Manual para la Evaluación y Puesta en Producción del Desarrollo de Software Seguro en la Universidad Nacional Abierta y a Distancia

Manual para la Evaluación y Puesta en Producción del Desarrollo de Software Seguro en la UNAD

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
Maestría en Ciberseguridad
Especialización en Seguridad Informática
CSIRT Académico UNAD

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Vicerrectoría de Innovación y Emprendimiento – VIEM

Gerencia de Plataformas e Infraestructura Tecnológica

Centro de Desarrollo Tecnológico
CSIRT Académico UNAD

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas
Vicerrector

Ing. Andrés Ernesto Salinas Duarte
Vicerrector de Innovación y Emprendimiento

Ing. Luis Fernando Zambrano Hernández
Líder CSIRT Académico UNAD

Adm. Libardo Cárdenas Corral
Analista 1 CSIRT Académico UNAD

Ing. Hernando José Peña Hidalgo
Analista 2 CISRT Académico UNAD

Ing. Néstor Raúl Cárdenas Corral
Analista 3 CSIRT Académico UNAD

Contenido

1. Introducción

La transformación digital y la creciente dependencia de soluciones informáticas en los procesos académicos, administrativos, investigativos y misionales de la Universidad Nacional Abierta y a Distancia UNAD, hacen imprescindible fortalecer las capacidades institucionales en materia de seguridad digital. En este contexto, el desarrollo de software propio o contratado se convierte en un componente crítico que debe cumplir estándares técnicos, normativos y de protección de activos de información.

Este documento tiene como propósito establecer lineamientos claros y obligatorios para la evaluación, validación, aprobación y seguimiento de los desarrollos de software que hacen parte del ecosistema tecnológico de la UNAD, en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) y conforme a las responsabilidades asignadas al Centro de Respuesta a Incidentes Informáticos – CSIRT Académico UNAD, como ente asesor y técnico en materia de ciberseguridad.

El documento define criterios de obligatoriedad, requisitos de seguridad bajo el modelo DevSecOps[1], pasos para la notificación y validación técnica, lineamientos para la aprobación en ambientes productivos y mecanismos de registro y monitoreo.

La implementación de estos lineamientos fortalece la cultura de seguridad digital de la comunidad universitaria y contribuye en la protección de la triada de la seguridad de la información: [I] Integridad, [C] Confidencialidad y [D] Disponibilidad de los activos digitales de la UNAD.

2. Recomendaciones previas

2.1. Uso de Manual de estilo para el desarrollo de software UNDISTA

Con el objetivo de informar a toda la comunidad universitaria, especialmente a las áreas responsables del desarrollo, adquisición y operación de soluciones tecnológicas, sobre la necesidad de validar y revisar todo desarrollo de software que implique el tratamiento de información sensible de la Universidad, se hace un llamado a la adopción del Manual de Estilo de Desarrollo de Software de la UNAD.

Dicho manual constituye el modelo oficial de referencia institucional. Su adopción busca garantizar la seguridad, calidad, interoperabilidad, trazabilidad y sostenibilidad de las soluciones tecnológicas, y asegurar que se respeten los estándares técnicos y normativos vigentes en materia de protección de la información y seguridad de los datos.

[1] https://www.redhat.com/en/topics/devops/what-is-devsecops

La observancia de estas disposiciones contribuye a minimizar riesgos asociados al manejo de datos personales, institucionales y estratégicos, y fortalece la capacidad de respuesta de la Universidad frente a incidentes de seguridad, vulnerabilidades y amenazas digitales.

En conjunto con la unidad responsable del desarrollo de software o de su contratación para la construcción de este, se solicita conocer, aplicar y garantizar el cumplimiento de los **manuales de estilo de desarrollo de software** y **para la Evaluación y Puesta en Producción del Desarrollo de Software Seguro en la UNAD,** como parte del compromiso institucional con la transformación digital, la mejora continua y la protección de la información.

3. Marco normativo y procedimental

El presente lineamiento se fundamenta en el marco jurídico y procedimental que rige la gestión de la seguridad de la información y el desarrollo de software en la Universidad Nacional Abierta y a Distancia – UNAD. Las siguientes disposiciones, resoluciones y documentos institucionales establecen los criterios que hacen obligatoria la validación técnica de todo desarrollo de software institucional por parte del CSIRT Académico UNAD:

3.1. Resolución Rectoral No. 007298 de 2023: Por medio de la cual se establece el Sistema de Gestión de Seguridad de la Información (SGSI) en la UNAD, adoptando como marco de referencia la norma ISO/IEC 27001:2022. Esta resolución define los principios, políticas, controles y procedimientos necesarios para proteger los activos de información de la Universidad, incluyendo los sistemas desarrollados internamente o contratados con terceros.

3.2. Resolución Rectoral No. 07132 de 2021: Por la cual se crea el Centro de Respuesta a Incidentes Informáticos – CSIRT Académico UNAD, como un Centro de Desarrollo Tecnológico, adscrito a la Vicerrectoría de Innovación y Emprendimiento, para potenciar la productividad, competitividad y el crecimiento de las regiones y su transformación digital, a partir del desarrollo y fortalecimiento de capacidades en ciberseguridad y realizar procesos de detección, identificación, protección, respuesta o recuperación ante un incidente informático los cuales permitan realizar procesos de I+D+i que contribuyan en el robustecimiento de la ciberseguridad del entorno digital UNADISTA.

3.3. Resolución MinTIC 1519 de 2020 Anexo 3: Establece Condiciones mínimas técnicas y de seguridad digital.

3.4. Procedimiento P-18-2 del SGSI UNAD: Documento procedimental del Sistema de Gestión de Calidad y del SGSI que regula la evaluación, aprobación y puesta en producción de desarrollos de software en entornos institucionales.

3.5. Documento fundante de la REDSIIUNAD: La Red de Sistemas Integrados de Información – REDSIIUNAD que se presenta como una estrategia institucional orientada a robustecer la gestión integral, segura y eficiente de los sistemas de información críticos de la Universidad Nacional Abierta y a Distancia – UNAD. Esta red, incorporada al CSIRT Académico UNAD y articulada con la Vicerrectoría de Innovación y Emprendimiento – VIEM, tiene como propósito principal garantizar la ciberseguridad, la interoperabilidad funcional y la adecuada toma de decisiones sobre los activos de información institucional. Su operatividad se fundamenta en el trabajo colaborativo y coordinado con las unidades estructurales del metasistema UNAD, en pro del cumplimiento del objeto misional de la universidad y del fortalecimiento de la cultura de la innovación, la transparencia y la transformación digital.

3.6. Política de Tratamiento de Datos Personales: establece el marco institucional para el manejo adecuado de datos personales, en cumplimiento con la Constitución Política, la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas conexas.

4. Objetivo

Establecer los lineamientos que deben seguir todas las unidades académicas, administrativas y de apoyo de la UNAD, así como los equipos de desarrollo internos o externos, para la validación y evaluación de seguridad de las soluciones de software, como requisito previo a su puesta en producción dentro del ecosistema digital institucional, recomendando además la aplicación del Manual de Estilos de Desarrollo de Software de la UNAD como guía para garantizar buenas prácticas de codificación, mantenibilidad y alineación con los estándares institucionales.

5. Alcance y obligatoriedad del reporte de desarrollos de software

Este lineamiento aplica a todo desarrollo de software que se diseñe, construya, implemente o mantenga en el marco de actividades académicas, administrativas, investigativas o contractuales de la Universidad Nacional Abierta y a Distancia UNAD, sin importar si es desarrollado directamente por personal de planta, contratistas, aliados externos o equipos de investigación.

Se considerará de obligatoria validación por parte del CSIRT Académico UNAD cualquier desarrollo de software que cumpla al menos una de las siguientes condiciones, teniendo además presente los lineamientos emanados por la Gerencia de Plataformas e Infraestructura Tecnológica para el despliegue seguro de aplicaciones dentro del ecosistema institucional:

5.1. Sea ejecutado en el marco de proyectos de investigación, convenios interinstitucionales, alianzas estratégicas, prácticas académicas, misiones de innovación, u órdenes contractuales con terceros.

5.2. Corresponda a desarrollos propios (in-house) impulsados por áreas misionales o de apoyo institucional, sin importar su alcance o escalabilidad inicial.

5.3. Genere, procese, almacene o transmita información institucional, confidencial, personal, académica, administrativa o sensible, en cualquier etapa del ciclo de vida del dato.

5.4. Esté destinado a brindar soluciones o mejoras a procesos relacionados con el core misional, académico, tecnológico o administrativo de la universidad.

5.5. Se proyecte para ser alojado en infraestructura tecnológica institucional, como servidores, nubes privadas, aulas virtuales, portales web o sistemas corporativos**.**

6. Requisitos técnicos y de validación de seguridad

Con el fin de garantizar que todo desarrollo de software institucional cumpla con las condiciones mínimas de seguridad antes de su puesta en producción, se establece la obligatoriedad de realizar procesos formales de validación y evaluación de seguridad, bajo lineamientos y conforme a las directrices emitidas por el CSIRT Académico UNAD y la Gerencia de Plataformas e Infraestructura Tecnológica. Estas validaciones buscan asegurar que las aplicaciones cumplan con los controles técnicos y operativos que mitiguen riesgos de vulnerabilidad y exposición de datos en los entornos institucionales.

Los requisitos mínimos para la evaluación de seguridad previa a la producción son:

6.1. **Evaluación de código fuente y librerías externas**

- Revisión automatizada del código mediante herramientas de análisis estático (SAST) para identificar vulnerabilidades comunes (inyección, XSS, CSRF, entre otras).
- Validación del uso de librerías y dependencias externas, verificando que no contengan vulnerabilidades conocidas (CVE) ni estén desactualizadas.

6.2. Pruebas de seguridad previas al despliegue

- Ejecución de pruebas dinámicas de seguridad (DAST) y pruebas de penetración controladas en ambientes de preproducción.
- Validación de integridad funcional y ausencia de vulnerabilidades críticas o altas antes del paso a producción.
- Registro, documentación y cierre de hallazgos como prerrequisito para la autorización de despliegue.

6.3. Revisión de configuración y controles de acceso

- Verificación de configuraciones de seguridad en el entorno de despliegue (servidores, contenedores, servicios, entro otros).
- Validación de controles de autenticación, autorización y gestión de sesiones, bajo el principio de mínimo privilegio y validación de matrices de usuario.

6.4. Protección de datos y comunicaciones

- Revisión de mecanismos de cifrado en tránsito actualizados y en reposo aplicados a datos sensibles.
- Confirmación del uso de cabeceras de seguridad HTTP y prevención de exposición no autorizada de datos.

6.5. Integración con sistemas de monitoreo y trazabilidad

- Validación de la integración del software con los mecanismos de logs, trazabilidad y monitoreo establecidos por el CSIRT Académico UNAD.

6.6. Revisión de respaldo y planes de recuperación por parte de la GPIT previa validación de criticidad de los activos de información

- Evaluación de la existencia y funcionalidad de políticas de respaldo y recuperación aplicables al sistema en producción.
- Validación de la restauración efectiva ante fallos o incidentes adversos.

Todo desarrollo de software que se someta a validación para su puesta en producción deberá cumplir, como mínimo, con los siguientes requisitos técnicos esenciales:

- **Documentación técnica del código fuente:** deberá incluir una descripción clara de la arquitectura del sistema, la funcionalidad de los módulos, las dependencias externas utilizadas, las rutas de ejecución principales y los puntos críticos de seguridad. Esta documentación debe ser suficiente para permitir el análisis y auditoría del software por parte del CSIRT Académico UNAD.
- **Estandarización del código fuente:** el código debe estar escrito en un solo idioma íntegramente teniendo claro los lenguajes de programación definidos para el proyecto. Además, deberá utilizar nombres claros, descriptivos y consistentes para variables, funciones, clases y otros elementos, así como seguir convenciones uniformes de estilo, indentación, espaciado y estructura lógica. Todo ello conforme a las buenas prácticas del lenguaje utilizado y, preferiblemente, alineado con guías oficiales (Convención de nomenclatura[2]).
- **Aplicación de buenas prácticas de desarrollo seguro:** se deberán seguir lineamientos técnicos que fortalezcan la calidad y seguridad del código, incluyendo:
    - Control de versiones en repositorio establecido por el CSIRT.
    - Modularización y reutilización del código.
    - Gestión de errores y excepciones adecuada.
    - Evitar código duplicado o inseguro.
    - Implementación de pruebas unitarias y de integración.
    - Uso responsable de librerías externas, verificando licencias y vulnerabilidades.
    - Uso de versionamiento semántico (Semantic Versioning[3])
    - Bitácora de registro de cambios (changelog)

Estos requisitos deben ser considerados como parte integral de cualquier proceso de desarrollo institucional, y su cumplimiento será objeto de verificación por parte del CSIRT Académico UNAD en las fases de validación técnica. La incorporación

[2] https://builtin.com/articles/pascal-case-vs-camel-case
[3] https://semver.org/lang/es/

oportuna de estas medidas no solo reduce la superficie de ataque, sino que fortalece la capacidad de resiliencia tecnológica de la Universidad.

7. Proceso de validación y aprobación técnica

La validación de desarrollos de software institucional es una etapa obligatoria dentro del ciclo de vida seguro del software. Tiene como propósito asegurar que los sistemas desarrollados cumplan con los requisitos técnicos, normativos y de seguridad definidos por la UNAD.

El proceso comprende las siguientes fases:

7.1. Identificación del desarrollo

En la fase de estructuración de proyectos, convenios, contratos o desarrollos internos, las dependencias responsables deberán identificar si el sistema a desarrollar:

- Accede o gestiona activos de información institucional.
- Impacta procesos críticos del quehacer universitario.
- Requiere alojamiento en la infraestructura tecnológica de la UNAD.

Esta identificación temprana permite anticipar los requerimientos de validación técnica y evitar reprocesos.

7.2. Notificación temprana al CSIRT Académico UNAD

Una vez se determine que el proyecto de desarrollo de software puede pasar a evaluación, la unidad responsable deberá notificar formalmente al CSIRT Académico UNAD mediante el correo electrónico csirt@unad.edu.co, remitiendo el formato establecido por el CSIRT.

7.3. Documentación y diligenciamiento de formatos

El CSIRT Académico proporcionará los formatos y/o requerimientos necesarios para dar inicio al proceso de validación.

7.4. Evaluación técnica de seguridad

El CSIRT realizará una evaluación exhaustiva que podrá incluir:

- Análisis estático del código fuente (SAST) y revisión de repositorios.
- Escaneos dinámicos (DAST) en entornos de prueba.
- Validación de cumplimiento con controles SGSI y principios de DevSecOps.

- Verificación de la implementación de medidas de protección de datos, autenticación, cifrado, gestión de sesiones, logs y respaldo.

Se podrán solicitar correcciones, parches o ajustes antes de emitir una recomendación final. El objetivo es reducir riesgos y aumentar la resiliencia digital del desarrollo.

7.5. **Acompañamiento y retroalimentación**

El proceso de validación del CSIRT se realiza bajo un enfoque técnico, colaborativo y formativo, por lo que:

- Se brindará asesoría y retroalimentación técnica a las unidades responsables respecto a hallazgos que comprometan la seguridad del proyecto.
- Se promoverá la incorporación de buenas prácticas de desarrollo seguro.
- Se mantendrá comunicación constante con los equipos responsables del desarrollo.

7.6. **Plazos y planificación**

Dado que el proceso de validación técnica exige un análisis detallado, se deberá realizar la notificación al CSIRT con al menos **15 días hábiles de anticipación** o más teniendo presente la complejidad o magnitud del proyecto y respecto al cronograma previsto para pruebas finales o puesta en producción, de modo que se puedan garantizar los tiempos necesarios de revisión y subsanación.

8. Aprobación formal para ambientes productivos

Una vez concluido el proceso de evaluación, y siempre que se verifique el cumplimiento integral de los criterios técnicos de seguridad, el CSIRT Académico UNAD emitirá un concepto técnico de aprobación, el cual se constituye en un requisito habilitante para el despliegue o puesta en funcionamiento del desarrollo en ambientes productivos.

8.1. **Emisión del concepto técnico de aprobación**

Este concepto incluirá:

- Resultado del análisis de seguridad (valoración de riesgos, cumplimiento técnico).
- Recomendaciones adicionales para el mantenimiento seguro del desarrollo.
- Condiciones específicas, en caso de que existan riesgos residuales controlados bajo monitoreo.
- Fecha de aprobación y responsables del seguimiento.

Importante: La aprobación técnica emitida por el CSIRT es vinculante dentro del marco del SGSI. Ningún desarrollo que no haya sido aprobado formalmente podrá ser publicado, alojado o referenciado en ambientes de producción de la UNAD (por ejemplo; portales institucionales, aulas virtuales, servidores corporativos o sistemas de gestión administrativa).

En caso de que se detecte un despliegue no autorizado, el CSIRT podrá solicitar su retiro inmediato del entorno productivo, además de informar a las instancias correspondientes para las acciones correctivas pertinentes.

9. Registro institucional y monitoreo posterior

Conforme a las políticas del Sistema de Gestión de Seguridad de la Información - SGSI, todo desarrollo de software que haya superado el proceso de validación y haya sido aprobado formalmente por el CSIRT Académico deberá cumplir con los siguientes lineamientos para su registro y seguimiento continuo:

9.1. Registro en el inventario de activos de información

Cada desarrollo aprobado será documentado y registrado como activo de información en el inventario institucional administrado por la REDSIIUNAD, conforme a la clasificación establecida en la política de gestión de activos.

El registro incluirá:

- Nombre del desarrollo, versión y fecha de puesta en producción.
- Responsable funcional y técnico.
- Descripción de funcionalidades y procesos del SIG que soporta.
- Infraestructura tecnológica utilizada (servidores, bases de datos, servicios asociados).
- Clasificación de la información tratada (pública, confidencial, sensible, reservada).
- Plan de continuidad y respaldo.

9.2. **Repositorios institucionales de código**

Todo desarrollo de software que sea propiedad de la UNAD ya sea realizado internamente o contratado mediante terceros, deberá estar alojado y mantenerse actualizado en el repositorio de código oficial designado por el CSIRT Académico UNAD.

Este repositorio institucional tiene como propósito asegurar la disponibilidad del código fuente, facilitar la revisión por parte del CSIRT y los procesos de auditoría técnica y centralizar la documentación técnica y de versiones.

El equipo desarrollador deberá coordinar con el CSIRT la integración del proyecto al repositorio y cumplir con las directrices de estructuración, control de versiones, documentación, licenciamiento y seguridad de código.

9.3. **Monitoreo de seguridad posterior a la implementación**

Una vez en producción, el desarrollo será objeto de monitoreo técnico continuo por parte del CSIRT Académico UNAD a través de sus sistemas de monitoreo, incluyendo:

- Inspección de logs, eventos de seguridad y comportamiento anómalo.
- Evaluaciones periódicas de vulnerabilidades.
- Integración con sistemas de alerta temprana y respuesta a incidentes.

9.4. **Gestión de cambios y versiones posteriores**

Todo cambio significativo en el código, funcionalidades, arquitectura o configuración de un desarrollo que ya se encuentre en producción, deberá ser notificado al CSIRT Académico para una nueva evaluación técnica. Esto incluye:

- Actualizaciones de versión.
- Cambios en componentes críticos o librerías.
- Migración de infraestructura.
- Integración con nuevas bases de datos o servicio

9.5. **Incumplimiento y medidas preventivas**

La implementación o exposición pública de desarrollos no validados por el CSIRT podrá representar una vulneración al SGSI, y podrá dar lugar a:

- Solicitud de suspensión del proyecto o retiro inmediato del entorno productivo.
- Revisión por parte de autoridades institucionales competentes.
- Emisión de alertas internas por riesgo de seguridad digital.

10. Consideraciones para Cambios en el Código después de la Puesta en Producción

Con el propósito de preservar la estabilidad, seguridad y trazabilidad de las aplicaciones institucionales, todo cambio que se realice sobre el código fuente de soluciones ya puestas en producción deberá cumplir con los siguientes lineamientos:

10.1. Control formal de cambios

Cualquier modificación posterior a la puesta en producción deberá estar documentada mediante una solicitud formal de cambio (RFC, por sus siglas en inglés), a través de los canales establecidos por el CSIRT Académico UNAD. Esta solicitud debe incluir:

- Listar módulos o archivos afectados por el cambio
- Descripción detallada del cambio realizado.
- Justificación técnica, operativa o normativa.
- Impacto potencial en la seguridad, disponibilidad o integridad del sistema.
- Evidencia de pruebas previas en ambiente de desarrollo y preproducción.

10.2. Evaluación de impacto y aprobación

Previo a la implementación, toda modificación deberá ser evaluada por el CSIRT Académico UNAD en conjunto con la Gerencia de Plataformas e Infraestructura Tecnológica, quienes determinarán:

- El nivel de riesgo asociado al cambio.
- Los controles compensatorios necesarios.
- La autorización o rechazo de su aplicación en el entorno productivo.
- La necesidad de ventanas de mantenimiento, monitoreo especial o planes de contingencia.

10.3. Buenas prácticas en la gestión del cambio

Todo cambio aprobado deberá seguir estas prácticas mínimas:

- Estar versionado correctamente, utilizando versionamiento semántico.

- Actualizar la bitácora de cambios correspondiente.
- Mantener documentación técnica sincronizada con los nuevos ajustes.
- Garantizar que se hayan aplicado pruebas unitarias, de regresión y seguridad antes de su despliegue.
- Notificar a los actores clave y usuarios impactados cuando se trate de funcionalidades críticas.

10.4. **Registro y auditoría**

Los cambios aplicados deberán quedar registrados en los sistemas institucionales de trazabilidad, y estarán sujetos a revisión periódica por parte de los órganos de control tecnológico. Se podrán realizar auditorías técnicas o forenses en caso de incidentes relacionados con modificaciones no autorizadas o mal implementadas.

10.5. **Incumplimientos**

Cualquier alteración al código en ambiente productivo sin la debida autorización, documentación o validación de seguridad será considerada una falta grave, sujeta a las medidas disciplinarias y contractuales correspondientes, además de activar protocolos de contingencia ante riesgos operativos o de ciberseguridad.

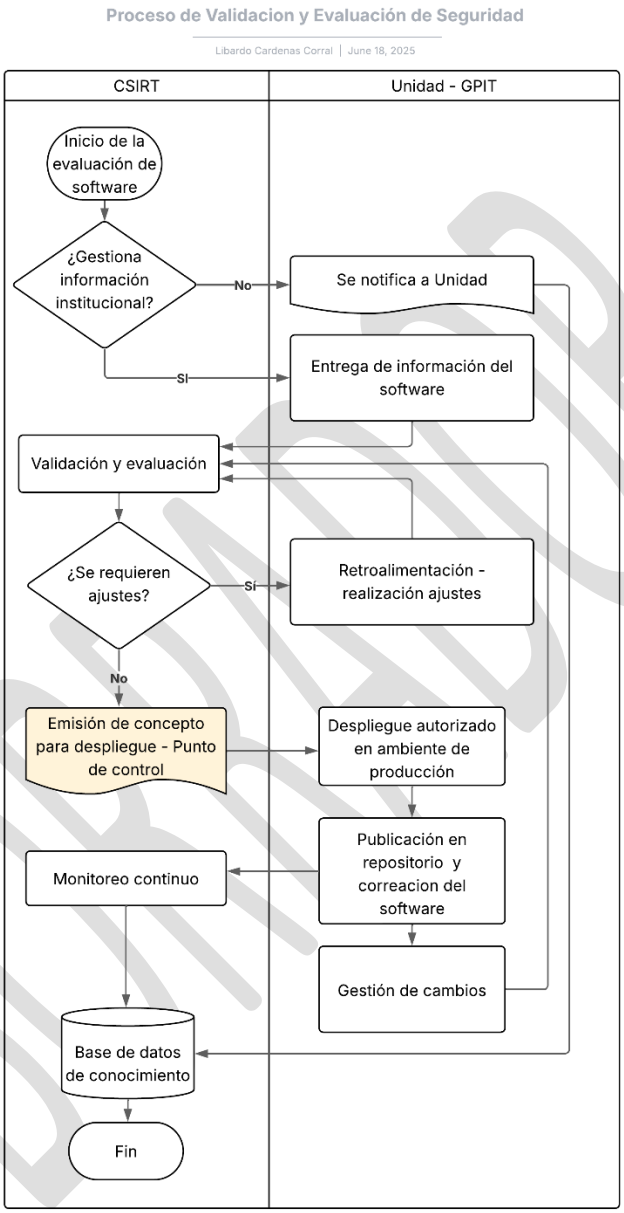
10.6. **Validación Técnica**

Se entiende por validación técnica el proceso estructurado de revisión, verificación y aceptación de un desarrollo de software institucional conforme a criterios de seguridad, funcionalidad y cumplimiento normativo establecidos por el SGSI y liderado por el CSIRT Académico UNAD.

10.7. **Proceso de Validación**

Ilustración 1.

Representación gráfica del proceso de validación y evaluación del SW



El diagrama de flujo establece el paso a paso que debe seguirse para validar y evaluar el software institucional antes de su despliegue en ambientes de producción. Está orientado a garantizar que todo desarrollo que gestione información institucional cumpla con los requisitos mínimos de seguridad definidos por el SGSI y el CSIRT Académico.

11. Compromiso institucional

La Universidad Nacional Abierta y a Distancia – UNAD reafirma su compromiso con la ciberseguridad, la protección de los activos de información y la adopción de buenas prácticas en el desarrollo y operación de sistemas informáticos. Invitamos a todas las unidades, equipos de desarrollo y actores contratistas a integrarse activamente a esta política preventiva y colaborativa, que busca salvaguardar la integridad, disponibilidad y confidencialidad de la información institucional.