minsait

An Indra company

INFORME DE VULNERABILIDADES SISTEMAS MISIONALES

MINISTERIO DE EDUCACIÓN NACIONAL

Octubre de 2022

minsait

MINISTERIO DE EDUCACIÓN NACIONAL

Índice

Índice de tablas

Índice de ilustraciones

Índice de gráficos

1 OBJETIVO

Presentar el resultado del escaneo y análisis de vulnerabilidades realizado durante la primera semana del mes de octubre del 2022 que corresponde con lo acordado en el plan de trabajo de seguridad informática aprobado con el Radicado No.2022-EE-243860, sobre las Aplicaciones Misionales del Ministerio de Educación Nacional registradas en el inventario de aplicaciones en su versión 127 que corresponde a la versión liberada al inicio del mes de octubre.

2 ALCANCE

El presente informe muestra el resultado de un escaneo de vulnerabilidades ejecutado sobre la infraestructura que soporta las aplicaciones catalogadas como Sistemas Misionales, según lo acordado con el Ministerio de Educación, y que son registradas en el inventario de aplicaciones del Ministerio de Educación Nacional para sus ambientes de certificación y de producción. Se tomó como referencia la versión más reciente del inventario de aplicaciones que para la primera semana del mes de octubre, correspondía a la versión 127. Estos sistemas se relacionan en la hoja “Sistemas” del archivo anexo “Sistemas_Trimestre_7.xlsx”, en donde se aclara además si la aplicación cuenta con ambiente de certificación y producción.

3 METODOLOGÍA

Una vez definido el alcance, se procedió a obtener las IPs que soportan el servicio de las aplicaciones de acuerdo al inventario de aplicaciones en su versión 127. A cada aplicación se le realizó un escaneo de vulnerabilidades a nivel de servidor(es) de aplicación y servidor(es) de bases de datos en su respectivo ambiente. Las aplicaciones evaluadas son entonces las siguientes:

Código Aplicación	Sigla Aplicación	Nombre del sistema
APP002	CNA	Sistema de Aseguramiento de Alta Calidad de Educacion Superior
APP003	CONVSUP	Convalidaciones Educación Superior (TMS)
APP005	EVI	Aplicacion para la Evaluacion Institucional y Reporte Financiero para Establecimientos Privados PBM
APP010	RRHH	Sistema de Informacion Humano (Secretarias)
APP012	SIET	Sistema de Informacion de la Educacion para el Trabajo y el desarrollo Humano
APP014	SIMAT	Sistema de Matriculas Estudiantil de Educacion Basica y Media
APP015	SIMPADE	Sistema de Informacion para el Monitoreo,la Prevencion y el Analisis de la Desercion Escolar
APP017	SINEB	Sistema de Informacion Nacional de Educacion Basica y Media.
APP018	SIPI	Sistema de Informacion de Primera Infancia
APP019	SNIES	Sistema Nacional de Informacion de la Educacion Superior
APP022	SAC V1	Secretarias de Educacion Atencion al Ciudadano
APP023	SACES	Sistema de Aseguramiento de la Calidad en Educacion Superior
APP029	SIPTA	Sistema de Informacion del Programa Todos a Aprender
APP030	CEBYM	Convalidaciones de Educación Básica y Media
APP033	SIET Consultas publicas	Sistema de Informacion de la Educacion para el Trabajo y el Desarrollo Humano (Consultas publicas)
APP034	SSDIPI	Sistema de Seguimiento al Desarrollo Integral de la Primera Infancia SSDIPI (Sistema de Seguimiento Niño a Niño)

Código Aplicación	Sigla Aplicación	Nombre del sistema
APP047	SIMAT BI13A y SIMPADE	Sistema de Matriculas Estudiantil de Educacion Basica y Media (BODEGA DATOS)
APP052	SEGUIMIENTO JU	Jornada Unica de seguimiento
APP054	SIACET	Sistema de Informacion para el Aseguramiento de la Calidad de la Educacion para el Trabajo y el Desarrollo Humana
APP055	HECAA	Herramienta de cargue de archivos
APP073	SIISSE	Sistema de informacion de inversion del sector solidario en educacion (COOPERATIVAS)
APP074	SIISSE HIST	Sistema de informacion de inversion del sector solidario en educacion (COOPERATIVAS HIST)
APP080	CONVSUPCH	Sistema de CONVALIDACIONES (CH)
APP084	PARES	Sistema de Banco de Pares
APP103	EMC	Elijo mi Colegio
APP104	SIPTA2 WEB	Sistema de Informacion del Programa Todos a Aprender (Version 2)
APP107	LALUPA	PROCESOS SANCIONATORIOS IES (LA LUPA)
APP111	CIER	Censo de Infraestructura Educativa Regional
APP113	SISMA	SISTEMA MAESTRO
APP114	SPADIES	Sistema para la Prevencion y Analisis de la Desercion en las Instituciones de Educacion Superior (NUEVO)
APP118	LDAP PCA	Protocolo ligero de acceso a directorios Colombia Aprende
APP119	VUMEN CRL	Ventanilla Unica de Tramites -Certificados de Representación Legal y de programa e idoneidad
APP120	VUMEN RE	Ventanilla Unica de Tramites - Reformas Estatutarias
APP121	VUMEN IR	Ventanilla Unica de Tramites - Inscripción de Rectores
APP125	SIFSE NVO	Sistema de Informacion de Fondos de Servicios Educactivos (Nuevo)
APP126	CNC	Concurso Nacional de Cuento
APP155	SINEB PLANTAS	Sistema de Informacion Nacional de Educacion Basica y Media (PLANTAS)
APP158	MOODLEPCA	Campus Virtual Colombia Aprende
APP160	CAS	CAS SERVER
APP174	DELREP	Delegados y Representantes
APP230	SICSUP	Convocatorias Superior
APP233	SIA3	Sistema de Autenticacion, Autorizacion y Auditoria
APP234	NUEVO SIGCE	Sistema de Información de Gestión de la Calidad Educativa (NVO)
APP237	SIUCE	Sistema de Información Unificado de Convivencia Escolar
APP244	SAC V2	Nuevo SAC - Secretarias
APP251	SUPSA	SUPERATE CON EL SABER
APP253	CATALOGO DE CONTENIDOS EDUCATIVOS	CATALOGO DE LA OFERTA NACIONAL DE RECURSOS DIGITALES (RED APRENDE MOVIL)
APP256	CONVALIDA	FORMULARIO CONVALIDA (BIZAGI)
APP263	SUPERATE	SUPERATE (Nueva Versión)
APP264	Tejido maestro	Sistema de información y distribución de maestros
APP269	THE B1	BETHEONE Challenge
APP274	CNE	CONCURSO NACIONAL DE ESCRITURA
APP276		Bienestar Docente
APP277	Nuevo Saces RC	Registro Calificado - NUEVO SACES

Código Aplicación	Sigla Aplicación	Nombre del sistema
APP322	GESPAR	Gestión de Pares
APP331	CNA	NUEVO CNA

Tabla 1. Aplicaciones Misionales registradas en el inventario de aplicaciones en su versión 127.

Los datos correspondientes a las IPs que serán objeto del escaneo se pueden verificar en la hoja "Infraestructura Sistemas" del archivo anexo "Sistemas_Trimestre_7.xlsx" en las columnas D, E, F y G. Luego de identificadas las IPs, se procedió a ejecutar el escaneo de vulnerabilidades. Este proceso se realizó utilizando el software Nessus, el cual se encuentra instalado en un equipo físico de INDRA que cuenta con comunicación a la infraestructura del ministerio.

El análisis se realizó sin usuario autenticado y sin vectores de evaluación que generaran denegación de servicio. La calificación de las vulnerabilidades se realizó directamente por la herramienta de escaneo de vulnerabilidades. De igual manera, el insumo para la mitigación de vulnerabilidades es el mismo reporte de la herramienta Nessus la cual indica la descripción y posible solución de cada una de ellas.

La cantidad de vulnerabilidades detectadas por cada IP se registran por aplicación de acuerdo al escenario evaluado en las últimas cuatro hojas del anexo "Sistemas_Trimestre_7.xlsx" mientras que sobre el anexo "Vulnerabilidades_Trimestre_7.xlsx", se registra el total de vulnerabilidades detectadas por la herramienta de NESSUS añadiendo en su última columna la aplicación que se vería afectada.

En la siguiente sección del informe, se registran las vulnerabilidades y recomendaciones por cada vulnerabilidad encontrada en cada escenario, relacionando el código de la aplicación en la que fue detectada.

4 EJECUCIÓN

Los escaneos realizados se dividieron en 4 escenarios y sus resultados son mostrados de la siguiente forma:

- Escaneo de Vulnerabilidades a Servidor de Aplicación Certificación: Escaneo a las IPs de los servidores en los que están soportadas las aplicaciones en el ambiente de certificación.

- Escaneo de Vulnerabilidades a Servidor de Bases de Datos de Certificación: Escaneo a las IPs de los servidores en los que están las bases de datos de las aplicaciones en el ambiente de certificación.

- Escaneo de Vulnerabilidades a Servidor de Aplicación Producción: Escaneo a las IPs de los servidores en los que están soportadas las aplicaciones en el ambiente de producción.

- Escaneo de Vulnerabilidades a Servidor de Bases de Datos de Producción: Escaneo a las IPs de los servidores en los que están las bases de datos de las aplicaciones del ambiente de producción.

Sobre las últimas cuatro hojas del anexo "Sistemas_Trimestre_7.xlsx" se contabilizan las vulnerabilidades encontradas por cada aplicación de acuerdo a los cuatro escenarios anteriormente mencionados, mientras que en el anexo denominado "Vulnerabilidades_Trimestre_7.xlsx", se encuentran los resultados tabulados de la herramienta NESSUS. Allí vale aclarar que los resultados están dados en función de la IP analizada, por lo cual existe una aparente disparidad entre la sumatoria de vulnerabilidades en los dos anexos mencionados.

Esta situación se debe al hecho de que un servidor puede prestar un servicio a diferentes sistemas de información, por lo cual, la vulnerabilidad de un servidor se vería reflejada sobre los diferentes sistemas de información con el cual tenga relación.

Por ejemplo, los sistemas con código APP119-VUMEN CRL, APP120-VUMEN RE y APP121-VUMEN IR comparten la misma infraestructura y su servidor de aplicación de producción tiene la IP 192.168.210.78 (E1APVUMEN01). Sobre esta IP se detectaron dos vulnerabilidades de severidad media. Por ello en la hoja

“Producción-App” del anexo “Sistemas_Trimestre_7.xlsx”, al validar la información de dichos sistemas se tiene la siguiente información:

Código Aplicación	Sigla Aplicación	CRITICA	ALTA	MEDIO	BAJA
APP119	VUMEN CRL	0	0	2	0
APP120	VUMEN RE	0	0	2	0
APP121	VUMEN IR	0	0	2	0

Ilustración 1: Cantidad de Vulnerabilidades detectadas para las aplicaciones APP119, APP120 y APP121

Una sumatoria de vulnerabilidades a partir de la representación de estos sistemas, arrojaría un total de 6 vulnerabilidades, cuando en realidad son dos las vulnerabilidades identificadas como se puede ver en el anexo “Vulnerabilidades_Trimestre_7.xlsx” al filtrar por la IP o nombre del servidor, en el cual se obtiene el siguiente resultado:

Escenario	Vulnerabilidad	IP
Producción Aplicación	TLS Version 1.0 Protocol Detection	192.168.210.78
Producción Aplicación	TLS Version 1.1 Protocol Deprecated	192.168.210.78

Ilustración 2: Cantidad de Vulnerabilidades detectadas sobre el servidor E1APVUMEN01-192.168.210.78.

Con lo cual, para este ejemplo, las vulnerabilidades que se deben remediar son dos, pero esta remediación se va a ver reflejado sobre tres diferentes sistemas de información y por consiguiente reduciría en seis las vulnerabilidades relacionadas a los sistemas cuando se realice su mitigación.

Sobre la columna aplicación de este último anexo, también se puede realizar el filtro por la aplicación a través de su código o sigla y también por facilidad, en la hoja denominada “Compilado”, se puede buscar por el código de la aplicación para identificar las vulnerabilidades asociadas por severidad (y de acuerdo a cada escenario). Vale aclarar también que en los resultados tabulados del NESSUS hay una variable adicional que corresponde al puerto detectado, por lo cual, si un servidor expone una misma vulnerabilidad sobre dos puertos distintos, aparecerá entonces dos veces la vulnerabilidad asociada al mismo servidor.

A continuación, se detallan las vulnerabilidades encontradas por cada escenario por criticidad en donde se realiza una descripción de las mismas y se registra la solución a la vulnerabilidad y también la(s) aplicación(es) en las que se detectó.

4.1 SITUACIÓN ACTUAL VULNERABILIDADES EN SERVIDORES DE APLICACIÓN EN CERTIFICACIÓN

A partir del inventario de aplicaciones, y de acuerdo a la columna “D” en la hoja “Infraestructura Sistemas” del archivo anexo “Sistemas_Trimestre_7.xlsx” se identifican los servidores en el cual está instalada la aplicación en el ambiente de certificación. El resultado obtenido por cada IP se tabula en la hoja “Certificación-App” del archivo anexo indicado anteriormente, en el que se muestra el resultado de las vulnerabilidades encontradas por aplicación de acuerdo a la criticidad de esta. El nivel de la criticidad está dado por las categorías crítica, alta, media y baja. En la siguiente tabla se registran las aplicaciones en las que se encontró alguna vulnerabilidad bajo este escenario:

Código Aplicación	Sigla Aplicación	CRITICA	ALTA	MEDIO	BAJA
APP002	CNA	0	1	1	0
APP014	SIMAT	1	0	0	0
APP017	SINEB	0	0	1	0
APP022	SAC V1	0	0	1	0
APP055	HECAA	0	0	6	1

Código Aplicación	Sigla Aplicación	CRITICA	ALTA	MEDIO	BAJA
APP080	CONVSUPCH	0	1	1	0
APP103	EMC	0	0	4	0
APP104	SIPTA2 WEB	1	0	0	0
APP111	CIER	1	6	6	1
APP114	SPADIES	2	0	0	0
APP155	SINEB PLANTAS	1	0	0	0
APP158	MOODLEPCA	0	0	3	0
APP174	DELREP	0	7	28	0
APP233	SIA3	1	0	4	0
APP237	SIUCE	1	0	0	0
APP251	SUPSA	0	0	1	0
APP256	CONVALIDA	0	1	4	0
APP263	SUPERATE	0	0	2	0
APP269	THE B1	0	2	0	0
APP274	CNE	0	2	12	0

Tabla 2. Aplicaciones Misionales en las que se encontró alguna vulnerabilidad sobre los servidores de aplicación del ambiente de certificación de los sistemas misionales

Las vulnerabilidades detectadas sobre este escenario están explicadas en las siguientes secciones, en donde se indica además el código de la aplicación donde se encontró la vulnerabilidad.

4.1.1 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES CRÍTICAS

Vulnerabilidad	Linux Multiple statd Packages Remote Format String
Riesgo	Crítico
Descripción	El servicio de statd puede desactivarse con un ataque de cadena de formato; ahora debe reiniciarse manualmente. Esto significa que un atacante puede ejecutar código arbitrario gracias a un error en este demonio.
Solución	Actualice a la última versión de rpc.statd.
Código Aplicaciones Afectadas	APP114-SPADIES

Vulnerabilidad	Oracle GlassFish Server 3.1.2.x < 3.1.2.15 Multiple Vulnerabilities (July 2016 CPU)
Riesgo	Crítico
Descripción	Según su número de versión autoinformado, el servidor Oracle GlassFish que se ejecuta en el host remoto es 3.1.2.x anterior a 3.1.2.15.
Solución	Actualice a Oracle GlassFish Server versión 3.1.2.15 o posterior
Código Aplicaciones Afectadas	APP111-CIER

Vulnerabilidad	Oracle WebLogic Unsupported Version Detection
Riesgo	Crítico
Descripción	Según la versión detectada, la instalación de Oracle WebLogic que se ejecuta en el host remoto ya no es soportada. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución	Actualice a una versión de Oracle WebLogic que actualmente sea compatible.
Código Aplicaciones Afectadas	APP014-SIMAT, APP104-SIPTA2 WEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP233-SIA3, APP237-SIUCE

Tabla 3. Vulnerabilidades críticas sobre los servidores de aplicación del ambiente de certificación de los sistemas misionales

4.1.2 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES ALTAS

Vulnerabilidad (x 6)	- Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities - Apache Tomcat 7.0.0 < 7.0.94 Remote Code Execution Vulnerability (Windows) - Apache Tomcat 7.0.41 < 7.0.90 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.57 Multiple Vulnerabilities (POODLE) - Apache Tomcat 7.0.x < 7.0.70 / 8.0.x < 8.0.36 / 8.5.x < 8.5.3 / 9.0.x < 9.0.0.M8 Denial of Service
Riesgo	Alto
Descripción	El servidor Apache Tomcat se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a Apache Tomcat versión 6.0.48, 7.0.100, 8.036, 8.5.51, 9.0.31 o posterior.
Código Aplicaciones Afectadas	APP174-DELREP

Vulnerabilidad	Apache HTTP Server Byte Range DoS
Riesgo	Alto
Descripción	La versión de Apache HTTP Server que se ejecuta en el host se ve afectada por una vulnerabilidad de denegación de servicio. Hacer una serie de solicitudes HTTP con rangos superpuestos en los encabezados de solicitud Range o Request-Range puede resultar en el agotamiento de la memoria y la CPU. Un atacante remoto no autenticado podría aprovechar esto para que el sistema no responda. El código de explotación está disponible públicamente.
Solución	Actualice a Apache httpd 2.2.21 o posterior. Alternativamente, aplique una de las soluciones en los avisos de Apache para CVE-2011-3192. La versión 2.2.20 solucionó el problema, pero también introdujo una regresión. Si el host ejecuta un servidor web basado en Apache httpd, comuníquese con el proveedor para obtener una solución.
Código Aplicaciones Afectadas	APP002-CNA, APP080-CONVSUPCH

Vulnerabilidad	Drupal 8.9.x < 8.9.16 / 9.x < 9.0.14 / 9.1.x < 9.1.9 Drupal Vulnerability (SA-CORE-2021-003)
Riesgo	Alto
Descripción	Según la versión detectada, la instancia de Drupal que se ejecuta en el servidor es 8.9.x anterior a 8.9.16, 9.x anterior a 9.0.14 o 9.1.x anterior a 9.1.9. El núcleo de Drupal utiliza la biblioteca CKEditor de terceros. Esta biblioteca tiene un error al analizar HTML que podría provocar un ataque XSS. CKEditor 4.16.1 y versiones posteriores incluyen la corrección. Los usuarios de la biblioteca CKEditor a través de medios distintos al núcleo de Drupal deben actualizar su código de terceros (por ejemplo, el módulo WYSIWYG para Drupal 7). La política del equipo de seguridad de Drupal es no alertar sobre problemas que afecten a bibliotecas de terceros, a menos que se envíen con el núcleo de Drupal. Consulte DRUPAL-SA-PSA-2016-004 para obtener más detalles. Este problema se mitiga por el hecho de que solo afecta a los sitios con CKEditor habilitado. (SA-CORE-2021-003)
Solución	Upgrade to Drupal version 8.9.16 / 9.0.14 / 9.1.9 or later.
Código Aplicaciones Afectadas	APP274-CNE

Vulnerabilidad	Microsoft ASP.NET MS-DOS Device Name DoS
Riesgo	Alto

Descripción	El servidor web que se ejecuta en el host parece estar usando Microsoft ASP.NET y puede verse afectado por una vulnerabilidad de denegación de servicio. Solicitar una URL que contenga un nombre de dispositivo MS-DOS puede hacer que el servidor web deje de responder temporalmente. Un atacante podría solicitar repetidamente estas URL, lo que resultaría en una denegación de servicio.
Solución	Utilice un filtro ISAPI para bloquear solicitudes de URL con nombres de dispositivo MS-DOS.
Código Aplicaciones Afectadas	APP256-CONVALIDA, APP269-THE B1

Vulnerabilidad (x2)	- Oracle GlassFish Server 2.1.1.x < 2.1.1.30 / 3.0.1.x < 3.0.1.15 / 3.1.2.x < 3.1.2.16 Multiple Vulnerabilities (January 2017 CPU) - Oracle GlassFish Server 3.0.1.x < 3.0.1.17 / 3.1.2.x < 3.1.2.18 (October 2017 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos se ve afectado por múltiples vulnerabilidades en varios de sus componentes.
Solución	Actualice a Oracle GlassFish Server versión 2.1.1.30, 3.0.1.17 o 3.1.2.18 o posterior como se indica en el aviso de actualización de parche crítico de Oracle de enero y octubre de 2017.
Código Aplicaciones Afectadas	APP111-CIER

Vulnerabilidad (x4)	- Oracle GlassFish Server Multiple Vulnerabilities (April 2015 CPU) (POODLE) - Oracle GlassFish Server Unspecified Vulnerability (January 2015 CPU) - Oracle GlassFish Server Multiple Vulnerabilities (July 2014 CPU) - Oracle GlassFish Server Multiple Vulnerabilities (July 2015 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos se ve afectado por múltiples vulnerabilidades en varios de sus componentes.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de acuerdo a la fecha de publicación.
Código Aplicaciones Afectadas	APP111-CIER

Vulnerabilidad	Unsupported Web Server Detection
Riesgo	Alto
Descripción	Según la versión detectada, el servidor web está obsoleto y su proveedor ya no lo mantiene. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, puede contener vulnerabilidades de seguridad.
Solución	Elimine el servidor web si ya no es necesario. De lo contrario, actualice a una versión compatible si es posible o cambie a otro servidor.
Código Aplicaciones Afectadas	APP174-DELREP

Tabla 4. Vulnerabilidades altas sobre los servidores de aplicación del ambiente de certificación de los sistemas misionales

4.1.3 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES MEDIAS

Vulnerabilidad	Apache HTTP Server httpOnly Cookie Information Disclosure
Riesgo	Medio
Descripción	La versión del servidor HTTP Apache que se ejecuta en el host se ve afectada por una vulnerabilidad de divulgación de información. Enviar una solicitud con encabezados HTTP lo suficientemente largos como para exceder el límite del servidor hace que el servidor web responda con un HTTP 400. De forma predeterminada, el encabezado y el valor HTTP ofensivos se muestran en la página de error

	400. Cuando se usa junto con otros ataques (por ejemplo, secuencias de comandos entre sitios), esto puede resultar en el compromiso de las cookies httpOnly.
Solución	Actualice a Apache versión 2.0.65 / 2.2.22 o posterior.
Código Aplicaciones Afectadas	APP002-CNA, APP080-CONVSUPCH

Vulnerabilidad	Apache mod_status /server-status Information Disclosure
Riesgo	Medio
Descripción	Un atacante remoto no autenticado puede obtener una descripción general de la actividad y el rendimiento del servidor web Apache remoto solicitando la URL '/estado-del-servidor'. Esta descripción general incluye información como los hosts actuales y las solicitudes que se procesan, la cantidad de trabajadores inactivos y solicitudes de servicio, y la utilización de la CPU.
Solución	Actualice los archivos de configuración de Apache para deshabilitar mod_status o restringir el acceso a hosts específicos.
Código Aplicaciones Afectadas	APP251-SUPSA

Vulnerabilidad	Apache Multiviews Arbitrary Directory Listing
Riesgo	Medio
Descripción	El servidor web Apache que se ejecuta en el host se ve afectado por una vulnerabilidad de divulgación de información. Un atacante remoto no autenticado puede explotar esto, enviando una solicitud manipulada, para mostrar una lista de un directorio remoto, incluso si existe un archivo de índice válido en el directorio. Para el servidor web Apache posterior a 1.3.22, revise la configuración del directorio de listas para evitar revelar información confidencial
Solución	Actualice a la versión de Apache 1.3.22 o posterior. Alternativamente, como solución alternativa, deshabilite Multiviews.
Código Aplicaciones Afectadas	APP022-SAC V1, APP263-SUPERATE

Vulnerabilidad (x25)	- Apache Tomcat < 7.0.67 Session Fixation - Apache Tomcat 6.0.16 < 6.0.50 / 7.0.x < 7.0.75 / 8.0.x < 8.0.41 / 8.5.x < 8.5.9 / 9.0.x < 9.0.0.M15 NIO HTTP Connector Information Disclosure - Apache Tomcat 6.0.x < 6.0.47 / 7.0.x < 7.0.72 / 8.0.x < 8.0.37 / 8.5.x < 8.5.5 / 9.0.x < 9.0.0.M10 Multiple Vulnerabilities - Apache Tomcat 6.0.x < 6.0.53 / 7.0.x < 7.0.77 / 8.0.x < 8.0.43 Pipelined Requests Information Disclosure - Apache Tomcat 7.0.0 < 7.0.104 Remote Code Execution - Apache Tomcat 7.0.0 < 7.0.107 Information Disclosure - Apache Tomcat 7.0.0 < 7.0.108 RCE - Apache Tomcat 7.0.0 < 7.0.85 Security Constraint Weakness - Apache Tomcat 7.0.0 < 7.0.91 Open Redirect Weakness - Apache Tomcat 7.0.41 < 7.0.79 Cache Poisoning Vulnerability - Apache Tomcat 7.0.x < 7.0.105 WebSocket DoS - Apache Tomcat 7.0.x < 7.0.53 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.54 XML Parser Information Disclosure - Apache Tomcat 7.0.x < 7.0.55 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.59 Security Manager Bypass - Apache Tomcat 7.0.x < 7.0.60 Multiple Vulnerabilities (FREAK) - Apache Tomcat 7.0.x < 7.0.65 / 8.0.x < 8.0.27 Directory Traversal - Apache Tomcat 7.0.x < 7.0.68 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.76 / 8.0.x < 8.0.42 / 8.5.x < 8.5.12 / 9.0.x < 9.0.0.M18 Improper Access Control - Apache Tomcat 7.0.x < 7.0.78 / 8.0.x < 8.0.44 / 8.5.x < 8.5.15 / 9.0.x < 9.0.0.M21 Remote Error Page Manipulation - Apache Tomcat 7.0.x < 7.0.81 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.82 / 8.5.x < 8.5.23 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.82 Multiple Vulnerabilities - Apache Tomcat 7.0.x < 7.0.88 Denial of Service - Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability

Riesgo	Medio
Descripción	La versión de Apache Tomcat detectada, se ve afectada por múltiples vulnerabilidades según lo especificado por los registros de cambios de las respectivas versiones corregidas.
Solución	Actualice a Apache Tomcat versión 7.0.108, 8.5.66, 9.0.46, 10.0.6 o posterior.
Código Aplicaciones Afectadas	APP174-DELREP

Vulnerabilidad	Apache Tomcat Default Files
Riesgo	Medio
Descripción	La página de error predeterminada, la página de índice predeterminada, los JSP de ejemplo y/o los servlets de ejemplo son instalados en el servidor Apache Tomcat. Estos archivos deben eliminarse, ya que pueden ayudar a un atacante a descubrir información sobre la instalación de Tomcat o el propio host.
Solución	Elimine la página de índice predeterminada y elimine el JSP y los servlets de ejemplo. Siga las instrucciones de Tomcat u OWASP para reemplazar o modificar la página de error predeterminada.
Código Aplicaciones Afectadas	APP174-DELREP

Vulnerabilidad	Apache Tomcat XSRF Token Disclosure
Riesgo	Medio
Descripción	El servidor web Apache Tomcat se ve afectado por una vulnerabilidad de divulgación de información en la página de índice de las aplicaciones Manager y Host Manager. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para obtener un token de falsificación de solicitud entre sitios (XSRF) válido durante la redirección emitida al solicitar /manager/ o /host-manager/. Este token puede ser utilizado por un atacante para construir un ataque XSRF.
Solución	Actualice a Apache Tomcat versión 7.0.68/8.0.32/9.0.0.M3 o posterior.
Código Aplicaciones Afectadas	APP174-DELREP

Vulnerabilidad (x6)	- Drupal 7.x < 7.73 / 8.8.x < 8.8.10 / 8.9.x < 8.9.6 / 9.0.x < 9.0.6 XSS (drupal-2020-09-16) - Drupal 7.x < 7.74 / 8.x < 8.8.11 / 8.9.x < 8.9.9 / 9.0.x < 9.0.8 RCE (SA-CORE-2020-012) - Drupal 7.x < 7.75 / 8.x < 8.8.12 / 8.9.x < 8.9.10 / 9.0.x < 9.0.9 Multiple Vulnerabilities (SA-CORE-2020-013) - Drupal 7.x < 7.78 / 8.9.x < 8.9.13 / 9.x < 9.0.11 / 9.1.x < 9.1.3 Directory Traversal (SA-CORE-2021-001) - Drupal 7.x < 7.80 / 8.9.x < 8.9.14 / 9.x < 9.0.12 / 9.1.x < 9.1.7 XSS (SA-CORE-2021-002) - Drupal 8.8.x < 8.8.10 / 8.9.x < 8.9.6 / 9.0.x < 9.0.6 Multiple Vulnerabilities (drupal-2020-09-16)
Riesgo	Medio
Descripción	Según la versión detectada, la instancia de Drupal que se ejecuta en el servidor web se ve afectada por múltiples vulnerabilidades.
Solución	Actualice a la versión de Drupal 7.80 / 8.8.12 / 8.9.14 / 9.0.9 / 9.1.7 o posterior.
Código Aplicaciones Afectadas	APP274-CNE

Vulnerabilidad (x4)	- JQuery 1.2 < 3.5.0 Multiple XSS - JQuery < 3.0.0 XSS - JQuery < 3.4.0 Object Prototype Pollution Vulnerability - JQuery 1.x < 1.12.0 / 2.x < 2.2.0 XSS
Riesgo	Medio
Descripción	Según la versión de JQuery alojada en el servidor web, se ve afectado por múltiples vulnerabilidades de secuencias de comandos entre sitios.
Solución	Actualice a JQuery versión 3.5.0 o posterior.

Código Aplicaciones Afectadas	APP103-EMC

Vulnerabilidad	Linux Kernel TCP Sequence Number Generation Security Weakness
Riesgo	Medio
Descripción	El kernel de Linux es propenso a una debilidad de seguridad relacionada con la generación de números de secuencia TCP. Los atacantes pueden aprovechar este problema para inyectar paquetes arbitrarios en las sesiones TCP mediante un ataque de fuerza bruta. Un atacante puede usar esta vulnerabilidad para crear una condición de denegación de servicio o un ataque de intermediario.
Solución	Comuníquese con el proveedor del sistema operativo para obtener una actualización/parche del kernel de Linux.
Código Aplicaciones Afectadas	APP017- SINEB

Vulnerabilidad (x3)	- Oracle GlassFish Embedded Server Vulnerabilities (January 2016 CPU) - Oracle GlassFish Server Multiple Vulnerabilities (October 2013 CPU) - Oracle GlassFish Server Unspecified Information Disclosure (October 2015 CPU)
Riesgo	Medio
Descripción	La versión de Oracle GlassFish Server que se ejecuta en el host se ve afectada por múltiples vulnerabilidades.
Solución	Actualice a Oracle GlassFish Server 3.0.1.13/3.1.2.13 o posterior como se indica en el aviso de actualización de parche crítico de Oracle de octubre de 2015.
Código Aplicaciones Afectadas	APP111-CIER

Vulnerabilidad (x3)	- Oracle GlassFish Server 3.1.2.x < 3.1.2.19 (October 2018 CPU) - Oracle GlassFish Server 3.0.1 / 3.1.2 / Enterprise 2.1.1 DoS - Oracle GlassFish Server 2.1.1.x < 2.1.1.29 / 3.0.1.x < 3.0.1.14 / 3.1.2.x < 3.1.2.15 Java Server Faces RCE (October 2016 CPU)
Riesgo	Medio
Descripción	Según la versión detectada, el servidor Oracle GlassFish que se ejecuta en el host se ve afectada por múltiples vulnerabilidades
Solución	Actualice a Oracle GlassFish Server versión 3.1.2.19 o posterior.
Código Aplicaciones Afectadas	APP111-CIER

Vulnerabilidad	PHP 7.4.x < 7.4.32 Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de PHP instalada en el host es anterior a la 7.4.32. Por lo tanto, se ve afectado por múltiples vulnerabilidades como se menciona en el aviso de la Versión 7.4.32.
Solución	Actualice a la versión de PHP 7.4.32 o posterior.
Código Aplicaciones Afectadas	APP158-MOODLEPCA

Vulnerabilidad	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Riesgo	Medio
Descripción	El host admite el uso de un cifrado de bloque con bloques de 64 bits en uno o más conjuntos de cifrado. Por lo tanto, se ve afectado por una vulnerabilidad, conocida como SWEET32, debido al uso de cifrados de bloque débiles de 64 bits. Un atacante intermediario que tenga suficientes recursos puede explotar esta vulnerabilidad, a través de un ataque de 'birthday', para detectar una colisión que filtre el XOR entre el secreto fijo y un texto plano conocido, permitiendo la divulgación del texto

	secreto, como las cookies HTTPS seguras, y posiblemente resulte en el secuestro de una sesión autenticada.
Solución	Reconfigure la aplicación afectada, si es posible, para evitar el uso de todos los cifrados de bloque de 64 bits. Alternativamente, establezca limitaciones en la cantidad de solicitudes que se pueden procesar a través de la misma conexión TLS para mitigar esta vulnerabilidad.
Código Aplicaciones Afectadas	APP055-HECAA

Vulnerabilidad	SSL Certificate Cannot Be Trusted
Riesgo	Medio
Descripción	No se puede confiar en el certificado SSL para este servicio.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP055-HECAA, APP233-SIA3

Vulnerabilidad	SSL Medium Strength Cipher Suites Supported (SWEET32)
Riesgo	Medio
Descripción	El host admite el uso de cifrados SSL que ofrecen cifrado de nivel medio. Nessus considera que la potencia media es cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el paquete de cifrado 3DES.
Solución	Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.
Código Aplicaciones Afectadas	APP055-HECAA

Vulnerabilidad	SSL Self-Signed Certificate
Riesgo	Medio
Descripción	La cadena de certificados X.509 para este servicio no está firmada por una autoridad certificadora reconocida. Si el host es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque man-in-the-middle contra el host.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP055-HECAA, APP233-SIA3

Vulnerabilidad	TLS Version 1.0 Protocol Detection
Riesgo	Medio
Descripción	El servicio acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 que tiene una serie de defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas contra estos defectos y deben usarse siempre que sea posible.
Solución	Habilite la compatibilidad con TLS 1.2 y 1.3 y desactive la compatibilidad con TLS 1.0.
Código Aplicaciones Afectadas	APP055-HECAA, APP256-CONVALIDA

Vulnerabilidad	TLS Version 1.1 Protocol Deprecated
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 no es compatible con los conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cálculo MAC y los modos de cifrado autenticado, como GCM, no se pueden usar con TLS 1.1
Solución	Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.

Código Aplicaciones Afectadas	APP055-HECAA, APP256-CONVALIDA

Vulnerabilidad	Web Server Error Page Information Disclosure
Riesgo	Medio
Descripción	La página de error predeterminada enviada por el servidor web remoto revela información que puede ayudar a un atacante, como la versión del servidor y los idiomas utilizados por el servidor web.
Solución	Modifique el servidor web para no revelar información detallada sobre el servidor web subyacente o utilice una página de error personalizada en su lugar.
Código Aplicaciones Afectadas	APP174-DELREP

Tabla 5. Vulnerabilidades Medias sobre los servidores de aplicación del ambiente de certificación de los sistemas misionales

4.1.4 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES BAJAS

Vulnerabilidad	Oracle GlassFish Server 3.1.2.x < 3.1.2.17 Java Server Faces Information Disclosure (April 2017 CPU)
Riesgo	Bajo
Descripción	Según su versión autoinformada, el servidor Oracle GlassFish que se ejecuta en el host remoto es 3.1.2.x anterior a 3.1.2.17. Por lo tanto, está afectado por una falla no especificada en el subcomponente Java Server Faces que permite que un atacante remoto no autenticado revele información potencialmente confidencial.
Solución	Actualice a Oracle GlassFish Server versión 3.1.2.17 o posterior, como se indica en el aviso de actualización de parches críticos de Oracle de abril de 2017.
Código Aplicaciones Afectadas	APP111-CIER

Vulnerabilidad	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
Riesgo	Bajo
Descripción	El host remoto permite conexiones SSL / TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits. A través del criptoanálisis, un tercero puede encontrar el secreto compartido en un corto período de tiempo (según el tamaño del módulo y los recursos del atacante). Esto puede permitir a un atacante recuperar el texto sin formato o potencialmente violar la integridad de las conexiones.
Solución	Vuelva a configurar el servicio para utilizar un módulo Diffie-Hellman único de 2048 bits o más.
Código Aplicaciones Afectadas	APP055-HECAA

Tabla 6. Vulnerabilidades Bajas sobre los servidores de aplicación del ambiente de certificación de los sistemas misionales

4.2 SITUACIÓN ACTUAL VULNERABILIDADES EN SERVIDORES DE BASES DE DATOS EN CERTIFICACIÓN

A partir del inventario de aplicaciones, y de acuerdo a la columna “D” en la hoja “Infraestructura Sistemas” del archivo anexo “Sistemas_Trimestre_7.xlsx” se identifican los servidores en el cual está instalada la aplicación en el ambiente de certificación. El resultado obtenido por cada IP se tabula en la hoja “Certificación-DB” del archivo anexo indicado anteriormente, en el que se muestra el resultado de las vulnerabilidades encontradas por aplicación de acuerdo a la criticidad de esta. El nivel de la criticidad está dado por las categorías crítica,

alta, media y baja. En la siguiente tabla se registran las aplicaciones en las que se encontró alguna vulnerabilidad bajo este escenario:

Código Aplicación	Sigla Aplicación	CRITICA	ALTA	MEDIO	BAJA
APP003	CONVSUP	0	0	2	0
APP005	EVI	0	12	0	0
APP010	RRHH	5	32	16	0
APP012	SIET	0	12	0	0
APP014	SIMAT	5	32	16	0
APP015	SIMPADE	5	32	16	0
APP017	SINEB	12	64	46	4
APP018	SIPI	5	32	16	0
APP019	SNIES	0	12	0	0
APP022	SAC V1	6	32	16	0
APP023	SACES	0	12	0	0
APP030	CEBYM	0	0	2	0
APP033	SIET Consultas publicas	0	12	0	0
APP034	SSDIPI	5	32	16	0
APP047	SIMAT BI13A y SIMPADE	0	0	4	0
APP054	SIACET	0	12	0	0
APP055	HECAA	6	32	16	0
APP073	SIISSE	0	0	2	0
APP074	SIISSE HIST	0	0	2	0
APP080	CONVSUPCH	0	12	0	0
APP084	PARES	0	12	0	0
APP103	EMC	0	0	4	0
APP104	SIPTA2 WEB	7	32	30	4
APP111	CIER	5	32	16	0
APP113	SISMA	7	32	30	4
APP114	SPADIES	13	64	46	4
APP119	VUMEN CRL	0	0	2	0
APP120	VUMEN RE	0	0	2	0
APP121	VUMEN IR	0	0	2	0
APP125	SIFSE NVO	12	64	46	4
APP155	SINEB PLANTAS	7	32	30	4
APP174	DELREP	5	32	16	0
APP233	SIA3	7	32	30	4
APP234	NUEVO SIGCE	13	64	46	4
APP237	SIUCE	7	32	30	4
APP244	SAC V2	6	32	16	0
APP256	CONVALIDA	0	0	2	0
APP263	SUPERATE	0	12	0	0
APP264	Tejido maestro	0	30	0	0
APP269	THE B1	7	32	30	4
APP274	CNE	0	12	0	0

Código Aplicación	Sigla Aplicación	CRITICA	ALTA	MEDIO	BAJA
APP277	Nuevo Saces RC	0	0	2	0
APP322	GESPAR	0	0	2	0

Tabla 7. Aplicaciones Misionales en las que se encontró alguna vulnerabilidad sobre los servidores de bases de datos del ambiente de certificación de los sistemas misionales

Las vulnerabilidades detectadas sobre este escenario están explicadas en las siguientes secciones, en donde se indica además el código de la aplicación donde se encontró la vulnerabilidad.

4.2.1 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES CRÍTICAS

Vulnerabilidad	Linux Multiple statd Packages Remote Format String
Riesgo	Crítico
Descripción	El servicio de statd puede desactivarse con un ataque de cadena de formato; ahora debe reiniciarse manualmente. Esto significa que un atacante puede ejecutar código arbitrario gracias a un error en este demonio.
Solución	Actualice a la última versión de rpc.statd.
Código Aplicaciones Afectadas	APP010-RRHH, APP014-SIMAT, APP015-SIMPADE, APP017-SINEB, APP018-SIPI, APP034-SSDIPI, APP111-CIER, APP125-SIFSE NVO, APP174-DELREP, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1, APP022-SAC V1, APP055-HECAA, APP244-SAC V2

Vulnerabilidad	Oracle Database Multiple Vulnerabilities (October 2015 CPU)
Riesgo	Crítico
Descripción	Al servidor de base de datos de Oracle remoto le falta la Actualización de revisión crítica (CPU) de octubre de 2015. Por lo tanto, se ve afectado por múltiples vulnerabilidades en los siguientes componentes: - RDBMS básico (CVE-2015-4857) - Programador de base de datos (CVE-2015-4873) - Java VM (CVE-2015-4794, CVE-2015-4796, CVE-2015-4888) - Clusterware portátil (CVE-2015-4863) - Base de datos XDB-XML (CVE-2015-4900)
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de octubre de 2015.
Código Aplicaciones Afectadas	APP010-RRHH, APP014-SIMAT, APP015-SIMPADE, APP017-SINEB, APP018-SIPI, APP034-SSDIPI, APP111-CIER, APP125-SIFSE NVO, APP174-DELREP, APP017- SINEB, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1, APP022-SAC V1, APP055-HECAA, APP244-SAC V2

Vulnerabilidad	Oracle Database Unsupported Version Detection
Riesgo	Crítico
Descripción	Según la versión detectada, la instalación de Oracle Database que se ejecuta en el host ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de Oracle Database que sea compatible actualmente.
Código Aplicaciones Afectadas	APP010-RRHH, APP014-SIMAT, APP015-SIMPADE, APP017-SINEB, APP018-SIPI, APP034-SSDIPI, APP111-CIER, APP125-SIFSE NVO, APP174-DELREP, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1, APP022-SAC V1, APP055-HECAA, APP244-SAC V2

Vulnerabilidad	SSL Version 2 and 3 Protocol Detection

Riesgo	Crítico
Descripción	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y/o SSL 3.0. Estas versiones de SSL se ven afectadas por varias fallas criptográficas, que incluyen: - Un esquema de relleno inseguro con cifrados CBC. - Esquemas inseguros de renegociación y reanudación de sesiones. Un atacante puede aprovechar estas fallas para realizar ataques de man-in-the-middle o para descifrar las comunicaciones entre el servicio afectado y los clientes. Aunque SSL/TLS tiene un medio seguro para elegir la versión más compatible del protocolo (de modo que estas versiones se usarán solo si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE). Por lo tanto, se recomienda que estos protocolos se deshabiliten por completo. NIST ha determinado que SSL 3.0 ya no es aceptable para comunicaciones seguras. A partir de la fecha de aplicación que se encuentra en PCI DSS v3.1, cualquier versión de SSL no cumplirá con la definición de "criptografía sólida" de PCI SSC.
Solución	Consulte la documentación de la aplicación para desactivar SSL 2.0 y 3.0. Utilice TLS 1.2 (con conjuntos de cifrado aprobados) o superior.
Código Aplicaciones Afectadas	APP017-SINEB, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1

Tabla 8. Vulnerabilidades críticas sobre los servidores de bases de datos del ambiente de certificación de los sistemas misionales

4.2.2 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES ALTAS

Vulnerabilidad (x16)	- Oracle Database Multiple Vulnerabilities (April 2015 CPU) - Oracle Database Multiple Vulnerabilities (April 2016 CPU) - Oracle Database Multiple Vulnerabilities (January 2015 CPU) - Oracle Database Multiple Vulnerabilities (January 2016 CPU) - Oracle Database Multiple Vulnerabilities (July 2015 CPU) - Oracle Database Multiple Vulnerabilities (July 2016 CPU) (FREAK) - Oracle Database Multiple Vulnerabilities (October 2014 CPU) - Oracle Database Multiple Vulnerabilities (October 2017 CPU) - Oracle Database Server Multiple Vulnerabilities (Apr 2019 CPU) - Oracle Database Server Multiple Vulnerabilities (Apr 2020 CPU) - Oracle Database Server Multiple Vulnerabilities (Jan 2020 CPU) - Oracle Database Server Multiple Vulnerabilities (Jul 2019 CPU) - Oracle Database Server Multiple Vulnerabilities (Jul 2020 CPU) - Oracle Database Server Multiple Vulnerabilities (July 2018 CPU) - Oracle Database Server Multiple Vulnerabilities (Oct 2019 CPU) - Oracle Database Server Multiple Vulnerabilities (October 2018 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades en varios de sus componentes.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de acuerdo a la fecha de publicación.
Código Aplicaciones Afectadas	APP005-EVI, APP263-SUPERATE, APP264-Tejido maestro, APP274-CNE, APP010-RRHH, APP014-SIMAT, APP015-SIMPADE, APP017-SINEB, APP018-SIPI, APP034-SSDIPI, APP111-CIER, APP125-SIFSE NVO, APP174-DELREP, APP012-SIET, APP019-SNIES, APP023-SACES, APP033-SIET Consultas publicas, APP080-CONVSUPCH, APP084-PARES, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1, APP022-SAC V1, APP055-HECAA, APP244-SAC V2, APP054-SIACET, APP074-SIISSE HIST

Tabla 9. Vulnerabilidades Altas sobre los servidores de bases de datos del ambiente de certificación de los sistemas misionales

4.2.3 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES MEDIAS

Vulnerabilidad (x4)	- JQuery 1.2 < 3.5.0 Multiple XSS - JQuery < 3.0.0 XSS - JQuery < 3.4.0 Object Prototype Pollution Vulnerability - JQuery 1.x < 1.12.0 / 2.x < 2.2.0 XSS
Riesgo	Medio
Descripción	Según la versión de JQuery alojada en el servidor web, se ve afectado por múltiples vulnerabilidades de secuencias de comandos entre sitios.
Solución	Actualice a JQuery versión 3.5.0 o posterior.
Código Aplicaciones Afectadas	APP103-EMC

Vulnerabilidad	Microsoft Windows IIS Default Index Page
Riesgo	Medio
Descripción	El servidor web remoto utiliza la página de índice IIS predeterminada. Esta página puede contener información adicional sobre la versión y es una indicación de un servidor mal configurado.
Solución	Elimina la página de índice predeterminada.
Código Aplicaciones Afectadas	APP047-SIMAT BI13A y SIMPADE

Vulnerabilidad (x8)	- Oracle Database Multiple Vulnerabilities (April 2017 CPU) - Oracle Database Multiple Vulnerabilities (January 2017 CPU) - Oracle Database Multiple Vulnerabilities (January 2018 CPU) - Oracle Database Multiple Vulnerabilities (July 2017 CPU) (POODLE) (SWEET32) - Oracle Database Multiple Vulnerabilities (October 2016 CPU) - Oracle Database Server CVE-2018-3110 - Oracle Database Server Java VM Unspecified Remote Code Execution (April 2018 CPU) - Oracle Database Server Multiple Vulnerabilities (Jan 2019 CPU)
Riesgo	Medio
Descripción	El servidor de base de datos se ve afectado por múltiples vulnerabilidades en varios de sus componentes.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de acuerdo a la fecha de publicación.
Código Aplicaciones Afectadas	APP010-RRHH, APP014-SIMAT, APP015-SIMPADE, APP017-SINEB, APP018-SIPI, APP034-SSDIPI, APP111-CIER, APP125-SIFSE NVO, APP174-DELREP, APP017-SINEB, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1, APP022-SAC V1, APP055-HECAA, APP114-SPADIES, APP234-NUEVO SIGCE, APP244-SAC V2

Vulnerabilidad	SSH Weak Algorithms Supported
Riesgo	Medio
Descripción	Se ha detectado que el servidor SSH está configurado para usar el cifrado de flujo de Arcfour o ningún cifrado. RFC 4253 desaconseja el uso de Arcfour debido a un problema con claves débiles.
Solución	Póngase en contacto con el proveedor o consulte la documentación del producto para eliminar los cifrados débiles.
Código Aplicaciones Afectadas	APP017-SINEB, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1

Vulnerabilidad	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Riesgo	Medio
Descripción	El host admite el uso de un cifrado de bloque con bloques de 64 bits en uno o más conjuntos de cifrado. Por lo tanto, se ve afectado por una vulnerabilidad, conocida como SWEET32, debido al uso de cifrados de bloque débiles de 64 bits. Un atacante intermediario que tenga suficientes recursos

	puede explotar esta vulnerabilidad, a través de un ataque de 'birthday', para detectar una colisión que filtre el XOR entre el secreto fijo y un texto plano conocido, permitiendo la divulgación del texto secreto, como las cookies HTTPS seguras, y posiblemente resulte en el secuestro de una sesión autenticada.
Solución	Reconfigure la aplicación afectada, si es posible, para evitar el uso de todos los cifrados de bloque de 64 bits. Alternativamente, establezca limitaciones en la cantidad de solicitudes que se pueden procesar a través de la misma conexión TLS para mitigar esta vulnerabilidad.
Código Aplicaciones Afectadas	APP017-SINEB, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1

Vulnerabilidad	SSL Certificate Cannot Be Trusted
Riesgo	Medio
Descripción	No se puede confiar en el certificado SSL para este servicio.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP003-CONVSUP, APP030-CEBYM, APP073-SIISSE, APP119-VUMEN CRL, APP120-VUMEN RE, APP121-VUMEN IR, APP017-SINEB, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1, APP074-SIISSE HIST, APP256-CONVALIDA, APP277-Nuevo Saces RC, APP322-GESPAR

Vulnerabilidad	SSL Certificate Expiry
Riesgo	Medio
Descripción	Este complemento verifica las fechas de vencimiento de los certificados asociados con los servicios habilitados para SSL en el destino e informa si alguno ya ha vencido.
Solución	Compre o genere un nuevo certificado SSL para reemplazar el existente.
Código Aplicaciones Afectadas	APP003-CONVSUP, APP030-CEBYM, APP073-SIISSE, APP119-VUMEN CRL, APP120-VUMEN RE, APP121-VUMEN IR, APP074-SIISSE HIST, APP256-CONVALIDA, APP277-Nuevo Saces RC, APP322-GESPAR

Vulnerabilidad	SSL Medium Strength Cipher Suites Supported (SWEET32)
Riesgo	Medio
Descripción	El host admite el uso de cifrados SSL que ofrecen cifrado de nivel medio. Nessus considera que la potencia media es cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el paquete de cifrado 3DES.
Solución	Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.
Código Aplicaciones Afectadas	APP017-SINEB, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1

Vulnerabilidad	SSL Self-Signed Certificate
Riesgo	Medio
Descripción	La cadena de certificados X.509 para este servicio no está firmada por una autoridad certificadora reconocida. Si el host es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque man-in-the-middle contra el host.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP017-SINEB, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1

Vulnerabilidad	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Riesgo	Medio
Descripción	El host se ve afectado por una vulnerabilidad de divulgación de información de man-in-the-middle (MitM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno al descifrar mensajes cifrados mediante cifrados de bloque en el modo de encadenamiento de bloques de cifrado (CBC). Los atacantes MitM pueden descifrar un byte

	seleccionado de un texto cifrado en tan solo 256 intentos si pueden obligar a una aplicación víctima a enviar repetidamente los mismos datos a través de conexiones SSL 3.0 recién creadas. Siempre que un cliente y un servicio sean compatibles con SSLv3, una conexión se puede "revertir" a SSLv3, incluso si el cliente y el servicio admiten TLSv1 o una versión posterior. El mecanismo TLS Fallback SCSV evita los ataques de "reversión de versiones" sin afectar a los clientes heredados; sin embargo, solo puede proteger las conexiones cuando el cliente y el servicio admiten el mecanismo. Los sitios que no pueden deshabilitar SSLv3 de inmediato deben habilitar este mecanismo. Esta es una vulnerabilidad en la especificación SSLv3, no en ninguna implementación de SSL en particular. Desactivar SSLv3 es la única forma de mitigar completamente la vulnerabilidad.
Solución	Desactive SSLv3. Los servicios que deben admitir SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que se pueda inhabilitar SSLv3.
Código Aplicaciones Afectadas	APP017-SINEB, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1

Vulnerabilidad	TLS Version 1.0 Protocol Detection
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 que tiene una serie de defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas contra estos defectos y deben usarse siempre que sea posible.
Solución	Habilite la compatibilidad con TLS 1.2 y 1.3 y desactive la compatibilidad con TLS 1.0.
Código Aplicaciones Afectadas	APP017-SINEB, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1, APP047-SIMAT BI

Vulnerabilidad	TLS Version 1.1 Protocol Deprecated
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 no es compatible con los conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cálculo MAC y los modos de cifrado autenticado, como GCM, no se pueden usar con TLS 1.1
Solución	Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.
Código Aplicaciones Afectadas	APP047-SIMAT BI13A y SIMPADE

Vulnerabilidad	Web Server HTTP Header Information Disclosure
Riesgo	Medio
Descripción	Los encabezados HTTP enviados por el servidor web remoto revelan información que puede ayudar a un atacante, como la versión del servidor y los idiomas utilizados por el servidor web.
Solución	Modifique los encabezados HTTP del servidor web para no revelar información detallada sobre el servidor web subyacente.
Código Aplicaciones Afectadas	APP047-SIMAT BI13A y SIMPADE

Tabla 10. Vulnerabilidades Medias sobre los servidores de bases de datos del ambiente de certificación de los sistemas misionales

4.2.4 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES BAJAS

Vulnerabilidad	SSH Server CBC Mode Ciphers Enabled
Riesgo	Bajo

Descripción	El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC). Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado.
Solución	Póngase en contacto con el proveedor o consulte la documentación del producto para deshabilitar el cifrado del modo de cifrado CBC y habilitar el cifrado del modo de cifrado CTR o GCM.
Código Aplicaciones Afectadas	APP017-SINEB, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1

Vulnerabilidad	SSH Weak MAC Algorithms Enabled
Riesgo	Bajo
Descripción	El servidor SSH remoto está configurado para permitir algoritmos MD5 o MAC de 96 bits, los cuales se consideran débiles.
Solución	Comuníquese con el proveedor o consulte la documentación del producto para deshabilitar los algoritmos MD5 y MAC de 96 bits.
Código Aplicaciones Afectadas	APP017-SINEB, APP104-SIPTA2 WEB, APP113-SISMA, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE, APP269-THE B1

Tabla 11. Vulnerabilidades Bajas sobre los servidores de bases de datos del ambiente de certificación de los sistemas misionales

4.3 SITUACIÓN ACTUAL VULNERABILIDADES EN SERVIDORES DE APLICACIÓN EN PRODUCCIÓN

A partir del inventario de aplicaciones, y de acuerdo a la columna “D” en la hoja “Infraestructura Sistemas” del archivo anexo “Sistemas_Trimestre_7.xlsx” se identifican los servidores en el cual está instalada la aplicación en el ambiente de certificación. El resultado obtenido por cada IP se tabula en la hoja “Producción-App” del archivo anexo indicado anteriormente, en el que se muestra el resultado de las vulnerabilidades encontradas por aplicación de acuerdo a la criticidad de esta. El nivel de la criticidad está dado por las categorías crítica, alta, media y baja. En la siguiente tabla se registran las aplicaciones en las que se encontró alguna vulnerabilidad bajo este escenario:

Código Aplicación	Sigla Aplicación	CRITICA	ALTA	MEDIO	BAJA
APP002	CNA	0	1	2	0
APP003	CONVSUP	0	0	2	0
APP010	RRHH	0	0	8	0
APP014	SIMAT	1	0	0	0
APP015	SIMPADE	1	0	0	0
APP017	SINEB	0	0	1	0
APP018	SIPI	1	0	0	0
APP022	SAC V1	0	0	4	0
APP030	CEBYM	0	0	3	0
APP054	SIACET	1	9	1	0
APP055	HECAA	1	0	0	0
APP073	SIISSE	0	0	3	0
APP074	SIISSE HIST	0	0	2	0
APP080	CONVSUPCH	0	1	2	0
APP103	EMC	0	0	4	0
APP104	SIPTA2 WEB	1	1	0	0
APP107	LALUPA	0	0	2	0
APP114	SPADIES	2	8	0	0

Código Aplicación	Sigla Aplicación	CRITICA	ALTA	MEDIO	BAJA
APP119	VUMEN CRL	0	0	2	0
APP120	VUMEN RE	0	0	2	0
APP121	VUMEN IR	0	0	2	0
APP125	SIFSE NVO	3	6	0	0
APP126	CNC	1	2	7	1
APP155	SINEB PLANTAS	1	2	0	0
APP158	MOODLEPCA	0	0	3	0
APP174	DELREP	0	0	4	0
APP233	SIA3	2	4	4	0
APP234	NUEVO SIGCE	2	8	0	0
APP237	SIUCE	1	2	0	0
APP256	CONVALIDA	0	0	9	0
APP269	THE B1	0	2	0	0
APP274	CNE	0	2	12	0
APP277	Nuevo Saces RC	0	0	8	0
APP322	GESPAR	0	0	4	0

Tabla 12. Aplicaciones Misionales en las que se encontró alguna vulnerabilidad sobre los servidores de aplicación del ambiente de producción de los sistemas misionales

Las vulnerabilidades detectadas sobre este escenario están explicadas en las siguientes secciones, en donde se indica además el código de la aplicación donde se encontró la vulnerabilidad.

4.3.1 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES CRÍTICAS

Vulnerabilidad	Linux Multiple statd Packages Remote Format String
Riesgo	Crítico
Descripción	El servicio de statd puede desactivarse con un ataque de cadena de formato; ahora debe reiniciarse manualmente. Esto significa que un atacante puede ejecutar código arbitrario gracias a un error en este demonio.
Solución	Actualice a la última versión de rpc.statd.
Código Aplicaciones Afectadas	APP055-HECAA, APP114-SPADIES

Vulnerabilidad	MySQL Unsupported Version Detection
Riesgo	Crítico
Descripción	Según su versión, la instalación de MySQL ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de MySQL que sea soportada actualmente.
Código Aplicaciones Afectadas	APP126-CNC

Vulnerabilidad	Oracle WebLogic Server Java Object Deserialization RCE (July 2016 CPU)
Riesgo	Crítico

Descripción	El Oracle WebLogic Server remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el componente WLS Core en la función readObject() debido a una desinfección incorrecta de la entrada proporcionada por el usuario. Un atacante remoto no autenticado puede explotar esto, a través de una carga útil de objeto manipulado, para eludir la lista negra ClassFilter.class y ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de julio de 2016.
Código Aplicaciones Afectadas	APP054-SIACET

Vulnerabilidad	Oracle WebLogic Unsupported Version Detection
Riesgo	Crítico
Descripción	Según la versión detectada, la instalación de Oracle WebLogic que se ejecuta en el host remoto ya no es soportada. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de Oracle WebLogic que actualmente sea compatible.
Código Aplicaciones Afectadas	APP014-SIMAT, APP015-SIMPADE, APP018-SIPI, APP104-SIPTA2 WEB, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP233-SIA3, APP234-NUEVO SIGCE, APP237-SIUCE

Tabla 13. Vulnerabilidades Críticas sobre los servidores de aplicación del ambiente de producción de los sistemas misionales

4.3.2 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES ALTAS

Vulnerabilidad	Apache HTTP Server Byte Range DoS
Riesgo	Alto
Descripción	La versión de Apache HTTP Server que se ejecuta en el host se ve afectada por una vulnerabilidad de denegación de servicio. Hacer una serie de solicitudes HTTP con rangos superpuestos en los encabezados de solicitud Range o Request-Range puede resultar en el agotamiento de la memoria y la CPU. Un atacante remoto no autenticado podría aprovechar esto para que el sistema no responda. El código de explotación está disponible públicamente.
Solución	Actualice a Apache httpd 2.2.21 o posterior. Alternativamente, aplique una de las soluciones en los avisos de Apache para CVE-2011-3192. La versión 2.2.20 solucionó el problema, pero también introdujo una regresión. Si el host ejecuta un servidor web basado en Apache httpd, comuníquese con el proveedor para obtener una solución.
Código Aplicaciones Afectadas	APP002-CNA, APP080-CONVSUPCH

Vulnerabilidad	Drupal 8.9.x < 8.9.16 / 9.x < 9.0.14 / 9.1.x < 9.1.9 Drupal Vulnerability (SA-CORE-2021-003)
Riesgo	Alto
Descripción	Según la versión detectada, la instancia de Drupal que se ejecuta en el servidor es 8.9.x anterior a 8.9.16, 9.x anterior a 9.0.14 o 9.1.x anterior a 9.1.9. El núcleo de Drupal utiliza la biblioteca CKEditor de terceros. Esta biblioteca tiene un error al analizar HTML que podría provocar un ataque XSS. CKEditor 4.16.1 y versiones posteriores incluyen la corrección. Los usuarios de la biblioteca CKEditor a través de medios distintos al núcleo de Drupal deben actualizar su código de terceros (por ejemplo, el módulo WYSIWYG para Drupal 7). La política del equipo de seguridad de Drupal es no alertar sobre problemas que afecten a bibliotecas de terceros, a menos que se envíen con el núcleo de Drupal. Consulte DRUPAL-SA-PSA-2016-004 para obtener más detalles. Este problema se mitiga por el hecho de que solo afecta a los sitios con CKEditor habilitado. (SA-CORE-2021-003)
Solución	Upgrade to Drupal version 8.9.16 / 9.0.14 / 9.1.9 or later.
Código Aplicaciones Afectadas	APP274-CNE

Vulnerabilidad	Microsoft ASP.NET MS-DOS Device Name DoS

Riesgo	Alto
Descripción	El servidor web que se ejecuta en el host parece estar usando Microsoft ASP.NET y puede verse afectado por una vulnerabilidad de denegación de servicio. Solicitar una URL que contenga un nombre de dispositivo MS-DOS puede hacer que el servidor web deje de responder temporalmente. Un atacante podría solicitar repetidamente estas URL, lo que resultaría en una denegación de servicio.
Solución	Utilice un filtro ISAPI para bloquear solicitudes de URL con nombres de dispositivo MS-DOS.
Código Aplicaciones Afectadas	APP269-THE B1

Vulnerabilidad (x2)	- MySQL < 5.0.90 / 5.1.43 / 5.5.0-m2 Multiple Buffer Overflows - MySQL < 5.0.83 Denial of Service
Riesgo	Alto
Descripción	El servidor de base de datos se ve afectado por múltiples vulnerabilidades
Solución	Actualice a MySQL versión 5.0.90, 5.1.43 o posterior.
Código Aplicaciones Afectadas	APP126-CNC

Vulnerabilidad	Oracle WebLogic Java Object Deserialization RCE
Riesgo	Alto
Descripción	El servidor Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el componente de seguridad WLS debido a llamadas de deserializado no seguras de objetos Java no autenticados a la biblioteca Apache Commons Collections (ACC). Un atacante remoto no autenticado puede explotar esto para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Actualice a la versión corregida relevante a la que se hace referencia en el aviso del proveedor.
Código Aplicaciones Afectadas	APP054-SIACET

Vulnerabilidad	Oracle WebLogic Java Object RMI Connect-Back Deserialization RCE (January 2017 CPU)
Riesgo	Alto
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserialización no segura de objetos Java por parte del registro RMI. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de enero de 2017.
Código Aplicaciones Afectadas	APP054-SIACET

Vulnerabilidad	Oracle WebLogic Server 10.3.6.0 / 12.1.3.0 / 12.2.1.3 Java Object Deserialization RCE (CVE-2018-3191)
Riesgo	Alto
Descripción	La versión de Oracle WebLogic Server instalada en el host se ve afectada por una vulnerabilidad de ejecución remota de código en el subcomponente WLS Core Components debido a la deserialización no segura de objetos Java por parte del registro RMI. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java serializado diseñado, para ejecutar código arbitrario.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de octubre de 2018.
Código Aplicaciones Afectadas	APP054-SIACET, APP104-SIPTA2 WEB, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE, APP237-SIUCE

Vulnerabilidad	Oracle WebLogic Server Deserialization RCE (CVE-2018-2628)

Riesgo	Alto
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserialización no segura de objetos Java por parte del registro RMI. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2018
Código Aplicaciones Afectadas	APP054-SIACET, APP114-SPADIES, APP233-SIA3, APP234-NUEVO SIGCE

Vulnerabilidad	Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)
Riesgo	Alto
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a una deserialización no segura de objetos Java. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de julio de 2018.
Código Aplicaciones Afectadas	APP054-SIACET, APP114-SPADIES, APP233-SIA3, APP234-NUEVO SIGCE

Vulnerabilidad	Oracle WebLogic Server Java Object Deserialization RCE (April 2016 CPU)
Riesgo	Alto
Descripción	El servidor Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Java Messaging Service en la función readExternal() debido a una sanitización incorrecta de la entrada proporcionada por el usuario. Un atacante remoto no autenticado puede explotar esto, a través de un payload manipulado, para eludir la lista negra ClassFilter.class y ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2016.
Código Aplicaciones Afectadas	APP054-SIACET

Vulnerabilidad	Oracle WebLogic Server Java Object Deserialization RCE (CVE-2018-3245)
Riesgo	Alto
Descripción	La versión de Oracle WebLogic Server instalada en el host se ve afectada por una vulnerabilidad de ejecución remota de código en el subcomponente WLS Core Components debido a la deserialización no segura de objetos Java por parte del registro RMI. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java serializado diseñado, para ejecutar código arbitrario.
Solución	Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de Oracle de octubre de 2018 o actualice a una versión compatible para la que haya un parche disponible.
Código Aplicaciones Afectadas	APP054-SIACET, APP114-SPADIES, APP125-SIFSE NVO, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE, APP237-SIUCE

Vulnerabilidad	Oracle WebLogic Server Java Object Deserialization RCE (October 2016 CPU)
Riesgo	Alto
Descripción	El servidor Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el componente de seguridad de WLS debido a llamadas de deserialización no seguras de objetos Java no autenticados a la biblioteca de carga de archivos de Apache Commons. Un atacante remoto no autenticado puede explotar esto, a través de un objeto DiskFileItem manipulado, para ejecutar código arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de octubre de 2016. También se informa que WebLogic 12.2.1.3 se ve afectado.
Código Aplicaciones Afectadas	APP054-SIACET

Vulnerabilidad	Oracle WebLogic WLS9-async Remote Code Execution (remote check)
Riesgo	Alto
Descripción	El servidor Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el componente WLS9-async debido a la deserialización no segura de objetos Java codificados en XML. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche al que se hace referencia en el aviso del proveedor.
Código Aplicaciones Afectadas	APP054-SIACET

Tabla 14. Vulnerabilidades Altas sobre los servidores de aplicación del ambiente de producción de los sistemas misionales

4.3.3 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES MEDIAS

Vulnerabilidad	Apache HTTP Server httpOnly Cookie Information Disclosure
Riesgo	Medio
Descripción	La versión de Apache HTTP Server que se ejecuta en el host remoto se ve afectada por una vulnerabilidad de divulgación de información. Enviar una solicitud con encabezados HTTP lo suficientemente largos como para exceder el límite del servidor hace que el servidor web responda con un HTTP 400. De forma predeterminada, el encabezado HTTP ofensivo y el valor se muestran en la página de error 400. Cuando se usa junto con otros ataques (p. ej., secuencias de comandos entre sitios), esto podría resultar en el compromiso de las cookies httpOnly.
Solución	Actualice a Apache versión 2.0.65 / 2.2.22 o posterior.
Código Aplicaciones Afectadas	APP002-CNA, APP080-CONVSUPCH, APP022-SAC V1

Vulnerabilidad (x6)	- Drupal 7.x < 7.73 / 8.8.x < 8.8.10 / 8.9.x < 8.9.6 / 9.0.x < 9.0.6 XSS (drupal-2020-09-16) - Drupal 7.x < 7.74 / 8.x < 8.8.11 / 8.9.x < 8.9.9 / 9.0.x < 9.0.8 RCE (SA-CORE-2020-012) - Drupal 7.x < 7.75 / 8.x < 8.8.12 / 8.9.x < 8.9.10 / 9.0.x < 9.0.9 Multiple Vulnerabilities (SA-CORE-2020-013) - Drupal 7.x < 7.78 / 8.9.x < 8.9.13 / 9.x < 9.0.11 / 9.1.x < 9.1.3 Directory Traversal (SA-CORE-2021-001) - Drupal 7.x < 7.80 / 8.9.x < 8.9.14 / 9.x < 9.0.12 / 9.1.x < 9.1.7 XSS (SA-CORE-2021-002) - Drupal 8.8.x < 8.8.10 / 8.9.x < 8.9.6 / 9.0.x < 9.0.6 Multiple Vulnerabilities (drupal-2020-09-16)
Riesgo	Medio
Descripción	Según la versión detectada, la instancia de Drupal que se ejecuta en el servidor web se ve afectada por múltiples vulnerabilidades.
Solución	Actualice a la versión de Drupal 7.80 / 8.8.12 / 8.9.14 / 9.0.9 / 9.1.7 o posterior.
Código Aplicaciones Afectadas	APP274-CNE

Vulnerabilidad	HTTP TRACE / TRACK Methods Allowed
Riesgo	Medio
Descripción	El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidor web.
Solución	Deshabilite estos métodos HTTP. Consulte la salida del complemento para obtener más información.
Código Aplicaciones Afectadas	APP022-SAC V1

Vulnerabilidad (x4)	- JQuery 1.2 < 3.5.0 Multiple XSS - JQuery < 3.0.0 XSS - JQuery < 3.4.0 Object Prototype Pollution Vulnerability - JQuery 1.x < 1.12.0 / 2.x < 2.2.0 XSS
Riesgo	Medio
Descripción	Según la versión de JQuery alojada en el servidor web, se ve afectado por múltiples vulnerabilidades de secuencias de comandos entre sitios.
Solución	Actualice a JQuery versión 3.5.0 o posterior.
Código Aplicaciones Afectadas	APP103-EMC, APP256-CONVALIDA

Vulnerabilidad	Linux Kernel TCP Sequence Number Generation Security Weakness
Riesgo	Medio
Descripción	El kernel de Linux es propenso a una debilidad de seguridad relacionada con la generación de números de secuencia TCP. Los atacantes pueden aprovechar este problema para inyectar paquetes arbitrarios en las sesiones TCP mediante un ataque de fuerza bruta. Un atacante puede usar esta vulnerabilidad para crear una condición de denegación de servicio o un ataque de intermediario. Tenga en cuenta que este complemento puede activarse como resultado de un dispositivo de red (como un equilibrador de carga, VPN, IPS, proxy transparente, etc.) que es vulnerable y que reescribe los números de secuencia de TCP, en lugar de que el propio host sea vulnerable.
Solución	Comuníquese con el proveedor del sistema operativo para obtener una actualización/parche del kernel de Linux.
Código Aplicaciones Afectadas	APP002-CNA, APP080-CONVSUPCH, APP017- SINEB, APP022-SAC V1

Vulnerabilidad (x5)	- MySQL < 5.0.88 / 5.1.42 / 5.5.0 / 6.0.14 MyISAM CREATE TABLE Privilege Check Bypass - MySQL < 5.0.92 Multiple Denial of Service - MySQL 5.0 < 5.0.88 Multiple Vulnerabilities - MySQL 5.0 < 5.0.95 Multiple Vulnerabilities - MySQL Community Server < 5.1.47 / 5.0.91 Multiple Vulnerabilities
Riesgo	Medio
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades
Solución	Actualice a MySQL versión 5.1.47, 5.0.95, 5.5.0 o 6.0.14 o posterior.
Código Aplicaciones Afectadas	APP126-CNC

Vulnerabilidad	MySQL Binary Log SQL Injection
Riesgo	Medio
Descripción	La versión de MySQL instalada en el host es anterior a 5.5.33 / 5.6.x anterior a 5.6.13 y, por lo tanto, está potencialmente afectada por múltiples vulnerabilidades de inyección de SQL. Los identificadores proporcionados por el usuario no se citan correctamente antes de escribirse en el registro binario. Un atacante con una cuenta válida y privilegios para modificar puede modificar tablas a las que no debería tener acceso.
Solución	Actualice a MySQL versión 5.5.33 / 5.6.13 o posterior.
Código Aplicaciones Afectadas	APP126-CNC

Vulnerabilidad	MySQL Denial of Service (Jul 2020 CPU)
Riesgo	Medio

Descripción	La versión de MySQL que se ejecuta en el host es menor a 5.7.29 o menor a 8.0.19. Por lo tanto, se ve afectado por una vulnerabilidad, como se indica en el aviso de actualización del parche crítico de julio de 2020: Una vulnerabilidad en el producto MySQL Server de Oracle MySQL (componente: Servidor: Replicación). Las versiones compatibles que se ven afectadas son menores a 5.7.29 y menores a 8.0.19. La vulnerabilidad fácilmente explotable permite que un atacante con muchos privilegios con acceso a la red a través de múltiples protocolos comprometa el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en la capacidad no autorizada de causar un bloqueo o un bloqueo repetible (DOS completo) de MySQL Server.
Solución	Consulte el aviso del proveedor.
Código Aplicaciones Afectadas	APP126-CNC

Vulnerabilidad	Oracle WebLogic WSAT Remote Code Execution
Riesgo	Medio
Descripción	El servidor Oracle WebLogic remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el extremo WSAT debido a la deserialización no segura de objetos Java codificados en XML. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parche crítico de Oracle de octubre de 2017.
Código Aplicaciones Afectadas	APP054-SIACET

Vulnerabilidad	PHP 7.4.x < 7.4.32 Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de PHP instalada en el host es anterior a la 7.4.32. Por lo tanto, se ve afectado por múltiples vulnerabilidades como se menciona en el aviso de la Versión 7.4.32.
Solución	Actualice a la versión de PHP 7.4.32 o posterior.
Código Aplicaciones Afectadas	APP158-MOODLEPCA

Vulnerabilidad	SSL Certificate Cannot Be Trusted
Riesgo	Medio
Descripción	No se puede confiar en el certificado SSL para este servicio.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP174-DELREP

Vulnerabilidad	SSL Certificate Signed Using Weak Hashing Algorithm
Riesgo	Medio
Descripción	El servicio remoto utiliza una cadena de certificados SSL que se ha firmado mediante un algoritmo de hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede aprovechar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se haga pasar por el servicio afectado.
Solución	Póngase en contacto con la autoridad de certificación para que se vuelva a emitir el certificado SSL.
Código Aplicaciones Afectadas	APP174-DELREP

Vulnerabilidad	SSL Certificate with Wrong Hostname

Riesgo	Medio
Descripción	El atributo 'commonName' (CN) del certificado SSL presentado para este servicio es para una máquina diferente.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP030-CEBYM, APP073-SIISSE, APP256-CONVALIDA

Vulnerabilidad	SSL Self-Signed Certificate
Riesgo	Medio
Descripción	La cadena de certificados X.509 para este servicio no está firmada por una autoridad certificadora reconocida. Si el host es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque man-in-the-middle contra el host.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP174-DELREP

Vulnerabilidad	TLS Version 1.0 Protocol Detection
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 que tiene una serie de defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas contra estos defectos y deben usarse siempre que sea posible.
Solución	Habilite la compatibilidad con TLS 1.2 y 1.3 y desactive la compatibilidad con TLS 1.0.
Código Aplicaciones Afectadas	APP003-CONVSUP, APP010-RRHH, APP030-CEBYM, APP073-SIISSE, APP074-SIISSE HIST, APP107-LALUPA, APP119-VUMEN CRL, APP120-VUMEN RE, APP121-VUMEN IR, APP233-SIA3, APP256-CONVALIDA, APP277-Nuevo Saces RC, APP322-GESPAR

Vulnerabilidad	TLS Version 1.1 Protocol Deprecated
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 no es compatible con los conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cálculo MAC y los modos de cifrado autenticado, como GCM, no se pueden usar con TLS 1.1
Solución	Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.
Código Aplicaciones Afectadas	APP003-CONVSUP, APP010-RRHH, APP030-CEBYM, APP073-SIISSE, APP074-SIISSE HIST, APP107-LALUPA, APP119-VUMEN CRL, APP120-VUMEN RE, APP121-VUMEN IR, APP233-SIA3, APP256-CONVALIDA, APP277-Nuevo Saces RC, APP322-GESPAR

Vulnerabilidad	Web Server Error Page Information Disclosure
Riesgo	Medio
Descripción	La página de error predeterminada enviada por el servidor web remoto revela información que puede ayudar a un atacante, como la versión del servidor y los idiomas utilizados por el servidor web.
Solución	Modifique el servidor web para no revelar información detallada sobre el servidor web subyacente o utilice una página de error personalizada en su lugar.
Código Aplicaciones Afectadas	APP174-DELREP

Vulnerabilidad	Web Server HTTP Header Information Disclosure
Riesgo	Medio
Descripción	Los encabezados HTTP enviados por el servidor web remoto revelan información que puede ayudar a un atacante, como la versión del servidor y los idiomas utilizados por el servidor web.
Solución	Modifique los encabezados HTTP del servidor web para no revelar información detallada sobre el servidor web subyacente.

Código Aplicaciones Afectadas	APP022-SAC V1

Tabla 15. Vulnerabilidades Medias sobre los servidores de aplicación del ambiente de producción de los sistemas misionales

4.3.4 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES BAJAS

Vulnerabilidad	MySQL < 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 Client XSS
Riesgo	Bajo
Descripción	La versión de MySQL instalada en el host remoto es anterior a 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 y, por lo tanto, no codifica correctamente los corchetes angulares cuando se usa la opción 'mysql --html'. Dependiendo de cómo se procese la salida del comando del cliente mysql, el usuario puede ser vulnerable a ataques de secuencias de comandos entre sitios.
Solución	Actualice a MySQL versión 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 o posterior.
Código Aplicaciones Afectadas	APP126-CNC

Tabla 16. Vulnerabilidades Bajas sobre los servidores de aplicación del ambiente de producción de los sistemas misionales

4.4 SITUACIÓN ACTUAL VULNERABILIDADES EN SERVIDORES DE BASES DE DATOS EN PRODUCCIÓN

A partir del inventario de aplicaciones, y de acuerdo a la columna “D” en la hoja “Infraestructura Sistemas” del archivo anexo “Sistemas_Trimestre_7.xlsx” se identifican los servidores en el cual está instalada la aplicación en el ambiente de certificación. El resultado obtenido por cada IP se tabula en la hoja “Producción-DB” del archivo anexo indicado anteriormente, en el que se muestra el resultado de las vulnerabilidades encontradas por aplicación de acuerdo a la criticidad de esta. El nivel de la criticidad está dado por las categorías crítica, alta, media y baja. El resultado es el siguiente:

Código Aplicación	Sigla Aplicación	CRITICA	ALTA	MEDIO	BAJA
APP002	CNA	4	5	11	0
APP003	CONVSUP	0	0	2	0
APP005	EVI	0	12	0	0
APP010	RRHH	9	48	24	0
APP012	SIET	12	64	32	0
APP014	SIMAT	9	64	32	0
APP015	SIMPADE	9	64	32	0
APP017	SINEB	7	32	22	0
APP018	SIPI	9	64	32	0
APP019	SNIES	12	64	32	0
APP022	SAC V1	5	32	16	0
APP023	SACES	16	69	43	0
APP030	CEBYM	0	0	2	0
APP033	SIET Consultas publicas	12	64	32	0
APP034	SSDIPI	6	32	16	0

Código Aplicación	Sigla Aplicación	CRITICA	ALTA	MEDIO	BAJA
APP047	SIMAT BI13A y SIMPADE	0	0	2	0
APP054	SIACET	12	64	32	0
APP055	HECAA	6	32	16	0
APP073	SIISSE	0	0	2	0
APP074	SIISSE HIST	0	0	2	0
APP080	CONVSUPCH	16	69	43	0
APP084	PARES	16	69	43	0
APP103	EMC	0	0	4	0
APP104	SIPTA2 WEB	6	32	16	0
APP107	LALUPA	0	1	4	0
APP111	CIER	2	32	16	0
APP113	SISMA	6	32	16	0
APP114	SPADIES	7	32	22	0
APP119	VUMEN CRL	0	0	2	0
APP120	VUMEN RE	0	0	2	0
APP121	VUMEN IR	0	0	2	0
APP125	SIFSE NVO	5	32	16	0
APP126	CNC	1	2	7	1
APP155	SINEB PLANTAS	7	32	22	0
APP174	DELREP	5	32	16	0
APP230	SICSUP	0	0	4	3
APP233	SIA3	5	32	16	0
APP234	NUEVO SIGCE	7	32	22	0
APP237	SIUCE	5	32	16	0
APP244	SAC V2	5	32	16	0
APP251	SUPSA	0	0	4	1
APP256	CONVALIDA	0	0	8	0
APP263	SUPERATE	0	12	0	0
APP269	THE B1	0	2	0	0
APP274	CNE	0	12	0	0
APP277	Nuevo Saces RC	0	0	8	0
APP322	GESPAR	0	0	8	0

Tabla 17. Aplicaciones Misionales en las que se encontró alguna vulnerabilidad sobre los servidores de bases de datos del ambiente de producción de los sistemas misionales

Las vulnerabilidades detectadas sobre este escenario están explicadas en las siguientes secciones, en donde se indica además el código de la aplicación donde se encontró la vulnerabilidad.

4.4.1 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES CRÍTICAS

Vulnerabilidad	Linux Multiple statd Packages Remote Format String
Riesgo	Crítico

Descripción	El servicio de statd puede desactivarse con un ataque de cadena de formato; ahora debe reiniciarse manualmente. Esto significa que un atacante puede ejecutar código arbitrario gracias a un error en este demonio.
Solución	Actualice a la última versión de rpc.statd.
Código Aplicaciones Afectadas	APP002-CNA, APP023-SACES, APP080-CONVSUPCH, APP084-PARES, APP010-RRHH, APP012-SIET, APP019-SNIES, APP033-SIET Consultas publicas, APP054-SIACET, APP014-SIMAT, APP015-SIMPADE, APP018-SIPI, APP017-SINEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE, APP022-SAC V1, APP111-CIER, APP034-SSDIPI, APP055-HECAA, APP104-SIPTA2 WEB, APP113-SISMA, APP125-SIFSE NVO, APP174-DELREP, APP233-SIA3, APP237-SIUCE, APP244-SAC V2

Vulnerabilidad	MySQL Unsupported Version Detection
Riesgo	Crítico
Descripción	Según su versión, la instalación de MySQL ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de MySQL que sea soportada actualmente.
Código Aplicaciones Afectadas	APP002-CNA, APP023-SACES, APP080-CONVSUPCH, APP084-PARES, APP126-CNC

Vulnerabilidad	Oracle Database Multiple Vulnerabilities (October 2015 CPU)
Riesgo	Crítico
Descripción	Al servidor de base de datos de Oracle remoto le falta la Actualización de revisión crítica (CPU) de octubre de 2015. Por lo tanto, se ve afectado por múltiples vulnerabilidades en los siguientes componentes: - RDBMS básico (CVE-2015-4857) - Programador de base de datos (CVE-2015-4873) - Java VM (CVE-2015-4794, CVE-2015-4796, CVE-2015-4888) - Clusterware portátil (CVE-2015-4863) - Base de datos XDB-XML (CVE-2015-4900)
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de octubre de 2015.
Código Aplicaciones Afectadas	APP010-RRHH, APP012-SIET, APP019-SNIES, APP023-SACES, APP033-SIET Consultas publicas, APP054-SIACET, APP080-CONVSUPCH, APP084-PARES, APP014-SIMAT, APP015-SIMPADE, APP018-SIPI, APP017-SINEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE, APP022-SAC V1, APP111-CIER, APP034-SSDIPI, APP055-HECAA, APP104-SIPTA2 WEB, APP113-SISMA, APP125-SIFSE NVO, APP174-DELREP, APP233-SIA3, APP237-SIUCE, APP244-SAC V2

Vulnerabilidad	Oracle Database Unsupported Version Detection
Riesgo	Crítico
Descripción	Según la versión detectada, la instalación de Oracle Database ejecutándose en el host ya no es soportada. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Actualice a una versión de Oracle Database que actualmente sea compatible.
Código Aplicaciones Afectadas	APP010-RRHH, APP012-SIET, APP019-SNIES, APP023-SACES, APP033-SIET Consultas publicas, APP054-SIACET, APP080-CONVSUPCH, APP084-PARES, APP014-SIMAT, APP015-SIMPADE, APP018-SIPI, APP017-SINEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE, APP022-SAC V1, APP111-CIER, APP034-SSDIPI, APP055-HECAA, APP104-SIPTA2 WEB, APP113-SISMA, APP125-SIFSE NVO, APP174-DELREP, APP233-SIA3, APP237-SIUCE, APP244-SAC V2

Vulnerabilidad	PostgreSQL 8.4 < 8.4.17 / 9.0 < 9.0.13 / 9.1 < 9.1.9 / 9.2 < 9.2.4 Multiple Vulnerabilities
Riesgo	Crítico
Descripción	La versión de PostgreSQL instalada en el host es 8.4.x anterior a 8.4.17, 9.0.x anterior a 9.0.13, 9.1.x anterior a 9.1.9 o 9.2.x anterior a 9.2.4. Por lo tanto, se ve potencialmente afectado por múltiples vulnerabilidades:

	- Los instaladores de Enterprise DB para Linux y Mac OS X crean un directorio y un archivo en '/tmp' con nombres predecibles. (CVE-2013-1902) - Los instaladores de Enterprise DB para Linux y Mac OS X pasan la contraseña de superusuario de la base de datos a un script de forma insegura. (CVE-2013-1903)
Solución	Actualice a PostgreSQL 8.4.17/9.0.13/9.1.9/9.2.4 o posterior.
Código Aplicaciones Afectadas	APP002-CNA, APP023-SACES, APP080-CONVSUPCH, APP084-PARES

Vulnerabilidad	PostgreSQL Unsupported Version Detection
Riesgo	Crítico
Descripción	Según su número de versión autoinformado, ya no se admite la instalación de PostgreSQL en el host remoto. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución	Upgrade to a version of PostgreSQL that is currently supported.
Código Aplicaciones Afectadas	APP002-CNA, APP023-SACES, APP080-CONVSUPCH, APP084-PARES

Vulnerabilidad	SSL Version 2 and 3 Protocol Detection
Riesgo	Crítico
Descripción	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y/o SSL 3.0. Estas versiones de SSL se ven afectadas por varias fallas criptográficas, que incluyen: - Un esquema de relleno inseguro con cifrados CBC. - Esquemas inseguros de renegociación y reanudación de sesiones. Un atacante puede aprovechar estas fallas para realizar ataques de man-in-the-middle o para descifrar las comunicaciones entre el servicio afectado y los clientes. Aunque SSL/TLS tiene un medio seguro para elegir la versión más compatible del protocolo (de modo que estas versiones se usarán solo si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE). Por lo tanto, se recomienda que estos protocolos se deshabiliten por completo. NIST ha determinado que SSL 3.0 ya no es aceptable para comunicaciones seguras. A partir de la fecha de aplicación que se encuentra en PCI DSS v3.1, cualquier versión de SSL no cumplirá con la definición de "criptografía sólida" de PCI SSC.
Solución	Consulte la documentación de la aplicación para desactivar SSL 2.0 y 3.0. Utilice TLS 1.2 (con conjuntos de cifrados aprobados) o superior.
Código Aplicaciones Afectadas	APP017- SINEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE

Tabla 18. Vulnerabilidades Críticas sobre los servidores de bases de datos del ambiente de producción de los sistemas misionales

4.4.2 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES ALTAS

Vulnerabilidad	Microsoft ASP.NET MS-DOS Device Name DoS
Riesgo	Alto
Descripción	El servidor web que se ejecuta en el host parece estar usando Microsoft ASP.NET y puede verse afectado por una vulnerabilidad de denegación de servicio. Solicitar una URL que contenga un nombre de dispositivo MS-DOS puede hacer que el servidor web deje de responder temporalmente. Un atacante podría solicitar repetidamente estas URL, lo que resultaría en una denegación de servicio.

Solución	Utilice un filtro ISAPI para bloquear solicitudes de URL con nombres de dispositivo MS-DOS.
Código Aplicaciones Afectadas	APP107-LALUPA, APP269-THE B1

Vulnerabilidad (x2)	- MySQL < 5.0.90 / 5.1.43 / 5.5.0-m2 Multiple Buffer Overflows - MySQL < 5.0.83 Denial of Service
Riesgo	Alto
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades
Solución	Actualice a MySQL versión 5.0.90 / 5.1.43 / 5.5.0-m2 o posterior.
Código Aplicaciones Afectadas	APP126-CNC

Vulnerabilidad (x16)	- Oracle Database Multiple Vulnerabilities (April 2015 CPU) - Oracle Database Multiple Vulnerabilities (April 2016 CPU) - Oracle Database Multiple Vulnerabilities (January 2015 CPU) - Oracle Database Multiple Vulnerabilities (January 2016 CPU) - Oracle Database Multiple Vulnerabilities (July 2015 CPU) - Oracle Database Multiple Vulnerabilities (July 2016 CPU) (FREAK) - Oracle Database Multiple Vulnerabilities (October 2014 CPU) - Oracle Database Multiple Vulnerabilities (October 2017 CPU) - Oracle Database Server Multiple Vulnerabilities (Apr 2019 CPU) - Oracle Database Server Multiple Vulnerabilities (Apr 2020 CPU) - Oracle Database Server Multiple Vulnerabilities (Jan 2020 CPU) - Oracle Database Server Multiple Vulnerabilities (Jul 2019 CPU) - Oracle Database Server Multiple Vulnerabilities (Jul 2020 CPU) - Oracle Database Server Multiple Vulnerabilities (July 2018 CPU) - Oracle Database Server Multiple Vulnerabilities (Oct 2019 CPU) - Oracle Database Server Multiple Vulnerabilities (October 2018 CPU)
Riesgo	Alto
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de la fecha correspondiente a la vulnerabilidad reportada.
Código Aplicaciones Afectadas	APP010-RRHH, APP012-SIET, APP019-SNIES, APP023-SACES, APP033-SIET Consultas publicas, APP054-SIACET, APP080-CONVSUPCH, APP084-PARES, APP014-SIMAT, APP015-SIMPADE, APP018-SIPI, APP017-SINEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE, APP022-SAC V1, APP111-CIER, APP034-SSDIPI, APP055-HECAA, APP104-SIPTA2 WEB, APP113-SISMA, APP125-SIFSE NVO, APP174-DELREP, APP233-SIA3, APP237-SIUCE, APP244-SAC V2, APP263-SUPERATE, APP274-CNE

Vulnerabilidad (x5)	- PostgreSQL 8.4 < 8.4.17 / 9.0 < 9.0.13 / 9.1 < 9.1.9 / 9.2 < 9.2.4 Predictable Random Number Generator - PostgreSQL 9.0 < 9.0.20 / 9.1 < 9.1.16 / 9.2 < 9.2.11 / 9.3 < 9.3.7 / 9.4 < 9.4.2 Multiple Vulnerabilities - PostgreSQL 9.1.x < 9.1.20 / 9.2.x < 9.2.15 / 9.3.x < 9.3.11 / 9.4.x < 9.4.6 / 9.5.x < 9.5.1 Multiple Vulnerabilities - PostgreSQL 9.1.x < 9.1.24 / 9.2.x < 9.2.19 / 9.3.x < 9.3.15 / 9.4.x < 9.4.10 / 9.5.x < 9.5.5 / 9.6.x < 9.6.1 Aggregate Functions Use-after-free DoS - PostgreSQL 9.2.x < 9.2.20 / 9.3.x < 9.3.16 / 9.4.x < 9.4.11 / 9.5.x < 9.5.6 / 9.6.x < 9.6.2 Multiple Vulnerabilities
Riesgo	Alto
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Actualice a PostgreSQL versión 8.4.17/9.0.20/9.1.24/9.2.20/9.3.16/9.4.11/9.5.6/9.6.2 o posterior.
Código Aplicaciones Afectadas	APP002-CNA, APP023-SACES, APP080-CONVSUPCH, APP084-PARES

Tabla 19. Vulnerabilidades Altas sobre los servidores de bases de datos del ambiente de producción de los sistemas misionales

4.4.3 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES MEDIAS

Vulnerabilidad (x4)	- JQuery 1.2 < 3.5.0 Multiple XSS - JQuery < 3.0.0 XSS - JQuery < 3.4.0 Object Prototype Pollution Vulnerability - JQuery 1.x < 1.12.0 / 2.x < 2.2.0 XSS
Riesgo	Medio
Descripción	Según la versión de JQuery alojada en el servidor web, se ve afectado por múltiples vulnerabilidades de secuencias de comandos entre sitios.
Solución	Actualice a JQuery versión 3.5.0 o posterior.
Código Aplicaciones Afectadas	APP103-EMC

Vulnerabilidad (x4)	- MariaDB 10.1.0 < 10.1.39 Multiple Vulnerabilities - MariaDB 10.1.0 < 10.1.44 A Vulnerability - MariaDB 10.1.0 < 10.1.45 Multiple Vulnerabilities - MariaDB 10.1.x < 10.1.42 Denial Of Service Vulnerability
Riesgo	Medio
Descripción	El servidor de base de datos se ve afectado por múltiples vulnerabilidades
Solución	Actualice a MariaDB versión 10.1.45 o posterior.
Código Aplicaciones Afectadas	APP251-SUPSA

Vulnerabilidad	Microsoft Windows IIS Default Index Page
Riesgo	Medio
Descripción	El servidor web remoto utiliza la página de índice IIS predeterminada. Esta página puede contener información adicional sobre la versión y es una indicación de un servidor mal configurado.
Solución	Elimina la página de índice predeterminada.
Código Aplicaciones Afectadas	APP047-SIMAT BI13A y SIMPADE

Vulnerabilidad (x5)	- MySQL < 5.0.88 / 5.1.42 / 5.5.0 / 6.0.14 MyISAM CREATE TABLE Privilege Check Bypass - MySQL < 5.0.92 Multiple Denial of Service - MySQL 5.0 < 5.0.88 Multiple Vulnerabilities - MySQL 5.0 < 5.0.95 Multiple Vulnerabilities - MySQL Community Server < 5.1.47 / 5.0.91 Multiple Vulnerabilities
Riesgo	Medio
Descripción	La versión de MySQL 5.0 instalada en el host se ve afectada por múltiples vulnerabilidades.
Solución	Actualice a MySQL versión 5.1.47, 5.5.0, 6.0.14 o posterior.
Código Aplicaciones Afectadas	APP126-CNC

Vulnerabilidad	MySQL 5.1.x < 5.7.3 SSL/TLS Downgrade MitM (BACKRONYM)
Riesgo	Medio
Descripción	La versión de MySQL instalada en el host se ve afectada por múltiples vulnerabilidades.
Solución	Actualice a MySQL versión 5.7.3 o posterior.
Código Aplicaciones Afectadas	APP002-CNA, APP023-SACES, APP080-CONVSUPCH, APP084-PARES

Vulnerabilidad	MySQL Binary Log SQL Injection

Riesgo	Medio
Descripción	La versión de MySQL instalada en el host es anterior a 5.5.33 / 5.6.x anterior a 5.6.13 y, por lo tanto, está potencialmente afectada por múltiples vulnerabilidades de inyección de SQL. Los identificadores proporcionados por el usuario no se citan correctamente antes de escribirse en el registro binario. Un atacante con una cuenta válida y privilegios para modificar puede modificar tablas a las que no debería tener acceso.
Solución	Actualice a MySQL versión 5.5.33 / 5.6.13 o posterior.
Código Aplicaciones Afectadas	APP002-CNA, APP023-SACES, APP080-CONVSUPCH, APP084-PARES, APP126-CNC

Vulnerabilidad	MySQL Denial of Service (Jul 2020 CPU)
Riesgo	Medio
Descripción	La versión de MySQL que se ejecuta en el host es menor a 5.7.29 o menor a 8.0.19. Por lo tanto, se ve afectado por una vulnerabilidad, como se indica en el aviso de actualización del parche crítico de julio de 2020: Una vulnerabilidad en el producto MySQL Server de Oracle MySQL (componente: Servidor: Replicación). Las versiones compatibles que se ven afectadas son menores a 5.7.29 y menores a 8.0.19. La vulnerabilidad fácilmente explotable permite que un atacante con muchos privilegios con acceso a la red a través de múltiples protocolos comprometa el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en la capacidad no autorizada de causar un bloqueo o un bloqueo repetible (DOS completo) de MySQL Server.
Solución	Consulte el aviso del proveedor.
Código Aplicaciones Afectadas	APP002-CNA, APP023-SACES, APP080-CONVSUPCH, APP084-PARES, APP126-CNC

Vulnerabilidad (x8)	- Oracle Database Multiple Vulnerabilities (April 2017 CPU) - Oracle Database Multiple Vulnerabilities (January 2017 CPU) - Oracle Database Multiple Vulnerabilities (January 2018 CPU) - Oracle Database Multiple Vulnerabilities (July 2017 CPU) (POODLE) (SWEET32) - Oracle Database Multiple Vulnerabilities (October 2016 CPU) - Oracle Database Server CVE-2018-3110 - Oracle Database Server Java VM Unspecified Remote Code Execution (April 2018 CPU) - Oracle Database Server Multiple Vulnerabilities (Jan 2019 CPU)
Riesgo	Medio
Descripción	El servidor de base de datos remoto se ve afectado por múltiples vulnerabilidades.
Solución	Aplique el parche apropiado de acuerdo con el aviso de actualización de parches críticos de Oracle de la fecha correspondiente al anuncio de la vulnerabilidad.
Código Aplicaciones Afectadas	APP010-RRHH, APP012-SIET, APP019-SNIES, APP023-SACES, APP033-SIET Consultas publicas, APP054-SIACET, APP080-CONVSUPCH, APP084-PARES, APP014-SIMAT, APP015-SIMPADE, APP018-SIPI, APP017- SINEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE, APP022-SAC V1, APP111-CIER, APP034-SSDIPI, APP055-HECAA, APP104-SIPTA2 WEB, APP113-SISMA, APP125-SIFSE NVO, APP174-DELREP, APP233-SIA3, APP237-SIUCE, APP244-SAC V2

Vulnerabilidad (x8)	- PostgreSQL 8.3 < 8.3.23 / 8.4 < 8.4.16 / 9.0 < 9.0.12 / 9.1 < 9.1.8 / 9.2 < 9.2.3 Denial of Service - PostgreSQL 8.4 < 8.4.20 / 9.0 < 9.0.16 / 9.1 < 9.1.12 / 9.2 < 9.2.7 / 9.3 < 9.3.3 Multiple Vulnerabilities - PostgreSQL 9.0 < 9.0.13 / 9.1 < 9.1.9 / 9.2 < 9.2.4 File Deletion - PostgreSQL 9.0 < 9.0.19 / 9.1 < 9.1.15 / 9.2 < 9.2.10 / 9.3 < 9.3.6 / 9.4 < 9.4.1 Multiple Vulnerabilities - PostgreSQL 9.0.x < 9.0.23 / 9.1.x < 9.1.19 / 9.2.x < 9.2.14 / 9.3.x < 9.3.10 / 9.4.x < 9.4.5 Multiple Vulnerabilities - PostgreSQL 9.1 < 9.1.9 / 9.2 < 9.2.4 Denial of Service - PostgreSQL 9.1.x < 9.1.23 / 9.2.x < 9.2.18 / 9.3.x < 9.3.14 / 9.4.x < 9.4.9 / 9.5.x < 9.5.4 Multiple Vulnerabilities - PostgreSQL 9.3 < 9.3.23 / 9.4 < 9.4.18 / 9.5 < 9.5.13 / 9.6 < 9.6.9 / 10.3 Insecure ACL Remote Issue
Riesgo	Medio
Descripción	La versión de PostgreSQL instalada en el host, se ve afectado por múltiples vulnerabilidades según lo especificado por los registros de cambios de las respectivas versiones corregidas.

Solución	Actualice a PostgreSQL 8.3.23/8.4.20/9.0.23/9.1.23/9.2.18/9.3.23/9.4.18/9.5.13/9.6.9/10.4 o posterior.
Código Aplicaciones Afectadas	APP002-CNA, APP023-SACES, APP080-CONVSUPCH, APP084-PARES

Vulnerabilidad	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Riesgo	Medio
Descripción	El host admite el uso de un cifrado de bloque con bloques de 64 bits en uno o más conjuntos de cifrado. Por lo tanto, se ve afectado por una vulnerabilidad, conocida como SWEET32, debido al uso de cifrados de bloque débiles de 64 bits. Un atacante intermediario que tenga suficientes recursos puede explotar esta vulnerabilidad, a través de un ataque de 'birthday', para detectar una colisión que filtre el XOR entre el secreto fijo y un texto plano conocido, permitiendo la divulgación del texto secreto, como las cookies HTTPS seguras, y posiblemente resulte en el secuestro de una sesión autenticada.
Solución	Reconfigure la aplicación afectada, si es posible, para evitar el uso de todos los cifrados de bloque de 64 bits. Alternativamente, establezca limitaciones en la cantidad de solicitudes que se pueden procesar a través de la misma conexión TLS para mitigar esta vulnerabilidad.
Código Aplicaciones Afectadas	APP017- SINEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE

Vulnerabilidad	SSL Certificate Cannot Be Trusted
Riesgo	Medio
Descripción	No se puede confiar en el certificado SSL para este servicio.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP017- SINEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE

Vulnerabilidad	SSL Medium Strength Cipher Suites Supported (SWEET32)
Riesgo	Medio
Descripción	El host admite el uso de cifrados SSL que ofrecen cifrado de nivel medio. Nessus considera que la potencia media es cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el paquete de cifrado 3DES.
Solución	Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.
Código Aplicaciones Afectadas	APP017- SINEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE

Vulnerabilidad	SSL Self-Signed Certificate
Riesgo	Medio
Descripción	La cadena de certificados X.509 para este servicio no está firmada por una autoridad certificadora reconocida. Si el host es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque man-in-the-middle contra el host.
Solución	Compre o genere un certificado SSL adecuado para este servicio.
Código Aplicaciones Afectadas	APP017- SINEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE

Vulnerabilidad	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Riesgo	Medio
Descripción	El host se ve afectado por una vulnerabilidad de divulgación de información de man-in-the-middle (MitM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno al descifrar mensajes cifrados mediante cifrados de bloque en el modo de encadenamiento de bloques de cifrado (CBC). Los atacantes MitM pueden descifrar un byte seleccionado de un texto cifrado en tan solo 256 intentos si pueden obligar a una aplicación víctima a enviar repetidamente los mismos datos a través de conexiones SSL 3.0 recién creadas.

	Siempre que un cliente y un servicio sean compatibles con SSLv3, una conexión se puede "revertir" a SSLv3, incluso si el cliente y el servicio admiten TLSv1 o una versión posterior. El mecanismo TLS Fallback SCSV evita los ataques de "reversión de versiones" sin afectar a los clientes heredados; sin embargo, solo puede proteger las conexiones cuando el cliente y el servicio admiten el mecanismo. Los sitios que no pueden deshabilitar SSLv3 de inmediato deben habilitar este mecanismo. Esta es una vulnerabilidad en la especificación SSLv3, no en ninguna implementación de SSL en particular. Desactivar SSLv3 es la única forma de mitigar completamente la vulnerabilidad.
Solución	Desactive SSLv3. Los servicios que deben admitir SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que se pueda inhabilitar SSLv3.
Código Aplicaciones Afectadas	APP017- SINEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE

Vulnerabilidad	TLS Version 1.0 Protocol Detection
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 que tiene una serie de defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas contra estos defectos y deben usarse siempre que sea posible.
Solución	Habilite la compatibilidad con TLS 1.2 y 1.3 y desactive la compatibilidad con TLS 1.0.
Código Aplicaciones Afectadas	APP003-CONVSUP, APP030-CEBYM, APP073-SIISSE, APP119-VUMEN CRL, APP120-VUMEN RE, APP121-VUMEN IR, APP017-SINEB, APP114-SPADIES, APP155-SINEB PLANTAS, APP234-NUEVO SIGCE, APP074-SIISSE HIST, APP107-LALUPA, APP230-SICSUP, APP256-CONVALIDA, APP277-Nuevo Saces RC, APP322-GESPAR

Vulnerabilidad	TLS Version 1.1 Protocol Deprecated
Riesgo	Medio
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 no es compatible con los conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cálculo MAC y los modos de cifrado autenticado, como GCM, no se pueden usar con TLS 1.1
Solución	Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.
Código Aplicaciones Afectadas	APP003-CONVSUP, APP030-CEBYM, APP073-SIISSE, APP119-VUMEN CRL, APP120-VUMEN RE, APP121-VUMEN IR, APP074-SIISSE HIST, APP107-LALUPA, APP230-SICSUP, APP256-CONVALIDA, APP277-Nuevo Saces RC, APP322-GESPAR

Vulnerabilidad	Web Server HTTP Header Information Disclosure
Riesgo	Medio
Descripción	Los encabezados HTTP enviados por el servidor web remoto revelan información que puede ayudar a un atacante, como la versión del servidor y los idiomas utilizados por el servidor web.
Solución	Modifique los encabezados HTTP del servidor web para no revelar información detallada sobre el servidor web subyacente.
Código Aplicaciones Afectadas	APP047-SIMAT BI13A y SIMPADE

Tabla 20. Vulnerabilidades Medias sobre los servidores de bases de datos del ambiente de producción de los sistemas misionales

4.4.4 ANÁLISIS Y RECOMENDACIÓN VULNERABILIDADES BAJAS

Vulnerabilidad	MariaDB 10.1.0 < 10.1.41 Multiple Vulnerabilities
Riesgo	Bajo
Descripción	La versión de MariaDB instalada en el host es anterior a la 10.1.41. Por lo tanto, se ve afectado por las siguientes vulnerabilidades, como se menciona en el aviso mdb-10141-rn. - Una vulnerabilidad en el 'Servidor: Autenticación conectable'

	subcomponente Esta es una vulnerabilidad fácilmente explotable que permite que un atacante altamente privilegiado con acceso a la red a través de múltiples protocolos comprometa el servidor MariaDB. Los ataques exitosos que involucren esta vulnerabilidad pueden resultar en la capacidad no autorizada de provocar un bloqueo o bloqueo repetible (DOS completo) del servidor MariaDB. (CVE-2019-2737) - Una vulnerabilidad en el 'Servidor: Seguridad: Privilegios' subcomponente Esta es una vulnerabilidad fácilmente explotable que permite que un atacante con muchos privilegios, que puede iniciar sesión en la infraestructura donde se ejecuta el servidor MariaDB, comprometa el servidor MariaDB. Los ataques exitosos que involucren esta vulnerabilidad pueden resultar en la capacidad no autorizada de provocar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) del servidor MariaDB, así como la actualización, inserción o eliminación no autorizadas del acceso a algunos de los datos accesibles al servidor MariaDB. (CVE-2019-2739) - Una vulnerabilidad en el subcomponente 'Servidor: XML'. Esta es una vulnerabilidad fácilmente explotable que permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos comprometa un servidor MariaDB. Los ataques exitosos que involucren esta vulnerabilidad pueden resultar en la capacidad no autorizada de provocar un bloqueo o falla repetible (DOS completo) de MariaDB Servidor. (CVE-2019-2740) - Una vulnerabilidad en el subcomponente 'Server: Parser'. Esta es una vulnerabilidad fácilmente explotable que permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos comprometa el servidor MariaDB. Los ataques exitosos que involucren esta vulnerabilidad pueden resultar en la capacidad no autorizada de provocar un bloqueo o bloqueo repetible (DOS completo) del servidor MariaDB. (CVE-2019-2805)
Solución	Actualice a MariaDB versión 10.1.41 o posterior
Código Aplicaciones Afectadas	APP251-SUPSA

Vulnerabilidad	MySQL < 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 Client XSS
Riesgo	Bajo
Descripción	La versión de MySQL instalada en el host es anterior a 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 y, por lo tanto, no codifica correctamente los corchetes angulares cuando se usa la opción 'mysql --html'. Dependiendo de cómo se procese la salida del comando del cliente mysql, el usuario puede ser vulnerable a ataques de secuencias de comandos entre sitios.
Solución	Actualice a MySQL versión 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 o posterior.
Código Aplicaciones Afectadas	APP126-CNC

Vulnerabilidad	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Riesgo	Bajo
Descripción	Al menos uno de los certificados X.509 enviados por el host remoto tiene una clave de menos de 2048 bits. De acuerdo con los estándares de la industria establecidos por el foro de la autoridad de certificación/navegador (CA/B), los certificados emitidos después del 1 de enero de 2014 deben tener al menos 2048 bits. Algunas implementaciones SSL de navegador pueden rechazar claves de menos de 2048 bits después del 1 de enero de 2014. Además, algunos proveedores de certificados SSL pueden revocar certificados de menos de 2048 bits antes del 1 de enero de 2014
Solución	Reemplace el certificado en la cadena con la clave RSA de menos de 2048 bits de longitud con una clave más larga y vuelva a emitir cualquier certificado firmado por el certificado anterior.
Código Aplicaciones Afectadas	APP230-SICSUP

Tabla 21. Vulnerabilidades Bajas sobre los servidores de bases de datos del ambiente de producción de los sistemas misionales

5 RESUMEN EJECUTIVO CRITICIDAD DE LAS VULNERABILIDADES IDENTIFICADAS

La criticidad de las diferentes vulnerabilidades detectadas en las aplicaciones seleccionadas del primer escenario, en donde se evaluaron los servidores de aplicación del ambiente de certificación, se resumen en la siguiente gráfica:

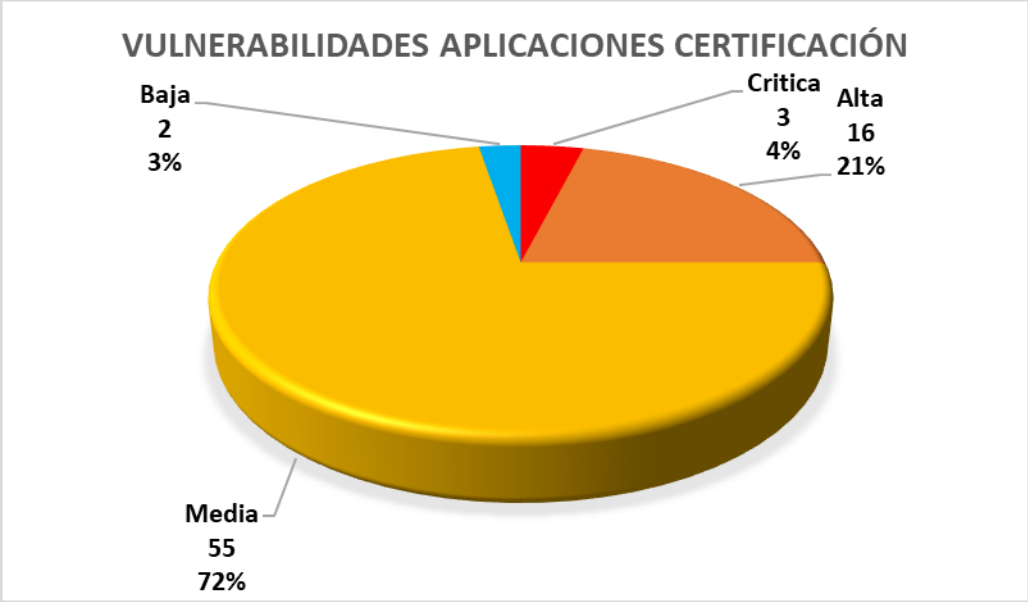

Gráfico 1: Criticidad de las vulnerabilidades detectadas en los servidores de aplicación del ambiente de certificación de los sistemas misionales

De allí se observa que más de la mitad de las vulnerabilidades identificadas tienen una criticidad de nivel medio, seguido de vulnerabilidades de criticidad alta, critica y baja. Para el caso de las vulnerabilidades distribuidas sobre los servidores de bases de datos en el ambiente de certificación, se tiene el siguiente resultado:

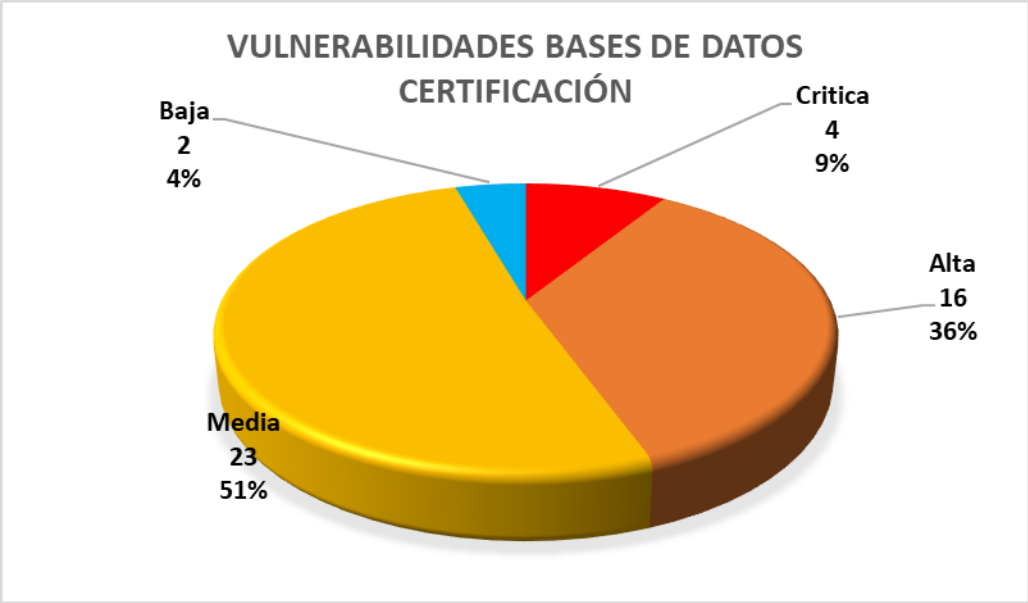

Gráfico 2: Criticidad de las vulnerabilidades detectadas en los servidores de bases de datos del ambiente de certificación de los sistemas misionales

Se presenta un caso similar en el sentido de que más de la mitad de las vulnerabilidades identificadas tienen una criticidad de nivel medio, seguido de vulnerabilidades de criticidad alta, crítica y baja. La mayoría de ellas tienen que ver con el versionamiento a nivel de Oracle, por lo cual su mitigación depende en gran medida de que se puedan actualizar las plataformas de bases de datos.

Para los servidores que soportan las aplicaciones seleccionadas del ambiente de producción, las diferentes vulnerabilidades encontradas tienen la siguiente distribución de criticidad.

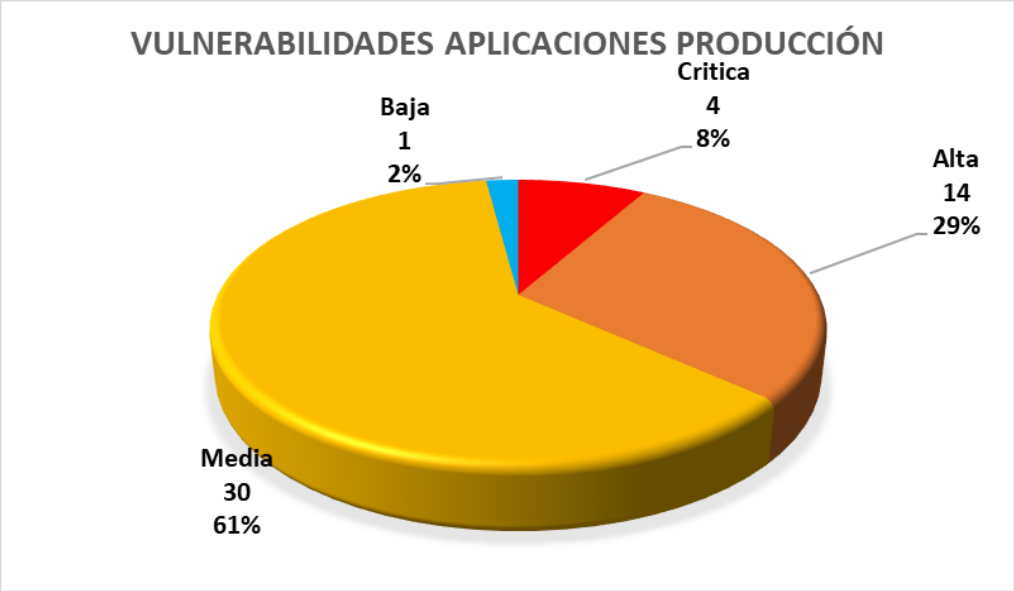

Gráfico 3: Criticidad de las vulnerabilidades detectadas en los servidores de aplicación del ambiente de producción de los sistemas misionales

Sobre estos servidores se encuentra una mayoría de vulnerabilidades de severidad media seguida de severidades alta, critica y baja. En cuanto a lo obtenido a nivel de bases de datos para las aplicaciones de producción, se tiene también una mayoría de vulnerabilidades de criticidad media, seguida por vulnerabilidades de criticidad alta, critica y baja como se puede ver en la siguiente imagen:

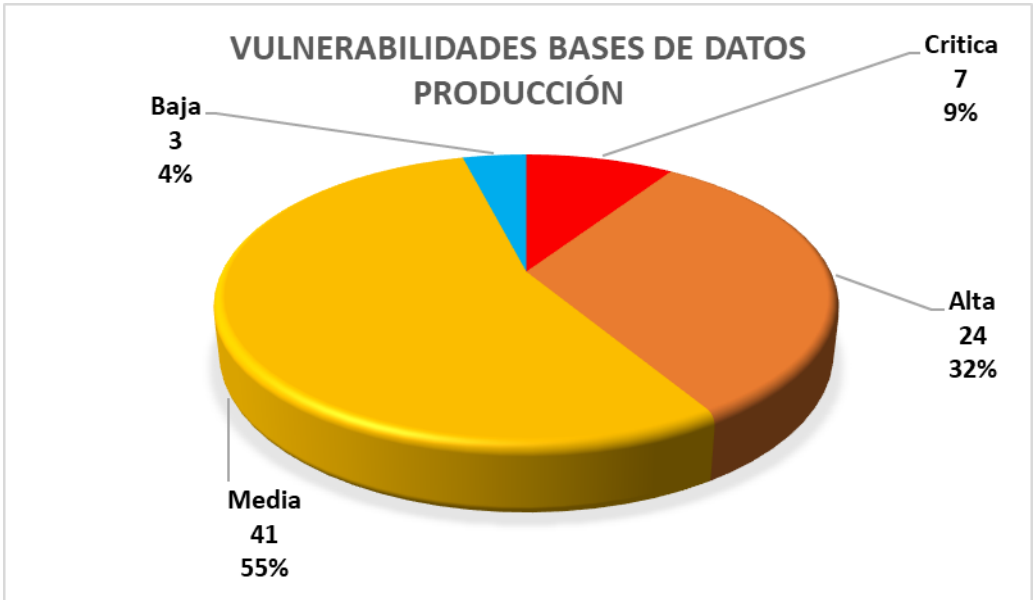

Gráfico 4: Criticidad de las vulnerabilidades detectadas en los servidores de bases de datos del ambiente de producción de los sistemas misionales

La mayoría de las vulnerabilidades representadas por las versiones detectadas de MariaDB, MySQL y Oracle y cuya mitigación depende en gran medida de un proceso de actualización. En base a las vulnerabilidades encontradas de acuerdo al anexo “Vulnerabilidades_Trimestre_7.xlsx”, clasificándolas por escenario y severidad, tenemos el siguiente resultado:

	Vulnerabilidades				
Escenario	**Criticas**	**Altas**	**Medias**	**Bajas**	**Total**
Certificación Aplicación	8	19	79	2	108
Certificación Base de Datos	18	150	87	4	259
Producción Aplicación	18	111	92	1	222
Producción Base de Datos	73	422	285	5	785
Total	**117**	**702**	**543**	**12**	**1374**

Tabla 22. Cantidad de Vulnerabilidades detectadas por criticidad y escenario en los servidores que soportan las aplicaciones misionales del Ministerio de Educación.

6 CONCLUSIONES Y RECOMENDACIONES

Una vez finalizado el proceso de escaneo y análisis de vulnerabilidades se presentan las siguientes conclusiones y recomendaciones:

- Se identifican vulnerabilidades asociadas a la utilización de software con algún nivel de obsolescencia como versiones de PHP, Apache Tomcat, Apache, Oracle, MySQL, jquery, entre otros, ya que la utilización de versiones obsoletas es la que más genera vulnerabilidades y su remediación depende principalmente de un proceso de actualización.

- Se recomienda a los especialistas en su proceso de mitigación dar prioridad a la remediación de las vulnerabilidades para las cuales existen exploits disponible y que tienen nivel de riesgo Crítico y Alto, debido a que la probabilidad de ser explotadas es mayor y la materialización del riesgo representaría un impacto considerable.

- Se recomienda al Ministerio evaluar el aislamiento a nivel de red de los servidores y servicios con vulnerabilidades que no puedan ser remediadas, de modo que sólo puedan ser accedidos por los usuarios y/o sistemas autorizados.

- Se recomienda al Ministerio evaluar la vigencia de las aplicaciones que se encuentran en desuso con el fin de disminuir una superficie de ataque con respecto a aplicaciones que por su antigüedad aportan mayor cantidad de vulnerabilidades.

7 ANEXOS

- Sistemas_Trimestre_7.xlsx
- Vulnerabilidades_Trimestre_7.xlsx
- SERVIDORES_CERT_APP.html
- SERVIDORES_CERT_BD.html
- SERVIDORES_PROD_APP.html
- SERVIDORES_PROD_BD.html

Información del documento

Fecha	Versión	Responsable	Revisado por	Aprobado por
24/10/2022	1.0	Especialista Seguridad Informática	Gerente de Proyecto Líder de Integración de Servicios y Operaciones Líder de Gestión Técnica y Seguridad	

Control de cambios

Fecha	Versión	Causa Cambio	Responsable
24/10/2022	1.0	Creación del Documento	Especialista Seguridad Informática

Edison Javier Guerrero Vergel
ejguerrero@eservicios.indracompany.com

Calle 96 # 13 - 11
Bogotá, Colombia

www.minsait.com