

ESET®  
**INTELLIGENCE  
LABS**

Servicios  
confiables,  
Negocios  
Seguros



ESET®  
**INTELLIGENCE  
LABS**

Servicios  
confiables,  
Negocios  
Seguros



Presentación de servicios  
profesionales



## Situación en Latinoamérica

Porcentaje de empresas, por país, que sufrieron un incidente relacionado con acceso indebido a aplicaciones y/o bases de datos



Accesos indebidos

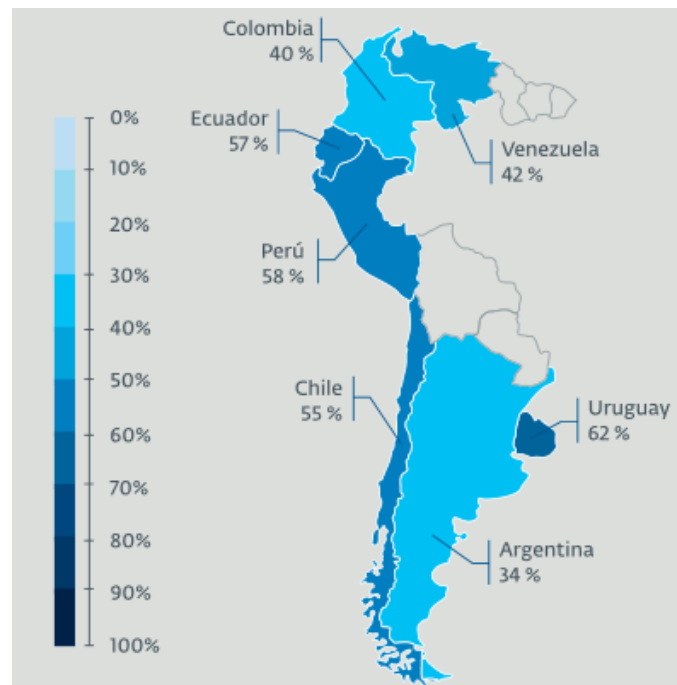
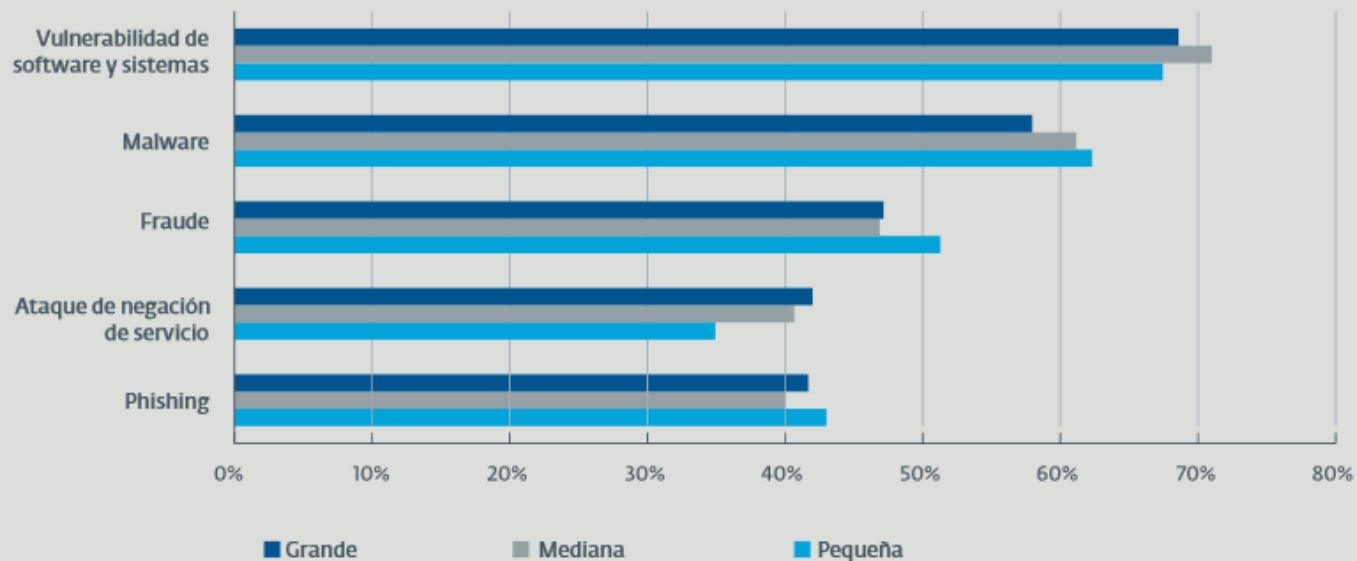


GRÁFICO 4 / Acceso indebido por país.

## Preocupaciones en términos de seguridad

Preocupaciones relacionadas con la seguridad de la información en las empresas encuestadas en Latam, clasificadas por tamaño de empresa



**GRÁFICO 1 /** Preocupaciones de la Seguridad de la Información de las empresas de acuerdo de su tamaño

## Situación en Latinoamérica

Porcentaje de empresas, por país, que sufrieron un incidente relacionado con Explotación de Vulnerabilidades

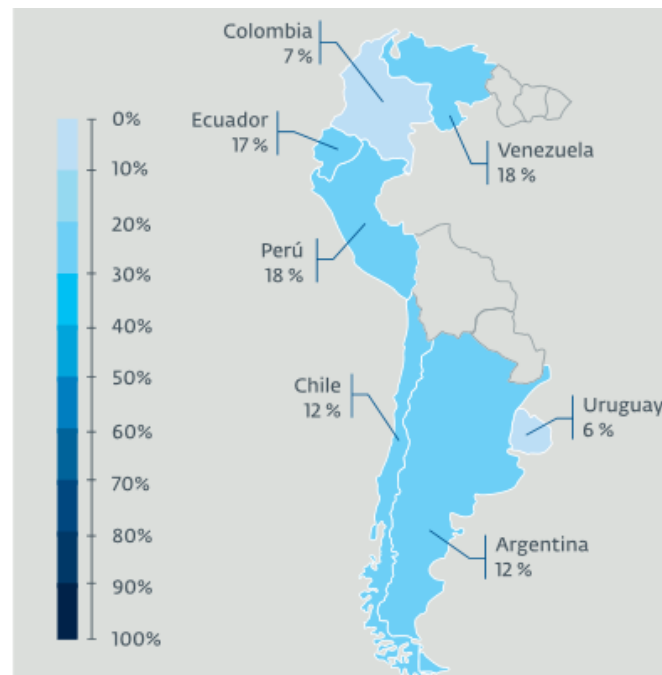
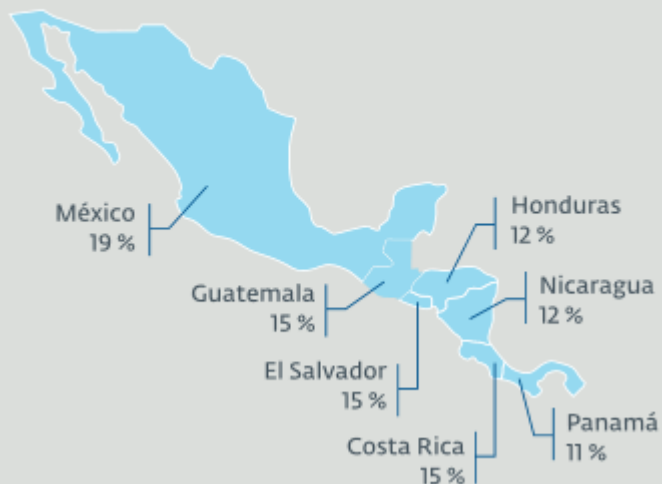
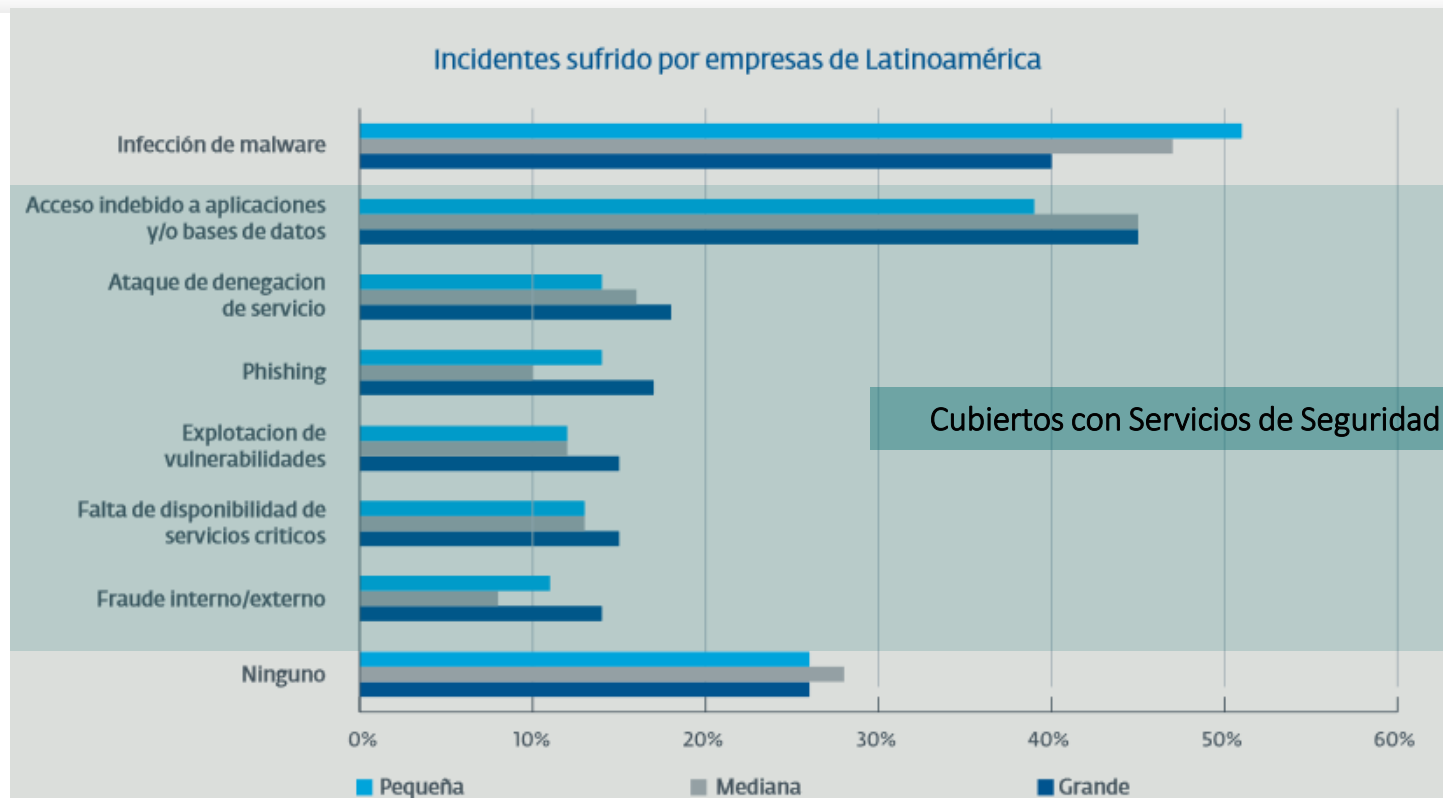


GRÁFICO 5 / Explotación de vulnerabilidades por país.

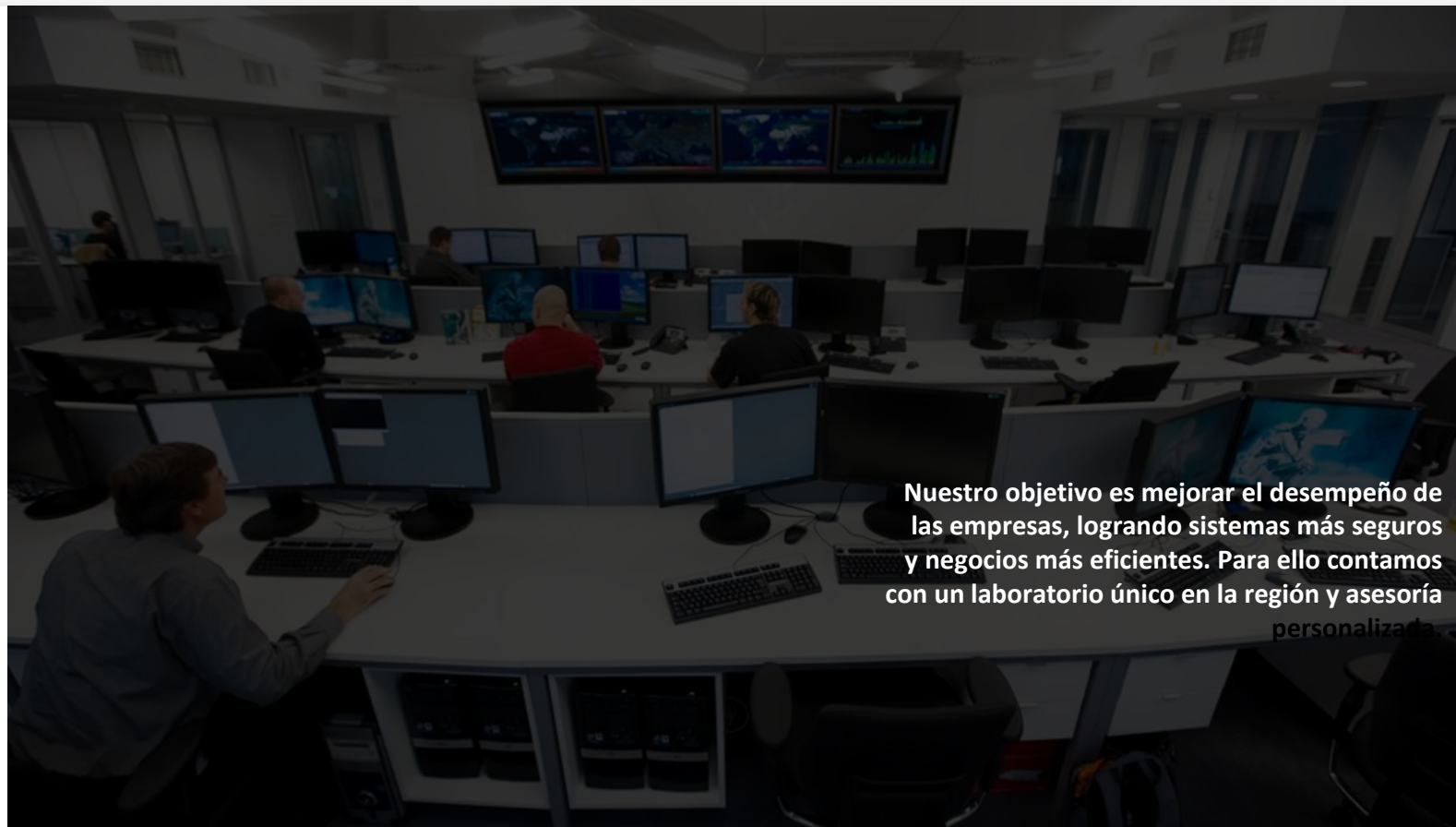
Explotación de vulnerabilidades



## ¿Qué incidentes sufrieron las empresas?



## ESET Intelligence Labs



Nuestro objetivo es mejorar el desempeño de las empresas, logrando sistemas más seguros y negocios más eficientes. Para ello contamos con un laboratorio único en la región y asesoría personalizada.

## ¿Por qué servicios de seguridad?



Conocer el nivel de seguridad dentro de la organización.



Conocer el nivel de seguridad hacia fuera de la organización.



Cumplir normativas y regulaciones sobre seguridad de la información.



Implementar y mejorar el proceso de “Gestión de Riesgos”.



# Vulnerability Assessment

Interno  
Externo

## Alcance del servicio



Localizar vulnerabilidades en una etapa temprana (antes que un atacante).



Relevar superficies de ataque



Informe sobre el estado actual de los servicios analizados.

# Penetration Testing

Interno  
Externo

## Alcance del servicio

- Análisis más extensivo que Vulnerability Assessment.
- Evalúa la explotación de la vulnerabilidad.
- Verifica los niveles de intrusión a los que se expone un sistema.

# Ransomware Prevention

## Alcance del servicio



Por medio de la ejecución de diferentes evaluaciones de seguridad, permite identificar y prevenir que una organización se vea afectada por este tipo de ataque.

Se incluyen tanto auditorias del tipo Penetration test, Red, Web, como evaluaciones que revelan el nivel de concientización de los usuarios.

# Web Penetration Testing

Externo

## Alcance del servicio

- De similares características que un Penetration Test pero orientado a web.
- Evalúa la explotación de las vulnerabilidades web.
- Verifica los niveles de intrusión a los que se expone un sistema.

# Mobile Penetration Test

Interno  
Externo

## Alcance del servicio



Análisis que se enfoca en evaluar aplicaciones móviles.



Puede llevarse a cabo tanto desde un punto de vista interno como externo.



¿Para que?

Para conocer el estado de la seguridad de la aplicación móvil de la organización.



# Social Engineering Testing

Externo

## Alcance del servicio

- Evaluar el grado de concientización de los usuarios de la organización en seguridad de la información.
- Entender si los usuarios están exponiendo a riesgos externos a la organización.
- Disparar acciones necesarias en materia de capacitación interna en seguridad de la información

# Gap Analysis

## Alcance del servicio

- Evalúa el riesgo de la existencia de fuga de información.
- Entrevistas por parte de un consultor con actores claves en la empresa.
- Analiza la existencia de políticas de seguridad y la funcionalidad de las mismas.
- Verifica el grado de cumplimiento de seguridad de una organización con respecto a una determinada normativa.

# WIFI Penetration Test

Interno

## Alcance del servicio



Evaluar el nivel de seguridad de las redes inalámbricas.



Comprender si un atacante, sin acceso a la red WIFI corporativa, podría conectarse de todas formas.



Detectar configuraciones débiles que implican riesgos para la red corporativa o bien a los usuarios de la misma.

# Continuous Security Assessment

Externo

## Alcance del servicio

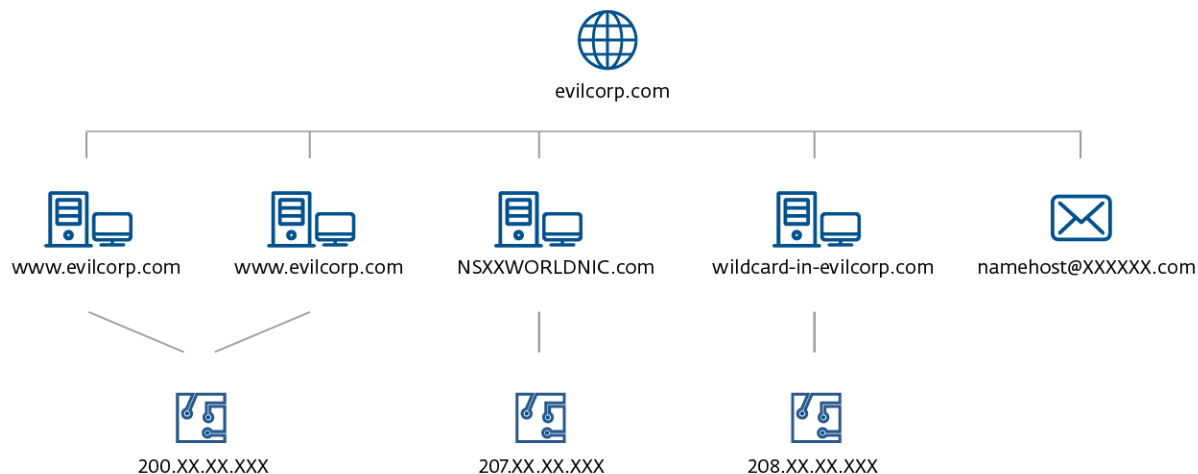
- Localizar debilidades y vulnerabilidades en una etapa temprana (antes que un atacante).
- Para constituir un ciclo de revisión y mejora para la seguridad.
- Dar seguimiento a la aplicación de parches y corrección de vulnerabilidades en la organización.
- Para contar con indicadores de gestión en la materia.

# Etapas de un Penetration Test



# Reconocimiento

## Etapa de reconocimiento de sistemas

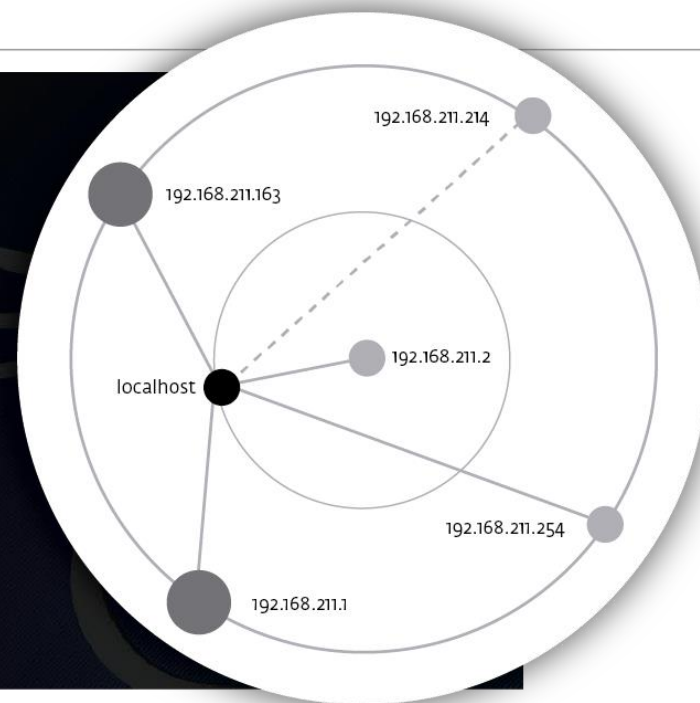


# Reconocimiento

## Detección de puertos y servicios

```
root@kali:~# nmap -sS -sV 192.168.211.163 -p1-65535

Starting Nmap 7.01 ( https://nmap.org ) at 2016-05-09 13:40 EDT
Nmap scan report for 192.168.211.163
Host is up (0.00015s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry    GNU Classpath grmiregistry
1524/tcp  open  shell          Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd        distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  X11            (access denied)
```

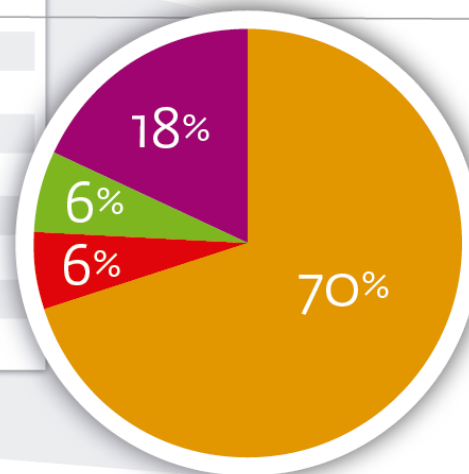


# Análisis de Vulnerabilidades

## Identificación de Vulnerabilidades unificadas por nombre

RIESGO	NOMBRE	ESTADO
CRITICAL	PHP Remote File Inclusion	Explotado
CRITICAL	Remote File Execution	Explotado
CRITICAL	Remote Command Execution	Explotado
HIGH	Microsoft Windows SMB Shares Unprivileged Access	Potencial
MEDIUM	SSL Certificate Expiry	Verificado
MEDIUM	SSL Version 2 and 3 Protocol Detection	Verificado
MEDIUM	SSL Weak Cipher Suites Supported	Verificado
MEDIUM	NFS Shares World Readable	Verificado
MEDIUM	SSL Medium Strength Cipher Suites Supported	Verificado

Total de vulnerabilidades

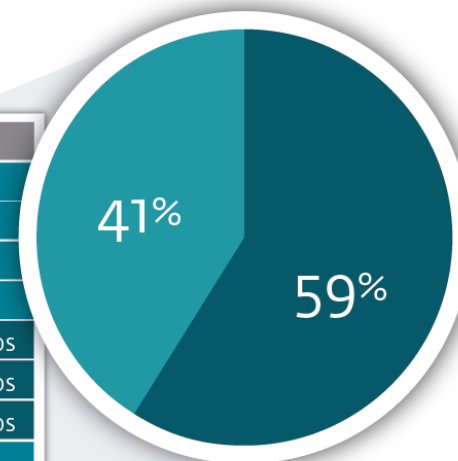


# Analisis de Vulnerabilidades

## Identificación de Vulnerabilidades unificadas por Tipo de Solución

RIESGO	NOMBRE	ESTADO
CRITICAL	PHP Remote File Inclusion	Configuración
CRITICAL	Remote File Execution	Configuración
CRITICAL	Remote Command Execution	Configuración
HIGH	Microsoft Windows SMB Shares Unprivileged Access	Configuración
MEDIUM	SSL Certificate Expiry	Problemas Criptográficos
MEDIUM	SSL Version 2 and 3 Protocol Detection	Problemas Criptográficos
MEDIUM	SSL Weak Cipher Suites Supported	Problemas Criptográficos
MEDIUM	NFS Shares World Readable	Configuración
MEDIUM	SSL Medium Strength Cipher Suites Supported	Problemas Criptográficos

Total de vulnerabilidades  
por tipo de Fix



# Explotación

## Explicación de cada Vulnerabilidad. Riesgo e impacto

### (CRITICAL) PHP Remote File Inclusion

Riesgo e impacto:

La vulnerabilidad de inclusión de archivo remota le permite a un atacante subir contenido malicioso al equipo. Mediante esta técnica puede utilizar el servidor afectado para alojar malware, phishing, exploit packs entre otros.

En este caso se utilizó la manipulación de formularios para subir imágenes mediante un proxy web para saltar medidas de seguridad como las...

CVSS Score

10,0

CWE

98

Existe exploit público

No se requiere

Sistemas Afectados

192.168.211.163

Estado

Explotado



# Explotación

## Evidencia

The image shows a screenshot of a web browser displaying the DVWA (Damn Vulnerable Web Application) File Upload page. The page is titled "Vulnerability: File Upload" and shows a list of files uploaded to the server. The file list includes files like "bin", "boot", "cdrom", "dev", "etc", "home", "initrd", "lib", "lost+found", "media", "mnt", "opt", "proc", "root", "sbin", "srv", "sys", "tmp", "usr", "var", "initrd.img", "nohup.out", and "vmlinuz". The file "vmlinuz" is highlighted in red, indicating it is the target of the exploit. The file's permissions are "rw-r--r--" and its size is 1.90 MB. The file's owner is "root" and its group is "root".

Below the file list, there is a "Change dir:" field with a dropdown menu showing the current directory as "/". A red arrow points to this field with the text "Directorio Raíz /".

On the left side of the browser window, there is a sidebar with various navigation links. The "Upload" link is highlighted in green. The "Upload" link is located under the "Vulnerability: File Upload" section.

At the top of the browser window, the address bar shows the URL "http://192.168.211.163/dvwa/vulnerability-file-upload.php". The browser's status bar shows the page title "Vulnerability: File Upload".

On the right side of the browser window, there is a terminal window showing the command prompt. The terminal displays the following information:

```
Username: Linux metasploit2 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 [ Google ] [ Exploit-DB ]
User: 33 ( www-data ) Group: 33 ( www-data )
Php: 5.2.4-2ubuntu5.10 Safe mode: OFF [ phpinfo ] Datetime: 2016-05-09 23:33:56
Hdd: 6.94 GB Free: 5.07 GB (72.95%)
Cwd: / drwxr-xr-x [ home ]
```

The terminal also shows the "Server IP:" and "Client IP:" information.

# Reportes / Conclusiones



**Durante esta etapa se elaboran los entregables.** Reporte ejecutivo y Reporte técnico que explican en detalle el nivel de riesgo y la postura de seguridad de la organización, al mismo tiempo que proveen al cliente un detalle exhaustivo sobre las tareas de remediación necesarias para mitigar los problemas detectados.

# ¡Muchas gracias!