DESARROLLO SEGURO

TIPO DE DOCUMENTO: Procedimiento

CÓDIGO: PRO GSI 046

I. AUTORIZACIONES

Elaboró:	*Revisó:*	*Autorizó:*
Ing. Rafael Fernando Mendoza Loza *Coordinador de Sistemas TI*	*Ing. Salvador Santiago Araujo* *Gerente Administrativo*	*C.P. Jerónimo Javier Mendoza Lara / Lic. Irais Dafne Mendoza Sánchez* *Director General / Director General Adjunto*

Última revisión: octubre 2025

No. de versión: 8

Fecha de emisión: Julio 2016

Revisó: GAD

Aprobó: DGE

ÍNDICE

CONTENIDO **PÁGINA**

II. OBJETIVO

Establecer los lineamientos que controlen el desarrollo seguro de las aplicaciones, así como las pruebas que deben de aplicarse a efecto de garantizar la operación correcta del software.

III. ALCANCE

Aplica a todas las áreas, procesos y activos de la Organización, involucradas en el Sistema de Gestión de Seguridad de la Información.

IV. HISTORIAL DE CAMBIOS

Versión	Descripción de cambios	Autor(es)	Fecha de cambio
1	Versión inicial.	MBS	Julio 2016
2	Cambio de Formato	LBR	Octubre 2016
3	Actualización en el punto 6 respecto a las pruebas del software durante su desarrollo.	LBR	Marzo 2017
4	Adecuaciones generales a referencias y al apartado de abreviaciones y definiciones	LBR	Mayo 2017
5	Revisión de controles	LBR	Diciembre 2018
6	Actualización de referencias, Principios de ingeniería de sistemas seguros.	LBR	Julio 2019
7	Actualización de Entorno de desarrollo seguro	RFML	Octubre 2020
8	Se realizan adecuaciones generales.	CST	Septiembre 2023

V. REFERENCIAS

- MAN GSI 001 Manual de gestión de seguridad de la información.
- MAP SIS 001 Mapa de procesos de sistemas.
- POL GIS 001 Políticas generales de seguridad de la información.
- FOR GSI 002 Hoja de vida e implementación.
- PRO GSI 039 Operativo para las TIC.

VI. ABREVIACIONES Y DEFINICIONES

Abreviaciones:

DGE	Director General / Director General Adjunto
GAD	Gerente Administrativo
CSG	Coordinador de Sistemas de Gestión
CST	Coordinador de Sistemas TI
DES	Desarrollador
N/A	No Aplica
SGC	Sistema de Gestión de Calidad
SGSI	Sistema de Gestión de Seguridad de la Información

Definiciones:

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Modelo SPIRA: Es una estructura y una metodología para el diseño, desarrollo y ejecución de soluciones de formación y desarrollo y consta de cuatro fases.

VII. DESARROLLO DE ACTIVIDADES

No.	Descripción	Responsable(s)
1	Generalidades	
1.1	Cuando el Desarrollador reciba una solicitud deberá: a) Antes de su aceptación, establecer, aprobar y documentar los requisitos operacionales de los sistemas serán establecidos, aprobados y documentados. b) Una vez aprobada o aceptada la solicitud, deberá realizar un análisis de las implicaciones de seguridad de la información, previo al desarrollo de la herramienta a través del formato de **Hoja de vida e implementación FOR GSI 002**. c) Durante el desarrollo del sistema se deberán tomar medidas para identificar y asegurar que no se haga mal uso de estos, y que puedan provocar fraudes financieros.	Desarrollador
2	Control de cambios en sistemas	
2.1	Para el control de nuevo sistema. la organización toma las siguientes medidas: a) Se cuenta con herramientas que permiten el control de versiones de software. b) Las versiones de software a lanzar a los ambientes de producción son revisadas cuidadosamente para no cometer errores; antes, durante y después del desarrollo o cambios del software.	Desarrollador
3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	
3.1	Las medidas de revisión técnica de las aplicaciones son: a) En caso de que los sistemas operativos (Windows, Linux) tengan alguna actualización o cambio de versión, el Área de Sistemas deberá de asegurarse de que las aplicaciones (BONSAIF, SICOB, OPTI-RISKS, ERP) no se presentan fallos o errores para su operación, de acuerdo con lo estipulado en el procedimiento para la aplicación de parches de seguridad y actualizaciones en los equipos del procedimiento **Operativo para las TIC PRO GSI 039**. b) Para las herramientas desarrolladas, antes de liberar las actualizaciones, el desarrollador deberá realizar pruebas en el ambiente de desarrollo seguro.	Sistemas
4	Restricciones a los cambios en los paquetes de software	

4.1	a) De requerirse algún cambio o actualización en uno de los sistemas adquiridos con proveedores, el personal de Sistemas deberá revisar los aspectos técnicos y de seguridad de la información. Se deberá contar con autorización de Dirección para su instalación. b) Para el caso de las herramientas creadas por el Área de Sistemas, estas no podrán ser actualizadas, ni alteradas, sin la realización de pruebas pertinentes y autorizadas.	Sistemas
5	Principios de ingeniería de sistemas seguros	
5.1	Los sistemas y aplicaciones de la Organización se desarrollan y operan bajo los siguientes principios: ➢ Cualquier cambio realizado debe estar documentado. ➢ Se debe realizar un análisis de seguridad en cada una de las etapas de desarrollo. ➢ El lenguaje de programación debe ser accesible y confiable. ➢ Contar con un ambiente aislado de pruebas con datos ficticios u obsoletos. ➢ Los datos que ingresan a la aplicación deben ser verificados para garantizar que lo que está ingresando a los sistemas es lo esperado. ➢ Cualquier funcionalidad debe agregarse de acuerdo con los requerimientos. ➢ Se deben realizar pruebas periódicas para el aseguramiento de la funcionalidad del sistema y la seguridad de la información. ➢ Revisar y mitigar las posibles vulnerabilidades de los sistemas a desarrollar. ➢ Partir de un modelo de permisos mínimos e ir escalando privilegios.	Sistemas
6	Entorno de desarrollo seguro	
6.1	Derivado a la naturaleza de los servicios que proporcionamos en la Organización, debemos contar con un área dedicada al desarrollo de aplicaciones y/o software, el área de Sistemas debe de establecer un marco organizacional para el desarrollo de software, en el cual se establezca una metodología para todo el ciclo de vida del desarrollo.	Sistemas / Desarrollo
6.2	Todos los proyectos de creación de software creados o desarrollado por el personal es propiedad de la organización.	Sistemas / Desarrollo
6.3	La organización cuenta con un ambiente de ejecución aislado, donde cada aplicativo, información y herramienta se encuentran en diferentes servidores con el fin de mitigar	Sistemas / Desarrollo

	riesgos en la seguridad de la información, por tal motivo la organización cuenta con 4 ambientes de desarrollo seguro. 1. Entorno de desarrollo. 2. Entorno de Testing 3. Entorno de UAT. 4. Entorno de producción.	
6.4	El departamento de desarrollo debe de basar los proyectos de software en la metodología SPIRAL, esto por la naturaleza de los servicios que proporcionamos.	Sistemas / Desarrollo
6.5	Todas las aplicaciones cuenten con un módulo de seguridad, mediante el cual solo sé administre y gestione el ABC (altas, bajas y cambios) de usuarios, asegurando la trazabilidad de las sesiones de cada usuario. Este módulo debe contar con herramientas para la generación de reportes del control de acceso y gestión de usuarios. El módulo de seguridad deberá alimentarse desde la base de datos de recursos humanos y mantenerse actualizada.	Sistemas / Desarrollo
6.6	El personal de desarrollo deberá: 1. Establecer un marco organizacional para el desarrollo de software, en el cual se establezca una metodología para todo el ciclo de vida del desarrollo. 2. Documentar todas las etapas del proceso de desarrollo de software en el formato de **Hoja de vida e implementación FOR GSI 002.** 3. Adoptar las metodologías organizacionales para el desarrollo de proyectos y cumplir con los lineamientos definidos por la organización. 4. Asegurar su participación continua durante el proyecto de desarrollo. 5. Proveer ambientes controlados para el desarrollo de software organizacional como son: • Entorno de desarrollo. • Entorno de Testing • Entorno de UAT. • Entorno de producción. 6. Utilizar GitHub con repositorio controlado para que contenga la documentación y el código fuente de los desarrollos organizacionales.	Desarrollador

	7. Utilizar Jira Software y Sentry para el control de versiones liberadas y gestión de los proyectos 8. Hay que asegurar que todo desarrollo organizacional cuente con una arquitectura documentada que contenga al menos los siguientes aspectos: • Modularidad. • Escalabilidad. • Integración con sistemas legados. • Seguridad. • Disponibilidad. • Confiabilidad. • Soporte.	
6.7	Todo cambio o modificación en ambiente productivo del software organizacional, deberán apegarse al proceso de control de cambios del área de Sistemas, el desarrollador deberá documentar estos cambios en la **Hoja de vida e implementación FOR GSI 002.**	Sistemas / Desarrollador
6.8	El gerente administrativo y/o el coordinador de sistemas de gestión revisarán que se consideren los aspectos de seguridad en todas las fases del desarrollo, asimismo, deberán coordinar con los responsables de los procesos de desarrollo, para que se cuente con las medidas de seguridad, para que el código de las soluciones tecnológicas, componentes, productos y demás elementos relacionados, no se copie, envíe, transmita o difunda por cualquier medio distinto a su desarrollo. Para los desarrollos subcontratados, es de vital importancia, definir de manera contractual la posesión del código fuente, para lo cual, deben existir mecanismos legales que permitan asegurar a la Institución mantener la titularidad del código fuente.	Gerente Administrativo / Coordinador de Sistemas de Gestión
6.9	Todos los datos de prueba deberán contar con un mecanismo de enmascaramiento de la información reservada y/o confidencial. Una vez utilizados los datos de prueba, el desarrollador deberá borrados antes de su pase a producción.	Desarrollador
6.10	Los entornos de Testing, UAT, en ningún momento se podrán conectar a internet, esto con el fin de que los datos de prueba no corran algún riesgo de seguridad.	Sistemas / Desarrollo
7	Externalización del desarrollo de software	
7.1		Sistemas

	a) Cuando se adquiera sistemas de terceros es necesario que se cumplan con los requisitos de seguridad establecidos, además de estar en acuerdo con la política de licenciamiento de software, descrita en las **políticas generales de seguridad de la información POL GSI 001.** b) Cuando se trate de desarrollo de software, el proveedor deberá apegarse a los lineamientos de seguridad de la información establecidos tanto en el contrato como del SGSI.	
7.2	**Acuerdos y contratos con proveedores de desarrollo de software** a) Se deberán establecer en los contratos de desarrollo de software, que la Organización tiene el derecho de propiedad sobre el código fuente del software (programa, actualizaciones y mejoras). b) Se deberán conservar los contratos o documentos que proporcionan la prueba de la propiedad del software por parte de la Organización, hasta que se deje de utilizar el software.	Sistemas
8	Pruebas funcionales de seguridad de sistemas	
8.1	a) Durante el análisis del previo, el desarrollador establecerá aquellas etapas relevantes para la revisión de funcionalidad y seguridad de los sistemas. b) Durante el desarrollo de nuevos sistemas, el desarrollador llevará a cabo pruebas de funcionalidad y deberán documentarse en la **bitácora de pruebas LIS GSI 012**.	Desarrollador
9	Pruebas de aceptación de sistemas	
9.1	a) El Área de Sistemas deberá establecer los criterios para la aceptación de nuevos sistemas, así como para las nuevas versiones y la programación de la realización de pruebas de acuerdo con los cambios que se van generando. b) La liberación de las herramientas se realizará a través de correo electrónico, solicitando la aceptación y revisión de este con el área solicitante.	Sistemas
10	Protección de los datos de prueba	
10.1	En caso de que, el desarrollador deberá realizar pruebas al software, (por ser nuevos o por ser actualizadas las versiones), se utilizarán datos ficticios u obsoletos para tal fin, por lo tanto, no se utilizarán datos reales que deban de ser protegidos y se documentarán en la **bitácora de pruebas LIS GSI 012.**	Desarrollador