## CONTENIDO

1 OBJETIVO ..... 2
2 DESTINATARIOS ..... 2
3 GLOSARIO ..... 2
4 REFERENCIAS NORMATIVAS ..... 3
5 GENERALIDADES ..... 3
6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO ..... 6
7 DESCRIPCION DE ETAPAS Y ACTIVIDADES ..... 7
7.1 ETAPA 1. INCLUIR REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN EN LOS DESARROLLOS ..... 8
7.1.1 Analizar los requisitos mínimos de seguridad de la información. ..... 8
7.1.2 Definir requisitos adicionales de seguridad de la información. ..... 11
7.1.3 Diseñar los requisitos de seguridad de la información ..... 12
7.1.4 Implementar los requisitos de seguridad de la información. ..... 12
7.2 ETAPA 2. IDENTIFICAR Y CORREGIR VULNERABILIDADES EN LOS SISTEMAS DE INFORMACIÓN a desarrollar ..... 12
7.2.1 Identificar y corregir vulnerabilidades en etapas tempranas del desarrollo del sistema de información. ..... 12
7.2.2 Identificar y analizar vulnerabilidades del sistema de información, previo al paso a producción. ..... 13
8 DOCUMENTOS RELACIONADOS ..... 14
8.1 DOCUMENTOS EXTERNOS ..... 14
9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN ..... 14

COPIA NO CONTROLADA OBSOLETA

| Elaborado por: | Revisado y Aprobado por: | Aprobación Metodológica por: |
|---|---|---|
| Nombre: Oscar Fabián Ramírez Torres<br><br>Cargo: Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital. | Nombre: Jaroslav López<br>Cargo: Jefe Oficina de Tecnología e Informática | Nombre: Amanda Estella Pedraza Rodríguez<br><br>Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad<br><br>Fecha: 2023-03-28 |

Cualquier copia impresa, electrónica o de reproducción de este documento sin la marca de agua o el sello de control de documentos, se constituye en copia no controlada.

## 1 OBJETIVO

Incluir la seguridad de la información como parte integral de los sistemas de información durante todo su ciclo de vida, a través de la identificación e implementación de requisitos de seguridad de la información y la ejecución de pruebas sobre los sistemas de información en desarrollo, lo cual será realizado por los colaboradores asignados de la Oficina de Tecnología e Informática - OTI.

**Nota**: Las actividades definidas en este documento, aplican para el desarrollo de nuevos sistemas de información o nuevos módulos de los sistemas existentes (servicios web, aplicaciones de escritorio, aplicaciones cliente - servidor, entre otros), de aplicabilidad a partir de la fecha de su aprobación.

## 2 DESTINATARIOS

Va dirigido a los servidores públicos y contratistas de la Superintendencia de Industria y Comercio, involucrados con el desarrollo de aplicaciones.

## 3 GLOSARIO

CONTROL: Políticas, procedimientos, prácticas y estructuras organizativas, concebidas para mantener los riesgos de seguridad de la información por debajo del nivel aceptable. Control es utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. Fuente: MinTIC.

OWASP: Proyecto Abierto de Seguridad de Aplicaciones Web (en inglés Open Web Application Security Project).

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

SDLC: Siglas en inglés Systems Development Life Cycle, Ciclo de vida del desarrollo de sistemas.

COPIA NO CONTROLADA OBSOLETA

## 4 REFERENCIAS NORMATIVAS

| Jerarquía de la norma | Numero/ Fecha | Título | Artículo | Aplicación Específica |
|---|---|---|---|---|
| Norma Técnica Colombiana NTC-ISO-IEC. | 27001:2013. | Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. | Todo el documento. | Todo el documento. |
| Guía. | Modelo de Seguridad y Privacidad de la Información. Versión: 3.0.2 del 29 de julio de 2016. | Seguridad y Privacidad de la Información. | Todo el documento. | Todo el documento. |
| Guía OWASP. | Versión 4.0.3 de octubre de 2021. | Estándar de Verificación de Seguridad en Aplicaciones. | Todo el documento. | Todo el documento. |

## 5 GENERALIDADES

De acuerdo con el Modelo de Seguridad y Privacidad de la Información - MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, las entidades deben establecer cómo se realiza la gestión de la seguridad de la información en los sistemas desarrollados internamente (in-house), verificando que se preserve la confidencialidad, integridad y disponibilidad de la información de la entidad.

Así mismo, en la norma NTC-ISO-27001:2013 se establecen los siguientes controles de seguridad de la información:

- Principios de construcción de sistemas seguros. (Control A.14.2.5), el cual establece que se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

- Análisis y especificaciones de los requisitos de seguridad de la información. (Control A.14.1.1), el cual indica que los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

COPIA NO CONTROLADA OBSOLETA

- Pruebas de seguridad de sistemas (Control A.14.2.8), el cual refiere a que durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
- En respuesta a lo anterior, la OTI ha elaborado el presente procedimiento, el cual cuenta con los lineamientos para definir los requisitos de seguridad de la información y establece el protocolo para realizar pruebas e identificación de vulnerabilidades en los nuevos sistemas de información o nuevos módulos de los sistemas existentes.

- De otra parte, para fortalecer la seguridad en el desarrollo de aplicaciones, se recomienda adoptar las siguientes recomendaciones y guías abiertas que OWASP proporciona:

| **Recomendaciones para desarrolladores** | |
|---|---|
| Arquitectura de seguridad en aplicaciones | OWASP recomienda la serie de **hoja de trucos de prevención**[1], como puntos de inicio óptimos para el diseño seguro de aplicaciones. |
| Controles de Seguridad Estándar | Los **controles proactivos de OWASP**[2] presentan controles estándares y efectivos para autorización, validación, prevención de CSRF, etc. |
| Ciclo de vida de desarrollo seguro | Para mejorar el proceso para crear aplicaciones y APIs, se recomienda el **Modelo de Garantía de la Madurez del Software (SAMM v2)**[3]. |
| Educación de la Seguridad en Aplicaciones | **OWASP proporciona material de formación**[4] para ayudar a los desarrolladores en apropiar temas de seguridad en aplicaciones web. |

| **Recomendaciones para administradores de aplicaciones** | |
|---|---|
| Administración de Requisitos y Recursos. | - Recolectar y negociar los requisitos de negocios para una aplicación, incluyendo confidencialidad, autenticidad, integridad y disponibilidad de todos los activos de datos y de las funciones de negocio.<br>- Recopilar los requerimientos técnicos incluyendo requerimientos de seguridad funcionales y no funcionales.<br>- Planear y negociar el presupuesto que cubre todos los aspectos de diseño, construcción, testeo y operación, incluyendo actividades de seguridad. |
| Solicitud de Propuestas (RFP) y Contrataciones | - Negociar requisitos con desarrolladores internos y externos, incluyendo lineamientos y requerimientos de seguridad con respecto a su programa de seguridad. Por ej. SDLC, mejores prácticas.<br>- Evaluar el cumplimiento de todos los requerimientos técnicos, incluyendo las fases de planificación y diseño.<br>- Negociar todos los requerimientos técnicos incluyendo diseño, seguridad y acuerdos de nivel de servicio (SLA). |

COPIA NO CONTROLADA DE SOLETA

[1] https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series
[2] https://owasp.org/www-project-proactive-controls/
[3] https://www.owasp.org/index.php/OWASP_SAMM_Project
[4] https://owasp.org/www-committee-education-and-training/

| Recomendaciones para administradores de aplicaciones | |
|---|---|
| Planificación y Diseño | Negociar la planificación y diseño con los desarrolladores, interesados internos y especialistas de seguridad.<br>Definir la arquitectura de seguridad, controles y contramedidas adecuadas a las necesidades de protección y el nivel de amenazas planificado. Esto debería contar con el apoyo de especialistas en seguridad.<br>Asegurar que el propietario de la aplicación acepta los riesgos remanentes o bien que provea recursos adicionales. |
| Despliegue, Pruebas y Puesta en Producción | Automatizar el despliegue seguro de la aplicación, interfaces y todo componente, incluyendo las autorizaciones requeridas.<br>Probar las funciones técnicas, integración a la arquitectura de TI, y coordinar pruebas de funciones de negocio.<br>Crear casos de uso y de abuso tanto desde el punto de vista netamente técnico como del negocio.<br>Administrar pruebas de seguridad de acuerdo con los procesos internos, las necesidades de protección y el nivel de amenazas asumido para la aplicación.<br>Poner la aplicación en operación y migrar las aplicaciones usadas previamente en caso de ser necesario.<br>Actualizar toda la documentación, incluyendo la Base de Datos de Gestión de la Seguridad (CMDB) y la arquitectura de seguridad. |
| Operación y Gestión del cambio | Operar incluyendo la administración de seguridad de la aplicación (por ej. administración de parches).<br>Aumentar la conciencia de seguridad de los usuarios y administrar conflictos de usabilidad vs seguridad.<br>Planificar y gestionar cambios, por ejemplo, la migración a nuevas versiones de la aplicación u otros componentes como sistema operativo, interfaces de software y bibliotecas.<br>Actualizar toda la documentación, incluyendo la Base de Datos de Gestión de la Seguridad (CMDB) y la arquitectura de seguridad. |
| Retiro de Sistemas | Cualquier dato requerido debe ser almacenado. Otros datos deben ser eliminados de forma segura.<br>Retirar la aplicación en forma segura, incluyendo el borrado de cuentas, roles y permisos no usados.<br>Establecer el estado de la aplicación a retirada en la CMDB. |

| Recomendaciones para testers | |
|---|---|
| Modelo de Amenazas. | El **Estándar de Verificación de Seguridad de Aplicaciones de OWASP (ASVS)**[5] y la **Guía de Revisión OWASP**[6] son un insumo para realizar el Modelado de Amenazas e identificar las prioridades en la verificación de la seguridad. |
| SDLC (Ciclo de desarrollo de sistemas). | El enfoque de la revisión de seguridad de aplicaciones debe ser altamente compatible con las personas, procesos y herramientas que usa en su SDLC. |

[5] https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
[6] https://owasp.org/www-project-web-security-testing-guide/

COPIA NO CONTROLADA OBSOLETA

| Recomendaciones para testers | |
|---|---|
| Estrategias de pruebas | El **Marco de Trabajo de Conocimiento de Seguridad**[7] de OWASP es una fuente para realizar las pruebas de seguridad. |
| Lograr cobertura y precisión | No comenzar por probarlo todo. Se recomienda iniciar con lo que es importante y ampliar el programa de verificación con el tiempo. Esto significa ampliar el conjunto de defensas y riesgos de seguridad que se prueban automáticamente, así como ampliar el conjunto de aplicaciones y APIs que se incluyen en el alcance. |
| Comunicar los mensajes claramente | Se recomienda describir claramente y sin jerga técnica como la aplicación puede ser vulnerada e incluir escenarios de ataque para hacerlo real. |

Así mismo, para fortalecer la calidad de los productos desarrollados se recomienda revisar la familia de normas ISO 25000, que proporciona una guía para el uso de la nueva serie de estándares internacionales llamada Requisitos y Evaluación de Calidad de Productos de Software conocida como (SQuaRE  System and Software Quality Requirements and Evaluation).

## 6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO

Las etapas y actividades, descritas en el presente documento, se encuentran estrictamente relacionadas con los procedimientos Ciclo de vida de construcción de software GS03-P03 y Procedimiento control de cambios DE04-P04, de la siguiente forma:

- La etapa No. 1, adiciona actividades para las fases de inicio, elaboración y construcción de software, definidas en el Procedimiento Ciclo de vida de construcción de software GS03-P03.

- La etapa No. 2, adiciona actividades para la fase de transición del Procedimiento Ciclo de vida de construcción de software GS03-P03 (realizar pruebas a los componentes).

La ejecución de las etapas 1 y 2 de este procedimiento, son un requisito para el paso a producción de un nuevo sistema de información o nuevo módulo de un sistema existente, por consiguiente, se incluyen actividades en las etapas de: 1) Registro y revisión de la solicitud y 2) Evaluación y aprobación del cambio, las cuales se encuentran definidas en el documento Procedimiento control de cambios DE04-P04.

COPIA NO CONTROLADA OBSOLETA

[7] https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework

A continuación, se muestra la representación esquemática del procedimiento:

| No. | ETAPAS | ENTRADAS | DESCRIPCIÓN DE LA ETAPA | RESPONSABLE | SALIDAS |
|---|---|---|---|---|---|
| 1 | Incluir requisitos de seguridad de la información en los desarrollos | Línea base de requisitos de seguridad.<br><br>Documentos con el detalle del sistema de información a desarrollar<br><br>(Ver documentos de salida del Procedimiento gestión de proyectos de TI DE04-P05, etapa 3) | En esta etapa se analizan, definen, diseñan e implementan los requisitos de seguridad que permitan mantener segura la información en los sistemas de información a desarrollar.<br><br>Esta etapa comprende las siguientes actividades:<br>- Analizar los requisitos mínimos de seguridad de la información.<br>- Definir requisitos adicionales de seguridad de la información.<br>- Diseñar los requisitos de seguridad de la información.<br>- Implementar los requisitos de seguridad de la información. | Coordinador del Grupo de Trabajo de Sistemas de Información.<br><br>Coordinador del Grupo de Trabajo de Gestión de Información y Proyectos Informáticos.<br><br>Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital.<br><br>Profesionales que apoyan la implementación del SGSI. | Lista de chequeo de requisitos de seguridad de la información, Formato GS03-F27 diligenciado. |
| 2. | Identificar y corregir vulnerabilidades en los sistemas de información a desarrollar. | Listado de Requisitos de seguridad de la información a incluir en los sistemas de información a desarrollar.<br><br>Requisitos de seguridad de la información diseñados.<br><br>Requisitos de seguridad de la información implementados en los sistemas de información. | En esta etapa se identifican y corrigen vulnerabilidades del sistema de información a desarrollar:<br><br>Esta etapa comprende las siguientes actividades:<br>- Identificar y corregir vulnerabilidades en etapas tempranas del desarrollo del sistema de información.<br>- Identificar y analizar vulnerabilidades del sistema de información, previo al paso a producción. | Coordinador del Grupo de Trabajo de Sistemas de Información.<br><br>Coordinador del Grupo de Trabajo de Gestión de Información y Proyectos Informáticos.<br><br>Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital.<br><br>Profesionales que apoyan la implementación del SGSI. | Informe de análisis de vulnerabilidades, Formato GS01-F23 diligenciado. |

COPIA NO CONTROLADA OBSOLETA

## 7 DESCRIPCION DE ETAPAS Y ACTIVIDADES

A continuación, se describen las etapas y actividades del procedimiento:

## 7.1 ETAPA 1. INCLUIR REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN EN LOS DESARROLLOS.

En esta etapa se definen, diseñan e implementan, los requisitos de seguridad de la información para los sistemas de información a desarrollar, de acuerdo con los riesgos y el nivel de clasificación de la información.

### 7.1.1 Analizar los requisitos mínimos de seguridad de la información.

El Grupo de Trabajo de Sistemas de Información y el Grupo de Trabajo de Gestión de Información y Proyectos Informáticos analiza la aplicabilidad de la línea base de seguridad de la información (requisitos mínimos), para cada sistema de información a desarrollar o nuevo módulo de un sistema existente.

A continuación, se presenta la línea base de seguridad, la cual fue construida siguiendo el Estándar de Verificación de Seguridad en Aplicaciones de OWASP, (ASVS por sus siglas en inglés).

| Id. | Categoría del requisito | Descripción |
|---|---|---|
| 1 | Acceso | Verificar que existe el principio de privilegio mínimo - los usuarios sólo deben ser capaces de acceder a las funciones, archivos de datos, URL, controladores, servicios y otros recursos, para los cuales poseen una autorización específica. Esto implica protección contra suplantación de identidad y elevación de privilegios.<br><br>Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación del sistema se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente el sistema verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas a realizar |
| 2 | Manejo de excepciones | Verificar que los controles de acceso fallen de forma segura, es decir, no se emitan mensajes de error o rastros de pilas que contengan datos sensibles que podrían ayudar a un atacante, incluyendo el identificador de sesión, versiones de software/entorno y datos personales. Las fallas deben ser identificadas por ID y documentadas en los manuales de la aplicación. |
| 3 | Perfil de usuario | El sistema debe permitir la gestión de usuarios, grupos de usuarios y asignación de roles y perfiles, permitiendo asociar las acciones disponibles en el sistema a los roles de usuario y parametrizar las funcionalidades que cada actor puede usar en el sistema. Los permisos de acceso al sistema para los usuarios podrán ser cambiados solamente por el administrador de acceso a datos. |
| 4 | Sesión de usuario | Al ingresar el usuario a la aplicación, se debe mostrar la última fecha y hora de ingreso. |
| 5 | Gestión de usuarios | Las aplicaciones deben generar un informe con los usuarios activos, los perfiles de los mismos, los usuarios inactivos con sus fechas de bajas y altas de la aplicación a fin de hacer auditorías de usuarios periódicamente. |

COPIA NO CONTROLADA OBSOLETA

| Id. | Categoría del requisito | Descripción |
|---|---|---|
| 6 | Auditorías de usuarios | El diseño del sistema debe tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del registro, tabla afectada, descripción del evento, tipo de evento, usuario que realiza la acción, identificación de sesión y dirección IP del usuario que efectuó la transacción. |
| 7 | Acceso | El sistema debe integrarse con LDAP  (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. El sistema debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos (por ejemplo: vigilados y ciudadanos) el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad del sistema de información. |
| 8 | Protección de datos personales | El sistema debe garantizar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales, debe permitir el manejo de excepciones previa autorización de los usuarios finales (ciudadanos), cuando los sistemas de información soliciten datos personales al usuario final se debe establecer un mecanismo que permita registrar que se ha autorizado el tratamiento de los mismos. |
| 9 | Autenticación segura y secreta | El sistema debe asegurar los aspectos de la transacción, asegurando la información de autenticación secreta de usuario (User´s Secret Authentication Information), validando y verificando que la transacción permanezca confidencial y que se mantenga la privacidad asociada con todas las partes involucradas. En este sentido, se debe:<br><br>a) Verificar que todos los controles de autenticación se realicen del lado del servidor.<br>b) Verificar que la funcionalidad de cambio de contraseña solicite la contraseña anterior, la nueva contraseña y una confirmación de la contraseña.<br>c) Verificar que las funciones de recuperar contraseña y acceso no revelen la contraseña actual y que la nueva contraseña no se envíe en texto plano al usuario.<br>d) Verificar que no se utilizan contraseñas por defecto en la aplicación o cualquiera de los componentes utilizados por la misma (como "admin/password").<br>e) Verificar que existen medidas para bloquear el uso de contraseñas comúnmente utilizadas y contraseñas débiles. |
| 10 | Bloqueo de usuarios | El sistema debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta |
| 11 | Captcha | Implementar un captcha como requisito de ingreso al sistema con el fin de evitar ataques de fuerza bruta. |
| 12 | Sesiones seguras | El sistema debe cerrar las transacciones luego de máximo 15 minutos de inactividad, así mismo, las sesiones se invalidan cuando el usuario cierra la sesión. |
| 13 | Sesiones seguras | Verificar que el identificador de sesión nunca se revele en URLs, mensajes de error o registros de bitácora. Esto incluye verificar que la aplicación sea compatible con la re-escritura de URL incluyendo el identificador de sesión. |
| 14 | Sesiones seguras | Verificar que toda autenticación exitosa y re-autenticaciones generen un nuevo identificador de sesión. |

COPIA NO CONTROLADA

| Id. | Categoría del requisito | Descripción |
|---|---|---|
| 15 | Sesiones seguras | Verificar que los identificadores de sesión son suficientemente largos, aleatorios y únicos para las sesiones activas. |
| 16 | Sesiones únicas | Verificar que la aplicación limita el número de sesiones concurrentes activas. Se define solo una sesión por usuario a menos que la razón de ser de la aplicación requiera lo contrario. |
| 17 | Sesiones seguras | Verificar que una lista de sesiones activas esté disponible en el perfil de cuenta o similar para cada usuario. El usuario debe ser capaz de terminar cualquier sesión activa. |
| 18 | Sesiones únicas | Verificar que al usuario se le sugiera la opción de terminar todas las otras sesiones activas después de un proceso de cambio de contraseña exitoso. |
| 19 | Manejo de Logs | Verificar que las fallas de validación de entradas de datos del lado del servidor sean rechazadas y registradas. |
| 20 | Validación de datos de entrada en formularios | Verificar que se aplican las rutinas de validación de entradas de datos del lado del servidor. |
| 21 | Transacciones seguras | Verificar que todas las consultas de SQL, HQL, OSQL, NOSQL, procedimientos almacenados y llamadas de procedimientos almacenados están protegidos por la utilización de declaraciones preparadas o parametrización de consultas, y por lo tanto no sean susceptibles a la inyección de SQL. |
| 22 | Asegurar HTML | Asegurar que todas las variables string utilizadas dentro del HTML u otro lenguaje web interpretado en el cliente, se encuentran apropiadamente codificadas, bien sea, manualmente o a través de plantillas que codifican automáticamente. Lo anterior, con el fin de asegurar que la aplicación no sea susceptible a ataques Cross-Site Scripting (XSS). |
| **23** | Headers y cookies seguros | De debe configurar los encabezados de respuesta HTTP para aumentar la seguridad de la aplicación y restringir la exposición a vulnerabilidades fácilmente evitables. La configuración se debe realizar con base en las recomendaciones del proyecto OWASP: https://owasp.org/www-project-secure-headers/. Algunos de los headers a configurar son los siguientes:<br>X-Frame-Options<br>X-XSS-Protection<br>X-Content-Type-Options<br>Content-Security-Policy<br>X-Permitted-Cross-Domain-Policies<br>Set-cookie |
| 24 | Envío seguro de datos | Verificar que toda información sensible es enviada al servidor en el cuerpo o cabeceras del mensaje HTTP (por ejemplo, los parámetros de la URL nunca se deben utilizar para enviar datos sensibles). |
| 25 | Escanear variables de entrada | Verificar que archivos no confiables enviados a la aplicación, no sean utilizados directamente por comandos de I/O (Entrada/Salida) de archivos, especialmente para proteger contra manipulaciones de rutas, archivo local incluido, manipulación de tipo mime y vulnerabilidades de inyección de comandos de sistema operativo. |
| 26 | SSL en la aplicación | El sistema debe permitir la implementación de certificados digitales, es decir, cifrar las comunicaciones de los servicios expuestos en internet o cualquier red otra red pública, haciendo uso de protocolos como HTTPS, SSL, entre otros. |

COPIA NO CONTROLADA OBSOLETA

| Id. | Categoría del requisito | Descripción |
|---|---|---|
| | | El sistema debe utilizar: certificados internos, cuando los sistemas de información vayan a ser consultados únicamente al interior de la entidad y certificados válidos públicamente, cuando los sistemas de información estén expuestos a internet. |
| 27 | Request seguro | Verificar que la aplicación acepte solo un conjunto definido de métodos de solicitud HTTP y que son necesarios, como GET y POST, y métodos no utilizados (por ejemplo: TRACE, PUT y DELETE) se encuentran explícitamente bloqueados. |
| 28 | Versiones actualizadas | Las aplicaciones deben poder ejecutarse sobre las versiones más recientes en todos sus componentes (software base, bases de datos, frameworks de desarrollo, etc.) y se debe garantizar dentro de los acuerdos de niveles del servicio con los proveedores el soporte para al menos las dos versiones de software siguientes a su salida a producción. |
| 29 | IPv6 / IPv4 | Es requerido que todas las aplicaciones sean desarrolladas de manera nativa sobre el estándar IPv6 con compatibilidad para IPv4. |

Cualquier exclusión de requisitos de la línea base, es comunicada, justificada y aprobada por el jefe de la Oficina de Tecnología e Informática (mediante correo electrónico).

Para establecer la aplicabilidad o no de un requisito de la línea base de seguridad, se recomienda realizar un análisis de riesgos sobre el nuevo sistema de información o nuevo módulo del sistema existente, utilizando la metodología de evaluación de riesgos de OWASP[8].

Una vez definida y aprobada la lista de requisitos de la línea base, los coordinadores del Grupo de Trabajo de Sistemas de Información y del Grupo de Trabajo de Gestión de Información y Proyectos Informáticos o a quien delegue, diligencia el formato Lista de chequeo de requisitos de seguridad de la información GS03-F27, seleccionando los requisitos aplicables y no aplicables.

7.1.2 Definir requisitos adicionales de seguridad de la información.

Los coordinadores del Grupo de Trabajo de Sistemas de Información y del Grupo de Trabajo de Gestión de Información y Proyectos Informáticos, remiten copia de los proyectos de desarrollo de sistemas de información al Grupo de Trabajo de Informática Forense y Seguridad Digital, con el objetivo de que este último, recomiende la inclusión de requisitos de seguridad que estén por fuera de la línea base de seguridad, los cuales debe ser justificados dependiendo de la clasificación y los riesgos asociados al aplicativo en construcción. Los nuevos requisitos son

[8] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

COPIA NO CONTROLADA OBSOLETA

propuestos y concertados con el acompañamiento de los profesionales que apoyan la implementación del SGSI en la entidad.
Los nuevos requisitos de seguridad son *validados* en el formato Lista de chequeo de requisitos de seguridad de la información GS03-F27.

7.1.3 Diseñar los requisitos de seguridad de la información.

Los coordinadores del Grupo de Trabajo de Sistemas de Información y del Grupo de Trabajo de Gestión de Información y Proyectos Informáticos, velan por que los requisitos de seguridad de la información definidos sean incluidos en el diseño del sistema de información desarrollar o nuevo módulo de un sistema de información existente. El diseño debe reflejarse, por ejemplo, en el diagrama de clases, diagrama de casos de uso, arquitectura, base de datos, interfaz, componentes, entre otros.

7.1.4 Implementar los requisitos de seguridad de la información.

El Grupo de Trabajo de Sistemas de Información y el Grupo de Trabajo de Gestión de Información y Proyectos Informáticos, verifica la implementación de los requisitos de seguridad de la información aprobados para el sistema de información a desarrollar o nuevo módulo de un sistema de información existente. Se verifica el formato Lista de chequeo de requisitos de seguridad de la información GS03-F27.

**Nota**: Es importante resaltar que el formato Lista de chequeo de requisitos de seguridad de la información GS03-F27, es un insumo para los miembros del comité de cambios de la OTI, a fin de verificar que el sistema de información desarrollado implementa controles para proteger la información de la Superintendencia de Industria y Comercio.

## 7.2 ETAPA 2. IDENTIFICAR Y CORREGIR VULNERABILIDADES EN LOS SISTEMAS DE INFORMACIÓN A DESARROLLAR.

En esta etapa se realizan las siguientes actividades:

7.2.1 Identificar y corregir vulnerabilidades en etapas tempranas del desarrollo del sistema de información.

El Grupo de Trabajo de Sistemas de Información y el Grupo de Trabajo de Gestión de Información y Proyectos Informáticos, tiene a su cargo una cuenta de usuario en la herramienta especializada de identificación de vulnerabilidades contratada por la Entidad, y cuando lo considere pertinente, podrá escanear su sistema de

COPIA NO CONTROLADA OBSOLETA

información en desarrollo, con el fin de identificar vulnerabilidades y realizar una corrección temprana de la misma.

Es de anotar que, los colaboradores de la OTI que tengan a su cargo una cuenta de usuario en dicha herramienta únicamente están autorizados para realizar escaneos sobre su sistema de información en desarrollo, y por ningún motivo deben realizar pruebas o escaneos sobre otros componentes o infraestructura tecnológica, por ejemplo, sistemas de información en producción, red corporativa, páginas web internas o externas, entre otros.

7.2.2 Identificar y analizar vulnerabilidades del sistema de información, previo al paso a producción.

Una vez el Grupo de Trabajo de Sistemas de Información o el Grupo de Trabajo de Gestión de Información y Proyectos Informáticos, considere que su sistema de información está listo para el paso a producción, el Coordinador del Grupo responsable remite vía correo electrónico o memorando, una solicitud al Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital para realizar pruebas completas para identificar vulnerabilidades y presentar un concepto técnico sobre los riesgos del sistema de información construido.

Para realizar estas pruebas, los profesionales que apoyan la implementación del SGSI, utilizan la herramienta especializada para la identificación de vulnerabilidades contratada por la entidad, con la cual se obtiene el informe con el listado de vulnerabilidades, clasificación y recomendaciones para la remediación. Es de precisar que, el alcance de las pruebas de seguridad no incluye el análisis de código, pruebas funcionales o desarrollo de código.

El Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital, o quien él delegue, remite al respectivo grupo de trabajo responsable del desarrollo, el mencionado informe y el concepto técnico a través de correo electrónico o memorando, haciendo uso del formato Informe de análisis de vulnerabilidades GS01-F23.

El Grupo de Trabajo de Sistemas de Información y/o Grupo de Trabajo de Gestión de Información y Proyectos Informáticos verifica los resultados presentados en el formato Informe de análisis de vulnerabilidades GS01-F23 y de ser necesario, remedian las vulnerabilidades encontradas.

**Nota*:*** Es importante resaltar que el informe de análisis de vulnerabilidades y la nota de aprobación en la herramienta de gestión de cambios por parte de la Coordinación del Grupo de Trabajo de Informática Forense y Seguridad Digital, son un insumo para los miembros del comité de cambios de la OTI, quienes, de

COPIA NO CONTROLADA OBSOLETA

presentarse el caso, asumirán los riesgos derivados de publicar en producción, un sistema de información con vulnerabilidades que pueda afectar la seguridad de la información de la Superintendencia de Industria y Comercio.

## 8 DOCUMENTOS RELACIONADOS

Ciclo de vida de construcción de software GS03-P03.
Políticas del Sistema de Gestión de Seguridad de la Información-SGSI SC05-POL01.
Procedimiento control de cambios DE04-P04.
Lista de chequeo de requisitos de seguridad de la información GS03-F27.
Informe de análisis de vulnerabilidades GS01 F23.

### 8.1 DOCUMENTOS EXTERNOS

- Norma Técnica Colombiana NTC-ISO-IEC: 27001:2013.
- Modelo de Seguridad y Privacidad de la Información. Versión: 3.0.2 del 29 de julio de 2016.
- Guía OWASP Estándar de Verificación de Seguridad en Aplicaciones Versión 4.0.3 de octubre de 2021.

## 9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

| |
|---|
| Se actualiza formato vigente de los procedimientos y los códigos de los documentos relacionados. |

Fin documento

COPIA NO CONTROLADA-OBSOLETA