

**SSIFO15-03**

INFORME EJECUTIVO DE ANÁLISIS DE VULNERABILIDADES

**Información General del Documento**

|  |  |  |  |
| --- | --- | --- | --- |
| **Documento** | **Clave** | **Documento** | **Medio** |
|  | SSIFO15 | Informe ejecutivo 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 | 16/08/2024 | Se actualiza diseño de encabezado y pie de página.  Se realizan correcciones ortográficas.  Se actualiza estructura del documento. |

**ÍNDICE**

[1. SOLICITANTE DEL SERVICIO 4](#_Toc174703680)

[2. INTRODUCCIÓN 4](#_Toc174703681)

[3. ANTECEDENTES 4](#_Toc174703682)

[4. OBJETIVO 4](#_Toc174703683)

[5. ALCANCE 4](#_Toc174703684)

[6. RESULTADOS GENERALES 5](#_Toc174703685)

[7. DETALLES DE LAS VULNERABILIDADES 6](#_Toc174703686)

[8. DESCRIPCIÓN DE LAS SEVERIDADES 8](#_Toc174703687)

[9. CATEGORIZACIÓN DE VULNERABILIDADES 9](#_Toc174703688)

[10. DEFINICIONES 9](#_Toc174703689)

[11. MARCO METODOLÓGICO 10](#_Toc174703690)

1. SOLICITANTE DEL SERVICIO

|  |  |  |
| --- | --- | --- |
| **Nombre** | **Puesto** | **Firma** |
|  |  |  |

1. INTRODUCCIÓN

Este informe ejecutivo 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.

1. 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.

1. 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»**.

1. 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.

1. RESULTADOS GENERALES

A continuación, se presenta a detalle los hallazgos en relación a las pruebas ejecutas al servidor:

**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.

Las vulnerabilidades identificadas en este análisis se pueden categorizar enlos siguientes tipos:

1. 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. |

1. CATEGORIZACIÓN DE VULNERABILIDADES

Las vulnerabilidades en el actual reporte se consideran según sus implicaciones y riesgos asociados en las siguientes categorías:

* **Actualización**: Falta de aplicación de las últimas actualizaciones y parches críticos que corrigen vulnerabilidades conocidas.
* **Configuración**: Errores en la configuración de sistemas, aplicaciones o servicios que pueden exponer información sensible o permitir accesos no autorizados.
* **Código inseguro**: Presencia de código que contiene vulnerabilidades conocidas o no estándares de codificación segura, facilitando posibles explotaciones.
* **Antimalware desactualizado**: Falta de actualización de las firmas y motor de detección de antivirus y antimalware, comprometiendo la capacidad de defensa contra amenazas actuales.
* **Ausencia de parches de seguridad**: Omisión en la aplicación de actualizaciones críticas diseñadas para corregir vulnerabilidades específicas y proteger contra ataques.
* **Sistema operativo sin soporte**: Uso de versiones de sistemas operativos que han dejado de recibir actualizaciones de seguridad, dejando el sistema vulnerable a exploits conocidos.
* **Versión desactualizada de software**: Empleo de versiones obsoletas de aplicaciones o software, que pueden contener vulnerabilidades conocidas y no corregidas.

1. 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

1. 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 la planeación de 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 envia por correo electrónico la notificación de fin de las actividades asi como el envio 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>

Los ciclos de prueba están planeados en tres etapas: el análisis inicial de vulnerabilidades, Retest 1 y Retest 2.

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 un sistema, 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 severidad 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)