

**SSIFO14-03**

INFORME TÉCNICO DE ANÁLISIS DE VULNERABILIDADES

**Información General del Documento**

|  |  |  |  |
| --- | --- | --- | --- |
| **Documento** | **Clave** | **Documento** | **Medio** |
|  | SSIFO14 | Informe técnico de análisis de vulnerabilidades | Electrónico e impreso |

| **Elaboración** | **Nombre** | **Puesto** | **Firma** |
| --- | --- | --- | --- |
|  | Israel Luna Guzman | Subdirector de Seguridad de la Información |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Validación** | **Nombre** | **Puesto** | **Firma** |
|  | Álvaro Moisés Díaz Díaz | Director de Soluciones Tecnológicas |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Aprobación** | **Nombre** | **Puesto** | **Firma** |
|  | Jaime Roman Carlos | Director General de Tecnologías de la Información |  |

**Control de cambios**

|  |  |  |
| --- | --- | --- |
| **Número de revisión** | **Fecha** | **Descripción del cambio** |
| 00 | 10/11/2022 | Emisión |
| 01 | 11/10/2023 | Se actualiza nombre del documento: Informe Técnico de Análisis de Vulnerabilidades  Se actualiza contenido, se ajusta formato y ortografía. |
| 02 | 15/07/2024 | Se agregaron las secciones de descripción de vulnerabilidades, tablas con detalle de vulnerabilidades, cambios en formato, se agrega la descripción de la severidad y actualización de contenido. |
| 03 | 15/08/2024 | Se actualiza diseño de encabezado y pie de página.  Se realizan correcciones ortográficas.  Se actualiza estructura del documento.  Se homologa la estructura del contenido del punto 6, para los diferentes tipos de análisis de vulnerabilidades:  Análisis de vulnerabilidades a servidor  Análisis de vulnerabilidades WEB  Análisis de vulnerabilidades a código |

**ÍNDICE**

[1. SOLICITANTE DEL SERVICIO 3](#_Toc176388715)

[2. INTRODUCCIÓN 4](#_Toc176388716)

[3. ANTECEDENTES 4](#_Toc176388717)

[4. OBJETIVO 4](#_Toc176388718)

[5. ALCANCE 4](#_Toc176388719)

[6. REPORTE TÉCNICO DE HALLAZGOS 6](#_Toc176388720)

[7. RECOMENDACIONES 8](#_Toc176388721)

[8. FORMATO Y ESTRUCTURA DE DESCRIPCIÓN DE VULNERABILIDADES 9](#_Toc176388722)

[9. DESCRIPCIÓN DE LAS SEVERIDADES 10](#_Toc176388723)

[10. DEFINICIONES 11](#_Toc176388724)

[11. MARCO METODOLÓGICO 12](#_Toc176388725)

## SOLICITANTE DEL SERVICIO

|  |  |  |
| --- | --- | --- |
| **Nombre** | **Puesto** | **Firma** |
| Horacio Alemán Alcántara | SubDireccion de Sistemas de Proteccion de Datos |  |

## INTRODUCCIÓN

Este informe técnico ofrece un análisis detallado de las vulnerabilidades detectadas, clasificándolas según su nivel de gravedad y a su vez ofrece directrices concretas para su rectificación. La gestión proactiva de estas vulnerabilidades se revela como un pilar fundamental en la preservación de un entorno digital seguro y robusto ante las amenazas.

## ANTECEDENTES

Dado el creciente riesgo y la diversidad de vectores de ataques cibernéticos que amenazan la integridad, confidencialidad y disponibilidad de las aplicaciones e infraestructura tecnológica del Instituto, resulta importante realizar análisis de vulnerabilidades con base en buenas prácticas y estándares internacionales. El propósito principal es evaluar, dentro de un alcance definido, el grado de madurez de la seguridad de la información en las aplicaciones e infraestructura tecnológica del Instituto. Este enfoque estratégico permitirá identificar y abordar las debilidades de manera proactiva, asegurando la protección adecuada de nuestros activos digitales y de infraestructura tecnológica garantizando la integridad, continuidad y disponibilidad de nuestras operaciones.

## OBJETIVO

Proporcionar los resultados de las pruebas a fondo de los posibles riesgos considerando el nivel de impactos y amenazas a los cuales podrían estar expuestos los aplicativos y la infraestructura tecnológica, así como las acciones recomendadas para la mitigación de los riesgos identificados. Así mismo, en este documento se encontrará la descripción e interpretación de los resultados de las pruebas de vulnerabilidades realizadas al sistema «**Aplicación»** en formato técnico.

## ALCANCE

Los siguientes indicadores corresponden a las pruebas de vulnerabilidades ejecutadas en los siguientes días: **3**

Las pruebas fueron de tipo:

|  |  |
| --- | --- |
| **Tipo de Actividad** | **Selección** |
| Análisis de vulnerabilidades a servidor |  |
| Análisis de vulnerabilidades WEB | x |
| Análisis de vulnerabilidades a código |  |

**Tabla 1** Selección de servicio

Ejecutadas a la aplicación «**Aplicación»** con dirección IP «**IP de Aplicación»** y al aplicativo con la dirección «**URL de Aplicación».**

* **Análisis de vulnerabilidades a servidor**

Esta evaluación de seguridad tiene como finalidad obtener todas las vulnerabilidades expuestas por el servidor, los resultados son obtenidos del análisis de los servicios y puertos que el servidor tiene abiertos en la red, por ejemplo, un puerto que usa el servicio de administración remota del servidor, con el análisis ejecutado podremos identificar fallas de configuración o uso de versiones obsoletas y con ello alguna vulnerabilidad relacionada que represente un riesgo.

* **Análisis de vulnerabilidades WEB**

Esta evaluación está orientada a realizar pruebas de seguridad directamente en el aplicativo WEB solicitado, en las pruebas de penetración se puede lograr identificar algún componente del aplicativo WEB que pueda representar un riesgo por una mala configuración, una versión obsoleta o con alguna vulnerabilidad reconocida la cual al ser explotada se convierta en un impacto para la organización.

* **Análisis de vulnerabilidades a código**

Esta evaluación de análisis estático de código fuente está orientada a realizar pruebas de seguridad directamente en el código de la aplicación en donde se puede lograr identificar algún componente que pueda representar un riesgo por una mala configuración o con alguna vulnerabilidad reconocida la cual al ser explotada se convierta en un impacto para la organización.

## REPORTE TÉCNICO DE HALLAZGOS

En la siguiente sección se enumeran y detallan las vulnerabilidades encontradas durante las diferentes fases de la evaluación, esta sección ofrece una amplia visión y descarta falsos positivos.

**Análisis de vulnerabilidades WEB**

A continuación, se presenta a detalle los hallazgos en relación a las pruebas ejecutadas a la aplicación WEB.

**Vulnerabilidades identificadas**

Durante el análisis de vulnerabilidades realizado a la aplicación, se identificó lo siguiente:

|  |
| --- |
| **Total de vulnerabilidades identificadas:** |
| «Total de vulnerabilidades» |

La siguiente gráfica proporciona una visión general de la postura de seguridad actual mostrando la cantidad de vulnerabilidades identificadas y catalogadas según su severidad[[1]](#footnote-2). Lo que permite identificar un nivel riesgo aproximado, dimensionar y priorizar las acciones correctivas.

**Detalles de vulnerabilidades**

**{{Sección de tablas de vulnerabilidades}}**

## RECOMENDACIONES

El documento adjunto (Archivo en formato Excel) se encuentra el registro detallado de cada vulnerabilidad identificada en las pruebas de seguridad, tiene como objetivo apoyar al equipo técnico del aplicativo afectado, cada registro cuenta con la información necesaria para identificar el objeto afectado, su ubicación, información sobre la vulnerabilidad y su solución, dentro de este archivo, se encuentran los siguientes puntos detallados:

* Nombre de la vulnerabilidad.
* Riesgo de la vulnerabilidad.
* Descripción de la vulnerabilidad.
* CVE de la vulnerabilidad (en caso de haber alguno asociado).
* URL del apartado vulnerable.
* Puerto.
* Solución de la vulnerabilidad.
* Referencias de apoyo.

## FORMATO Y ESTRUCTURA DE DESCRIPCIÓN DE VULNERABILIDADES

Para cada vulnerabilidad identificada en este informe, se ha definido un modelo de representación de la información, con la estructura mostrada a continuación:

|  |  |  |
| --- | --- | --- |
| **Nombre de la vulnerabilidad** | | **SEVERIDAD C.V.S.S. BASE** |
| **DESCRIPCIÓN** | Descripción de la vulnerabilidad en el sistema detallada de la de manera general redactada desde un punto de vista técnico. | |
| **PROPUESTA DE REMEDIACIÓN** | Descripción de las acciones y medidas recomendadas para abordar y corregir la vulnerabilidad identificada en el sistema, con el objetivo de mitigar o eliminar los riesgos asociados y fortalecer la seguridad de la infraestructura tecnológica. | |
| **REFERENCIAS** | 1. Se utiliza el estilo de referencia IEEE para referencias consultadas manualmente, comúnmente empleado en ámbitos como la ingeniería, tecnología y ciencias de la computación. Si se usan las referencias empleadas en las herramientas usadas, tan solo irán numeradas. 2. Autor(es) del sitio web. "Título del sitio web". Nombre del sitio web o dominio. Disponible en: URL. Accedido en: fecha. 3. Ejemplo: https://my.f5.com/manage/s/article/K95208524 | |
| **SISTEMAS O RUTAS AFECTADOS** | * Ruta específica en donde se encuentra la vulnerabilidad. Ejemplo: http://www.example.com:80/page/index.html * Sistema afectado expresado en formato de identificador uniforme de recursos (URI) estándar RFC 3986. Esquema o protocolo de acceso (por ejemplo, ftp:), Autoridad (por ejemplo, //www.example.com), Ruta (por ejemplo, /domains/example), Consulta (por ejemplo, ?clave=valor), y Fragmento (por ejemplo, #vista). Ejemplo: ftp://example.com:21 | |
| **DETALLE DE PRUEBAS DE SEGURIDAD** | | |
| Se presenta la evidencia de la prueba realizada, incluyendo la salida de la herramienta de detección y las imágenes que respalden la descripción de la vulnerabilidad. El objetivo principal es describir la explotación de la vulnerabilidad para facilitar el entendimiento al responsable del sistema o del activo.  Por ejemplo: La prueba de la vulnerabilidad consistió en la detección de la siguiente respuesta al interactuar con el sistema:   |  | | --- | | «SalidaDeHerramienta» | | | |

## DESCRIPCIÓN DE LAS SEVERIDADES

Para la evaluación de la severidad[[2]](#footnote-3), se emplea la siguiente categorización:

|  |  |
| --- | --- |
| **Colorimetría** | **Criticidad** |
|  | **CRÍTICA:** Severidad de vulnerabilidades que, al ser explotadas mediante diversas técnicas, permiten al atacante comprometer de manera crucial la operación del equipo, sistema, aplicativo o módulo. Estas vulnerabilidades tienen una puntuación C.V.S.S. base y general de 9.0 a 10.0. |
|  | **ALTA:** Severidad de vulnerabilidades que, al ser explotadas mediante diversas técnicas, permiten al atacante comprometer de manera grave la operación del equipo, sistema, aplicativo o módulo. Estas vulnerabilidades pueden ser explotadas fácilmente por un atacante poniendo en riesgo los activos de la empresa. Su puntuación C.V.S.S. base y general es de 7.0 a 8.9. |
|  | **MEDIA:** Severidad de vulnerabilidades que, al ser explotados mediante diversas técnicas, permiten al atacante comprometer de manera parcial el aplicativo. Su puntuación C.V.S.S. base y general es de 4.0 a 6.9. |
|  | **BAJA:** Severidad de vulnerabilidades que al ser explotadas y usados para obtener más información del objetivo. Su puntuación C.V.S.S. base y general es de 0.1 a 3.9. |
|  | **INFORMATIVA:** Notificaciones de sistema que no representan una vulnerabilidad, son de carácter informativo de algún puerto o servicio descubierto durante la aplicación de la prueba. Su puntuación C.V.S.S. base y general es nulo es decir es 0.0. |

## DEFINICIONES

Para facilitar la lectura y comprensión de este procedimiento, se contemplarán las siguientes definiciones:

|  |  |
| --- | --- |
| **Concepto** | **Definición** |
| Riesgo | Es la probabilidad de que una amenaza se materialice sobre un activo de información. |
| Amenaza | Es la causa potencial de un incidente no deseado, el cual puede resultar en un daño a un sistema de información u organización. |
| Vector de ataque | Método que utiliza un atacante al intentar obtener acceso ilegítimo a un sistema. |
| Ataque | Acción de tratar de traspasar los controles de seguridad en un sistema de información. |
| Análisis de vulnerabilidades | Es el proceso de identificación, estudio e interpretación de las fallas o debilidades de un sistema. |
| Control de seguridad | Preservación de la confidencialidad, integridad y disponibilidad de la información. |
| Falso positivo | Cuando se detecta una vulnerabilidad inexistente. |
| Falso negativo | Cuando no se detecta una vulnerabilidad existente |
| Vulnerabilidad | La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. |
| Puertos | Canal por el cual se expone un servicio. |
| Servicios | Programa que ofrece una interacción por medio de un puerto. |
| Análisis estático | El análisis estático es el análisis automatizado del código fuente sin ejecutar la aplicación. |
| Código fuente | Todo el texto legible por un ser humano y redactado en un lenguaje de programación determinado. |
| Explotación de una vulnerabilidad | Ejecución de técnicas especializadas aprovechando la vulnerabilidad de un sistema para obtener acceso a la información. |
| CVE | Identificador único que le es asignado a una vulnerabilidad para ser clasificada de forma global. |
| URL | Dirección WEB de una aplicación para ser visualizada a través de un navegador WEB. |
| NFS | NFS es un protocolo que permite acceder y compartir archivos entre equipos de una misma red. Conoce sus versiones, ventajas, usos y cómo usarlo en Windows con Samba. |

**Tabla 2** Definiciones

## MARCO METODOLÓGICO

El estudio de análisis de vulnerabilidades tiene como finalidad identificar las debilidades, huecos y áreas de oportunidad en materia de seguridad de la información a las que está expuesta la infraestructura tecnológica, identificando el origen de la vulnerabilidad (producto de la deficiencia en la implementación del control de seguridad), y emitiendo las recomendaciones pertinentes para su mitigación.

Los ciclos de prueba se dividen en tres etapas: análisis inicial de vulnerabilidades, Retest 1 y Retest 2. A continuación, se enumeran las actividades realizadas en cada ciclo de prueba:

1. La dirección URL se obtiene tras recibir una solicitud de pruebas de seguridad por correo electrónico o bien por la planeación del análisis de seguridad programados.
2. Se notifica por correo electrónico el inicio de las actividades de evaluación de seguridad de la aplicación.
3. Las pruebas de seguridad se llevan a cabo de la siguiente manera:
   1. Se realiza un análisis exhaustivo de los sistemas mediante técnicas manuales y automatizadas. Para evaluar aplicaciones e infraestructuras, se podrán utilizar herramientas licenciadas como Nessus Expert, entre otras. Las pruebas manuales se analizarán con el uso de proxies como Burp Suite y ZAP Proxy. Aunque estas son las herramientas principales, también se usan herramientas adicionales de la suite Kali Linux, como Dirb, Nikto, Nuclei, entre otras.
   2. Durante este proceso, se analizan e identifican riesgos relacionados vulnerabilidades, debilidades y configuraciones inseguras en la aplicación.
   3. Se descartan falsos positivos y se analizan los resultados obtenidos de herramientas de aplicación, scripts desarrollados y solicitudes de protocolo directas.
4. Se envía por correo electrónico la notificación de fin de las actividades, así como él envió de resultados mediante reportes.

Como parte de la metodología empleada para la clasificación de Vulnerabilidades se utiliza la métrica provista por el CVSS (Common Vulnerability Scoring System) en su versión 3.1.

Grupo Base. Comprende vulnerabilidades que se mantienen constantes con el tiempo y en los entornos de los usuarios, los aspectos en que se basa son:

* El tipo de Vector de Acceso que se requiere para que la vulnerabilidad sea explotada (Local o Acceso a la red).
* El nivel de complejidad que se requiere explotar la vulnerabilidad (Alto, Medio Bajo).
* El nivel de autenticación requerido para explotar la vulnerabilidad.
* El impacto de exponer información sensible si es explotada la vulnerabilidad.
* El impacto de la integridad de la información si es explotada la vulnerabilidad.
* El impacto de la disponibilidad de la información si es explotada la vulnerabilidad.

Las ecuaciones y los valores de las variables para cada uno de los grupos pueden ser consultados en: <https://www.first.org/cvss/user-guide>

1. *El recuento de vulnerabilidades se realiza identificando cada incidencia de forma única, considerando la vulnerabilidad específica, la dirección IP o el nombre del activo afectado o ruta y el puerto o servicio expuesto. Por ejemplo, dos instancias de un mismo tipo de vulnerabilidad en una aplicación, pero en puertos diferentes se registran como vulnerabilidades separadas, en el caso de aplicaciones se cuentan rutas completas cuando no está presente el dominio principal como afectación.* [↑](#footnote-ref-2)
2. *La criticidad de las vulnerabilidades mencionadas en este reporte, se cataloga de acuerdo con el escenario evaluado empleando las metodologías descritas en la sección correspondiente, por lo tanto, esta puede variar respecto al criterio del cliente al igual que el nivel de prioridad para su remediación.* [↑](#footnote-ref-3)