, despliegues e incidentes.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

Revisión independiente del cambio: La revisión final de un desarrollo, ajuste, actualización o mejora, no deberá quedar únicamente a cargo de la persona que realizó el cambio. Antes de su liberación, el código, la funcionalidad o la configuración modificada deberá ser revisada por al menos otro integrante del equipo con conocimiento técnico suficiente, quien verificará, como mínimo, que el cambio cumpla con los requerimientos definidos, no introduzca vulnerabilidades evidentes, mantenga los controles de seguridad aplicables y cuente con las pruebas correspondientes.

Para equipos pequeños, esta revisión podrá ser realizada por otro desarrollador, el líder técnico, el responsable de pruebas o, cuando corresponda, por el responsable de seguridad o arquitectura. La revisión deberá dejar una evidencia sencilla y verificable, por ejemplo, mediante la aprobación de un pull request, registro en la herramienta de gestión de proyectos, lista de chequeo, acta o evidencia de pruebas.

Este principio busca aplicar una validación de segunda instancia o “doble control”, reduciendo el riesgo de errores no detectados, cambios no autorizados o debilidades de seguridad, sin requerir la creación de roles adicionales dentro del equipo.

6. DEFINICIONES

Amenaza: circunstancia, evento o acción que puede aprovechar una vulnerabilidad y afectar la confidencialidad, integridad o disponibilidad de la información o de un sistema.

Análisis de amenazas: actividad mediante la cual se identifican posibles amenazas sobre una funcionalidad, componente, integración o flujo de información, con el propósito de establecer medidas de tratamiento.

Anonimización: proceso mediante el cual se modifican o eliminan los datos que permiten identificar, directa o indirectamente, a una persona, procurando que la identificación no pueda revertirse razonablemente.

API: interfaz de programación de aplicaciones que permite la comunicación e intercambio de información entre sistemas, aplicaciones o componentes de software.

Autenticación: proceso utilizado para verificar la identidad de un usuario, servicio, dispositivo o

componente antes de permitirle acceder a un sistema.

Autenticación multifactor -MFA-: mecanismo de autenticación que exige dos o más factores de verificación, como contraseña, código temporal, aplicación de autenticación o elemento biométrico.

Autorización: proceso mediante el cual se determina qué funcionalidades, recursos, operaciones o datos puede utilizar una identidad previamente autenticada.

Cifrado: mecanismo criptográfico que transforma la información para impedir su lectura por personas o sistemas no autorizados.

Criterio de seguridad: condición verificable que debe cumplir una historia de usuario, funcionalidad o cambio para reducir los riesgos de seguridad asociados con su implementación.

DAST -Dynamic Application Security Testing-: análisis dinámico de seguridad realizado sobre una aplicación en ejecución para identificar vulnerabilidades observables desde su funcionamiento externo.

Datos sensibles: información cuyo uso indebido puede afectar la intimidad de una persona o generar discriminación, riesgo o afectación significativa para su titular.

Datos sintéticos: información generada artificialmente para realizar pruebas y que conserva las características o formatos necesarios sin utilizar datos personales reales.

Defensa en profundidad: principio que establece la aplicación conjunta de diferentes controles de seguridad, de manera que la protección no dependa de una única medida.

Definición de Terminado -DoD-: conjunto de condiciones que debe cumplir una historia, funcionalidad o cambio para considerarse finalizado, incluyendo las revisiones, pruebas y evidencias de seguridad aplicables.

Desarrollo seguro: práctica de incorporar requisitos, controles, revisiones y pruebas de seguridad durante todas las fases del ciclo de vida del software.

DevSecOps: enfoque que integra la seguridad dentro de las actividades de desarrollo, pruebas, despliegue y operación, procurando que los controles se ejecuten de manera continua y, cuando sea posible, automatizada.

Enmascaramiento de datos: técnica que sustituye u oculta información real mediante valores ficticios o transformados, conservando el formato requerido para las pruebas.

Evidencia de seguridad: registro verificable que demuestra la aplicación de un control, como un ticket, aprobación de *pull request*, reporte de análisis, captura, log, acta o resultado de pruebas.

Gate de liberación: punto de control previo al despliegue en el cual se verifica que el cambio cumple los requisitos definidos y que no existen vulnerabilidades críticas o altas pendientes sin tratamiento o aceptación formal.

Gestión de vulnerabilidades: proceso de identificación, análisis, priorización, corrección y seguimiento de las vulnerabilidades que afectan los sistemas, aplicaciones o componentes tecnológicos.

Hallazgo de seguridad: debilidad, incumplimiento, error o condición identificada durante una revisión o prueba que puede afectar la seguridad de la solución.

Hardening o endurecimiento: aplicación de configuraciones seguras para reducir la superficie de ataque de servidores, bases de datos, contenedores, aplicaciones y demás componentes tecnológicos.

Infraestructura como código -IaC-: práctica de definir y administrar la infraestructura tecnológica mediante archivos de configuración versionados y ejecutables.

Logs o registros de eventos: información generada por los sistemas para dejar trazabilidad de accesos, errores, cambios, operaciones críticas y demás eventos relevantes para el monitoreo y la investigación de incidentes.

Mínimo privilegio: principio según el cual cada usuario, servicio, aplicación o componente recibe exclusivamente los permisos necesarios para cumplir sus funciones.

Modelo de Seguridad y Privacidad de la Información -MSPI-: marco establecido para orientar la gestión de la seguridad y privacidad de la información en las entidades públicas, mediante políticas, riesgos, controles, seguimiento y mejora continua.

OWASP: organización internacional que desarrolla metodologías, herramientas y referencias abiertas para mejorar la seguridad del software, entre ellas OWASP Top 10 para aplicaciones web y APIs.

Pipeline de CI/CD: secuencia automatizada de actividades utilizada para integrar, probar, analizar, construir y desplegar cambios de software.

Predeterminado seguro: principio según el cual un sistema debe iniciar y operar con la configuración más restrictiva y segura, denegando el acceso cuando falten permisos o exista una configuración incompleta.

Pull Request o Merge Request -PR/MR-: solicitud formal para revisar, aprobar e integrar cambios de código en una rama del repositorio.

Revisión independiente: validación efectuada por una persona diferente de quien desarrolló el cambio, con el fin de verificar su calidad, funcionamiento y cumplimiento de los controles de seguridad.

Riesgo de seguridad: posibilidad de que una amenaza aproveche una vulnerabilidad y produzca un impacto negativo sobre la información, el sistema o la operación institucional.

Rollback o reversión: procedimiento que permite retornar una aplicación, configuración o componente a una versión estable anterior cuando una implementación presenta fallas.

RPO -Recovery Point Objective-: cantidad máxima de información que puede perderse, medida en tiempo, después de una interrupción o incidente.

RTO -Recovery Time Objective-: tiempo máximo esperado para restablecer un sistema o servicio después de una interrupción.

SAST -Static Application Security Testing-: análisis del código fuente o de los componentes compilados, sin ejecutar la aplicación, para identificar posibles vulnerabilidades o prácticas inseguras.

SCA -Software Composition Analysis-: análisis de librerías, paquetes y dependencias de terceros para identificar vulnerabilidades conocidas, versiones desactualizadas o riesgos de licenciamiento.

SBOM -Software Bill of Materials-: inventario estructurado de los componentes, librerías, versiones y dependencias que conforman una solución de software.

Secreto: información utilizada para autenticar o proteger el acceso a sistemas, como contraseñas, tokens, certificados, llaves criptográficas y credenciales de servicios.

SSDLC -Secure Software Development Life Cycle-: ciclo de vida de desarrollo de software que incorpora actividades de seguridad desde la definición de requisitos hasta el mantenimiento y retiro de la solución.

STRIDE: metodología de análisis de amenazas que evalúa riesgos relacionados con suplantación, alteración, repudio, divulgación de información, denegación de servicio y elevación de privilegios.

TLS -Transport Layer Security-: protocolo criptográfico utilizado para proteger la confidencialidad e integridad de la información transmitida entre sistemas.

Trazabilidad: capacidad de identificar y reconstruir las actividades, decisiones, cambios, revisiones y evidencias relacionadas con el desarrollo y operación de una solución.

Vulnerabilidad: debilidad técnica, funcional, procedimental o de configuración que puede ser aprovechada por una amenaza para afectar un sistema o su información.

7. FLUJO MÍNIMO DE DESARROLLO SEGURO

El equipo puede aplicar la guía usando seis momentos. La seguridad se integra al trabajo normal de Scrum y no requiere un proceso paralelo.

Tabla 3. Flujo mínimo de desarrollo seguro

Momento	¿Qué hacer?	Evidencia mínima
1. Requerimientos	Identificar datos, usuarios, roles, integraciones y riesgos. Agregar criterios de seguridad en la historia cuando aplique.	Historia/ticket con criterios de seguridad.
2. Diseño	Definir autenticación, autorización, manejo de datos, errores, logs e integraciones. Para cambios significativos realizar un STRIDE breve.	Diagrama o nota técnica; amenazas principales y mitigaciones.
3. Desarrollo	Usar revisión de código, linter/SAST, gestión segura de secretos y dependencias.	PR aprobada + reporte o captura de análisis.
4. Pruebas	Ejecutar casos negativos y verificaciones OWASP web/API aplicables; DAST cuando esté disponible.	Evidencias de pruebas y registro de hallazgos.
5. Implementación	Validar configuración segura, variables/secreros, TLS, logs, rollback y aprobación de despliegue.	Checklist de liberación + ticket/cambio.
6. Mantenimiento	Actualizar componentes, revisar vulnerabilidades, accesos y eventos de seguridad.	Registro periódico de revisión y acciones.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

7.1. ¿Cuándo hacer análisis de amenazas?

Aplicar un análisis breve STRIDE cuando exista al menos una de estas condiciones: nueva autenticación o autorización; manejo de datos sensibles; nueva API o integración; exposición a Internet; carga de archivos; cambios de infraestructura; procesamiento crítico; cambio sustancial en permisos o flujo de negocio.

Para cambios menores de interfaz, textos, reportes sin datos nuevos o correcciones sin impacto de seguridad, basta documentar “No aplica” y la justificación. DREAD puede utilizarse opcionalmente para priorizar amenazas cuando existan varias y el equipo necesite decidir el orden de tratamiento.

8. CONTROLES MÍNIMOS OBLIGATORIOS

Tabla 4. Controles obligatorios a implementar

ID	Control	Aplicación mínima	Evidencia
C01	Criterios de seguridad en el backlog	Las historias que afecten acceso, datos, archivos, integraciones o infraestructura incluyen al menos un criterio de seguridad.	Historia/ticket.
C02	Revisión de código y rama protegida	Todo cambio a la rama principal requiere PR/MR y revisión por otra persona. No se permiten pushes directos a producción.	PR/MR aprobada.
C03	Secretos fuera del código	Contraseñas, tokens y llaves no se almacenan en código, repositorios, archivos públicos ni URLs.	Escaneo/revisión + configuración de variables protegidas.
C04	Dependencias controladas	Se usan versiones definidas, fuentes confiables y se revisan vulnerabilidades de librerías antes de liberar.	Reporte SCA/dependencias o evidencia equivalente.
C05	Validación de entradas	El servidor valida tipo, longitud, formato, rangos y archivos; las consultas usan parametrización/ORM seguro.	Pruebas negativas + revisión.
C06	Autenticación y sesiones	Se usan mecanismos institucionales/robustos; cookies y tokens tienen expiración y atributos seguros; MFA para privilegios cuando aplique.	Configuración + prueba.
C07	Autorización y mínimo privilegio	La autorización se valida en backend a nivel de función y objeto; los roles sólo tienen permisos necesarios.	Matriz simple de roles + prueba 401/403.
C08	Configuración y cifrado	Producción opera sin debug, con TLS, encabezados/configuraciones seguras y datos sensibles protegidos en reposo cuando aplique.	Checklist/configuración.
C09	Errores y excepciones	El usuario no recibe stack traces, rutas, SQL ni	Pruebas de error.

ID	Control	Aplicación mínima	Evidencia
	seguras	secretos; ante fallas de autorización o transacción el sistema falla cerrado.	
C10	Logs y trazabilidad	Se registran autenticaciones, fallos, cambios de permisos y acciones críticas sin guardar contraseñas, tokens o PII innecesaria.	Log de ejemplo / configuración.
C11	Pruebas de seguridad	Se ejecutan casos negativos y checklist OWASP aplicable; cuando sea viable, SAST/SCA/DAST se automatizan.	Reporte/capturas/casos de prueba.
C12	Gate de liberación y recuperación	No se libera con vulnerabilidades críticas o altas sin tratamiento o aceptación formal; existe rollback y responsables definidos.	Checklist de release + aprobación.
C13	Separación de ambientes	Desarrollo, pruebas y producción están separados lógica o físicamente. No se desarrolla, depura ni se realizan ajustes directos en producción, y las credenciales, llaves y bases de datos no se comparten entre ambientes.	Inventario o diagrama de ambientes + configuración diferenciada.
C14	Datos de prueba protegidos	No se utilizan datos personales reales en desarrollo ni en pruebas. Si resulta indispensable, se anonimizan o enmascaran previa autorización del dueño de la información, se restringe el acceso y se eliminan al terminar la actividad.	Autorización, procedimiento de enmascaramiento y acta de eliminación.
C15	Gestión de cambios y versionamiento	Todo paso a producción tiene solicitud, aprobación, versión etiquetada (tag/release), ventana definida y plan de reversión. Los cambios de emergencia se ejecutan y se documentan a más tardar dentro de los dos días hábiles siguientes.	Ticket de cambio aprobado + tag o release en el repositorio.
C16	Línea base de configuración y hardening	Servidores, contenedores, bases de datos y servicios se despliegan desde una línea base endurecida: servicios y puertos mínimos, cuentas y credenciales por defecto deshabilitadas, parches vigentes y configuración versionada.	Checklist de hardening (Anexo D) + configuración o laC versionada.
C17	Criptografía y gestión de llaves	Se emplean únicamente algoritmos y longitudes vigentes (TLS 1.2 o superior, AES-256, SHA-256 o superior, Argon2id o bcrypt para contraseñas). Las llaves y secretos se custodian en el gestor institucional, tienen responsable asignado y se rotan ante compromiso, vencimiento o cambio de personal.	Configuración de cifrado + registro de custodia y rotación de llaves.
C18	Respaldo y recuperación verificados	Los datos, el código y la configuración cuentan con respaldo según la criticidad del sistema. Al menos una vez al año se ejecuta una prueba de restauración documentada que verifique los tiempos objetivo de recuperación (RTO) y de pérdida de datos (RPO) acordados.	Registro de respaldos + acta de prueba de restauración.
C19	Seguridad del pipeline e infraestructura como código	El CI/CD opera con credenciales propias de mínimo privilegio, sus secretos son variables protegidas, las imágenes base provienen de repositorios confiables y se escanean imágenes de contenedor e laC antes de desplegar.	Configuración del pipeline + reporte de escaneo de imagen e laC.
C20	Uso responsable de asistentes de inteligencia artificial	No se envía código propietario, datos personales, credenciales ni información clasificada a herramientas de IA no autorizadas por la entidad. Todo código sugerido por IA se revisa, se prueba y queda bajo la responsabilidad del desarrollador que lo integra.	Declaración en el PR + revisión de código y reporte SAST/SCA.
C21	Desarrollo y componentes de terceros	Los contratos, órdenes de servicio y acuerdos de nivel de servicio incluyen obligaciones de desarrollo seguro, entrega de código y documentación, resultados de pruebas de seguridad y confidencialidad. El producto entregado por un tercero se verifica antes de aceptarlo.	Cláusulas contractuales + acta de verificación y aceptación.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

9. VERIFICACIONES OWASP SIMPLIFICADAS

Se recomienda utilizar el siguiente subconjunto como punto de inicio y ampliar el detalle cuando el riesgo lo requiera.

Tabla 5. Verificaciones OWASP

OWASP Web Top 10 2025	Verificación mínima
A01 Broken Access Control	Deny-by-default; autorización por objeto y función; roles mínimos; CORS/CSRF cuando aplique.
A02 Security Misconfiguration	TLS; headers; debug desactivado; errores no verbosos; almacenamiento no público.
A03 Software Supply Chain Failures	SCA, lockfiles, repositorios confiables, ramas protegidas, imágenes/dependencias actualizadas.
A04 Cryptographic Failures	TLS, cifrado de datos sensibles, llaves fuera del código, hash seguro de contraseñas, JWT bien validado.
A05 Injection	Consultas parametrizadas; validación allowlist; encoding de salida; XSS; carga de archivos segura.
A06 Insecure Design	Threat modeling cuando aplique; criterios de seguridad; fail-safe defaults; defensa en profundidad.
A07 Authentication Failures	MFA privilegiado; fuerza bruta; cookies/sesiones seguras; recuperación de cuenta y revocación.
A08 Software or Data Integrity Failures	Artefactos/fuentes confiables; deserialización segura; webhooks firmados; validación del lado servidor.
A09 Security Logging and Alerting Failures	Eventos críticos, alertas, correlación, retención y protección de logs; no registrar secretos.
A10 Mishandling of Exceptional Conditions	Manejo centralizado; fail closed; rollback; límites, timeouts y observabilidad de errores.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

9.1. Si el desarrollo expone o consume APIs

Tabla 6. OWASP si el desarrollo expone o consume APIs

OWASP API Top 10 2023	Aplicación sencilla
API1 / API5	Probar autorización por objeto y por función; no confiar sólo en gateway o interfaz.
API2	Validar tokens, expiración, issuer/audience y protección contra fuerza bruta.
API3	Exponer únicamente propiedades necesarias; impedir mass assignment y cambios de campos privilegiados.
API4	Aplicar rate limiting, límites de tamaño, paginación, timeouts y cuotas.
API6	Proteger flujos sensibles contra automatización, abuso, saltos de pasos y reintentos.
API7	Mitigar SSRF mediante allowlist, restricción de salidas, protocolos permitidos y timeouts.
API8	Configurar gateway, CORS, TLS, endpoints internos y runtime de forma segura.
API9	Mantener inventario de APIs, versiones, owners y retirar endpoints obsoletos.
API10	Validar respuestas de terceros; proteger webhooks; usar timeouts/circuit breakers y secretos con scopes mínimos.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

10. INTEGRACIÓN CON SCRUM

Tabla 7. Integración con scrum

Evento / artefacto	Actividad mínima de seguridad
Product Backlog	Agregar etiqueta "Security" sólo cuando la historia tenga impacto de seguridad. Incluir criterio de aceptación.
Sprint Planning	Identificar controles y pruebas de seguridad de las historias seleccionadas.
Daily	Mencionar únicamente hallazgos de seguridad que bloqueen o pongan en riesgo la entrega.
PR / Code Review	Aplicar checklist corto de código seguro y validar SAST/SCA cuando esté disponible.
Sprint Review	Mostrar resultado de pruebas y hallazgos relevantes; registrar aceptación de riesgo si existe.
Retrospectiva	Incluir acciones de mejora sólo cuando exista un incidente, vulnerabilidad repetitiva o falla del proceso.
Release	Aplicar gate de liberación y conservar evidencias.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

11. DEFINICIÓN DE TERMINADO (DoD) MÍNIMA

- PR revisada y aprobada.
- Sin secretos en código.
- Dependencias revisadas.
- Pruebas funcionales y casos negativos satisfactorios.
- SAST/SCA sin hallazgos críticos o altos pendientes, cuando existan estas herramientas.
- Checklist OWASP aplicable ejecutado.
- Errores y logs verificados.
- Evidencia enlazada al ticket o release.
- Ambientes separados y sin datos personales reales en desarrollo o pruebas.
- Cambio registrado y aprobado, versión etiquetada y plan de reversión definido.
- Configuración desplegada desde línea base endurecida y sin credenciales por defecto.
- Respaldo vigente del dato y la configuración afectados por el cambio.
- Código asistido por inteligencia artificial revisado y aprobado por una persona responsable.

12. CLASIFICACIÓN PRÁCTICA DEL CAMBIO

Tabla 8. Clasificación de práctica del cambio

Nivel	¿Cuándo aplica?	Controles	Resultado esperado
Básico	Cambio menor sin datos nuevos, permisos, integraciones ni infraestructura.	C02, C03, C04, C05, C09, C11, C15, C20 y evidencia del cambio.	Evidencias completas y hallazgos gestionados antes de liberar.
Estándar	Nueva funcionalidad, módulo o cambio con datos, roles, archivos o API interna.	Los 21 controles + checklist OWASP aplicable + separación de ambientes y datos de prueba protegidos (C13, C14).	Evidencias completas y hallazgos gestionados antes de liberar.
Reforzado	Internet, datos sensibles, autenticación, pagos/trámites críticos, privilegios, nueva infraestructura o integración externa relevante.	Los 21 controles + STRIDE + pruebas de seguridad ampliadas + revisión de Seguridad/Infraestructura + aceptación formal de riesgos residuales + prueba de restauración vigente y concepto del Área de Seguridad de la Información.	Evidencias completas y hallazgos gestionados antes de liberar.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

13. GESTIÓN DE HALLAZGOS Y CRITERIOS DE LIBERACIÓN

Los hallazgos se registran con severidad, responsable, fecha objetivo y estado. La guía adopta un criterio simple para no detener innecesariamente al equipo, pero mantener control del riesgo.

Tabla 9. Gestión de hallazgos y criterios de liberación

Severidad	Regla	Tratamiento
Crítica	Bloquea liberación. Debe corregirse antes de producción.	No se admite excepción operativa ordinaria.
Alta	Bloquea liberación salvo aceptación formal de riesgo por el dueño del sistema y concepto técnico.	Plan de remediación inmediato.
Media	Puede liberarse con plan y fecha de corrección documentados, según contexto.	Seguimiento obligatorio.
Baja	Se programa en backlog de mejora.	Seguimiento proporcional.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

14. MANTENIMIENTO Y OPERACIÓN SEGURA

Tabla 10. Mantenimiento y operación segura

Frecuencia / evento	Actividad mínima
Mensual o por release	Revisar dependencias y vulnerabilidades relevantes; aplicar parches prioritarios.
Por cambio de personal o roles	Retirar accesos innecesarios y revisar privilegios.
Semestral	Revisión de usuarios activos y roles/perfiles en producción; identificar cuentas huérfanas y privilegios no justificados.
Según criticidad	Revisar logs: semanal para sistemas críticos, mensual para criticidad media y trimestral o a demanda para criticidad baja.
Ante incidente o hallazgo	Registrar, escalar y corregir; actualizar controles o pruebas para evitar recurrencia.
Previo a cambios relevantes	Confirmar respaldo, rollback y capacidad de recuperación.
Anual	Ejecutar y documentar una prueba de restauración de respaldos, validando los tiempos objetivo de recuperación (RTO) y de pérdida de datos (RPO) definidos para el sistema.
Trimestral	Verificar vigencia de certificados TLS, dominios, llaves y tokens de integración; programar su renovación con anticipación suficiente.
Semestral	Actualizar el inventario de aplicaciones, APIs, versiones, dependencias y responsables; identificar y planear el retiro de componentes sin soporte del fabricante.
Ante retiro de personal o compromiso de credenciales	Rotar secretos, llaves, tokens y contraseñas de servicio asociados a la persona o al componente afectado.
Continuo	Monitorear avisos de seguridad y CVE de los componentes, librerías, imágenes base y servicios de nube utilizados; evaluar su aplicabilidad y priorizar la remediación.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

15. CONTRIBUCIÓN PRÁCTICA AL MSPI

La aplicación de esta guía genera evidencias de seguridad durante el ciclo de software y apoya la implementación del MSPI en aspectos relacionados con gestión de riesgos, control de acceso, protección de información, gestión de vulnerabilidades, registro y monitoreo, gestión de incidentes, continuidad y mejora. La relación que sigue es operativa y no sustituye la matriz oficial de controles del MSPI vigente en la entidad.

Tabla 11. Interrelación con el MSPI

Ámbito apoyado	Evidencia generada por la guía
Gestión de riesgos de seguridad	Clasificación del cambio, STRIDE cuando aplica, registro de hallazgos y aceptación de riesgo.
Control de acceso	Autenticación, autorización por rol/objeto, mínimo privilegio, revisión semestral de accesos.
Protección de información	TLS, cifrado en reposo según criticidad, manejo seguro de llaves y secretos, minimización de datos.
Seguridad en adquisición/desarrollo/mantenimiento	Requisitos de seguridad, DoD, revisión de código, SAST/SCA/DAST, dependencias y hardening.
Registro y monitoreo	Logs de eventos críticos, trazabilidad, alertas y protección de registros.
Gestión de vulnerabilidades	Escaneo, priorización, remediación y control de liberación.
Gestión de incidentes	Escalamiento de eventos, runbooks, evidencias y acciones correctivas.
Continuidad y recuperación	Backups, rollback, manejo de excepciones, resiliencia y fallos controlados.
Mejora continua	Retrospectiva, backlog de deuda de seguridad y actualización de prácticas/herramientas.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

16. HERRAMIENTAS SUGERIDAS (NO OBLIGATORIAS)

Tabla 12. Herramientas sugeridas

Uso	Alternativa
Editor / desarrollo	SonarLint o linter equivalente con reglas de seguridad.
SAST	SonarQube u otra herramienta institucional disponible.
SCA	OWASP Dependency-Check, Dependabot o equivalente.
DAST web	OWASP ZAP.
Pruebas API	Postman/Burp o pruebas automatizadas de contrato y autorización.
Threat modeling	OWASP Threat Dragon o plantilla simple STRIDE.
Secretos	Gestor institucional de secretos / variables protegidas del CI/CD.
Contenedores/laC	Escáner de imágenes e laC cuando el stack lo requiera.
Detección de secretos	Gitleaks, TruffleHog o el escaneo de secretos del repositorio institucional.
Contenedores e imágenes	Trivy, Gripe o el escáner del registro de contenedores.
Infraestructura como código	Checkov, tfsec o KICS.
Datos de prueba	Scripts de anonimización o generadores de datos sintéticos (Faker, Mockaroo o equivalente).
Configuración web y TLS	testssl.sh, SSL Labs o Mozilla Observatory para verificar cifrado y cabeceras.
Gestión de vulnerabilidades	Registro centralizado en la herramienta institucional de tickets, con severidad CVSS, responsable y fecha objetivo.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

17. GESTIÓN DE AMBIENTES Y DATOS DE PRUEBA

La separación de ambientes y el tratamiento de los datos de prueba son controles exigidos por el Anexo A de la norma ISO/IEC 27001:2022 (A.8.31 y A.8.33) y constituyen uno de los riesgos más frecuentes en entidades públicas, por el uso de copias de producción con datos personales reales en ambientes de menor protección. La siguiente tabla define el uso permitido de cada ambiente.

Tabla 13. Usos permitidos por ambientes

Ambiente	Uso permitido	Datos permitidos	Accesos	Evidencia
Desarrollo	Construcción, depuración y pruebas unitarias.	Datos sintéticos o ficticios exclusivamente.	Equipo de desarrollo. Sin acceso ni conexión a bases de datos de producción.	Configuración del ambiente y cadena de conexión.
Pruebas / QA	Pruebas funcionales, casos negativos y pruebas de seguridad.	Datos sintéticos o datos anonimizados/enmascarados con autorización previa.	QA y desarrollo, con credenciales propias del ambiente.	Autorización y registro del proceso de anonimización.
Preproducción	Validación final, pruebas de despliegue y de rendimiento.	Subconjunto anonimizado y mínimo necesario; nunca la base completa de producción.	Acceso restringido, nominal y temporal.	Ticket de acceso temporal con fecha de retiro.
Producción	Operación del servicio. No se desarrolla, depura ni se ejecutan ajustes manuales.	Datos reales bajo control de acceso, cifrado y retención definida.	Mínimo privilegio, autenticación multifactor para administración y acceso nominal (sin cuentas compartidas).	Matriz de accesos y revisión semestral de privilegios.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

Reglas mínimas para datos de prueba: (i) está prohibido copiar información de producción a otros ambientes sin autorización escrita del dueño de la información; (ii) los identificadores directos (documento de identidad, nombres, correo, teléfono, dirección, datos bancarios y datos sensibles) deben enmascarse, sustituirse o generarse sintéticamente conservando el formato requerido por las pruebas; (iii) el conjunto de datos debe limitarse al volumen mínimo necesario; (iv) al finalizar la

actividad los datos se eliminan de forma segura y se deja constancia; y (v) las credenciales, tokens e integraciones del ambiente de pruebas deben ser distintas de las de producción. Este control materializa el principio de privacidad desde el diseño y por defecto y reduce el riesgo de incidentes con datos personales.

18. GESTIÓN DE CAMBIOS, RESPALDO Y RECUPERACIÓN

El documento original define un gate de liberación, pero no un procedimiento de gestión de cambios ni requisitos de respaldo verificables, que son controles explícitos del Anexo A de la norma ISO/IEC 27001:2022 (A.8.32 y A.8.13) y del MSPI. La siguiente clasificación permite aplicar el control sin frenar la operación.

Tabla 14. Tipos de cambio, aprobación y reversión

Tipo de cambio	Requisitos mínimos	Aprobación	Reversión
Estándar (bajo riesgo, repetitivo y preautorizado)	Ticket, pruebas ejecutadas y versión registrada.	Líder técnico.	Retorno a la versión anterior.
Normal	Ticket con descripción de impacto, pruebas, checklist de liberación y ventana de mantenimiento definida.	Líder técnico y dueño funcional del sistema.	Plan de reversión documentado y verificado.
Emergencia	Ejecución inmediata con registro posterior dentro de los dos días hábiles siguientes y análisis de causa raíz.	Autorización del dueño del sistema, confirmada por escrito.	Rollback disponible de forma inmediata.
Cambio con impacto en datos personales, autenticación, privilegios o exposición a Internet	Evaluación de riesgo, análisis STRIDE y respaldo previo verificado.	Dueño del sistema y concepto del Área de Seguridad de la Información.	Respaldo previo verificado y punto de restauración identificado.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

Respaldo y recuperación: cada sistema debe tener definidos el tiempo objetivo de recuperación (RTO) y el punto objetivo de recuperación (RPO) acordados con el dueño funcional. Los respaldos incluyen datos, configuración, código fuente y secretos de infraestructura; se almacenan cifrados, con al menos una copia fuera del ambiente productivo, con retención definida y con acceso restringido. Una prueba de restauración anual, documentada en acta, es la única evidencia válida de que el respaldo funciona; un respaldo no probado no se considera control implementado.

19. USO DE ASISTENTES DE INTELIGENCIA ARTIFICIAL Y COMPONENTES DE TERCEROS

El uso de asistentes de inteligencia artificial para generar código y la incorporación de librerías y servicios de terceros son hoy parte habitual del desarrollo y constituyen un vector real de fuga de información y de compromiso de la cadena de suministro. Las siguientes reglas complementan los controles C04, C20 y C21.

Tabla 15. Reglas para inteligencia artificial y componentes de terceros

Situación	Regla	Evidencia
Código sugerido por herramientas de IA	Se revisa línea por línea, se ejecutan pruebas y análisis SAST/SCA. La responsabilidad sobre el código integrado es del desarrollador que lo incorpora, no de la herramienta.	PR con revisión y reporte de análisis.
Información enviada a herramientas de IA	Está prohibido enviar credenciales, llaves, datos personales, información clasificada o código con lógica sensible a herramientas no autorizadas por la entidad.	Listado institucional de herramientas autorizadas y su configuración.

Situación	Regla	Evidencia
Licenciamiento y propiedad intelectual	Se verifica la licencia del código o librería incorporada; no se integran componentes con licencias incompatibles con el uso institucional o con la contratación vigente.	Registro de licencias o inventario de componentes (SBOM).
Librerías y componentes de código abierto	Se verifica origen del paquete, mantenimiento activo, versión vigente y vulnerabilidades conocidas; se evita la instalación de paquetes con nombres similares a los oficiales (typosquatting).	Reporte SCA y archivo de bloqueo (lockfile).
Desarrollo contratado con terceros	El contrato exige la aplicación de esta guía, la entrega de código y documentación, los resultados de pruebas de seguridad y el compromiso de confidencialidad; la entidad verifica antes de aceptar.	Cláusulas contractuales y acta de verificación y aceptación.
Servicios en la nube y SaaS	Se verifica el modelo de responsabilidad compartida, la ubicación y el tratamiento de los datos, el cifrado, el respaldo, el registro de eventos y las condiciones de salida del servicio.	Ficha técnica del servicio y concepto de Seguridad de la Información.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

20. TRAZABILIDAD CON EL ANEXO A DE LA NORMA ISO/IEC 27001:2022

La siguiente tabla relaciona cada control de la guía con los controles del Anexo A de la norma ISO/IEC 27001:2022 que soporta. Su propósito es facilitar la recolección de evidencias en auditorías internas y en la autoevaluación del MSPI. La relación es orientativa y debe conciliarse con la Declaración de Aplicabilidad (SoA) y con la matriz de controles vigente en la entidad.

Tabla 16. Trazabilidad de los controles de la guía con ISO/IEC 27001:2022

Control de la guía	Controles del Anexo A ISO/IEC 27001:2022	Ámbito del MSPI
C01 Criterios de seguridad en el backlog	A.5.8 Seguridad de la información en la gestión de proyectos; A.8.26 Requisitos de seguridad de las aplicaciones	Planificación y gestión de riesgos
C02 Revisión de código y rama protegida	A.8.4 Acceso al código fuente; A.8.25 Ciclo de vida de desarrollo seguro; A.8.28 Codificación segura	Desarrollo seguro
C03 Secretos fuera del código	A.5.17 Información de autenticación; A.8.4 Acceso al código fuente; A.8.24 Uso de criptografía	Control de acceso y criptografía
C04 Dependencias controladas	A.5.21 Gestión de la seguridad en la cadena de suministro TIC; A.8.8 Gestión de vulnerabilidades técnicas	Gestión de vulnerabilidades
C05 Validación de entradas	A.8.26 Requisitos de seguridad de las aplicaciones; A.8.28 Codificación segura	Desarrollo seguro
C06 Autenticación y sesiones	A.5.16 Gestión de identidades; A.5.17 Información de autenticación; A.8.5 Autenticación segura	Control de acceso
C07 Autorización y mínimo privilegio	A.5.15 Control de acceso; A.5.18 Derechos de acceso; A.8.2 Derechos de acceso privilegiado; A.8.3 Restricción del acceso a la información	Control de acceso
C08 Configuración y cifrado	A.8.9 Gestión de la configuración; A.8.24 Uso de criptografía	Protección de la información
C09 Errores y excepciones seguras	A.8.26 Requisitos de seguridad de las aplicaciones; A.8.28 Codificación segura	Desarrollo seguro
C10 Logs y trazabilidad	A.8.15 Registro de eventos; A.8.16 Actividades de monitoreo; A.8.11 Enmascaramiento de datos	Registro y monitoreo
C11 Pruebas de seguridad	A.8.29 Pruebas de seguridad en desarrollo y aceptación; A.8.8 Gestión de vulnerabilidades técnicas	Gestión de vulnerabilidades

Control de la guía	Controles del Anexo A ISO/IEC 27001:2022	Ámbito del MSPI
C12 Gate de liberación y recuperación	A.8.19 Instalación de software en sistemas operativos; A.8.29 Pruebas de seguridad; A.8.32 Gestión de cambios	Gestión de cambios
C13 Separación de ambientes	A.8.31 Separación de los ambientes de desarrollo, prueba y producción	Desarrollo seguro
C14 Datos de prueba protegidos	A.8.33 Información de prueba; A.8.11 Enmascaramiento de datos; A.8.10 Eliminación de información	Protección de datos personales
C15 Gestión de cambios y versionamiento	A.8.32 Gestión de cambios	Gestión de cambios
C16 Línea base de configuración y hardening	A.8.9 Gestión de la configuración; A.8.19 Instalación de software en sistemas operativos	Protección de la información
C17 Criptografía y gestión de llaves	A.8.24 Uso de criptografía; A.5.17 Información de autenticación	Criptografía
C18 Respaldo y recuperación verificados	A.8.13 Copias de respaldo de la información; A.5.29 Seguridad durante la disrupción; A.5.30 Preparación de las TIC para la continuidad del negocio	Continuidad y recuperación
C19 Seguridad del pipeline e infraestructura como código	A.8.9 Gestión de la configuración; A.8.25 Ciclo de vida de desarrollo seguro; A.8.31 Separación de ambientes	Desarrollo seguro
C20 Uso responsable de asistentes de IA	A.5.10 Uso aceptable de la información y de los activos; A.5.32 Derechos de propiedad intelectual; A.8.28 Codificación segura	Uso aceptable y desarrollo seguro
C21 Desarrollo y componentes de terceros	A.8.30 Desarrollo contratado externamente; A.5.19 Seguridad en las relaciones con proveedores; A.5.20 Acuerdos con proveedores; A.5.21 Cadena de suministro TIC	Relaciones con proveedores

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

21. CRIPTOGRAFÍA MÍNIMA ACEPTADA

Los siguientes valores constituyen el mínimo aceptable para los desarrollos de la entidad. Cualquier excepción debe contar con el concepto técnico del profesional de seguridad de la información y la aceptación formal del riesgo, por parte del dueño del sistema de información y/ aplicativo.

Tabla 17. Criptografía mínima

Uso	Aceptado	No se debe utilizar
Transporte	TLS 1.2 o TLS 1.3 con suites de cifrado vigentes.	SSL 2.0, SSL 3.0, TLS 1.0 y TLS 1.1.
Cifrado simétrico	AES de 128 o 256 bits en modo GCM, o CBC acompañado de HMAC.	DES, 3DES, RC4 y el modo ECB.
Funciones hash	SHA-256, SHA-384 o SHA-512.	MD5 y SHA-1.
Almacenamiento de contraseñas	Argon2id, scrypt o bcrypt, con sal única por usuario.	MD5 o SHA sin sal, y cualquier cifrado reversible.
Llave pública y firma	RSA de 2048 bits o más; ECDSA o EdDSA con curvas estándar.	RSA menor a 2048 bits y llaves reutilizadas entre ambientes.
Generación de valores aleatorios	Generadores criptográficamente seguros (CSPRNG) del lenguaje o del sistema operativo.	Funciones de aleatoriedad no criptográfica.
Custodia de llaves y secretos	Gestor de secretos institucional o bóveda del proveedor de nube, con responsable asignado, control de acceso y rotación.	Llaves en código fuente, repositorios, archivos de configuración, hojas de cálculo o correo electrónico.

Fuente. Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, Idartes.

Anexo A. Checklist corto por historia o release

#	Verificación	Cumple	No cumple	No aplica	Evidencia / enlace
1	¿La historia identifica si maneja datos sensibles, roles, archivos, API o integraciones?	☐	☐	☐	
2	¿Los criterios de aceptación incluyen seguridad cuando aplica?	☐	☐	☐	
3	¿El cambio fue revisado por otra persona antes del merge?	☐	☐	☐	
4	¿Se confirmó que no existen secretos en código o repositorio?	☐	☐	☐	
5	¿Las dependencias fueron revisadas y no hay vulnerabilidades críticas/altas sin tratamiento?	☐	☐	☐	
6	¿Las entradas se validan en servidor y las consultas son parametrizadas/seguras?	☐	☐	☐	
7	¿Autenticación, sesiones y autorización funcionan con mínimo privilegio?	☐	☐	☐	
8	¿Producción está sin debug y con configuración/TLS seguros?	☐	☐	☐	
9	¿Los errores son genéricos para el usuario y no exponen información interna?	☐	☐	☐	
10	¿Los logs registran eventos críticos sin secretos ni datos sensibles innecesarios?	☐	☐	☐	
11	¿Se ejecutaron pruebas negativas y verificaciones OWASP web/API aplicables?	☐	☐	☐	
12	¿Existe rollback y no quedan hallazgos críticos/altos pendientes sin aprobación?	☐	☐	☐	
13	¿El cambio se probó en un ambiente distinto de producción y sin datos personales reales?	☐	☐	☐	
14	¿El cambio cuenta con solicitud aprobada, versión etiquetada y plan de reversión?	☐	☐	☐	
15	¿La configuración desplegada parte de una línea base endurecida y versionada, sin credenciales por	☐	☐	☐	

#	Verificación	Cumple	No cumple	No aplica	Evidencia / enlace
	defecto?				
16	¿Se usan algoritmos criptográficos vigentes y las llaves están custodiadas en el gestor institucional?	☐	☐	☐	
17	¿Existe respaldo vigente del dato y la configuración afectados, con restauración probada?	☐	☐	☐	
18	¿Se escanearon las imágenes de contenedor y la infraestructura como código, cuando aplique?	☐	☐	☐	
19	¿El código asistido por IA fue revisado y no se expuso información institucional a herramientas no autorizadas?	☐	☐	☐	
20	¿El componente o desarrollo entregado por un tercero fue verificado y aceptado formalmente?	☐	☐	☐	

Anexo B. Plantilla STRIDE simplificada

Usar sólo para cambios estándar o reforzados cuando la funcionalidad lo amerite. Registrar máximo las amenazas relevantes; no es necesario llenar categorías sin aplicación.

Componente/flujo	STRIDE	Amenaza	Mitigación	Responsable/estado

Referencia rápida STRIDE: S = suplantación; T = alteración; R = repudio; I = divulgación de información; D = denegación de servicio; E = elevación de privilegios.

Anexo C. Registro simple de hallazgos y excepciones

#	Hallazgo	Severidad	Acción	Responsable	Fecha	Estado / aprobación

Anexo D. Checklist de configuración segura (hardening) y criptografía mínima

Se aplica antes de cada liberación a producción y en la revisión periódica de los sistemas en operación. Cuando una verificación no aplique al tipo de solución, se marca “No aplica” y se justifica brevemente.

Ámbito	Configuración esperada	Cumple	No cumple	No aplica
Transporte	TLS 1.2 o superior, redirección de HTTP a HTTPS, HSTS habilitado y certificado vigente con alerta de vencimiento.	☐	☐	☐
Cabeceras de seguridad	Content-Security-Policy, X-Content-Type-Options: nosniff, Referrer-Policy, X-Frame-Options o frame-ancestors y Permissions-Policy.	☐	☐	☐
Cookies	Atributos Secure, HttpOnly y SameSite; expiración definida y renovación del identificador de sesión después de iniciar sesión.	☐	☐	☐
Sesiones y tokens	Expiración e inactividad definidas, revocación al cerrar sesión y validación de firma, emisor y audiencia en tokens JWT.	☐	☐	☐
Contraseñas	Almacenamiento con Argon2id, scrypt o bcrypt con sal; longitud mínima; bloqueo o retardo progresivo tras intentos fallidos; sin envío de contraseñas por correo.	☐	☐	☐
Errores	Página de error genérica, sin trazas de pila, rutas, versiones de componentes ni consultas SQL.	☐	☐	☐
Exposición de la aplicación	Modo de depuración desactivado; consolas de administración, documentación de API y endpoints internos restringidos; listado de directorios deshabilitado.	☐	☐	☐
Carga de archivos	Tipo, extensión y tamaño validados en servidor; almacenamiento fuera de la raíz web; nombre saneado; análisis antimalware cuando aplique.	☐	☐	☐
CORS	Orígenes declarados explícitamente (sin comodín cuando se envían credenciales); métodos y cabeceras mínimos necesarios.	☐	☐	☐
Límites y disponibilidad	Rate limiting, tiempos de espera, tamaño máximo de petición y paginación en servicios expuestos.	☐	☐	☐
Base de datos	Usuario de aplicación sin privilegios administrativos; puerto no expuesto a Internet; cifrado en reposo según criticidad; credenciales en el gestor de secretos.	☐	☐	☐
Registro de eventos	Autenticaciones, fallos de autorización y cambios de permisos registrados; hora sincronizada (NTP); retención definida; sin contraseñas, tokens ni datos personales innecesarios.	☐	☐	☐
Respaldo	Respaldo vigente y cifrado del dato y la configuración, con prueba de restauración registrada.	☐	☐	☐
Ambientes	Ambiente productivo separado, sin datos de prueba y sin cuentas o accesos temporales vigentes.	☐	☐	☐



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA RECREACIÓN Y DEPORTE
Instituto Distrital de las Artes

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS
1	2026-10-02	Emisión inicial

CONTROL DE APROBACIÓN

ESTADO	FECHA	NOMBRE	CARGO
ELABORÓ	2026-09-23	MARYURY FORERO BOHORQUEZ	ENLACE MIPG
REVISÓ	2026-09-23	MARYURY FORERO BOHORQUEZ	REFERENTE MIPG
APROBÓ	2026-10-02	DANIEL SANCHEZ ROJAS	LIDER DE PROCESO
AVALÓ	2026-10-02	DANIEL SANCHEZ ROJAS	JEFE DE LA OFICINA ASESORA DE PLANEACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN

COLABORADORES

NOMBRE
JONATHAN GONZALEZ BOLANOS
MARIA CRISTINA HERRERA CALDERON