Seguridad Informática

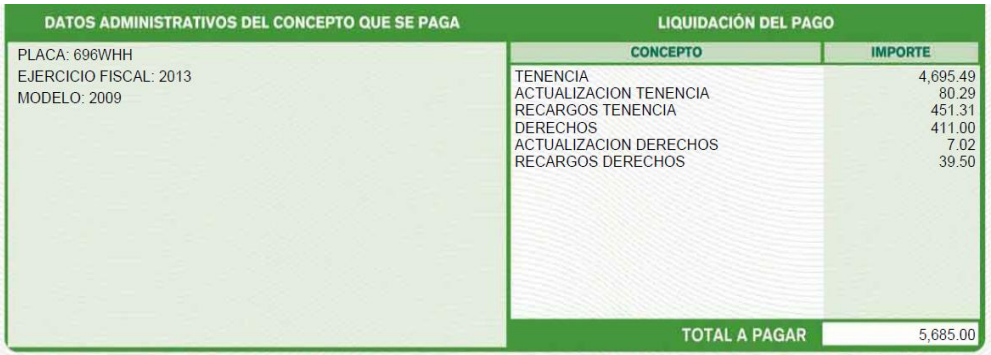
Seguridad Informátca

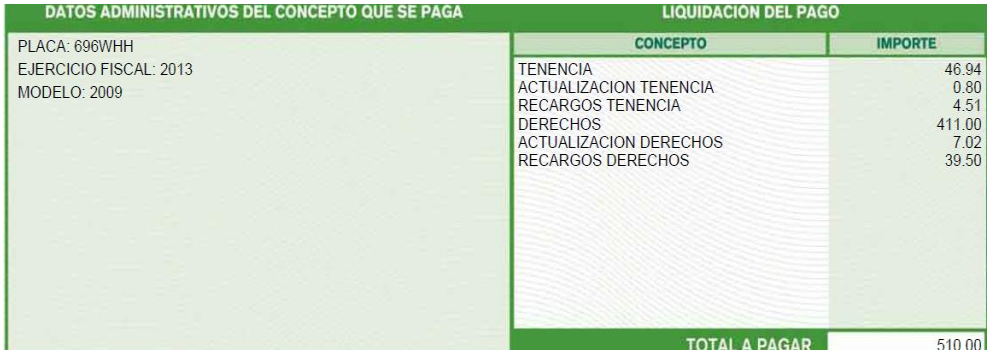
Hackeos Internos

Hack Interno – Beneficio $$$

Sistema anterior - Hackeable

Pago por la 10ma parte





SQL Injection

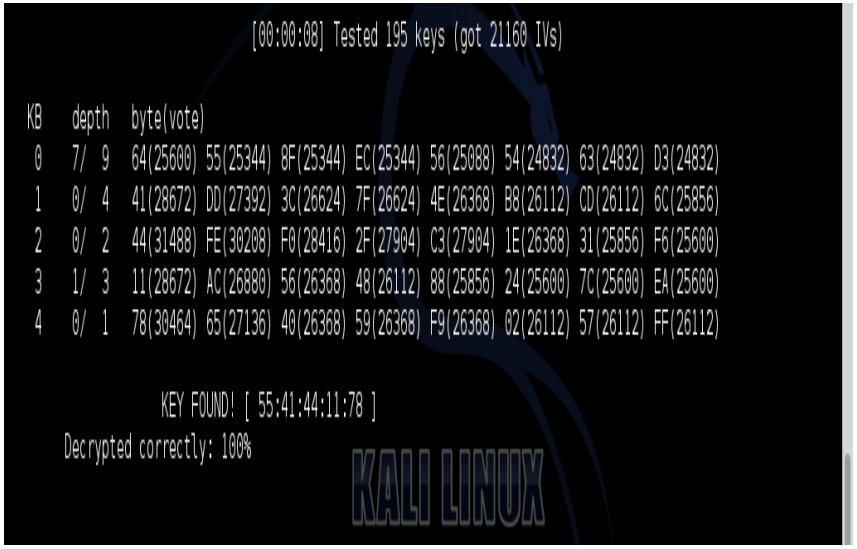
Aplicación Web Sanitizada

Extracción Baes de Datos

War Walking

Mapeo de Infraestructura

Hackeo de Cifrados Débiles



Investigaciones Forenses

Procurador

Date	Recipient	Subject	Opened?
14-Mar	leephdes@ gmail. com	RE: predial	not yet.
14-Mar	kevdaw2120@ gmail. com	RE: predial	17-Mar-14 15:48:32

Password help for leephdes@gmail.com

Reset your password using the verification method below:

Get a verification code (via SMS) on my phone: ••••••••95

Enter full phone number Hint: ••••••••95

Continue

Can't access this recovery option? Verify your identity by answering multiple questions about your account.

Defacement Página

Apoyo Investigación PDI

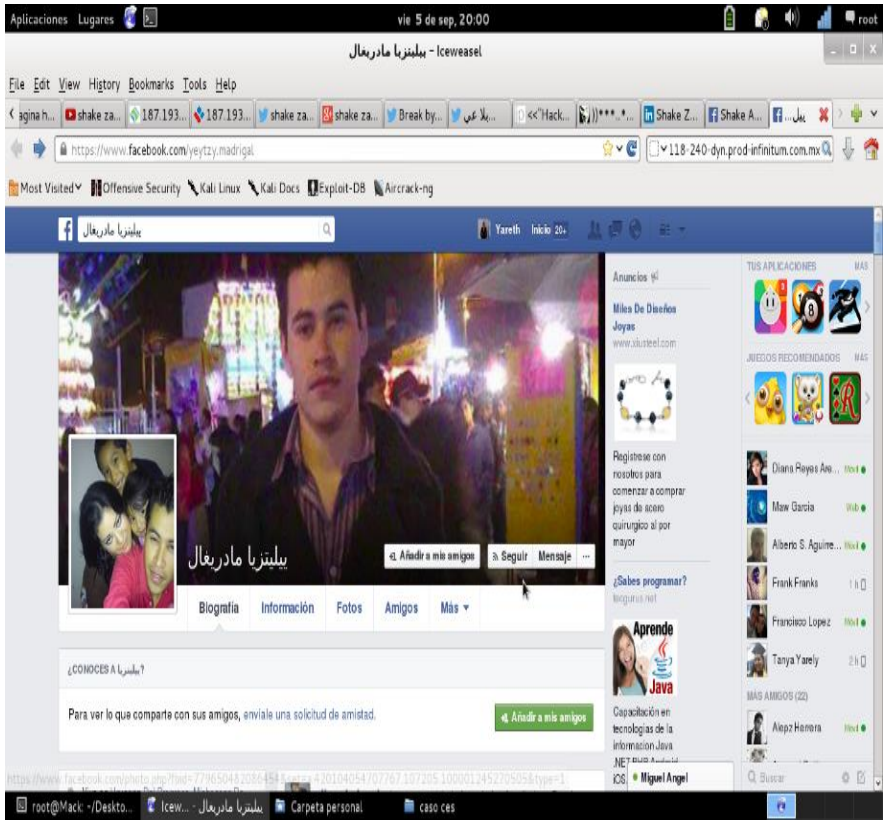


Ilustración 3 Facebook de donde se extrajeron fotos de "shakezaid"

Seguridad Informátca

Remediación a problemas de seguridad

Migración sistema de cálculo

Sanitización de campos de entrada

```
private function chksql_max($cadena)
{
        $patrones = '/(\W|\s+)\bALTER\b(\W|\s+)|(\W|\s+)\bSELECT\b(\W|\s+)|(\W|\s+)\bUPDATE\b(\W|\s+)';
        $patrones .= '|(\W|\s+)\bINSERT\b(\W|\s+)|(\W|\s+)\bDELETE\b(\W|\s+)|(\W|\s+)\bDROP\b(\W|\s+)';
        $patrones .= '|(\W|\s+)\bFROM\b(\W|\s+)|(\W|\s+)\bWHERE\b(\W|\s+)|(\W|\s+)\bLIKE\b(\W|\s+)';
        $patrones .= '|(\W|\s+)\bBETWEEN\b(\W|\s+)|(\W|\s+)\bCREATE\b(\W|\s+)|(\W|\s+)\bAND\b(\W|\s+)';
        $patrones .= '|(\W|\s+)\bOR\b(\W|\s+)|(\W|\s+)\bROOT\b(\W|\s+)|(\W|\s+)\bINNER\b(\W|\s+)';
        $patrones .= '|(\W|\s+)\bXMLTYPE\b(\W|\s+)|(\W|\s+)\bUPPER\(\s*\w*\s?\)(\W|\s+)|(\W|\s+)\bLOWER\(\s
        $patrones .= '|(\W*|\s+)\bxp_(\w+|\d+|\s+)|(\W|\s+)\bVALUES\b(\W|\s+)|(\W|\s+)\bCHR\(\s*\w*\s?\)(\W
        $patrones .= '|(\W|\s+)\bADMIN\b(\W|\s+)|(\W|\s+)\bEXEC\b(\W|\s+)|[\|\^\,\|\{\}\[\]\"\^\x00\x1a\x0a

        $val = preg_match($patrones,$cadena,$salidas);
```

Cadena de entrada: SELECT ascii('A');
Valores resultado: ascii(A)

Cadena de entrada: SELECT CAST('1â€² as int);
Valores resultado: CAST(1â€² as int)

Cadena de entrada: SELECT CAST(1 as char);
Valores resultado: CAST(1 as char)

Cadena de entrada: SELECT 'A' + 'B';
Valores resultado: A + B

Cadena de entrada: IF (1=1) SELECT 1 ELSE SELECT 2;
Valores resultado: IF (1=1) 1 ELSE 2

Cadena de entrada: SELECT CASE WHEN 1=1 THEN 1 ELSE 2 END;
Valores resultado: CASE WHEN 1=1 THEN 1 ELSE 2 END

Cadena de entrada: SELECT char(65)+char(66);
Valores resultado: char(65)+char(66)

Cadena de entrada: Â WAITFOR DELAY '0:0:5â€²;
Valores resultado: Â WAITFOR DELAY 0:0:5â€²

Cadena de entrada: EXEC xp_cmdshell 'net user';
Valores resultado: cmdshell net user

Cadena de entrada: EXEC sp_configure 'show advanced options', 1;
Valores resultado: sp_configure show advanced options, 1

Cadena de entrada: SELECT is_srvrolemember('serveradmin');
Valores resultado: is_srvrolemember(serveradmin)

Cadena de entrada: SELECT is_srvrolemember('setupadmin');
Valores resultado: is_srvrolemember(setupadmin)

Cadena de entrada: SELECT is_srvrolemember('securityadmin');
Valores resultado: is_srvrolemember(securityadmin)

Cadena de entrada: SELECT name FROM master..syslogins WHERE denylogin = 0;
Valores resultado: name FROM master..syslogins WHERE denylogin = 0

Cadena de entrada: SELECT name FROM master..syslogins WHERE hasaccess = 1;
Valores resultado: name FROM master..syslogins WHERE hasaccess = 1

Cadena de entrada: SELECT name FROM master..syslogins WHERE isntname = 0;
Valores resultado: name FROM master..syslogins WHERE isntname = 0

Cadena de entrada: SELECT name FROM master..syslogins WHERE isntgroup = 0;
Valores resultado: name FROM master..syslogins WHERE isntgroup = 0

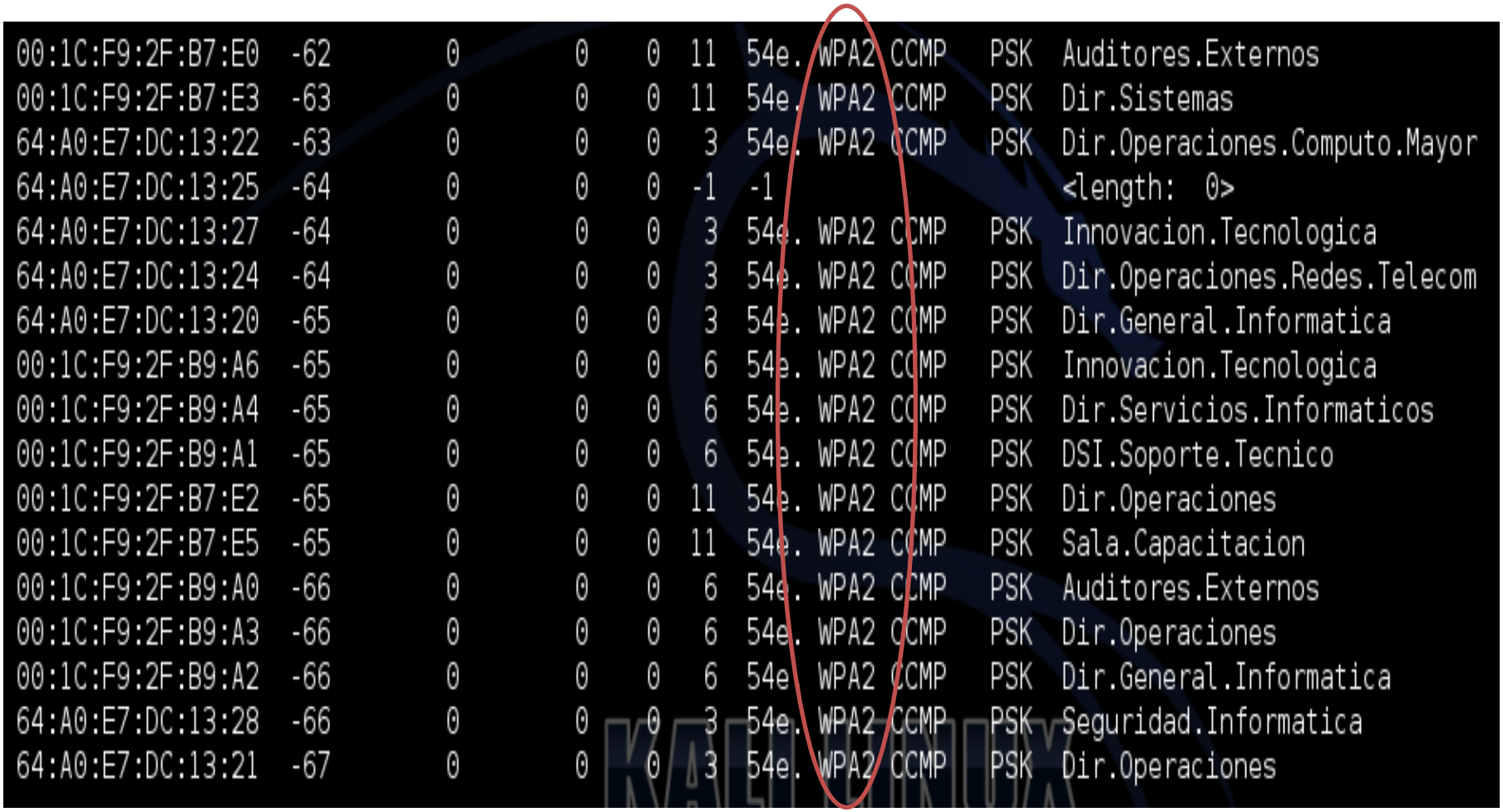
Cadena de entrada: SELECT name FROM master..syslogins WHERE sysadmin = 1;
Valores resultado: name FROM master..syslogins WHERE sysadmin = 1

Cadena de entrada: SELECT name FROM master..syslogins WHERE securityadmin = 1;
Valores resultado: name FROM master..syslogins WHERE securityadmin = 1

Cadena de entrada: SELECT name FROM master..syslogins WHERE serveradmin = 1;
Valores resultado: name FROM master..syslogins WHERE serveradmin = 1

Cadena de entrada: SELECT name FROM master..syslogins WHERE setupadmin = 1;
Valores resultado: name FROM master..syslogins WHERE setupadmin = 1

Migración mecanismos de cifrado

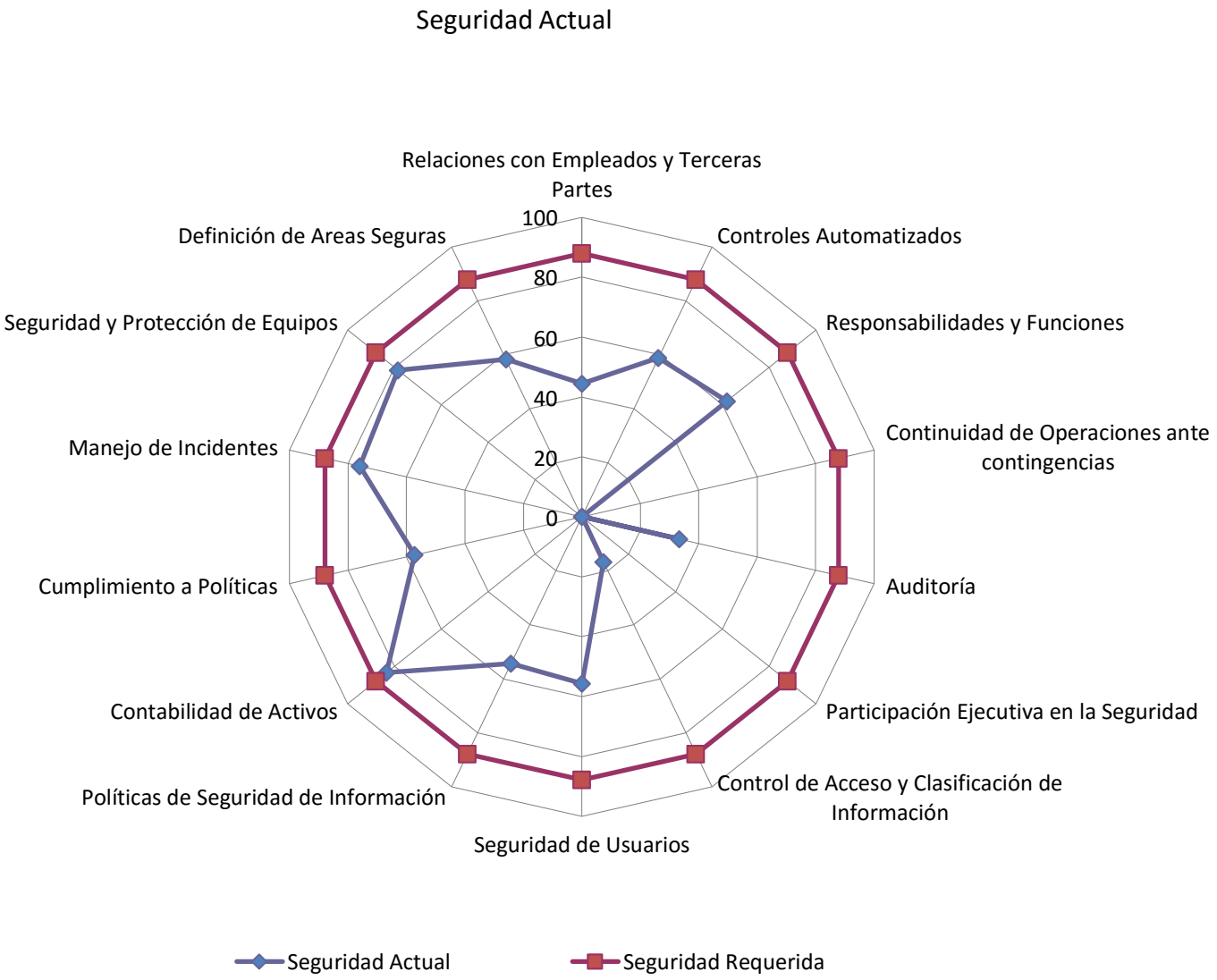


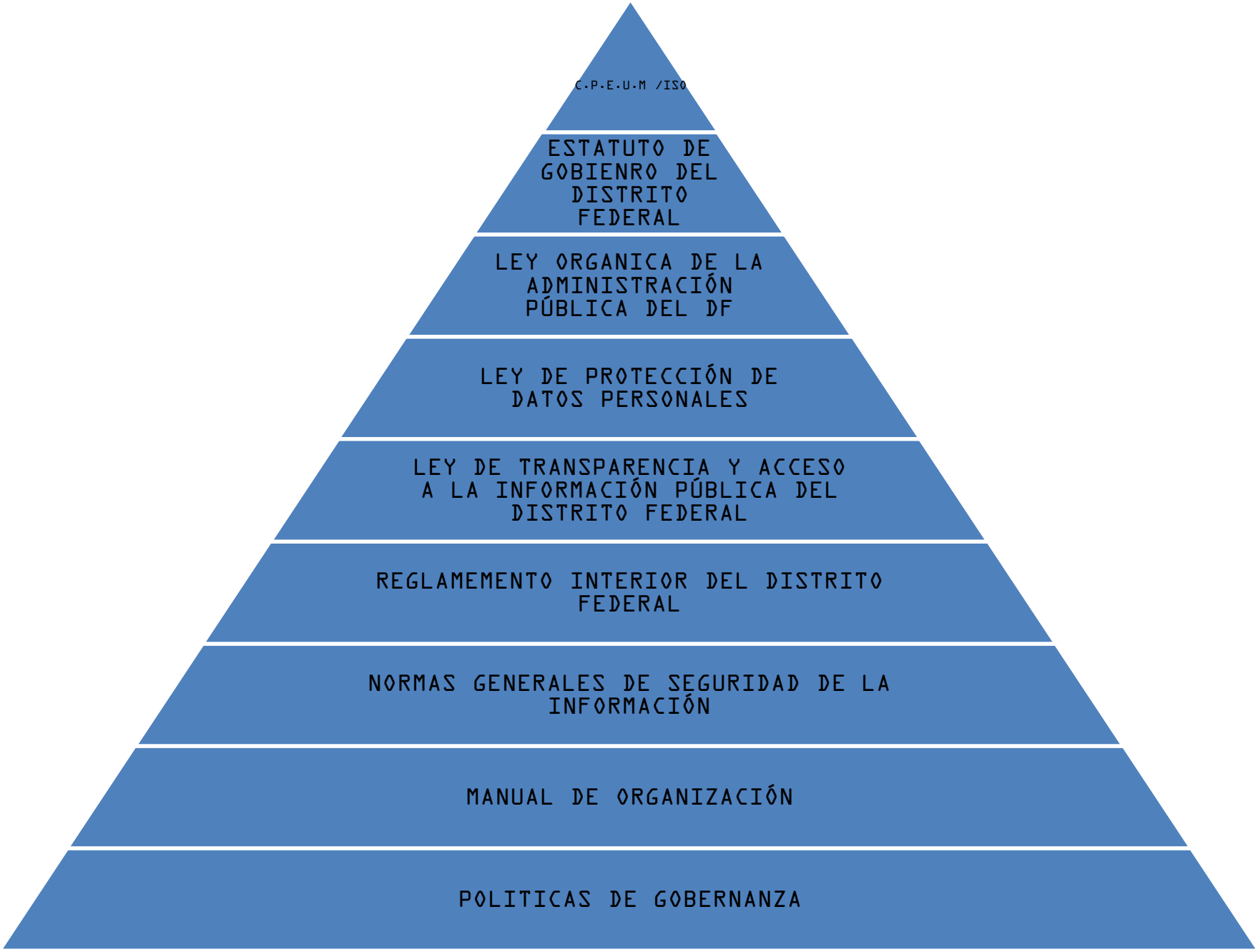
```
00:1C:F9:2F:B7:E0  -62        0        0    0  11  54e. WPA2 CCMP   PSK  Auditores.Externos
00:1C:F9:2F:B7:E3  -63        0        0    0  11  54e. WPA2 CCMP   PSK  Dir.Sistemas
64:A0:E7:DC:13:22  -63        0        0    0   3  54e. WPA2 CCMP   PSK  Dir.Operaciones.Computo.Mayor
64:A0:E7:DC:13:25  -64        0        0    0  -1  -1                    <length:  0>
64:A0:E7:DC:13:27  -64        0        0    0   3  54e. WPA2 CCMP   PSK  Innovacion.Tecnologica
64:A0:E7:DC:13:24  -64        0        0    0   3  54e. WPA2 CCMP   PSK  Dir.Operaciones.Redes.Telecom
64:A0:E7:DC:13:20  -65        0        0    0   3  54e. WPA2 CCMP   PSK  Dir.General.Informatica
00:1C:F9:2F:B9:A6  -65        0        0    0   6  54e. WPA2 CCMP   PSK  Innovacion.Tecnologica
00:1C:F9:2F:B9:A4  -65        0        0    0   6  54e. WPA2 CCMP   PSK  Dir.Servicios.Informaticos
00:1C:F9:2F:B9:A1  -65        0        0    0   6  54e. WPA2 CCMP   PSK  DSI.Soporte.Tecnico
00:1C:F9:2F:B7:E2  -65        0        0    0  11  54e. WPA2 CCMP   PSK  Dir.Operaciones
00:1C:F9:2F:B7:E5  -65        0        0    0  11  54e. WPA2 CCMP   PSK  Sala.Capacitacion
00:1C:F9:2F:B9:A0  -66        0        0    0   6  54e. WPA2 CCMP   PSK  Auditores.Externos
00:1C:F9:2F:B9:A3  -66        0        0    0   6  54e. WPA2 CCMP   PSK  Dir.Operaciones
00:1C:F9:2F:B9:A2  -66        0        0    0   6  54e  WPA2 CCMP   PSK  Dir.General.Informatica
64:A0:E7:DC:13:28  -66        0        0    0   3  54e. WPA2 CCMP   PSK  Seguridad.Informatica
64:A0:E7:DC:13:21  -67        0        0    0   3  54e. WPA2 CCMP   PSK  Dir.Operaciones
```

Seguridad Informátca

Respecto al método empleado y sus procesos

Assessment Seguridad Informática

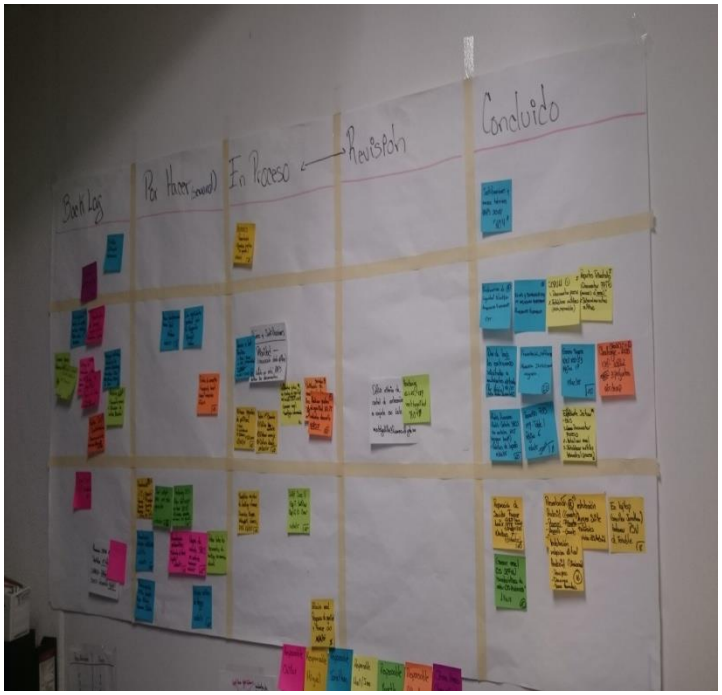


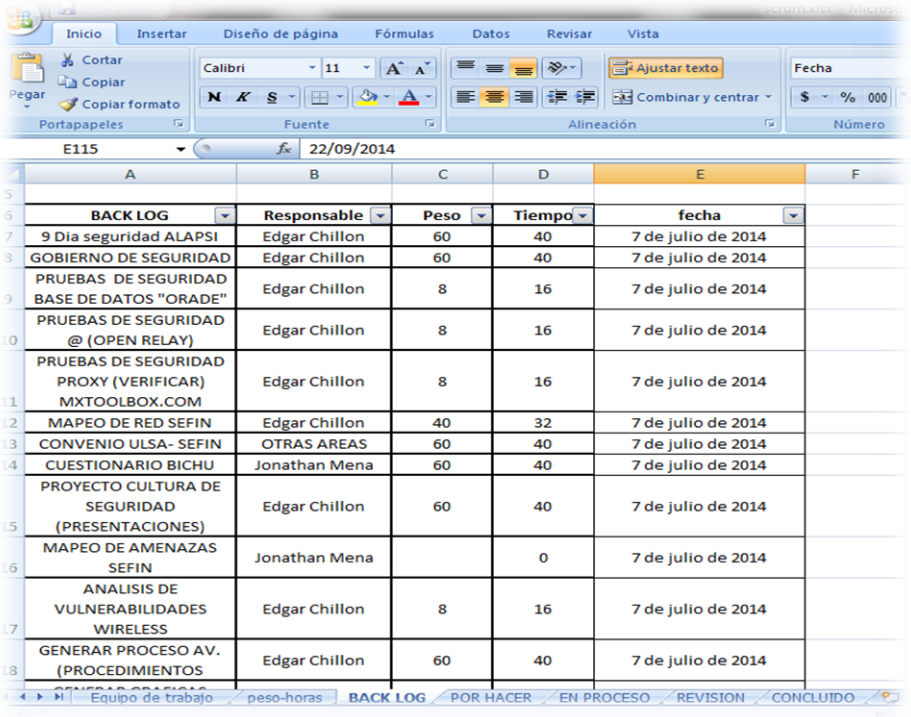

C.P.E.U.M /ISO
ESTATUTO DE GOBIENRO DEL DISTRITO FEDERAL
LEY ORGANICA DE LA ADMINISTRACIÓN PÚBLICA DEL DF
LEY DE PROTECCIÓN DE DATOS PERSONALES
LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL DISTRITO FEDERAL
REGLAMEMENTO INTERIOR DEL DISTRITO FEDERAL
NORMAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN
MANUAL DE ORGANIZACIÓN
POLITICAS DE GOBERNANZA

NOMBRE DEL PROYECTO	ISO 27001	Reglamento Inerior del Distrito Federal	Manual de Organización de la SF	Normas Generales de Seguridad de la Información	Políticas de Gobernanza III.9.2
CONTINUIDAD Y ASEGURAMIENTO DE OPERACIONES NOC/SOC	4.2.3 Monitorear y Revisar el SGSI, A.10.10 Monitoreo, A.13.2.2 Aprendizaje de los incidentes en la Seguridad de la información	artículo 87 fracción I, artículo 119 C fracción VI y XIII	Objetivo 1 función 1 de Jud de Monitoreo	7.6 Monitoreo de Sistemas, 7.6.2 Monitoreo de Sistemas y Recursos en uso	III.9.2
Cumplimiento Regulatorio Int/Ext	1.2 aplicación y 2 Reformas Normativas	artículo 87 fracciones II y V	Objetivo 3 funciones 1, 2 y 3, objetivo 5 funciones 1, 2, 3, 4 y 5 de la Subdirección de Seguridad Informática, Objetivo 2 función 1 de JUDAR	artículos 2, 4, 7, capitulo III, 12 numeral 1, 12 , 12.1. Y 12.1.1	I.4.1.,II.2.1 , III.3.1., y IV.1.1
	3.6 incidente de seguridad de la información, 3.11 análisis de riesgo, 3.12 valuación de riesgo, 3.13 evaluación de riesgo , 3.14 gestión de riesgo y 3.15 tratamiento del riesgo	artículo 87 fracción XV, 119 C fracción XIII	objetivo 1 función 1, 2, 3, 4, 5, 6 y 7 de SSI, objetivo 1, funciones 1,2 y 3, objetivo 2 funciones 2,3 y 4 de JUDAR, objetivo 2 funciones 1 y 2 y objetivo 3 funciones 1 y 3	artículos 2, capitulo III inciso 6), 1.1, 1.2,	I.5.1, I.6.1 y III.2.1
Cultura de Seguridad	Pláticas Bimestrales (Seguridad (Dominios y Controles ISO 27001:2013)	artículo 87 fraccioón XI , 119 C fracción XII	objetivo 6 funciones 1, 2 y 3 de la SSI	artículo 1 fracción I, capitulo III 1), 2), 4), 5.2.1, artículo 11 fracción IV	no hay referencia
	4.2.2. e), 5.2.2 y A.8.2.2	artículo 87 fracción XIV		capitulo III pfo 1, 3.1.1., 5.2.1.	
Análisis de Vulnerabilidades	A.10.3.2. y A.14.1.4	artículo 87 fracción XV, 119 C fracciones IX	Ssi objetivo 1 funciones 1,2, 3, 4, 5, 6 y 7, JUDAR objetivo 2 funciones 1,2, 3 y 4 y JUDCM objetivo 2 funciones 1, 2, 3 y objetivo 3 funciones 1, 2 y 3	artículo 4, capitulo III 3), 6) y 9), articulo 11 fracción II, articulo 12, 1,1, 9, 10 y 11	I.5.1., I.6.1
	4.2.1 d) 3), 4.2.1. e) 2), 7.2 e), A.12.6, A.12.6.1, A.13, A.13.1, A.13.1.1., A.13.1.2, A.13.2, A.13.2.1, A.13.2.2 y a.13.2.3	artículo 87 fracción IV, VIII, XV y artículo 119 C fracción XIII	SSI objetivo 2 funciones 3, 4, 5, 6 y 7, JUDAR objetivo 1 funciones 1, 2 y 3 y JUDCM objetivo 1 funciones 1, 2, 3 y 4	artículo 4, capitulo III 8) y 9), artíuclo 11 fracciones III, IV y V, 3.1, 3.1.1., 6.1.2, 7, 8, 9 y 11	III.9.1.

Estructura de planeación de trabajo

SCRUM





Inicio | Insertar | Diseño de página | Fórmulas | Datos | Revisar | Vista

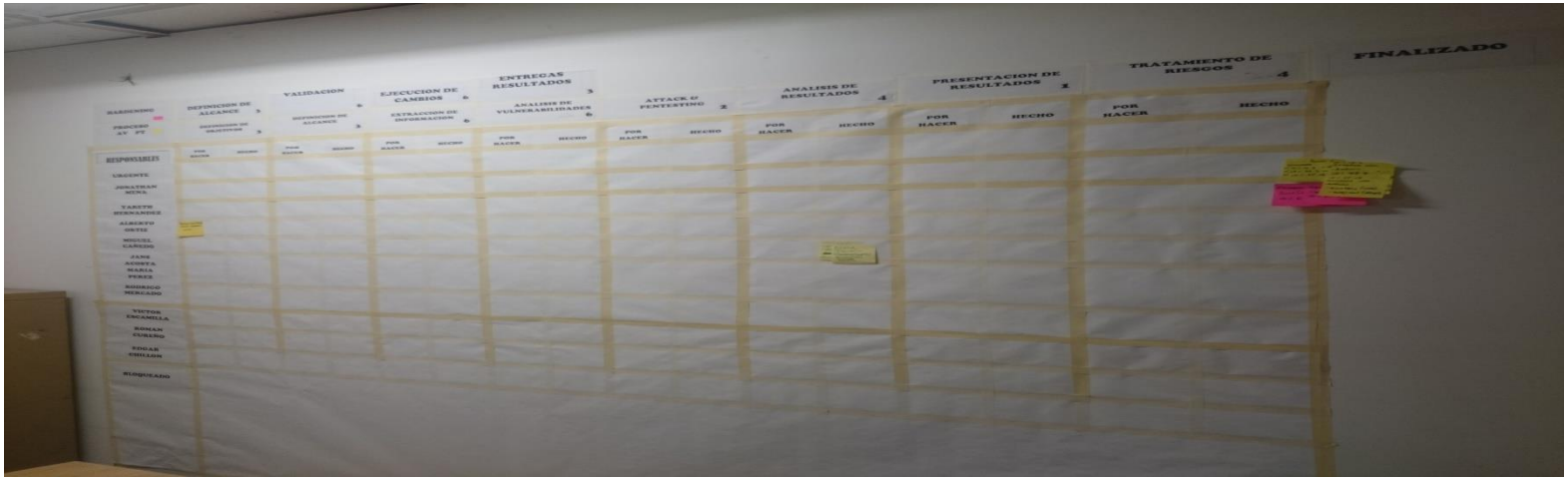
Cortar · Copiar · Copiar formato · Pegar · Portapapeles · Calibri · 11 · Fuente · Ajustar texto · Combinar y centrar · Alineación · Fecha · Número

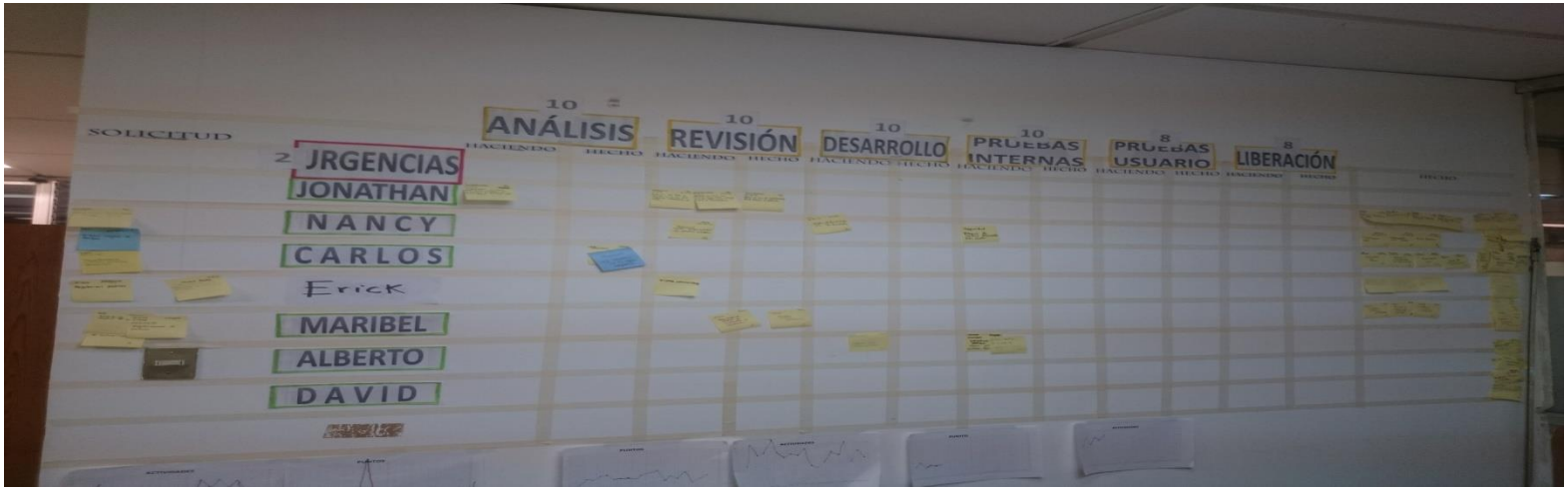
E115 | 22/09/2014

BACK LOG	Responsable	Peso	Tiempo	fecha
9 Dia seguridad ALAPSI	Edgar Chillon	60	40	7 de julio de 2014
GOBIERNO DE SEGURIDAD	Edgar Chillon	60	40	7 de julio de 2014
PRUEBAS DE SEGURIDAD BASE DE DATOS "ORADE"	Edgar Chillon	8	16	7 de julio de 2014
PRUEBAS DE SEGURIDAD @ (OPEN RELAY)	Edgar Chillon	8	16	7 de julio de 2014
PRUEBAS DE SEGURIDAD PROXY (VERIFICAR) MXTOOLBOX.COM	Edgar Chillon	8	16	7 de julio de 2014
MAPEO DE RED SEFIN	Edgar Chillon	40	32	7 de julio de 2014
CONVENIO ULSA- SEFIN	OTRAS AREAS	60	40	7 de julio de 2014
CUESTIONARIO BICHU	Jonathan Mena	60	40	7 de julio de 2014
PROYECTO CULTURA DE SEGURIDAD (PRESENTACIONES)	Edgar Chillon	60	40	7 de julio de 2014
MAPEO DE AMENAZAS SEFIN	Jonathan Mena		0	7 de julio de 2014
ANALISIS DE VULNERABILIDADES WIRELESS	Edgar Chillon	8	16	7 de julio de 2014
GENERAR PROCESO AV. (PROCEDIMIENTOS	Edgar Chillon	60	40	7 de julio de 2014

Equipo de trabajo | peso-horas | BACK LOG | POR HACER | EN PROCESO | REVISION | CONCLUIDO

Kanban / SCRUM



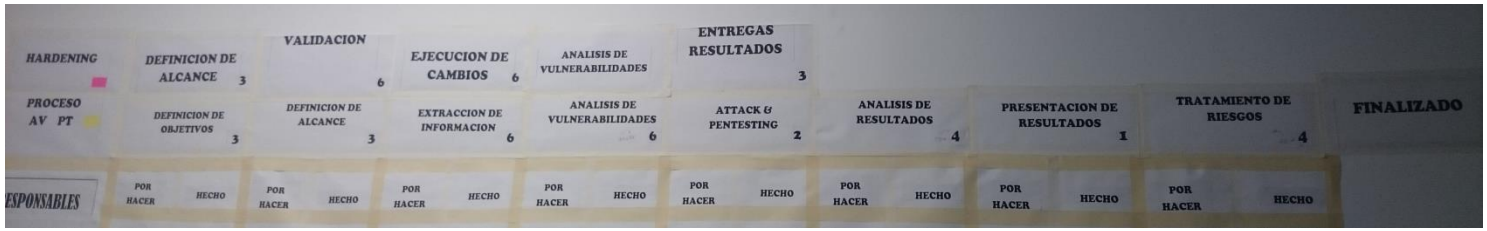


HARDENING

- DEFINICION DE OBJETIVOS
- DEFINICION DE ALCANCE
- EXTRACCION DE INFORMACION
- ANALISIS DE VULNERABILIDADES
- ATTACK & PENTESTING
- ANALISIS DE RESULTADOS
- PRESENTACION DE RESULTADOS
- TRATAMIENTO DE RESULTADO
- FINALIZADO

PROCESO AV /PT

- DEFINICION DE ALCANCE
- VALIDACION
- EJECUCION DE CAMBIOS
- ANALISIS DE VULNERABILIDADES
- ENTREGA DE RESULTADOS

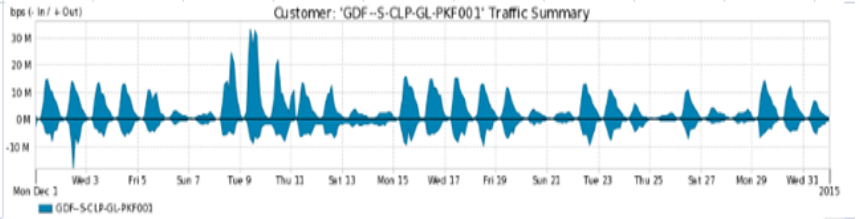


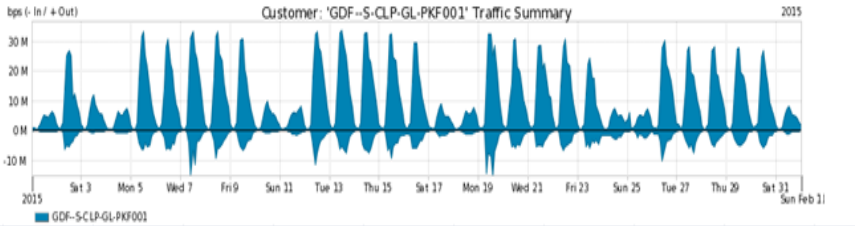
HARDENING			
Operating system	Linux		
Operating system name	**Ubuntu**		
Operating system version	**14.04 LTS**		
Kernel version (full)	3.13.0-24-generic		
Hardware platform	x86_64		
Sistema		Aplicativo	
Antes	Después	Antes	Después
54% Hardened	**55% Hardened**		
Tests Performed			
185	**185**		
Total Tests			
315	**315**		

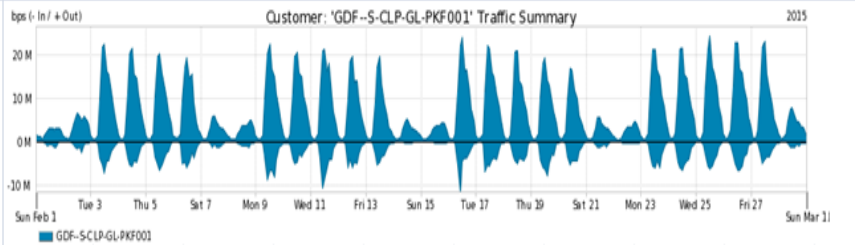
HARDENING			
Operating system	Linux		
Operating system name	**SUSE**		
Operating system version	**SUSE Linux Enterprise Server 11**		
Kernel version (full)	3.0.76-0.11-default		
Hardware platform	x86_64		
Sistema		Aplicativo	
Antes	Después	Antes	Después
44% Hardened	**46% Hardened**		
Tests Performed			
188	**188**		
Total Tests			
315	**315**		

Expediente Seguridad Externos

FECHA	REMITENTE	FOLIO	CASO	REPORTE
02/01/2015	SCITUM	S/N	TRÁFICO SEGURO	Reportes del mes de Diciembre Trafico Seguro
03/02/2015	SCITUM	S/N	TRÁFICO SEGURO	Reportes del mes de Enero Trafico Seguro
04/03/2015	SCITUM	S/N	TRÁFICO SEGURO	Reportes del mes de Febrero Trafico Seguro
30/03/2015	SCITUM	AS-GDF-0000031	ATAQUES / INDICIOS DE NEGACION DE SERVICIO /	Dictamen de Actividad Sospechosa
30/03/2015	SCITUM	AS-GDF-0000032	ATAQUES / INDICIOS DE NEGACION DE SERVICIO /	Dictamen de Actividad Sospechosa
30/03/2015	SCITUM	AS-GDF-0000033	ATAQUES / INDICIOS DE NEGACION DE SERVICIO /	Dictamen de Actividad Sospechosa







Riesgos Cuantitativos

ISECOM - RISK ASSESSMENT VALUES

OPSEC	
Visibility	229
Access	874
Trust	0

Class A	CONTROLS	Missing
Authentication	0	1103
Indemnification	0	1103
Resistance	0	1103
Subjugation	0	1103
Continuity	0	1103
Class B		
Non-Repudiation	0	1103
Confidentiality	0	1103
Privacy	0	1103
Integrity	0	1103
Alarm	0	1103

	LIMITATIONS	Total
Vulnerabilities	179	910.03031
Weaknesses	0	0.00000
Concerns	0	0.00000
Exposures	2095	7038.85534
Anomalies	0	0.00000

CALCULATION WORKSHEET	
Porosity	1103
Total Controls	0
Class A Controls	0
Class B Controls	0
Whole Coverage	0.00%
True Coverage	0.00%
True Coverage A	0.00%
True Coverage B	0.00%
Missing Controls	11030
Missing Controls A	5515
Missing Controls B	5515
Coverage Missing	100.00%
Total # Limitations	2274
Limitations Value	7948.885643

Vulnerability	5.08396820
Weakness	4.82072676
Concern	4.82072676
Exposure	3.35983548
Anomaly	4.75921443

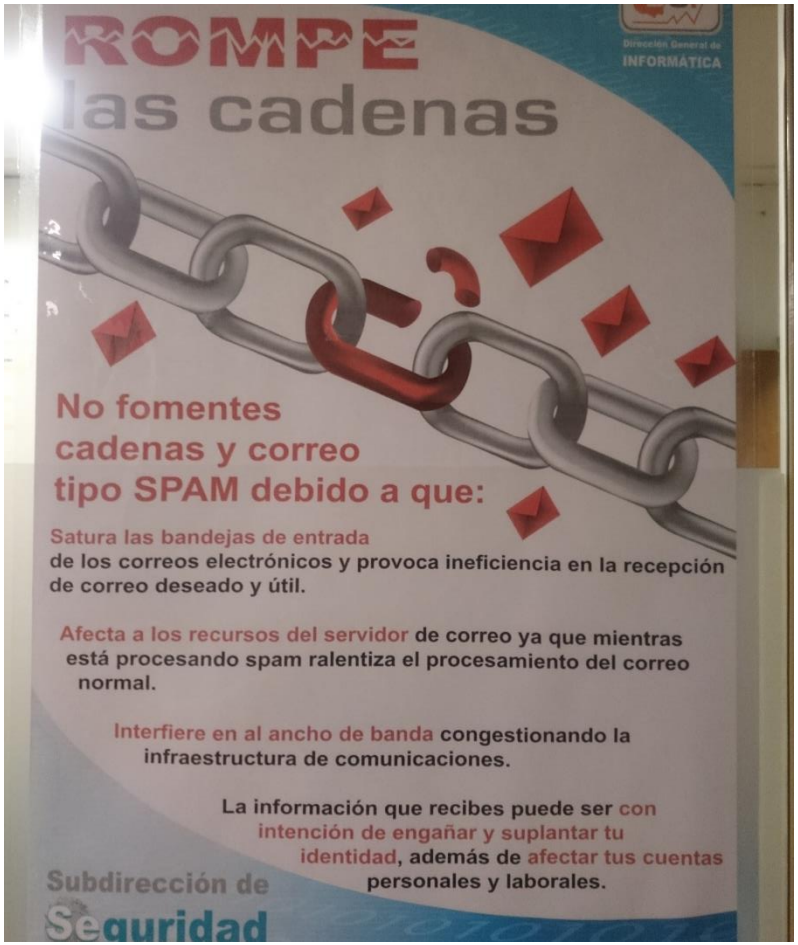
	RAV TOTALS
OPSEC	25.42760751
CONTROLS	0.00000000
LIMITATIONS	34.81362028
Δ	-60.24122779

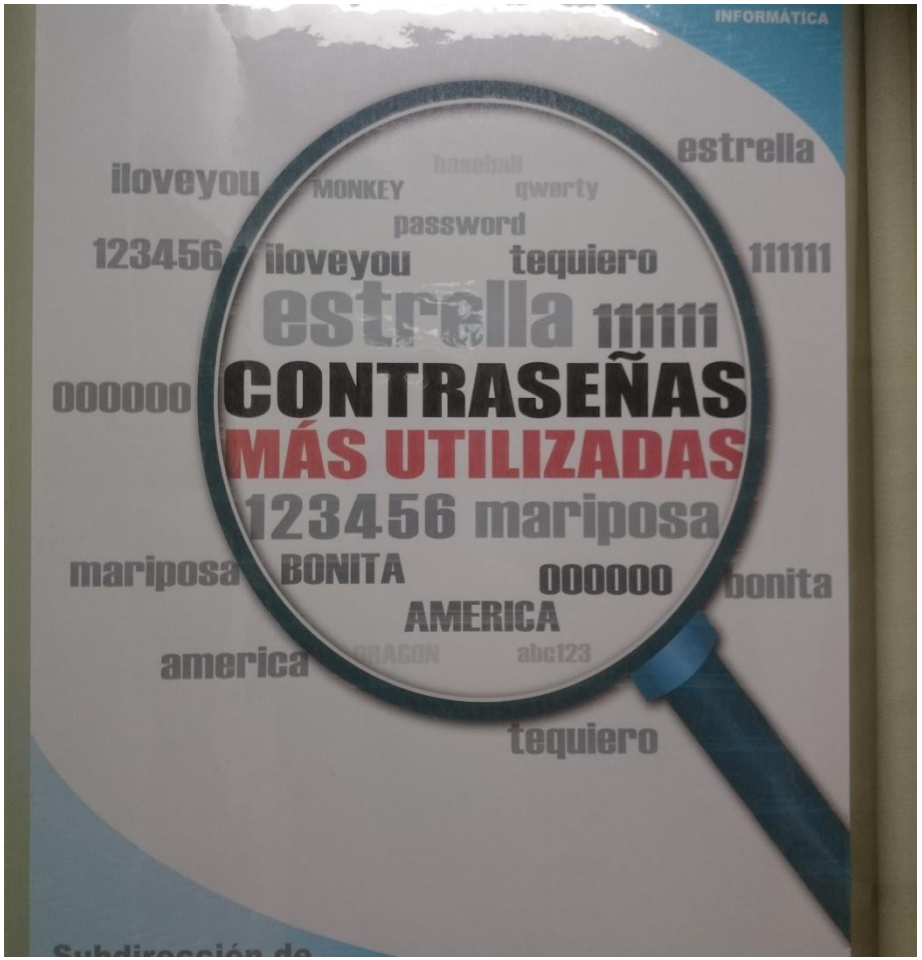
RAV	48.61104294

Resultados Pruebas Seguridad

¿Y nuestra gente?

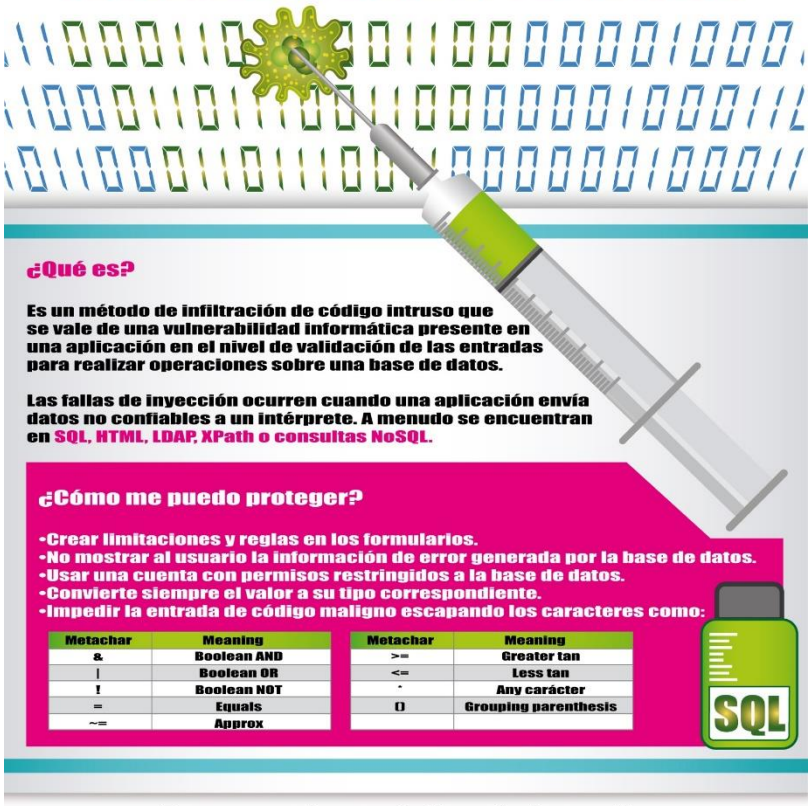
Conciencia - Cultura seguridad general





Equipos especializados

ATAQUES POR INYECCIÓN DE CÓDIGO



¿Qué es?

Es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

Las fallas de inyección ocurren cuando una aplicación envía datos no confiables a un intérprete. A menudo se encuentran en SQL, HTML, LDAP, XPath o consultas NoSQL.

¿Cómo me puedo proteger?

- Crear limitaciones y reglas en los formularios.
- No mostrar al usuario la información de error generada por la base de datos.
- Usar una cuenta con permisos restringidos a la base de datos.
- Convierte siempre el valor a su tipo correspondiente.
- Impedir la entrada de código maligno escapando los caracteres como:

Metachar	Meaning	Metachar	Meaning
&	Boolean AND	>=	Greater tan
|	Boolean OR	<=	Less tan
!	Boolean NOT	*	Any carácter
=	Equals	()	Grouping parenthesis
~=	Approx		

SQL

Por unas mejores prácticas de desarrollo, recuerda que la seguridad es prioridad de todos.
Protege tu código, Protege tu aplicación, Protege tu empresa.

FORTALECE tu seguridad

Para lograrlo SON IMPORTANTES estas consideraciones:

- No utilices en tu contraseña información personal o que pueda relacionarse contigo.
- No utilices palabras (en cualquier idioma) que puedan encontrarse en un diccionario.
- Debes tener contraseñas distintas en cada sistema.
- Nunca realices actividades bancarias en computadoras públicas como lo son los cafés Internet.
- No reveles tu contraseña a ninguna persona.
- Cambia de forma periódica tu contraseña.
- Debe contar con una longitud mínima de 9 caracteres: Letras mayúsculas, letras minúsculas, números y al menos un caracter especial: ¡!#$%&/()=?¡@


Gracias