intiza

Norma de Desarrollo Seguro

Versión: 3.0

Confeccionó	Revisó	Aprobó
BDO **Consultoría Externa**	 **Carla Leiva - CISO**	 **Francisco Canale - Director**

NORMA DE DESARROLLO SEGURO	intiza Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 10/07/2024
Código: NO-SI-21- Desarrollo Seguro	Versión: 3.0

Contenido

1. Objetivo

Definir lineamientos, directrices y responsabilidades para garantizar la seguridad de la información en todas las etapas del desarrollo de software.

2. Alcance

Esta norma es aplicable a todos los desarrollos que se realizan en INTIZA, tanto de forma interna como por proveedores externos.

3. Responsabilidades

Equipo de Desarrollo es responsable de la construcción de software robusto, considerando los aspectos y buenas prácticas de software seguro.

Gerente de Desarrollo valida que el software desarrollado cuente con la calidad y seguridad requerida.

QA es responsable de realizar las pruebas funcionales y de seguridad de cada desarrollo.

El **Project Manager** gestiona los proyectos de desarrollo.

Seguridad de la Información centraliza la definición, gobierno y control de los aspectos de seguridad, tales como: autenticación, autorización, protección de la información, control y monitoreo de los despliegues, participando también en las pruebas previas a la puesta en producción.

4. Desarrollo

4.1. Seguridad de la Información en el desarrollo de Software

Se deberán tener en cuenta aspectos de seguridad de la Información desde el comienzo en todos los proyectos de desarrollo o modificación de software y en todas las etapas de éste, a saber:

- Definición / redefinición de procesos.
- Análisis de requerimientos.
- Diseño.
- Codificación / Programación.
- Pruebas (Testing funcional y de seguridad).
- Implementación.

Para garantizar la seguridad de los desarrollos de software, se debe cumplir con los requerimientos establecidos en el Registro **"RE-SI-08 Requisitos de Seguridad de la adquisición/desarrollo de Software"**. Estos requerimientos se han establecido para garantizar que los desarrollos cumplan con los estándares de seguridad necesarios para proteger la información y prevenir posibles amenazas cibernéticas.

Adicionalmente se deben tener en cuenta los lineamientos definidos en la norma **"NO-SI-09 - Gestión de ambientes"**, con el fin de garantizar que cada uno de los siguientes procesos se lleven a cabo en ambientes separados.

4.2. Codificación del Desarrollo

En el desarrollo de una nueva solución o en la modificación de una solución existente, se deben considerar buenas prácticas de desarrollo de manera que se eviten vulnerabilidades y brechas de seguridad en el código. Entre los aspectos para tener en cuenta se encuentran:

- Pruebas de código (análisis estáticos de seguridad) utilizando las herramientas provistas por la plataforma utilizada para el proceso de Desarrollo Seguro, como, por ejemplo:
    - Autenticación y gestión de accesos.
    - Autorización.
    - Gestión de sesiones de usuario.
    - Integridad de datos.
    - Protección de datos.
    - Manejo de excepciones.
    - Auditoría y login.
- Utilización de bibliotecas de seguridad estándar ya conocidas y probadas, de manera que se utilicen para el nuevo código y agilizar el proceso de desarrollo de la solución.
- Considerar aspectos de desarrollo seguro (concepto de OWASP), y de esta forma prevenir la materialización de riesgos de seguridad de la información, tales como:
    - Pérdida de autenticación.
    - Pérdida de control de acceso.
    - Exposición de datos sensibles.
    - Codificación con vulnerabilidades conocidas.
    - Registro y monitoreo insuficiente.
    - Configuración de seguridad incorrecta.

4.3. Testing previo a la Puesta en Producción

En esta etapa se debe probar el software desarrollado, ejecutando pruebas dinámicas de seguridad, las cuales deberán abarcar:

- Pruebas de integridad de datos y entradas inesperadas.

- Vulnerabilidades de seguridad del software y de la plataforma de infraestructura, siguiendo los lineamientos de la norma **NO-SI-13 Gestión de Vulnerabilidades y Parches.**
- Test de penetración del software y plataforma de infraestructura, el cual puede ser ejecutado durante el proceso de monitoreo una vez puesta en marcha.

4.4. Puesta en Producción

Al momento de implementar los cambios diseñados en etapas anteriores, se deberá tener en cuenta lo establecido en la norma **"NO-SI-18 - Gestión de Cambios".** además de las siguientes consideraciones:

- Implementar mecanismos de integridad, de manera que se asegure que la versión del código a ser liberada sea la probada en etapas anteriores.
- Establecer listas blancas de archivos (Bibliotecas) que puedan ejecutarse en los servidores de producción.
- Restringir las ejecuciones a sólo aquellas que provengan de herramientas o scripts autorizados.
- Se deberá formalizar el canal de comunicación ante un posible cambio de emergencia.

4.5. Auditoría y Control

- El registro de eventos de seguridad, así como el de actividades de los usuarios deberá estar habilitado para el proceso de Desarrollo Seguro, de manera de determinar:
    - Autorizaciones de pases entre ambientes.
    - Aprobaciones de UAT.
    - Modificaciones excepcionales en el flujo de aprobaciones.
    - Autorizaciones para implementación en producción.

- Se deberá tener especial cuidado en el tratamiento de los datos productivos, utilizándose procedimientos de enmascarado y/u ofuscación en entornos no productivos y/o no utilizándolos para pruebas en ambientes no productivos, para ello se debe tener en cuenta lo establecido en la norma **"NO-SI-20 - Cifrado de la Información".**
- Se deberán establecer mecanismos de protección de datos considerados confidenciales mediante encriptación cuando estos estén en modo "reposo" o en "tránsito".

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Norma	Gestión de cambios	NO-SI-18
Norma	Gestión de Ambientes	NO-SI-09
Norma	Gestión de Vulnerabilidades y Parches	NO-SI-13
Norma	Cifrado de Información	NO-SI-20
Procedimiento	Desarrollo Seguro	PR-SI-10
Registro	Requisitos de Seguridad de la adquisición/desarrollo de Software.	RE-SI-08

5.2. Definiciones

Término	Descripción
Pruebas de Seguridad	Se define como el conjunto de actividades que se llevan a cabo para encontrar fallas y vulnerabilidades en las aplicaciones, buscando disminuir el impacto de ataques a ellas y pérdida de información importante.
Test de penetración	Una prueba de penetración, o pentest, es un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos. El proceso consiste en identificar el o los sistemas que representan el objetivo de ataque.
Scripts	Se denomina script a una serie de comandos que se almacenan dentro de un archivo de texto, el cual contiene instrucciones, escritas en códigos de programación. El script es un lenguaje de programación que ejecuta diversas funciones en el interior de un software.
UAT (User Acceptance Test)	La prueba de aceptación del usuario (UAT), también conocida como prueba beta o de usuario final, se define como la prueba del software por parte del usuario o dueño del mismo para determinar si puede ser aceptado o no. El objetivo principal de esta prueba es validar el software frente a los requisitos y especificaciones funcionales.

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	17/02/2022	Creación de la Norma de Desarrollo Seguro.
1.0	24/06/2022	Aprobado por Comité de Dirección: MI-DI-05- Minuta de Comité de Dirección N° 5
2.0	20/07/2023	Se agrega referencia a los requisitos de Seguridad para el desarrollo de Software “RE-SI-08”.
2.0	21/07/2023	Aprobado por CTO y CISO.
3.0	10/07/2024	Se agregaron nuevos responsables y se realizó mención a las normas relacionadas en cada proceso. También se agregó clasificación del documento en el encabezado y se eliminó del pie de página. Se reclasificó el documento a “Restringido”.