Unidad Auditoría Interna

TEST DE PENETRACIÓN EN SERVIDORES
PEN TEST

INFORME UAI N° 06/2019

SRT
Superintendencia de Riesgos del Trabajo

Ministerio de Producción y Trabajo
Superintendencia de Riesgos del Trabajo

Unidad de Auditoría Interna

INFORME EJECUTIVO

INFORME ANALITICO

INFORME EJECUTIVO

TEST DE PENETRACIÓN EN SERVIDORES - PEN TEST

1. OBJETO

Evaluar mediante la ejecución del Test de Penetración Interno en Servidores – PenTest, tendiente a detectar la eventual existencia de vulnerabilidades que puedan facilitar accesos internos no autorizados en los servidores del organismo: Sede Central, Sedes Jurisdiccionales, Datacenter PVNet y la Comisión Médica - CM09 Neuquén, los que se encuentran bajo el control y supervisión de la Subgerencia de Sistemas, en la órbita de la Gerencia Técnica.

2. ALCANCE

La labor se desarrolló entre los meses de marzo y mayo de 2019, de conformidad con las Normas de Auditoría Gubernamental establecidas en la Resolución SGN N° 152/2002, mediante la aplicación de procedimientos usuales de Auditoria de Sistemas y otros que se consideraron necesarios en la circunstancia.

Se aclara que el presente informe se encuentra circunscripto al tipo de ataque informático interno, descripto en detalle en el punto 6.2 del presente informe, el día 12/04/19 y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido.

3 OBSERVACIONES Y RECOMENDACIONES

A continuación se trascriben las observaciones formuladas como resultado de la labor realizada.

Cabe señalar, que los resultados de la ejecución del PenTest se remitieron al sector auditado mediante un "Informe Confidencial", con el detalle de las Vulnerabilidades Críticas detectadas, con indicación de Sedes, direcciones IP de los Servidores, Nombres, Plugins ID, Sinopsis (brindada por el software) y las Soluciones, como así también los Anexos, los cuales para el presente informe los nombres y las IP allí consignados, han sido modificados por cuestiones de seguridad.

1. Observación

Como resultado de la ejecución del PenTest, se detectaron 1743 vulnerabilidades entre las sedes del Organismo, de las cuales 7 de ellas resultaron críticas: 115 altas, 1283 medias y 338 de Bajo impacto.

Puntualmente, las referidas fallas se distribuyeron según la siguiente proporción: el **2,8%** de los servidores sufrieron vulnerabilidades críticas (*critical*), un **22,7%** evidenciaron un alto riesgo (*high*), concentrándose en un 23,9% del total los servidores testeados.

Recomendación

La Gerencia Técnica deberá impulsar la adopción de un plan de tareas para actualizar las versiones de software o instalar los parches indicados en la documentación técnica que se remite Informe Confidencial entregado por separado, a efectos de mitigar vulnerabilidades, prevenir y evitar accesos no autorizados a la información o sistemas del Organismo.

4. Conclusión

De acuerdo a la evaluación practicada, conforme al objeto y alcance de las mismas, esta Unidad de Control estima que las operaciones vinculadas con la gestión del sector auditado, se desarrollan en términos generales de manera razonable.

Sin perjuicio de ello, en atención a los hallazgos verificados durante la ejecución de la auditoría, se han detectado vulnerabilidades con diferentes niveles de criticidad en la red interna de talladas en el punto 7.2 del presente, cuyas especificaciones fueron objeto del Informe Confidencial remitido a la Subgerencia de Sistemas, tal como se lo señaló en el Apartado 5 - Tarea Realizada; cuya subsanación contribuirá a incrementar los niveles de seguridad existentes, en tanto oportunidad de mejora, a fin de preservar la Seguridad de la Información de esta Superintendencia.

Buenos Aires, 03 de julio de 2019.

.

INFORME ANALÍTICO DE AUDITORIA

TEST DE PENETRACIÓN EN SERVIDORES - PEN TEST

1. OBJETO

Evaluar mediante la ejecución del Test de Penetración Interno en Servidores – PenTest, tendiente a detectar la eventual existencia de vulnerabilidades que puedan facilitar accesos internos no autorizados en los servidores del organismo: Sede Central, Sedes Jurisdiccionales, Datacenter PVNet y la Comisión Médica - CM09 Neuquén, los que se encuentran bajo el control y supervisión de la Subgerencia de Sistemas, en la órbita de la Gerencia Técnica.

2. ALCANCE

La labor se desarrolló entre los meses de marzo y mayo de 2019, de conformidad con las Normas de Auditoría Gubernamental establecidas en la Resolución SGN N° 152/2002, mediante la aplicación de procedimientos usuales de Auditoria de Sistemas y otros que se consideraron necesarios en la circunstancia.

Se aclara que el presente informe se encuentra circunscripto al tipo de ataque informático interno, descripto en detalle en el punto 6.2 del presente informe, el día 12/04/19 y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido.

3. ANTECEDENTES

Normativos:

- Resolución SRT N° 231/2009 "Política de Seguridad de la Información de la Superintendencia de Riesgos del Trabajo".

Documentales

- Informe UAI SRT N° 34/2008 "Seguridad en Servidores",
- Informe UAI SRT N° 12/2014 "Test de Penetración en Servidores",
- Informe UAI SRT N° 21/2017 "Seguridad Informática",

- Informe UAI SRT N° 42/2017 "Plan de Contingencia",
- Informe UAI SRT N° 36/2018 "Licencias de Software",
- Documentación del programa Tenable.io

Informáticos:

- Tenable.io (Nessus Managed in the Cloud) (Versión: 7.1.1)

4. MARCO DE REFERENCIA

Entre las acciones previstas en las Políticas de Seguridad de la Información, aprobadas mediante la Resolución SRT N° 231/09, se contemplan específicamente en su apartado 6.3.2 - Comunicación de Fallas y/o Amenazas en Materia de Seguridad, "… *la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad de sistemas informáticos*… *previa conformidad del Responsable de la Seguridad de la Información, detallando la metodología y alcance de las pruebas".*

Por ello, la Unidad de Auditoría Interna, ejecutó en forma controlada, con N° de Proyecto 3.10.14, un test de penetración interno en servidores, buscando posibles vulnerabilidades de explotación por parte de personal malintencionado, previo consentimiento del Departamento de Comunicaciones y Seguridad; y de Servidores Centrales y Equipamiento; dependientes de la Gerencia Técnica.

5. TAREA REALIZADA

La tarea realizada consistió en la ejecución de los siguientes procedimientos de auditoría y/o verificaciones:

- Recopilación de antecedentes;
- Entrevistas con los responsables del sector auditado;
- A efectos de ejecutar el Pen Test, se seleccionó la totalidad de los servidores de Sede Sarmiento, Reconquista Moreno, datacenter PVNet, se incluyó por selección aleatoria la Comisión Médica - CM09 Neuquén; en un total de 61 CM, por resultar representativa en cantidad de servidores instalados y operativos, sin ser una CM crítica;

- Ejecución del ataque interno a los servidores del organismo mencionados en el punto precedente;
- Recopilación y análisis los resultados obtenidos en el ataque.

Cabe señalar, que los resultados de la ejecución del PenTest se remitieron al sector auditado mediante un "Informe Confidencial", con el detalle de las Vulnerabilidades Críticas detectadas, con indicación de Sedes, direcciones IP de los Servidores, Nombres, Plugins ID, Sinopsis (brindada por el software) y las Soluciones, como así también los Anexos, los cuales para el presente informe los nombres y las IP allí consignados, han sido modificados por cuestiones de seguridad.

Mediante comunicación de fecha 28/05/2019 la Subgerencia de Sistemas informó que ha adoptado medidas tendientes a la subsanación de las observaciones formuladas

6. ACLARACIONES PREVIAS

El Test de Penetración o Pen Test, se ejecuta para identificar posibles amenazas en los sistemas IT por errores en la configuración de equipos, redes de comunicación o aplicaciones web, como así también actúa detectando la falta de actualizaciones o parches en sus aplicativos.

Este proceso, asimismo conocido como Hacking Ético (*Ethical Hacking*) consiste en un ataque informático simulado, similar a los que realizaría un Cracker o *Black Hat Hacker*[1].

Esta clase de ataque se caracteriza por no poner en riesgo la información o la disponibilidad de los servicios de las diferentes áreas involucradas de la Subgerencia de Sistemas, al disponerse de medidas preventivas planificadas.

Los ataques informáticos se diferencian según su fuente de origen:

- **6.1 Ataque Informático Remoto**

[1] ***BLACK HAT HACKER***: Es utilizado para describir un hacker que irrumpe en un sistema informático o red con malas intenciones. A diferencia de un *white hat hacker*, el *Black hat hacker* se aprovecha del robo, quizá para destruir archivos o robar datos. El *Black hat hacker* también da a conocer el exploit a otros hackers sin notificar a la víctima. Dando así la oportunidad que otros exploten la vulnerabilidad antes de que el organismo sea capaz de asegurarlo.

En esta modalidad el atacante procura acceder desde fuera de la red, con la finalidad de encontrar fallas y acceder a la información del Organismo o bien, posicionarse como administrador del sistema.

A efectos de mitigar el riesgo de accesos no autorizados a la red interna el Organismo, se ha dispuesto un esquema de Firewall y Zona Desmilitarizada (DMZ) y que de concretarse son monitoreados por el sector Seguridad Informática, mediante la utilización de procedimientos tales como: la "Revisión Interna Externa - *Ethical Hacking*" y la "Revisión de Seguridad de Errores y Bloqueos URL - IPS".

La aplicación práctica de lo expuesto surge del expediente 62548/13 en el cual la Subgerencia de Sistemas instrumentó la ejecución de un test de penetración sobre los *sitios web del organismo*, el que fue llevado a cabo en el mes de enero de 2014.

Asimismo, mediante expediente EX-2018-00567350-APN-SF#SRT se realizó una contratación directa del servicio de PenTest, sobre *Sitios Web y dispositivos IP* publicados en la red de SRT, el cual se ejecutó en julio 2018.

- **6.2 Ataque Informático Interno**

Un individuo que cuente con acceso autorizado a la red, puede intentar ingresar a los sistemas y a las bases de datos más allá de los privilegios que tenga otorgados. Cabe reiterar, que precisamente sobre este tipo de ataque se centra el presente informe, tal como se lo señaló líneas atrás en el punto **2. Alcance**.

Consecuentemente, de manera preventiva, el organismo ha implementado en el marco de las Políticas de Seguridad, una serie de restricciones que mitigan el riesgo de sufrir ataques internos, tales como las limitaciones a la instalación de un software no autorizado, vedar accesos a CDs, puertos USB y a servidores, acorde a cada perfil.

7. DESCRIPCIÓN, OBSERVACIONES Y RECOMENDACIONES

En los apartados que se indican a continuación, se describen los aspectos verificados, las observaciones surgidas de la labor y las recomendaciones que esta Unidad de Control sugiere para mejorar la gestión y operatoria en aquellos aspectos que constituyeron materia de examen.

Cabe mencionar, que en este el presente informe se omitió dejar asentadas especificaciones técnicas que den precisiones sobre las vulnerabilidades detectadas y los equipos involucrados, las que fueron objeto del Informe Confidencial remitido al sector auditado, tal como se lo indicó en el Apartado 5 - Tarea Realizada.

Dicha información se encuentra disponible en esta unidad y se entrega por cuerda separada y en un único ejemplar a la Gerencia Técnica y Subgerencia de Sistemas

7.1 Vulnerabilidades de los Servidores

Descripción:

- **Software Utilizado**

Para la selección del software que satisfaga el objeto de esta auditoría, se decidió utilizar el software Tenable.io (Nessus Managed in the Cloud) en su versión de Agentes 7.1.1, por ser un software registrado por este Organismo. El mismo brinda toda su funcionalidad y la posibilidad de escanear hasta 254 *Direcciones IP*[2] en cada proceso.

- **Preparación y Ejecución del PenTestT**

Se ejecutó el PenTest, desde una PC del Departamento de Comunicaciones y Seguridad, para así tener bajo control cualquier incidente que se suscitara.

El usuario utilizado para esta auditoría "*PenTestSRT*", fue creado a pedido de esta Unidad, días previo a la ejecución y se le asignó un perfil símil a "Jefe de Área", para así poseer mayor cantidad de atributos en características generales, como ser: acceso a USB, a bases de datos y servidores, ya que el común de los agentes del Organismo no posee.

Los ataques se efectuaron por sede, de acuerdo al siguiente cronograma:

Sede	Desde	Hasta	Día	Servidores
Sarmiento	08:42	09:36	12-abr	124
Reconquista	09:43	10:03	12-abr	16

[2] ***DIRECCIONES IP***: Las direcciones IP (Internet Protocol) son un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP. Una dirección IP es un conjunto de cuatro números del 0 al 255, separados por puntos.

Moreno	10:12	10:29	12-abr	16
CM09 Neuquén	10:36	10:48	12-abr	18
PVNet	20:00	20:23	10-abr	73

Los ataques internos en las diferentes sedes, se llevaron a cabo el día viernes 12 de Abril del corriente año, con excepción de los servidores de PVNet; que por su criticidad se decidió utilizar el PenTest el día miércoles 10 de abril, debido a que el Departamento de Comunicaciones y Seguridad posee configurado la ejecución del test de penetración en forma automática todos los días miércoles fuera de horario laboral, (20:00 Hs.), para poder controlar su seguridad y no perjudicar la performance de los servidores en horarios críticos.

- **Nivel de Severidad**

Crítico:

- La vulnerabilidad posibilitaría un acceso a nivel *root*[3] de los servidores o dispositivos de infraestructura.

High:

- Estas vulnerabilidades son difíciles de explotar.
- La explotación podría resultar en adquirir elevación de privilegios.
- La explotación podría resultar en una pérdida significativa de datos o tiempo de inactividad.

Medium:

- Esta vulnerabilidad requiere que el atacante manipule a víctimas individuales mediante tácticas de ingeniería social.
- Vulnerabilidades de denegación de servicio que son difíciles de configurar. Esta vulnerabilidad requiere que un atacante resida en la misma red local que la víctima.
- Son vulnerabilidades donde la explotación proporciona un acceso muy limitado.

[3] **Nivel Root**, Es un nivel de usuario principal o administrador. Es la cuenta con máximos atributos.

- Esta vulnerabilidad requiere privilegios de un usuario para una explotación exitosa.

Low:

- Las vulnerabilidades en el rango bajo suelen tener muy poco impacto en el negocio de una organización. La explotación de tales vulnerabilidades generalmente requiere acceso local o físico al sistema.

- **Resultado del escaneo**

Se exhiben en el informe, las vulnerabilidades detectadas en los servidores del organismo, producto de la configuración y ejecución del software de ataque antes mencionado, intentando penetrar solo en servidores que se encuentren en la red interna y facilitando el eventual acceso de información a personas que intenten con éxito accesos no autorizados.

- **Tratamiento de los Reportes del software de PenTest**

Primeramente, se efectuó la separación de los reportes por Sede. El conjunto de servidores testeados, no solo incluye a la Sede Sarmiento 1962, sino que también comprende Reconquista 723 y Moreno 401. Adicionalmente el proceso incluyó los servidores del datacenter PVNet, como punto crítico en el cual se realizan los espejamientos, BackUps y por revestir la calidad de sitio de contingencia *Allways On*[4] del Organismo.

Por último, se incluyó en la muestra en forma aleatoria a la CM09 Neuquén; de un total de 61 CM, por resultar representiva la cantidad de servidores instalados y operativos, sin ser una CM crítica.

El software dividió las vulnerabilidades en cuatro niveles de riesgo: Crítico, Alto, Moderado, Bajo. Y se diferencian usualmente por las siguientes características.

[4] ***Alwas On***, Es un datacenter paralelo al productivo, espejando la información como respaldo, donde también se encuentran los centros de proceso de datos y se encarga de estar 'siempre en funcionamiento'. En caso de un incidente o desastre, el *Always On*, levanta los procesos y el Negocio continúa.

En un total de 247 servidores entre todas las sedes, 19 de ellos no tuvieron vulnerabilidad alguna, siendo el 7.7% del total del parque.

7.2 Vulnerabilidades Detectadas

El relevamiento expuesto resulta de suma utilidad a los fines de impulsar las tareas tendientes a minimizar la existencia de vulnerabilidades, cuya resolución se encuentra supeditada a la actualización en su última versión del software actualmente en uso por el sector auditado.

Se estima procedente destacar que los intentos de penetración a la red interna del Organismo fueron detectados por el Departamento de Servidores Centrales y Equipamiento; pues se había consensuado la semana de ejecución, pero no se especificó el día y hora.

Por otro lado, la CM09 Neuquén, al no estar informada de la auditoría en curso, contactó al Departamento de Comunicaciones y Seguridad, por las permanentes alertas del Antivirus, que detectaba y los intentos de penetración a los servidores, por parte del software en uso.

A continuación, se expone el detalle de la distribución de vulnerabilidades detectadas por sede:

Sede	Critical	High	Medium	Low	Info
Sarmiento	0	70	609	143	4545
Reconquista	3	14	73	20	458
Moreno	2	15	97	23	515
CM09 Neuquén	1	1	98	37	589
PVNet	1	15	406	115	2798
Total de resultados	*7*	*115*	*1283*	*338*	*8905*

1. Observación

Como resultado de la ejecución del Pen test se detectaron 1743 vulnerabilidades entre las sedes del Organismo, de las cuales 7 de ellas resultaron críticas: 115 altas, 1283 medias y 338 de Bajo impacto.

Puntualmente, las referidas fallas se distribuyeron según la siguiente proporción: el **2,8%** de los servidores sufrieron vulnerabilidades críticas (*critical*), un **22,7%** evidenciaron un alto riesgo (*high*), concentrándose en un 23,9% del total los servidores testeados.

Recomendación

La Gerencia Técnica deberá impulsar la adopción de un plan de tareas para actualizar las versiones de software o instalar los parches indicados en la documentación técnica que se remite Informe Confidencial entregado por separado, a efectos de mitigar vulnerabilidades, prevenir y evitar accesos no autorizados a la información o sistemas del Organismo.

Respuesta del Sector Auditado

Como respuesta al Informe Confidencial remitido al sector auditado en el cual se detallan las vulnerabilidades detectadas, la Subgerencia de Sistemas informó, mediante comunicación de fecha 28 de mayo de 2019 que ha adoptado medidas tendientes a la subsanación de las observaciones formuladas.

Puntualmente, para las observaciones referidas al Área de Servidores y Equipamiento Central, se informó que "…*la tarea está en proceso de mejora y se estima concluirla en aproximadamente treinta (30) días*", medida que será objeto de constatación en futuras tareas de auditoría.

Por su parte, el Área de Comunicaciones y Seguridad presentó documentación respaldatoria sobre la resolución de la vulnerabilidad exhibida por la CM Neuquén, y las demás 26 CM del Organismo.

8. SEGUIMIENTO DE OBSERVACIONES DE INFORMES DE AUDITORÍA

La observación objeto de seguimiento del Informe UAI SRT Nº 12/2014 y la calificación individual de su estado de situación conforme el examen realizado, se encuentra detallada en el Anexo I del presente.

A continuación se sintetizan los resultados obtenidos:

Estado de situación de las observaciones objeto de seguimiento				
Regularizada	Con Acción Correctiva Informada	Sin Acción Correctiva	No Compartida	No Regularizable
1	0	0	0	1
Total: 2				

9. **CONCLUSIÓN**

De acuerdo a la evaluación practicada, conforme al objeto y alcance de las mismas, esta Unidad de Control estima que las operaciones vinculadas con la gestión del sector auditado, se desarrollan en términos generales de manera razonable.

Sin perjuicio de ello, en atención a los hallazgos verificados durante la ejecución de la auditoría, se han detectado vulnerabilidades con diferentes niveles de criticidad en la red interna detalladas en el punto 7.2 del presente, cuyas especificaciones fueron objeto del Informe Confidencial remitido a la Subgerencia de Sistemas, tal como se lo señaló en el Apartado 5 - Tarea Realizada; cuya subsanación contribuirá a incrementar los niveles de seguridad existentes en tanto oportunidad de mejora, a fin de preservar la Seguridad de la Información de esta Superintendencia.

Buenos Aires, 03 de julio de 2019.

ANEXO I

INFORMES DE AUDITORÍA - OBSERVACIONES OBJETO DE SEGUIMIENTO

Informe N°	N° de Orden	Observación	Recomendación	Estado de Situación					Área/s Responsable/s	Comentario
				R	CAI	SAC	NC	NR		
12/14	1	Si bien el riesgo de sufrir un ataque interno malicioso se encuentra minimizado por medidas de mitigación implementadas en el Organismo, existen vulnerabilidades que podrían ser explotadas por quienes dispongan del conocimiento necesario para sortear tales medidas.	Con el propósito de ampliar las limitaciones existentes para prevenir accesos no autorizados a la información o sistemas del Organismo, la Gerencia de Sistemas debe instrumentar un plan de tareas para actualizar las versiones de software o los parches indicados en la documentación técnica que se gira por cuerda separada.					X		Mudanza y Obsolescencia de la Observación para esta temática.

ANEXO II

DISTRIBUCIÓN DE VULNERABILIDADES POR SERVIDOR

El nombre y las IP de los servidores han sido cambiados, a fin de preservar la confidencialidad de la información que podría resultar sensible. Entregándose este mismo anexo con los nombres pertinentes a la subgerencia de sistemas.

Reconquista					
16 Servers	Critical	High	Medium	Low	Info
1	1	0	1	0	21
2	1	0	1	0	21
3	0	0	6	2	39
4	0	0	6	2	40
10	0	0	5	1	36
11	0	1	11	2	43
12	0	0	5	1	31
14	0	1	1	0	9
15	0	1	9	5	44
16	0	5	4	0	29
17	0	0	5	1	30
20	0	0	4	3	25
23	1	5	7	0	30
50	0	0	5	1	35
100	0	1	3	2	22
230	0	0	0	0	3
Totales por Severidad	3	14	73	20	458

Cuadro ANEXO: Distribución de vulnerabilidades por servidor RECONQUISTA.

Moreno					
16 Servers	Critical	High	Medium	Low	Info
1	0	0	1	0	22
2	0	1	9	3	40
3	0	1	9	3	40
4	0	0	4	3	24
14	0	0	5	1	37
56	1	5	7	0	30
61	1	5	7	0	27
62	0	0	5	0	52
99	0	3	13	4	23
100	0	0	5	1	34
144	0	0	4	1	34
154	0	0	7	2	33
155	0	0	7	2	35
160	0	0	3	0	14
187	0	0	7	2	39
208	0	0	4	1	31
Totales por Severidad	2	15	97	23	515

Cuadro ANEXO: Distribución de vulnerabilidades por servidor MORENO.

Neuquen					
18 Servers	Critical	High	Medium	Low	Info
1	0	0	5	2	45
2	0	0	5	1	37
10	0	0	5	1	38
21	0	0	8	3	37
22	0	0	8	3	39
23	0	0	8	3	39
24	0	0	8	3	39
25	0	0	8	3	39
101	0	0	8	3	39
103	0	0	8	3	39
171	0	0	8	3	39
181	0	0	8	3	42
183	0	0	8	3	44
230	0	0	2	1	20
231	0	1	0	2	16
244	0	0	0	0	11
245	0	0	0	0	11
254	1	0	1	0	15
Totales por Severidad	1	1	98	37	589

Cuadro ANEXO: Distribución de vulnerabilidades por servidor CM09 NEUQUEN.

Sarmiento					
124 Servers	**Critical**	**High**	**Medium**	**Low**	**Info**
4	0	4	3	0	32
5	0	1	4	1	33
16	0	0	5	3	31
30	0	4	3	0	32
31	0	4	3	0	31
32	0	4	3	0	32
33	0	4	3	0	32
34	0	4	3	0	32
35	0	4	3	0	32
36	0	4	3	1	35
37	0	4	3	0	31
54	0	0	0	0	22
55	0	0	0	0	15
71	0	0	1	2	19
75	0	0	1	0	27
84	0	0	7	1	37
103	0	0	6	2	39
115	0	0	2	0	10
123	0	0	0	0	19
126	0	1	2	0	31
132	0	0	2	0	21
142	0	0	0	0	19
150	0	0	2	0	26
151	0	0	2	1	27
153	0	0	6	1	38
158	0	0	5	0	57
159	0	0	2	0	34
162	0	0	0	0	18
169	0	2	2	0	31
170	0	0	6	0	23
200	0	0	3	1	35
210	0	0	2	0	28
214	0	0	2	1	25
215	0	0	0	0	8

Sarmiento					
124 Servers	**Critical**	**High**	**Medium**	**Low**	**Info**
230	0	0	0	0	18
252	0	0	1	0	26
253	0	0	1	0	26
controlambiental	0	0	2	0	13
desa-app	0	0	7	2	44
desa-sql	0	1	10	4	47
prod-app	0	0	7	2	38
prod-rap	0	0	7	2	39
prod-sql	0	0	9	2	45
dns	0	1	6	1	34
sar1962	0	7	3	0	31
mysql	0	0	8	2	40
naslanadmin	0	1	5	0	61
prtg-com	0	0	7	2	33
pruebas-tmsql	0	0	9	3	36
saben	0	1	6	2	53
selfservice	0	1	8	2	41
tableau	0	0	9	2	42
desadocker	0	0	5	1	35
digicard	0	0	5	1	39
net01	0	4	3	0	31
tableau	0	3	3	0	31
esxitrend	0	3	3	0	31
1	0	0	4	1	52
2	0	0	4	1	53
fsps02	0	0	5	1	35
intercambio	0	0	7	2	37
iwsva140	0	0	5	3	33
iwsva141	0	0	5	3	33
2	0	0	5	1	34
1	0	0	5	1	33
sp	0	0	3	0	24
desa	0	0	7	3	42
0	0	0	8	3	45
1	0	0	8	3	48
rw-02	0	0	8	3	46

Sarmiento					
124 Servers	**Critical**	**High**	**Medium**	**Low**	**Info**
test	0	0	8	2	44
notes-01	0	0	5	1	35
notes-02	0	0	5	1	35
notes-03	0	0	5	1	34
notes-0800	0	0	5	1	35
notes-desa	0	0	6	1	41
notes-desa2	0	1	9	1	45
officescan	0	0	5	1	42
provision	0	0	5	1	41
prtg-cl	0	0	7	1	41
sfbfe01	0	1	6	1	49
sqlbkp01	0	1	8	2	42
sqlrestore	0	1	10	4	39
tableau-01	0	0	5	1	39
tableau-02	0	0	5	1	39
tableau-03	0	0	5	1	40
tableau-04	0	0	5	1	33
tableau-05	0	0	5	1	34
tableau01	0	0	5	1	39
testsql2019	0	0	5	0	35
tfs	0	0	4	1	39
tmcm	0	0	7	1	49
vcenter	0	0	1	0	25
vdi-01	0	1	1	0	27
vonecloud	0	0	2	0	27
webapp01	0	0	6	1	49
webapp02	0	0	6	1	49
webapp03	0	0	6	1	49
webapp04	0	0	6	1	49
webapp05	0	0	6	1	49
webapp06	0	0	6	1	49
webapp07	0	0	6	1	50
webapp08	0	0	6	1	45
webapptm	0	0	5	1	39
webappum	0	0	5	1	41
webdesa01	0	0	6	1	50

Sarmiento					
124 Servers	**Critical**	**High**	**Medium**	**Low**	**Info**
webdesa02	0	0	6	1	49
webpp01	0	0	6	1	49
wsus	0	0	5	1	39
srtdc01	0	0	7	2	57
srtdc02	0	0	6	3	44
srtdc03	0	0	6	2	44
srtdc04	0	0	6	2	44
super06	0	0	9	3	41
super09	0	0	6	2	39
super12	0	0	9	3	41
super13	0	0	9	3	42
super18	0	1	10	4	44
super22	0	0	9	3	42
super40	0	1	10	4	43
test-dba	0	0	6	2	43
veeam-01	0	1	9	3	50
wikisrt	0	0	0	0	20
win10	0	0	5	0	35
Totales por Severidad	0	70	609	143	4545

Cuadro ANEXO: Distribución de vulnerabilidades por servidor SARMIENTO.

PVNET					
73 Servers	**Critical**	**High**	**Medium**	**Low**	**Info**
52	0	0	9	3	41
53	0	0	9	3	42
56	0	0	9	3	40
82	0	0	0	0	16
84	0	0	4	3	28
85	0	0	4	3	28
100	0	0	12	4	37
101	0	0	0	0	18
102	0	0	0	0	7
103	0	0	0	0	14
104	0	0	0	0	7
105	0	0	0	0	19
112	0	0	4	1	21
118	0	1	1	1	33
120	0	1	1	1	33
121	0	0	2	2	25
122	0	0	0	0	4
123	0	0	0	0	4
126	0	0	1	0	26
desarrolloestablecimiento	0	1	1	1	32
desarrollomon	0	1	1	1	35
Inweb5	0	0	6	1	42
prtg	0	1	1	1	28
balanceador04	0	1	1	1	34
dc01	0	1	9	4	49
dc02	0	0	6	2	42
docker01	0	0	5	1	33
ekran	0	0	5	1	42
exch-01	0	0	6	1	51
exch-02	0	0	6	1	52
fs01	1	1	8	2	45
ipam01	0	0	5	1	34
monitoreo	0	0	6	3	49
nessus	0	0	5	1	29

PVNET					
73 Servers	**Critical**	**High**	**Medium**	**Low**	**Info**
notes01	0	0	7	2	40
notes02	0	0	7	2	39
notes03	0	1	11	2	48
notes04	0	1	11	2	47
notes05	0	1	11	3	46
notes06	0	1	11	3	48
notes07	0	1	11	3	47
ofscan	0	0	7	2	43
prtg	0	0	7	1	40
prtgcys	0	0	7	1	40
rapps	0	1	12	2	48
sfbfe01	0	1	6	1	47
sqlbkp01	0	0	7	3	42
sqldesa01	0	0	9	3	43
sqlprod02	0	0	9	3	42
sqlprod03	0	0	9	3	45
sqlprod04	0	0	6	2	42
sqlprod06	0	0	9	3	43
sqlprod07	0	0	9	3	44
sqlprod08	0	0	7	1	43
squidcm	0	0	5	3	47
telefonia	0	0	1	0	15
webapp01	0	0	6	1	52
webapp02	0	0	6	1	52
webapp03	0	0	6	1	50
webapp04	0	0	6	1	49
webapp05	0	0	6	1	52
webapp06	0	0	6	1	50
webapp07	0	0	5	1	52
webapp08	0	0	6	1	52
webapp09	0	0	6	1	52
webappum	0	0	5	1	41
webdesa01	0	0	7	3	44
webdesa02	0	0	5	1	52
webdesa03	0	0	6	1	50
webdesa04	0	0	6	1	48

PVNET					
73 Servers	**Critical**	**High**	**Medium**	**Low**	**Info**
webdesa05	0	0	5	1	35
wsus	0	0	5	1	39
2	0	0	8	3	49
Totales por Severidad	1	15	406	115	2798

Cuadro ANEXO: Distribución de vulnerabilidades por servidor PVNET.