Entidad	Fondo de Previsión Social del Congreso de la República - FONPRECON		
Fecha de la prueba	21/06/2025		
Fecha del informe	25/06/2025		
Tipo de reporte	Prueba de Vulnerabilidades red interna		
Activos	10.0.0.1	10.0.0.24	10.0.0.42
	10.0.0.102	10.0.0.25	10.0.0.43
	10.0.0.11	10.0.0.26	10.0.0.44
	10.0.0.13	10.0.0.27	10.0.0.47
	10.0.0.14	10.0.0.28	10.0.0.50
	10.0.0.15	10.0.0.29	10.0.0.8
	10.0.0.151	10.0.0.30	10.0.0.9
	10.0.0.160	10.0.0.31	10.0.0.90
	10.0.0.17	10.0.0.32	10.0.0.91
	10.0.0.18	10.0.0.34	10.0.0.98
	10.0.0.19	10.0.0.35	fdonas2
	10.0.0.20	10.0.0.36	fdorespaldos
	10.0.0.21	10.0.0.37	fdostg01.fonprecon.red
	10.0.0.22	10.0.0.40	
	10.0.0.23	10.0.0.41	
Observaciones	Total direcciones IP 43		

Descripción de la prueba:

Esta prueba se realiza sobre la infraestructura local (Red LAN) del Fondo de Previsión Social del Congreso de la República - FONPRECON, tanto para dispositivos como para servicios web, según su disposición de inventario. Se aplican para evaluar el nivel de vulnerabilidad de los dispositivos que gestionan internamente la infraestructura informática de la entidad.

El escenario empleado para la prueba es el correspondiente a Caja Gris o también llamadas Sombrero Gris. En este escenario se tiene visibilidad de los activos sin injerencia de los equipos de seguridad de la entidad, lo que permite una mayor profundidad de las pruebas.

No obstante, es de precisar que no se cuentan con las credenciales de los activos a escanear.

Previo al escaneo de vulnerabilidades, fue realizado un sondeo con la herramienta para identificar, a partir de los segmentos de red, los activos accesibles y los que serían objeto de la evaluación.

Resumen del informe:

Producto del análisis de vulnerabilidades realizado desde el CSIRT Salud a la infraestructura tecnológica interna de FONPRECON, se presentan a continuación los resultados obtenidos:

Crítico	Alto	Medio	Bajo	Total
135	101	366	84	686

Tabla 1 Resultados por criticidad

De acuerdo con las pruebas ejecutadas se identificaron **686** vulnerabilidades **Totales**[1] que incluyen **135** vulnerabilidades de nivel **Crítico**, **101** de vinel **Alto**, **366** de nivel **Medio** y **84** de nivel **Bajo**. La distribución de las vulnerabilidades se presenta a continuación:

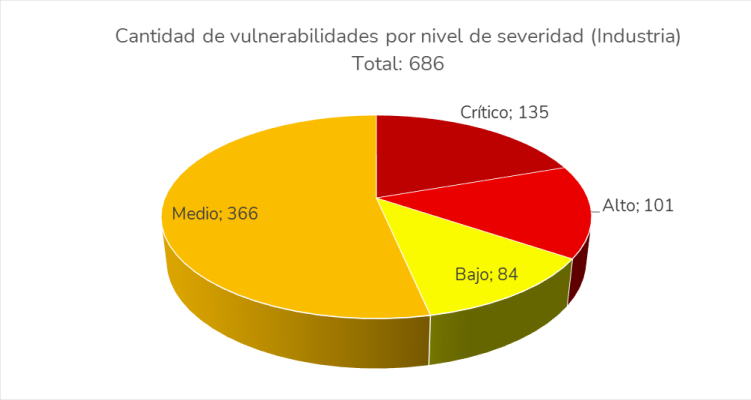


Ilustración 1. Vulnerabilidades por nivel de severidad

[1] Las vulnerabilidades se encuentran distribuidas sobre todos los dispositivos evaluados. Sin embargo, estas se pueden encontrar en más de un equipo, en un mismo equipo por más de un puerto y/o relacionadas por la misma versión vulnerable. Por lo tanto, una acción de remediación sobre una vulnerabilidad podría corregir múltiples vulnerabilidades en el mismo equipo.

A continuación, se presenta el top 10 de los activos con vulnerabilidades más críticas:

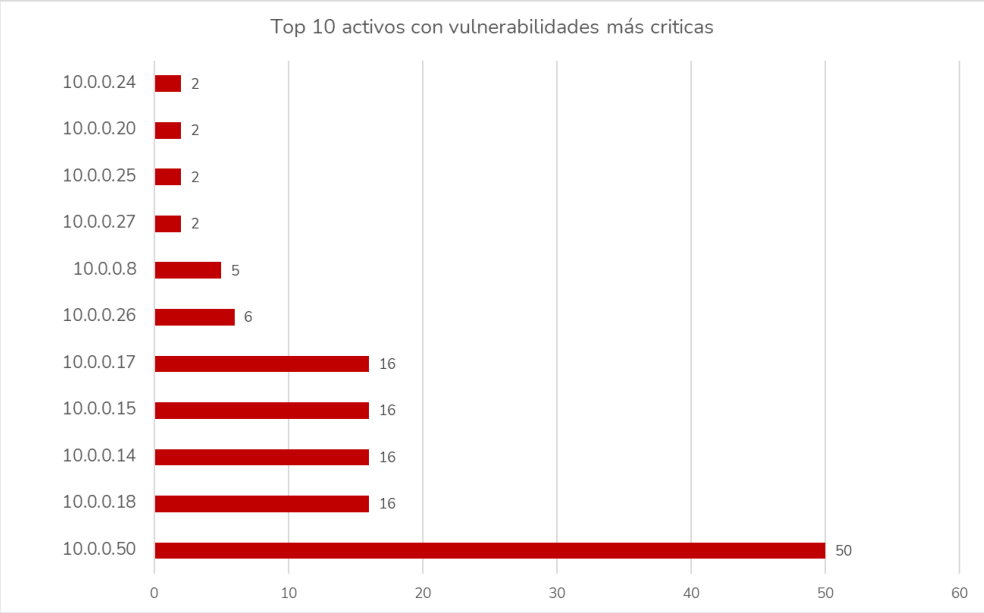


Ilustración 2. Top de activos con vulnerabilidades más críticas

De acuerdo con la ilustración 2 se puede identificar que el activo **10.0.0.50** cuenta con la mayor cantidad de vulnerabilidades críticas (50).

Por otro lado, se presentan a continuación las vulnerabilidades con mayor criticidad:

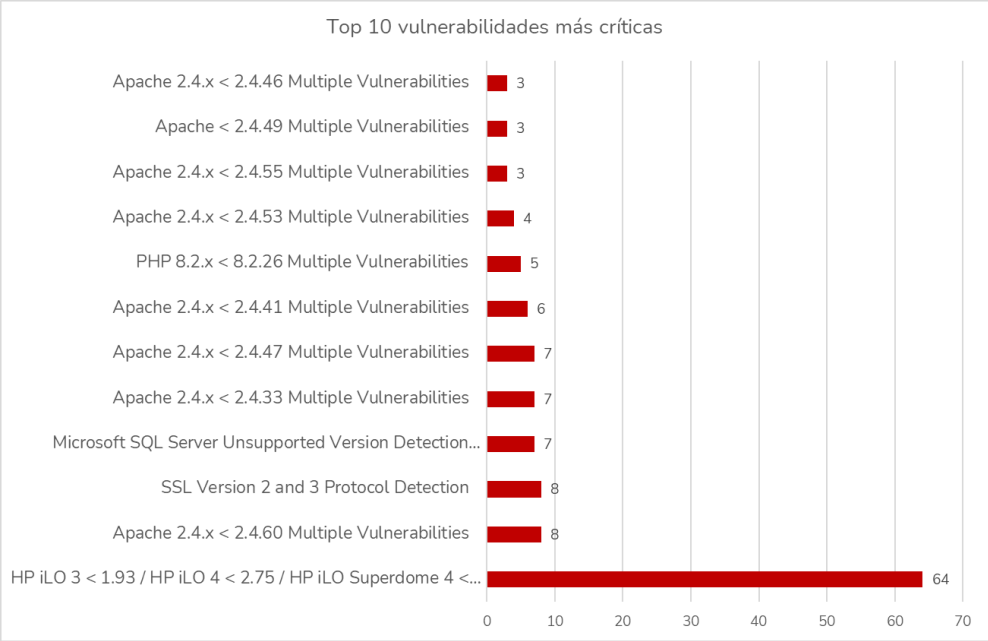


Ilustración 3. Top de vulnerabilidades más críticas

Las vulnerabilidades más críticas están relacionadas con interfaces de administración iLO (de Hewlett Packard) desactualizadas, versiones vulnerables del software de Apache y PHP, protocolos de SSLv2/v3 implementados, así como una versión de Microsoft SQL que ya no se encuentra soportada.

1. Vulnerabilidades identificadas de nivel Crítico:

Conforme a los resultados obtenidos fueron identificadas 135 vulnerabilidades de nivel Crítico. A continuación, se presentan las instancias asociadas por vulnerabilidad:

Vulnerabilidad	Cantidad	No Instancias	Instancia
HP iLO 3 < 1.93 / HP iLO 4 < 2.75 / HP iLO Superdome 4 < 1.64 / HP iLO 5 < 2.18 / HP Moonshot/Edgeline iLO 5 < 2.30 Ripple20 Multiple vulnerabilities • Installed version: 2.70	64	4	10.0.0.14 10.0.0.15 10.0.0.17 10.0.0.18

Vulnerabilidad	Cantidad	No Instancias	Instancia
SSL Version 2 and 3 Protocol Detection	8	5	10.0.0.20 10.0.0.24 10.0.0.25 10.0.0.26 10.0.0.27
Microsoft SQL Server Unsupported Version Detection (remote check). • SQL Server Instance: VEEAMSQL2012 - version: 11.0.7507.0 • SQL Server Instance: VEEAMSQL2012 - version: 11.0.7507.0 • SQL Server Instance: MSSQLSERVER - version: 12.0.5223.0 • SQL Server Instance: PREPRUEBAS - version: 12.0.5223.0 • SQL Server Instance: DESARROLLO - version: 12.0.5223.0 • SQL Server Instance: MSSQLSERVER - version: 10.50.4339.0 • SQL Server Instance: SAT - version: 13.0.5893.0	7	5	10.0.0.24 10.0.0.25 10.0.0.26 10.0.0.27 10.0.0.47
Dell iDRAC Buffer Overflow Vulnerability (CVE-2020-5344) • Installed version: iDRAC7 with firmware 2.52.52.52.12	1	1	10.0.0.110
PHP 8.2.x < 8.2.26 Multiple Vulnerabilities	5	1	10.0.0.8
PHP Unsupported Version Detection • Installed version: 5.4.45	1	1	10.0.0.50
Apache 2.4.x < 2.4.60 Multiple Vulnerabilities	8	1	
Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	7	1	
Apache 2.4.x < 2.4.47 Multiple Vulnerabilities	7	1	
Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	6	1	
Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	4	1	
Apache < 2.4.49 Multiple Vulnerabilities	3	1	
Apache 2.4.x < 2.4.46 Multiple Vulnerabilities	3	1	
Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	3	1	
Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	2	1	
Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	2	1	

Vulnerabilidad	Cantidad	No Instancias	Instancia
Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	2	1	
Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow	1	1	
Apache 2.4.x < 2.4.54 Authentication Bypass	1	1	

Tabla 2 Vulnerabilidades críticas, instancias

Para más información y detalle sobre las vulnerabilidades críticas se puede consultar el documento "**Anexo 1. Matriz de vulnerabilidades tecnológicas**".

2. Vulnerabilidades identificadas de nivel Alto:

Conforme a los resultados obtenidos fueron identificadas 101 vulnerabilidades con nivel de criticidad Alto. A continuación, se presentan las instancias asociadas por vulnerabilidad:

Vulnerabilidad	Cantidad	No Instancias	Instancia
SSL Medium Strength Cipher Suites Supported (SWEET32)	41	28	10.0.0.102, 10.0.0.11, 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.160, 10.0.0.17, 10.0.0.18, 10.0.0.19, 10.0.0.20, 10.0.0.21, 10.0.0.22, 10.0.0.23, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27, 10.0.0.28, 10.0.0.34, 10.0.0.35, 10.0.0.36, 10.0.0.40, 10.0.0.41, 10.0.0.42, 10.0.0.47, 10.0.0.50, 10.0.0.90, 10.0.0.91
SSH Protocol Version 1 Session Key Retrieval	9	3	10.0.0.151, 10.0.0.31, 10.0.0.32
iLO 4 < 2.80 DoS • Installed version : 2.70	8	4	10.0.0.14, 10.0.0.15, 10.0.0.17, 10.0.0.18
SNMP Agent Default Community Name (public)	5	5	10.0.0.109, 10.0.0.110, 10.0.0.162, 10.0.0.20, 10.0.0.98
PHP 8.2.x < 8.2.28 Multiple Vulnerabilities	5	1	10.0.0.8

Vulnerabilidad	Cantidad	No Instancias	Instancia
Dell iDRAC Products Multiple Vulnerabilities (June 2018) • Installed version: iDRAC7 with firmware 2.52.52.52.12	4	1	10.0.0.110
Dell iDRAC Products Multiple Vulnerabilities (December 2018) • Installed version: iDRAC7 with firmware 2.52.52.52.12	2	1	10.0.0.110
IPMI v2.0 Password Hash Disclosure	3	3	10.0.0.13, 10.0.0.15, 10.0.0.18
PHP < 7.3.24 Multiple Vulnerabilities • Installed version: 5.4.45	1	1	10.0.0.50
Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	2	1	10.0.0.50
Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	2	1	
Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)	2	1	
Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	3	1	
Apache 2.4.x < 2.4.59 Multiple Vulnerabilities	3	1	
Apache 2.4.x < 2.4.39 Multiple Vulnerabilities	6	1	
Apache >= 2.4.17 < 2.4.49 mod_http2	1	1	
Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	1	1	
Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)	1	1	

Vulnerabilidad	Cantidad	No Instancias	Instancia
Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability	1	1	
Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)	1	1	

Tabla 3 Vulnerabilidades altas, instancias

Para más información y detalle sobre las vulnerabilidades Altas se puede consultar el documento "**Anexo 1. Matriz de vulnerabilidades tecnológicas**".

3. Vulnerabilidades identificadas de nivel Medio:

Conforme a los resultados obtenidos fueron identificadas 366 vulnerabilidades de nivel Medio. A continuación, se presentan las instancias asociadas por vulnerabilidad:

Vulnerabilidad	Cantidad	No Instancias	Instancia
SSL Certificate Cannot Be Trusted	59	36	10.0.0.1, 10.0.0.102, 10.0.0.109, 10.0.0.11, 10.0.0.110, 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.160, 10.0.0.162, 10.0.0.17, 10.0.0.18, 10.0.0.19, 10.0.0.20, 10.0.0.21, 10.0.0.22, 10.0.0.23, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27, 10.0.0.28, 10.0.0.29, 10.0.0.34, 10.0.0.35, 10.0.0.36, 10.0.0.40, 10.0.0.41, 10.0.0.42, 10.0.0.43, 10.0.0.44, 10.0.0.47, 10.0.0.50, 10.0.0.9, 10.0.0.90, 10.0.0.91
SSL Self-Signed Certificate	47	29	10.0.0.1, 10.0.0.102, 10.0.0.109, 10.0.0.11, 10.0.0.110, 10.0.0.160, 10.0.0.162, 10.0.0.19, 10.0.0.20, 10.0.0.21, 10.0.0.22, 10.0.0.23, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27, 10.0.0.28, 10.0.0.34, 10.0.0.35, 10.0.0.36, 10.0.0.40, 10.0.0.41, 10.0.0.42, 10.0.0.43,

Vulnerabilidad	Cantidad	No Instancias	Instancia
			10.0.0.47, 10.0.0.50, 10.0.0.9, 10.0.0.90, 10.0.0.91
TLS Version 1.1 Deprecated Protocol	42	28	10.0.0.102, 10.0.0.109, 10.0.0.11, 10.0.0.110, 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.160, 10.0.0.162, 10.0.0.17, 10.0.0.18, 10.0.0.19, 10.0.0.23, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27, 10.0.0.28, 10.0.0.34, 10.0.0.35, 10.0.0.36 10.0.0.40, 10.0.0.41, 10.0.0.42, 10.0.0.47, 10.0.0.50, 10.0.0.90, 10.0.0.91
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	42	11	10.0.0.160, 10.0.0.19, 10.0.0.20, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27, 10.0.0.35, 10.0.0.42, 10.0.0.47, 10.0.0.50
TLS Version 1.0 Protocol Detection	39	26	10.0.0.102, 10.0.0.11, 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.160, 10.0.0.17, 10.0.0.18, 10.0.0.19, 10.0.0.20, 10.0.0.23, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27, 10.0.0.28, 10.0.0.34, 10.0.0.35, 10.0.0.36, 10.0.0.40, 10.0.0.41, 10.0.0.42, 10.0.0.47, 10.0.0.50, 10.0.0.90, 10.0.0.91
SSL Certificate with Wrong Hostname	36	22	10.0.0.102, 10.0.0.160, 10.0.0.19, 10.0.0.21, 10.0.0.22, 10.0.0.23, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27, 10.0.0.28, 10.0.0.34, 10.0.0.35, 10.0.0.36, 10.0.0.40, 10.0.0.41, 10.0.0.42, 10.0.0.47, 10.0.0.50, 10.0.0.9, 10.0.0.90, 10.0.0.91
SSL Certificate Signed Using Weak Hashing Algorithm	34	11	10.0.0.109, 10.0.0.11, 10.0.0.110, 10.0.0.13, 10.0.0.18, 10.0.0.20, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27, 10.0.0.47
SMB Signing not required	20	20	10.0.0.102, 10.0.0.160, 10.0.0.19, 10.0.0.23, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27, 10.0.0.28,

Vulnerabilidad	Cantidad	No Instancias	Instancia
			10.0.0.34, 10.0.0.35, 10.0.0.36, 10.0.0.40, 10.0.0.41, 10.0.0.42, 10.0.0.47, 10.0.0.50, 10.0.0.9, 10.0.0.90, 10.0.0.91
SSL Certificate Expiry	11	7	10.0.0.109, 10.0.0.11, 10.0.0.110, 10.0.0.160, 10.0.0.20, 10.0.0.29, 10.0.0.44
Terminal Services Doesn't Use Network Level Authentication (NLA) Only	8	8	10.0.0.19, 10.0.0.27, 10.0.0.35, 10.0.0.40, 10.0.0.41, 10.0.0.50, 10.0.0.90, 10.0.0.91
JQuery 1.2 < 3.5.0 Multiple XSS	4	2	10.0.0.1 10.0.0.43
Unencrypted Telnet Server	4	4	10.0.0.11, 10.0.0.151, 10.0.0.31, 10.0.0.32
SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	3	3	10.0.0.109 10.0.0.110 10.0.0.162
SSH Weak Algorithms Supported	3	3	10.0.0.151 10.0.0.20 10.0.0.32
SNMP 'GETBULK' Reflection DDoS	1	1	10.0.0.98
Remote Desktop Protocol Server Man-in-the-Middle Weakness	1	1	10.0.0.27
Terminal Services Encryption Level is Medium or Low	1	1	10.0.0.27
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	1	1	10.0.0.20

Vulnerabilidad	Cantidad	No Instancias	Instancia
HTTP TRACE / TRACK Methods Allowed	3	1	10.0.0.50
PHP < 7.3.28 Email Header Injection	1	1	10.0.0.50
Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)	1	1	10.0.0.50
Apache 2.4.x < 2.4.42 Multiple Vulnerabilities	2	1	10.0.0.50
Apache Multiviews Arbitrary Directory Listing	2	2	10.0.0.30 10.0.0.37
Apache 2.4.x < 2.4.35 DoS	1	1	10.0.0.50

Tabla 4 Vulnerabilidades medias, instancias

Para más información y detalle sobre las vulnerabilidades Medias se puede consultar el documento "**Anexo 1. Matriz de vulnerabilidades tecnológicas**".

4. Vulnerabilidades identificadas de nivel Bajo:

Conforme a los resultados obtenidos fueron identificadas 84 vulnerabilidades de nivel Bajo. A continuación, se presentan las instancias asociadas por vulnerabilidad:

Vulnerabilidad	Cantidad	No Instancias	Instancia
ICMP Timestamp Request Remote Date Disclosure	30	30	10.0.0.102, 10.0.0.151, 10.0.0.160, 10.0.0.19, 10.0.0.20, 10.0.0.21, 10.0.0.22, 10.0.0.23, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27, 10.0.0.28, 10.0.0.30, 10.0.0.31, 10.0.0.32, 10.0.0.34, 10.0.0.35, 10.0.0.36, 10.0.0.37, 10.0.0.40,

Vulnerabilidad	Cantidad	No Instancias	Instancia
			10.0.0.41, 10.0.0.42, 10.0.0.44, 10.0.0.47, 10.0.0.50, 10.0.0.8, 10.0.0.9, 10.0.0.90, 10.0.0.91
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	14	10	10.0.0.109, 10.0.0.110, 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.17, 10.0.0.18, 10.0.0.20, 10.0.0.26, 10.0.0.27
SSH Weak Key Exchange Algorithms Enabled	10	10	10.0.0.11, 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.151, 10.0.0.17, 10.0.0.18, 10.0.0.20, 10.0.0.31, 10.0.0.32
SSH Weak MAC Algorithms Enabled	9	9	10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.151, 10.0.0.17, 10.0.0.18, 10.0.0.20, 10.0.0.31, 10.0.0.32
SSH Server CBC Mode Ciphers Enabled	9	9	10.0.0.11, 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.151, 10.0.0.17, 10.0.0.18, 10.0.0.20, 10.0.0.32
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	7	7	10.0.0.20, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	4	2	10.0.0.24 10.0.0.25
Terminal Services Encryption Level is not FIPS-140 Compliant	1	1	10.0.0.27

Tabla 5 Vulnerabilidades bajas, instancias

Para más información y detalle sobre las vulnerabilidades Bajas se puede consultar el documento "**Anexo 1. Matriz de vulnerabilidades tecnológicas**".

5. Recomendaciones para la mitigación:

Desde el CSIRT Salud se pone en consideración las siguientes recomendaciones para la respectiva evaluación y/o adopción por parte del equipo de infraestructura y/o desarrollo:

- Vulnerabilidades de nivel Crítico:

Vulnerabilidad	Recomendación
HP iLO 3 < 1.93 / HP iLO 4 < 2.75 / HP iLO Superdome 4 < 1.64 / HP iLO 5 < 2.18 / HP Moonshot/Edgeline iLO 5 < 2.30 Ripple20 Multiple vulnerabilities	Actualizar a la versión de firmware HP iLO 3 1.93 o posterior, a la versión de firmware 2.75 o posterior de iLO 4, o a la versión 1.64 o posterior de iLO 4 para Superdome, o a la versión 2.18 del firmware HP iLO 5 o a la versión 2.30 o posterior.
Apache 2.4.x < 2.4.60 Multiple Vulnerabilities	Actualizar a la versión 2.4.60 o posterior de Apache.
SSL Version 2 and 3 Protocol Detection	Consultar la documentación de la aplicación para desactivar SSL 2.0 y 3.0. En su lugar, utilizar TLS 1.2 (con conjuntos de cifrado aprobados) o superior.
Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	Actualizar a la versión 2.4.33 o posterior de Apache.
Apache 2.4.x < 2.4.47 Multiple Vulnerabilities	Actualizar a la versión 2.4.47 o posterior de Apache.
Microsoft SQL Server Unsupported Version Detection (remote check)	Actualizar a una versión de Microsoft SQL Server que tenga soporte actualmente.
Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	Actualizar a la versión 2.4.41 o posterior de Apache.
PHP 8.2.x < 8.2.26 Multiple Vulnerabilities	Actualizar a la versión 8.2.26 o posterior de PHP.
Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	Actualizar a la versión 2.4.53 o posterior de Apache.
Apache < 2.4.49 Multiple Vulnerabilities	Actualizar a la versión 2.4.49 o posterior de Apache.
Apache 2.4.x < 2.4.46 Multiple Vulnerabilities	Actualizar a la versión 2.4.46 o posterior de Apache.
Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	Actualizar a la versión 2.4.55 o posterior de Apache.
Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Actualizar a la versión 2.4.54 o posterior de Apache.
Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Actualizar a la versión 2.4.56 o posterior de Apache.
Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	Actualizar a la versión 2.4.52 o posterior de Apache.
Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow	Actualizar a la versión 2.4.52 o posterior de Apache.
Apache 2.4.x < 2.4.54 Authentication Bypass	Actualizar a la versión 2.4.54 o posterior de Apache.

Vulnerabilidad	Recomendación
Dell iDRAC Buffer Overflow Vulnerability (CVE-2020-5344)	Actualizar el host remoto a iDRAC7 firmware 2.65.65.65 o iDRAC8 firmware 2.70.70.70, o iDRAC9 firmware 4.00.00.00 o superior.
PHP Unsupported Version Detection	Actualizar a una versión de PHP que sea compatible actualmente.

Tabla 6 Recomendaciones de mitigación, vulnerabilidades críticas

- Vulnerabilidades de nivel Alto:

Vulnerabilidad	Recomendación
SSL Medium Strength Cipher Suites Supported (SWEET32)	Volver a configurar la aplicación afectada si es posible para evitar el uso de cifrados de intensidad media.
SSH Protocol Version 1 Session Key Retrieval	Deshabilitar la compatibilidad con la versión 1 del protocolo SSH.
iLO 4 < 2.80 DoS	Actualizar el firmware a la versión 2.80 o posterior.
Apache 2.4.x < 2.4.39 Multiple Vulnerabilities	Actualizar a la versión 2.4.39 o posterior de Apache.
SNMP Agent Default Community Name (public)	Deshabilitar el servicio SNMP en el host remoto si no lo utiliza. Filtrar los paquetes UDP entrantes que van a este puerto o cambie la cadena de comunidad predeterminada.
PHP 8.2.x < 8.2.28 Multiple Vulnerabilities	Actualizar a la versión 8.2.28 o posterior de PHP.
Dell iDRAC Products Multiple Vulnerabilities (June 2018)	Actualizar el host remoto a iDRAC 6 firmware 2.91, iDRAC7/iDRAC8 firmware 2.60.60.60 o iDRAC9 firmware 3.21.21.21 o superior.
IPMI v2.0 Password Hash Disclosure	No hay parche para esta vulnerabilidad; es un problema inherente a la especificación de IPMI v2.0. Entre las mitigaciones sugeridas se incluyen las siguientes: • Deshabilitar IPMI a través de LAN si no es necesario. • Filtrar el tráfico dirigido hacia el puerto TCP 623 en los equipos que tienen esta vulnerabilidad. • Usar contraseñas seguras para limitar el éxito de los ataques de diccionario fuera de línea.

Vulnerabilidad	Recomendación
	• Usar listas de control de acceso (ACL) o redes aisladas para limitar el acceso a las interfaces de administración de IPMI.
Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	Actualizar a la versión 2.4.38 o posterior de Apache.
Apache 2.4.x < 2.4.59 Multiple Vulnerabilities	Actualizar a la versión 2.4.59 o posterior de Apache.
Dell iDRAC Products Multiple Vulnerabilities (December 2018)	Actualizar el host remoto a iDRAC7/iDRAC8 firmware 2.61.60.60 o iDRAC9 firmware 3.20.21.20, 3.21.24.22, 3.21.26.22, 3.23.23.23 o superior.
Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	Actualizar a la versión 2.4.34 o posterior de Apache.
Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	Actualizar a la versión 2.4.58 o posterior de Apache.
Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)	Actualizar a la versión 2.4.54 o posterior de Apache.
PHP < 7.3.24 Multiple Vulnerabilities	Actualizar a la versión 7.3.24 o posterior de PHP.
Apache >= 2.4.17 < 2.4.49 mod_http2	Actualizar a la versión 2.4.49 o posterior de Apache.
Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Actualizar a la versión 2.4.54 o posterior de Apache.
Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)	Actualizar a la versión 2.4.58 o posterior de Apache.
Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability	Actualizar a la versión 2.4.54 o posterior de Apache.
Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)	Actualizar a la versión 2.4.62 o posterior de Apache.

Tabla 7 Recomendaciones de mitigación, vulnerabilidades altas

- Vulnerabilidades medias:

Vulnerabilidad	Recomendación
SSL Certificate Cannot Be Trusted	Comprar o generar un certificado SSL adecuado para este servicio. Si el certificado corresponde a una interfaz de administración que tenga los equipos, para la cual no es requerido adquirir un certificado, entonces la Entidad podría aceptar el riesgo temporalmente y/o asegurarse de que los certificados estén correctamente generados por el aplicativo que los genera de manera autofirmada.

Vulnerabilidad	Recomendación
SSL Self-Signed Certificate	Comprar o generar un certificado SSL adecuado para este servicio. Si el certificado corresponde a una interfaz de administración que tenga los equipos, para la cual no es requerido adquirir un certificado, entonces la Entidad podría aceptar el riesgo temporalmente y/o asegurarse de que los certificados estén correctamente generados por el aplicativo que los genera de manera autofirmada.
TLS Version 1.1 Deprecated Protocol	Habilitar la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Volver a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere la posibilidad de usar TLS 1.2 con conjuntos de aplicaciones AES-GCM sujeto a la compatibilidad con navegadores y servidores web.
TLS Version 1.0 Protocol Detection	Habilitar la compatibilidad con TLS 1.2 y 1.3 y deshabilite la compatibilidad con TLS 1.0.
SSL Certificate with Wrong Hostname	Revisar el contenido del certificado de tal forma que coincida con el nombre del hostname del equipo. En caso de que se requier, entonces se recomienda comprar o generar un certificado SSL adecuado para este servicio. Si el certificado corresponde a una interfaz de administración que tenga los equipos, para la cual no es requerido adquirir un certificado, entonces la Entidad podría aceptar el riesgo temporalmente y/o asegurarse de que los certificados estén correctamente generados por el aplicativo que los genera de manera autofirmada.
SSL Certificate Signed Using Weak Hashing Algorithm	Ponerse en contacto con la autoridad de certificación para que se vuelva a emitir el certificado SSL. Si es un certificado autofirmado, entonces realizar la generación del mismo nuevamente con los últimos algoritmos criptográficos disponibles.
SMB Signing not required	Aplicar la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red de Microsoft: Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'. Consultar el siguiente enlace para ajustar la configuración en Windows:

Vulnerabilidad	Recomendación
	• http://technet.microsoft.com/en-us/library/cc731957.aspx
SSL Certificate Expiry	Comprar o generar un nuevo certificado SSL para reemplazar el existente.
Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Habilitar la autenticación de nivel de red (NLA) en el servidor RDP remoto. Esto generalmente se hace en la pestaña 'Remoto' de la configuración 'Sistema' en Windows.
JQuery 1.2 < 3.5.0 Multiple XSS	Actualizar a la versión 3.5.0 o posterior de JQuery.
Unencrypted Telnet Server	Deshabilitar el servicio Telnet (Puerto TCP23) y usar SSH en su lugar.
SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	Validar con el proveedor del firmware del equipo de tal forma que se pueda obtener una actualización con las estrictas contramedidas de intercambio de claves o deshabilite los algoritmos afectados.
HTTP TRACE / TRACK Methods Allowed	Deshabilitar estos métodos HTTP. Consultar la salida del complemento para obtener más información.
SSH Weak Algorithms Supported	Validar con el proveedor del firmware del equipo o consultar la documentación del producto para eliminar y/o deshabiltiar los cifrados débiles.
Apache 2.4.x < 2.4.42 Multiple Vulnerabilities	Actualizar a la versión 2.4.42 o posterior de Apache.
Apache Multiviews Arbitrary Directory Listing	Actualizar a la versión 1.3.22 o posterior de Apache. Como alternativa, como solución alternativa, deshabilitar MultiviewsActualice a la versión 1.3.22 o posterior de Apache. Como alternativa y/o solución alternativa, deshabilitar Multiviews.
SNMP 'GETBULK' Reflection DDoS	Deshabilitar el servicio SNMP en el host remoto si no se utiliza. De lo contrario, restringir y supervisar el acceso a este servicio, y considerar la posibilidad de cambiar el nombre de la comunidad "pública" predeterminada. Por ejemplo a números aleatorios o palabras que no se encuentren en un diccionario.
Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)	Actualizar a la versión 2.4.54 o posterior de Apache.
PHP < 7.3.28 Email Header Injection	Actualizar a la versión 7.3.28 o posterior de PHP.
Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Forzar el uso de SSL como capa de transporte para este servicio si se admite.

Vulnerabilidad	Recomendación
	- En los sistemas operativos Microsoft Windows, seleccionar la opción "Permitir conexiones solo desde equipos que ejecutan Escritorio remoto con autenticación de nivel de red" si está disponible.
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Deshabilitar SSLv2 y los conjuntos de cifrado de criptografía de grado de exportación. Asegurar que las claves privadas no se utilicen en ningún lugar con software de servidor que admita conexiones SSLv2.
Apache 2.4.x < 2.4.35 DoS	Actualizar a la versión 2.4.35 o posterior de Apache.
Terminal Services Encryption Level is Medium or Low	Cambiar el nivel de cifrado RDP a uno de los siguientes: 3. Alto 4. Cumple con FIPS

Tabla 8. Recomendaciones de mitigación, vulnerabilidades medias

- Vulnerabilidades bajas:

Vulnerabilidad	Recomendación
ICMP Timestamp Request Remote Date Disclosure	Filtrar las solicitudes de marca de tiempo ICMP (13) y las respuestas de marca de tiempo ICMP salientes (14).
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Reemplazar el certificado de la cadena por la clave RSA de menos de 2048 bits de longitud por una clave más larga y vuelva a emitir los certificados firmados por el certificado anterior.
SSH Weak Key Exchange Algorithms Enabled	Validar con el proveedor del firmware del equipo o consultar la documentación del producto para desactivar los algoritmos débiles.
SSH Weak MAC Algorithms Enabled	Validar con el proveedor del firmware del equipo o consultar la documentación del producto para desactivar los algoritmos MD5 y MAC de 96 bits.
SSH Server CBC Mode Ciphers Enabled	Validar con el proveedor del firmware del equipo o consultar la documentación del producto para deshabilitar el cifrado de cifrado en modo CBC y habilitar el cifrado en modo de cifrado CTR o GCM.
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Deshabilitar SSLv3. Los servicios que deben admitir SSLv3 deben habilitar el mecanismo SCSV de reserva de TLS hasta que se pueda deshabilitar SSLv3.

Vulnerabilidad	Recomendación
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Configurar el servicio para usar un módulo Diffie-Hellman único de 2048 bits o superior.
Terminal Services Encryption Level is not FIPS-140 Compliant	Cambiar el nivel de cifrado de RDP a: 4. Cumple con FIPS

Tabla 9. Recomendaciones de mitigación, vulnerabilidades bajas

6. Recomendaciones generales del CSIRT Salud

Como complemento a la información técnica dispuesta en el presente documento se hacen las siguientes recomendaciones:

- Implementar cada una de las recomendaciones de remediación que se plantean para las vulnerabilidades identificadas dentro del presente informe y el Anexo 1. Matriz de vulnerabilidades tecnológicas. De igual forma, es importante seguir el resultado plasmado dentro del informe técnico con el fin de priorizar la remediación de las vulnerabilidades de nivel Crítico (135), nivel Alto (101), nivel Medio (366), y finalmente nivel Bajo (84).

- Documentar un plan remediación de vulnerabilidades con fechas y responsables que permita cumplir en el corto plazo con la mitigación de todos los hallazgos. Por lo menos debe contemplar la remediación de las vulnerabilidades de nivel crítico y alto.

- Aplicar listas de aseguramiento para los productos de Apache, PHP, ILO, SQL, iDRAC, Windows, las cuales permiten corregir múltiples vulnerabilidades y vectores de ataque. Esto frustra los ataques de reconocimiento de servicios, de vulnerabilidades y reduce el nivel de exposición a nuevos ataques y no conocidos. En la siguiente referencia se pueden identificar diferentes plantillas para uso interno.
    - https://www.cisecurity.org/cis-benchmarks/