



**CLAIN2015**

XIX CONGRESO LATINOAMERICANO DE  
**AUDITORIA INTERNA  
Y EVALUACIÓN DE RIESGOS**



## Banca Electrónica Móvil

Alejandro Rodríguez Moreno

Subdirector de Auditoría Interna  
Grupo Financiero Multiva



# ALEJANDRO RODRÍGUEZ MORENO

- Responsable de la función de auditoría a los Sistemas de Seguridad y de la Información de las empresas del Grupo Financiero
- Vicepresidente de Isaca Capítulo Cd. De México.



# AGENDA

- ENTENDIMIENTO DE LA BANCA ELECTRÓNICA MÓVIL
- ASPECTOS DE SEGURIDAD
- ENFOQUE DEL AUDITOR DE TI
- FORENSIA DIGITAL

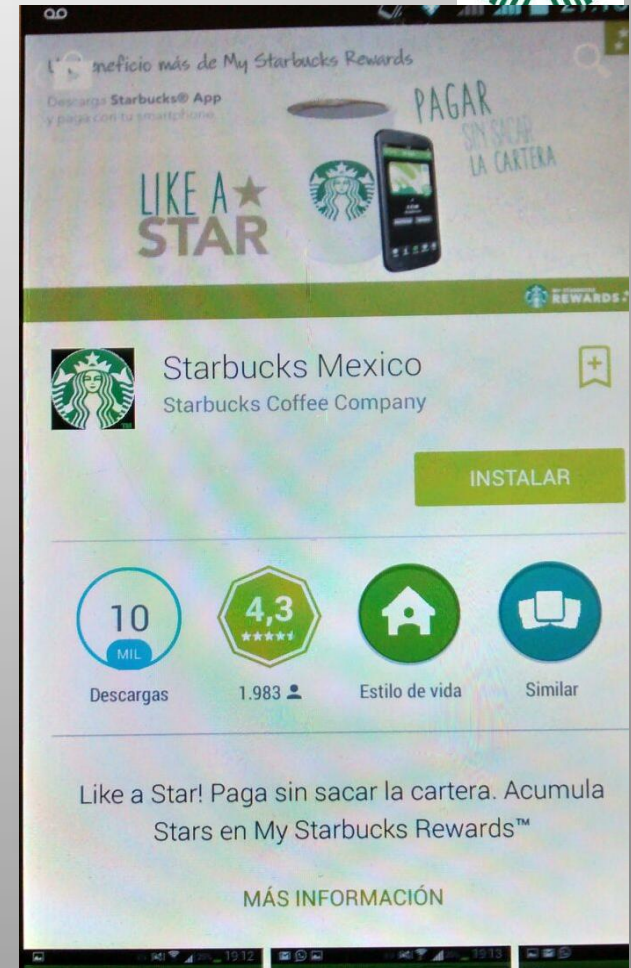
# ALGUNAS TENDENCIAS ¿FUTURISTAS?

- Dinero virtual  
- Apps para consumo cotidiano..  
Pago de taxis, estéticas, etc.
- Bancarizar “changarros”
- Sucursales “online”
- Mobile Banking (Banca móvil)
- Mobile POS
- Mobile Bill
- Mobile Token
- Mobile Marketing
- Mobile survey
- Mobile shopping
- Mobile geoposition
- Mobile cash
- Mobile loyalty
- ...

# ALGUNAS TENDENCIAS ¿FUTURISTAS?...



- La nueva Starbucks App, permitirá a los usuarios pagar utilizando su teléfono móvil y la tarjeta de lealtad Starbucks Rewards.. La nueva aplicación permite también recargar la tarjeta Starbucks Rewards con una tarjeta de crédito, consultar el saldo, ubicar las unidades más cercanas hasta con realidad aumentada y diseñar bebidas, por lo que al llegar al mostrador no sólo se puede pagar sino ordenar la bebida.





# FUNCIONAMIENTO TÍPICO DE BANCA ELECTRÓNICA

## Devices

Feature Phones &  
Smart Phones

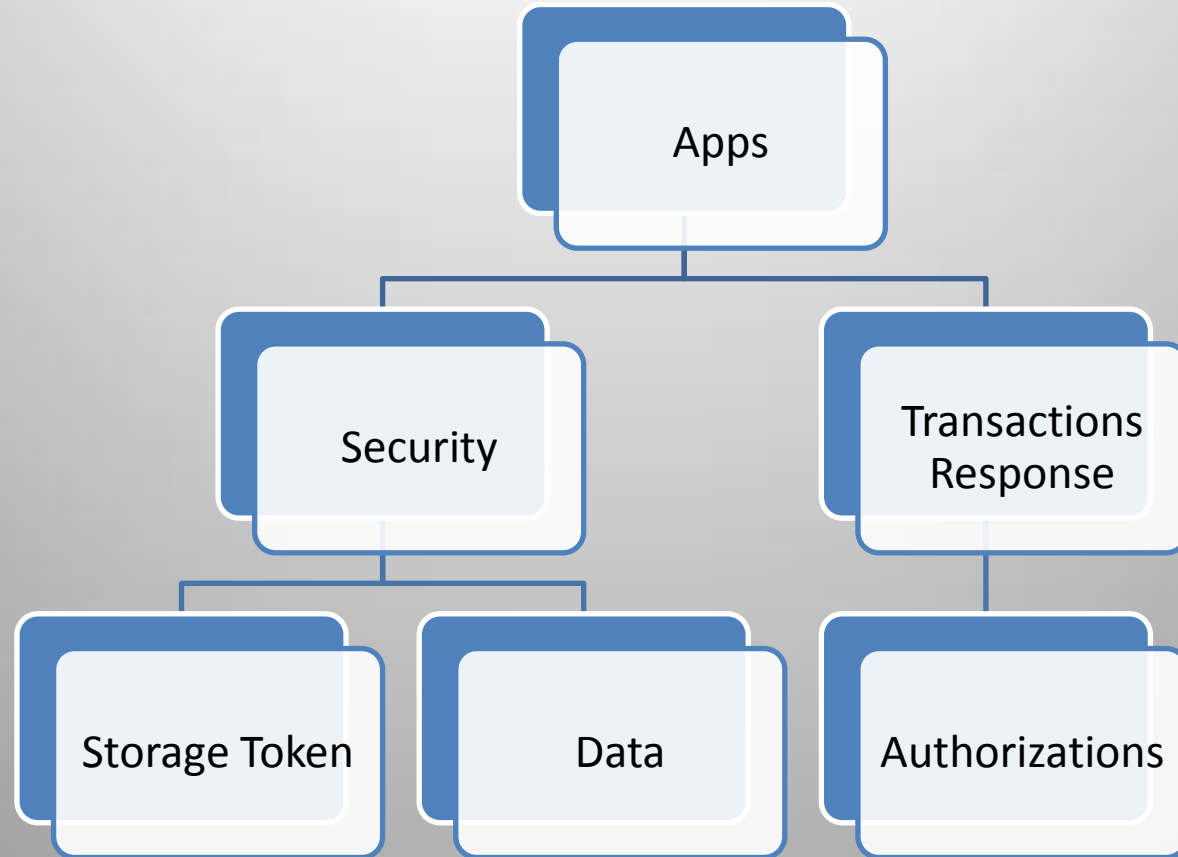


Apps for  
Mobile  
Banking



Authorizator

# ADMINISTRACIÓN DE LA APLICACIÓN



# QUE NOS DEBE DE INTERESAR DE LOS COMPONENTES DE BANCA ELECTRÓNICA?

- **Comunication Server**
- **SMS Chanel**
- **Core Server**
- **User Application**
- **Application Deployer**
- **Bases de Datos**
- **Herramientas y utilidades**



# OTROS COMPONENTES

## – Bases de datos

- SQL, Oracle, etc.

## – Herramientas y Utilidades

- Audit Viewer
- CMD Audit Viewer
- Log Viewer

# CARACTERÍSTICAS DE SEGURIDAD

## – Sesion Management

- Sign On de usuario
- Time Out de sesión

## – Seguridad Local (dispositivo)

- Password local
- Application forward lock (Digital Rights Management)
- Almacenamiento seguro (cifrado)

## – Seguridad integral

- Dispositivo firmado por el Banco (ej.IMEI)

# **PARTICIPANTES EN UN PROYECTO DE BANCA ELECTRÓNICA Y CUMPLIMIENTO NORMATIVO**

## **– Instituciones Bancarias**

- Definen el modelo de negocio

## **– Entidades regulatorias**

- Definen el marco normativo e incluso de seguridad

## **– Marcas (Visa, Mastercard, etc.)**

- Definen parámetros operativos y de seguridad –  
Certificaciones

## **– Integradores**

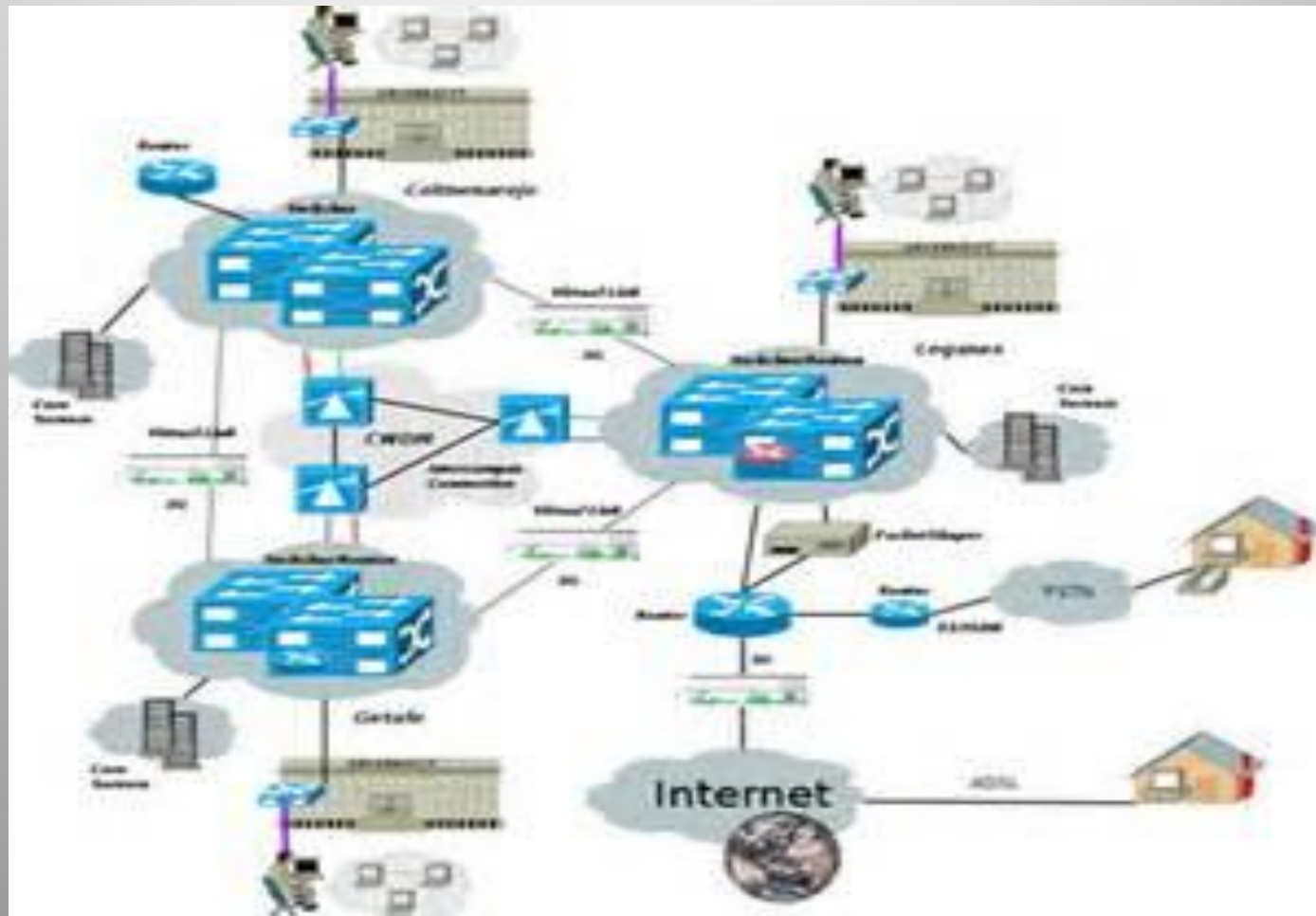
- AKII Pagos, Paypal, Sr. Pago, etc. o

# ROL DEL AUDITOR EN BANCA ELECTRÓNICA

– Que enfoque le damos??



# PRIMER PASO.. PEDIR LA ARQUITECTURA DE BE ?



# PRIMER PASO...





## ANTES DE ESO...

- Adicional a las auditorías típicas.. (CGTI, Cumplimiento)
- Conocer “concerns” de la alta dirección (robo de datos) y,  
Enfocarse en temas como:



# BACKDOOR EN VALIDACIÓN DE TOKENS -SEMILLAS

– IF .. Else..

```
root@kali:~/webcoo# ./webcoo.pl -E -w http://127.0.0.1/backdoor.php

webCoop 0.2.2 - Web Backdoor Cookie Script Kit
Copyright (C) 2011-2012 Anestis Bechtsoudis
[ @anestisb | anestis@bechtsoudis.com | http://www.bechtsoudis.com ]

[+] Connecting to remote server as...
uid=33(www-data) gid=33(www-data) groups=33(www-data)

[*] Type 'load' to use an extension module.
[*] Type 'exit' to quit terminal.

webcoop load
Currently available extension modules:
  MySQL-CLI: MySQL Command Line Module
              mysql-cli <IP[:port]> <user> <pass> (ex. 'mysql-cli 10.0.1.11 admin pAs5')
  PSQL-CLI: Postgres Command Line Module
              psql-cli <IP[:port]> <db> <user> <pass> (ex. 'psql-cli 10.0.1.12 testDB root pAs5')
  upload: File upload Module
              upload <local_file> <remote_dir> (ex. 'upload exploit.c /tmp/')

[*] Type the module name with the correct args.

http://esdn...> psql-cli 127.0.0.1 test db user db @cc3se
Announce esdn.microsoft.com HTTP/1.1 200 OK GET /esdn.aspx HTTP/1.1
Accept: */*
Referer: http://...
```

# DISPOSITIVOS SENSIBLES, EJ. TPV'S

rp\_Verizon-DBIR-2014\_en\_xg.pdf - Adobe Reader

Archivo Edición Ver Ventana Ayuda

Mis archivos 18 (20 de 60) 137% Herramientas Firmar Comentario

POINT-OF-SALE INTRUSIONS

**Figure 24.**  
Top 5 discovery methods for POS Intrusions (n=197)

All External	99%
All Internal	1%
Ext - law enforcement	75%
Ext - fraud detection	14%
Ext - customer	11%
Int - NIDS	<1%
Int - reported by user	<1%

Regardless of how large the victim organization was or which methods were used to steal payment card information, there is another commonality shared in 99% of the cases: someone else told the victim they had suffered a breach. This is no different than in years past, and we continue to see notification by law enforcement and fraud detection as the most common discovery methods. In many cases, investigations into breaches will uncover other victims, which explains why law enforcement

WEBAPP ATTACKS

The timelines in Figure 25 reinforce both the compromise vectors and the discovery methods. Entry is often extremely quick, as one would expect when exploiting stolen or weak passwords. Most often it takes weeks to discover, and that's based entirely on when the criminals want to start cashing in on their bounty.

**Figure 25.**  
Timespan of events within POS Intrusions

Time Interval	Percentage
0-15 min	51%
15-30 min	36%
30-45 min	1%
45-60 min	1%
60-90 min	11%
90-120 min	1%
120-150 min	0%
150-180 min	0%

Time Interval	Percentage
0-15 min	1%
15-30 min	88%
30-45 min	1%
45-60 min	1%
60-90 min	11%
90-120 min	0%
120-150 min	0%
150-180 min	0%

ES 08:05 p.m. 10/09/2014

# DISCOS DUROS

- De quien?
- Que se encuentra?
- Tengo herramientas para revisar?
- Existe algún DLP?



BCO- Base Ctes Camp Act Abr14 GPA - Microsoft Excel

A1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	SUCURSAL	EJECUTIVO	NUMERO DE	NOMBRE CLI	CUENTA	PRODUCTO	RFC	TELEFONO D	TELEFONO O	TELEFONO C	CORREO ELE	CORREO ELE	CALLE	NUM. EXT.	NUM.INT	COLONIA	DELEGA
1																	
2		10110	10110	SERGIO GASF	1000240758	MAYA BISTR	00001749738	1023	MABM91041	5552452351	5552452351	55182236901	mirmaya13@gmail.com	FUENTE DEL 18-C			
3		40104	40104	JEARIME SAL	1000265811	CEJA ESPINO	00002506815	1023	CEEA450831	4771364506	4771364506	3338081011	ceja.seguros@live.com.m	C DOS ORIEN	429		
4		40101	40101	GABRIELA PH	1000160635	TRUJILLO VE	00000631795	1029	TUVS7302061	3336243517	3335875630		sergiotrujillo_vega@hotmail	RINCONADA	102		
5		10116	10116	GABRIEL ARR	10001159059	RAMIREZ EL	00000814008	1023	RAEL5005136	5557107443	5557107443			SALTILLO	43		
6		10106	10106	ERIKA SELEN	1000238370	ROCHA FARI	00001706438	1020	ROFC790221	5555275673	5553999872		rochaodont@hotmail.com	LAGO CHIEM	48 D 301		
7		20101	20101	RAQUEL GON	1000223607	DIAZ DAVILA	00001416235	1023	DIDC740130	8113528186	8113528186	8112613069	diazclao@hotmail.com	CERRADA GA	128		
8		10105	10105	ILSE MARIBE	1000231578	RUBI GALLAR	00001573667	1026	RUGJ691123	5535855119	5535855119			CALLE 2	84		
9		10102	10102	ARACELI VEL	1000157230	HURTADO M	00002068092	1020	HUNC601024	5555821648	5555685014			CAMPESINO	243		
10		30101	30101	JUAN CARLO	1000253566	LOPEZ QUIN	00002132451	1023	LOQV380420	2222466368	2222466368	2224610725		5 NORTE	606	12	PUEBLA CEN/ PUEBLA
11		10106	10106	B. Patrimoni	1000143257	ENCISO LOPI	00001642154	1023	EILA730906	5555920518	5555168677			CUMBRE	25		
12		40102	40102	Ejecutivos SI	1000119267	SCHIEL LAWF	00000280488	1020	SIXL401120	3767667011	3767667011	3313841675	joyceschiel@gmail.com	LIBRAMIEN	98	403B	
13		10106	10106	B. Patrimoni	1000398991	GONZALEZ L	00003421295	1026	GOLJ750721	5536892115	5530030033			CONDESA	277		
14		40103	40103	GRACIELA MI	1000168102	GUZMAN NU	00000684813	1023	GUNA600702	3338331908	3338331908			CAMPO ALEC	288		04-feb
15		10116	10116	KARLA JOSEL	1000221256	PEREZ OROZ	00001282611	1023	VISJ640227	5558930908	5558930908	5528588524	gperez@fundacionbest.o	DE LAS CUES	10		
16		30101	30101	ALEJANDRO	1000238756	VILLAGOMEZ	00001711008	1023	VISJ640227	5558930908	5558930908	5514175988		BOSQUES BR	17	301	
17		20102	20102	EDGAR RICAI	1000405196	GRAJALES SI	00003459691	1023	GASE800508	8186568812	8186568812			PIZARRO	414	SUR	
18		10109	10109	JESSICA SAM	1000216868	PONCE OLIV	00001058398	1020	POCG310204	5979761091	5520980933			CONTINUACI	SN		
19		10119	10119	JESSICA SAM	1000266396	GARCIA FLO	00002519526	1023	GAFE781108	5562356034	5562356034	5534063037	rubitsa08@yahoo.com.m	POPOCATEPI	440	B202	
20		10109	10109	JOSE MANUE	1000368820	OSORIO MA	00003289036	1026	OOMM79052	5547569479	5559590530			RETORNO DE	MZ43	LT10	
21		10112	10112	ELIZABETH D	1000236931	PEREZ MONS	00001673448	1020	PEMLS50621	5532299020	5532299020	5585859249	aldayli6@msn.com	FAROLITO	317		1
22		30101	30101	JUAN CARLO	1000188569	PAEZ CARBA	00000818477	1023	PACI5007315	2222430700	2226151552		lpaezcarballo@hotmail.c	CDA RIVERA	6		
23		10105	10105	IRMA ALEJAN	1000173870	ABURTO BA	00000726807	1001	AUBK940621	5551351940	5552945200		klaburto210x.karla.aburto	HEROES DE N	37	12 B	
24		10103	10103	Ejecutivos SI	1000202740	GUTIERREZ G	00000915629	1024	GUGA830211	5552952722	5552638888	5535665018	andreas_122@hotmail.co	AV BOSQUES	27	202	
25		10103	10103	VICTOR MAR	1000203786	SANCHEZ GC	00000924296	1026	SAGG690830	5558201532	5552638888	5521300629	gonzalosanchez2@hotm	2DA CDA AL COND5		CS 5	

# IMPRESORAS

## – Que guardan?

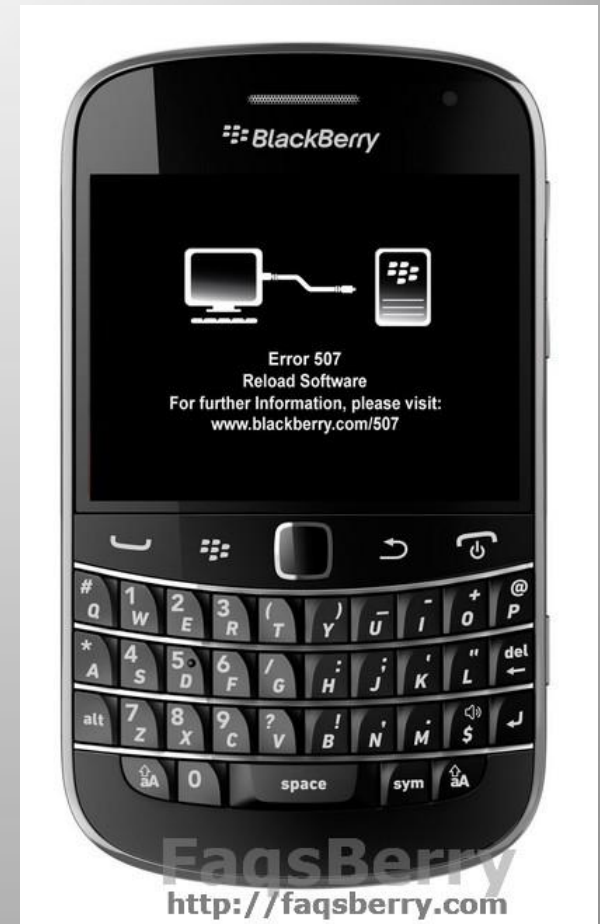
The screenshot shows the Kyocera Command Center RX web interface. The browser address bar displays 'http://10.160.10.169/'. The interface includes a navigation menu on the left with options like 'Inicio', 'Inicio de sesión de administrador', 'Información del dispositivo', 'Estado del trabajo', 'Buzón de documentos', 'Libr. direc.', and 'Enlaces'. The main content area shows the 'Estado del trabajo' (Job Status) section, which includes a 'Registro de trabajo de impresión' (Print Job Log) and a table of print jobs. The table has columns for 'Nro.', 'Fecha fin', 'Tipo', 'Nombre trabajo', 'Usuario', and 'Resultado'. The jobs listed are all 'Completo.' (Completed).

Nro.	Fecha fin	Tipo	Nombre trabajo	Usuario	Resultado
<a href="#">129903</a>	09/26 13:11		<a href="#">doc129903201409_26131122</a>		Completo.
<a href="#">129902</a>	09/26 13:02		<a href="#">BCO RESP CNBV O_260914_130049</a>	fernando.garcia leon	Completo.
<a href="#">129901</a>	09/26 13:02		<a href="#">doc129901201409_26130204</a>		Completo.
<a href="#">129900</a>	09/26 13:02		<a href="#">Microsoft Office_260914_130008</a>	elena.garrido	Completo.
<a href="#">129899</a>	09/26 13:01		<a href="#">BCO RESP CNBV O_260914_125935</a>	fernando.garcia leon	Completo.
<a href="#">129898</a>	09/26 13:01		<a href="#">BCO ASEG 25 SEP_260914_125906</a>	veronica.falcon	Completo.
<a href="#">129897</a>	09/26 12:56		<a href="#">BANCO ASEGURAMI_260914_125356</a>	veronica.falcon	Completo.
<a href="#">129896</a>	09/26 12:55		<a href="#">BCO RESP CNBV O_260914_125314</a>	fernando.garcia leon	Completo.



# ERRORES OPERATIVOS?

- Quien los corrige?
- Queda una bitácora?





# USO DE OTROS ESTÁNDARES

- Si pero, bajarlas al nivel de la operación de la empresa!

- PCI **no está diseñado** para frenar intrusiones
- El cumplimiento PCI **no está diseñado** para llevarlos por encima de la línea de pobreza de la seguridad
- PCI **está diseñado** para ser asequible y realizable

Una protección adecuada requiere más

# MAPA DE LOS 20 CONTROLES CRÍTICOS

- **1: Inventory of Authorized and Unauthorized Devices (Laptops)**
- **2: Inventory of Authorized and Unauthorized Software (Back doors)**
- 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- 4: Continuous Vulnerability Assessment and Remediation
- 5: Malware Defenses
- 6: Application Software Security
- 7: Wireless Access Control
- 8: Data Recovery Capability
- 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- 11: Limitation and Control of Network Ports, Protocols, and Services
- 12: Controlled Use of Administrative Privileges
- 13: Boundary Defense
- **14: Maintenance, Monitoring, and Analysis of Audit Logs**
- 15: Controlled Access Based on the Need to Know
- 16: Account Monitoring and Control
- **17: Data Protection**
- 18: Incident Response and Management
- 19: Secure Network Engineering
- 20: Penetration Tests and Red Team Exercises

Fuente : SANS

# FORENSIA DIGITAL

- Aún y con todo ello, se siguen presentando fraudes! Si..



- Por lo que es importante conocer:
- Técnicas de revisión
- Herramientas de análisis
- Crear Comité Especial

# FTK IMAGER

AccessData FTK Imager 3.1.0.1514

File View Mode Help

Evidence Tree


- Game Explorer
- History
- Ringtones
- SchCache
- Temporary Internet Files
  - Content.IE5
    - 08Z0KEWE
    - 2Z6H46T0
    - 825PNP60
    - CL8SH9BM
    - D59UVQQG
    - EARE500M
    - H0MHRC0I
    - IU02MA2C
    - JFBLMYF7
    - TN6HHH8Y
    - U6SP87BS
    - Z64CCVVD

File List

Name	Size	Type	Date Modified
1036240[1].jpg	25	Regular File	05/09/2014 02:...
1036262[1].jpg	21	Regular File	05/09/2014 07:...
1036306[1].jpg	96	Regular File	05/09/2014 07:...
1036307[1].jpg	120	Regular File	05/09/2014 07:...
1036341[1].jpg	25	Regular File	05/09/2014 07:...
1036354[1].jpg	40	Regular File	05/09/2014 07:...
1036401[1].jpg	16	Regular File	05/09/2014 07:...
1036454[1].jpg	16	Regular File	05/09/2014 07:...
1036783[1].jpg	10	Regular File	08/09/2014 11:...
1036798[1].jpg	18	Regular File	08/09/2014 11:...
1037222[1].ico	12	Regular File	08/09/2014 10:...

Custom Content Sources

Evidence:File System|Path|File Options



New Edit Remove Remove All Create Image

Properties Hex Value Interpreter Custom Content Sources

C:\NONAME [NTFS]\[root]\Users\alejandro.rodriguez\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Z64CCVVD\1036307[1].jpg

ES 07:43 p.m. 11/09/2014

# ARCHIVOS BORRADOS

The screenshot shows the AccessData FTK Imager 3.1.0.1514 interface. The 'Evidence Tree' on the left shows a file system structure with folders like 'Media', 'data', and 'emoji'. The 'File List' on the right displays a table of files, with '\$B8GG1EG.docx' selected. The preview pane below the file list shows the content of the selected file, which is a document titled 'CONTRATO POR SERVICIO DE CONSERJERIA SF.docx'.

Name	Size	Type	Date Modified
\$ISOCM9U.zip	1	Regular File	20/04/2015 09:...
\$IOWJ2K5.pdf	1	Regular File	20/04/2015 09:...
\$ITR8JGP.pdf	1	Regular File	20/04/2015 09:...
\$IFC19T8.pdf	1	Regular File	20/04/2015 09:...
\$ILU82F8.pdf	1	Regular File	20/04/2015 09:...
\$IH6GNXZ.pdf	1	Regular File	20/04/2015 09:...
\$IBKJVS6.pdf	1	Regular File	20/04/2015 09:...
\$ITQLQ0S.pdf	1	Regular File	20/04/2015 09:...
\$IOEJ29T.pdf	1	Regular File	20/04/2015 09:...
\$B8GG1EG.docx	1	Regular File	20/04/2015 09:...
\$IGRJRFZ.zip	1	Regular File	20/04/2015 09:...

GH'8™.\*{BC:\Users\alejandro.rodriguez\Downloads\CONTRATO POR SERVICIO DE CONSERJERIA SF.docx



# KERNEL OST/PST

Kernel for Outlook PST Repair - Evaluation Version

File View Find Help

Repair Save Save Snapshot Load Snapshot Find Help Buy Now

**KERNEL**  
for Outlook PST Repair

Folder List

- Bandeja Septie...
- 2010
  - Bandeja Abril 11
  - Bandeja Agosto
  - Bandeja Diciem
  - Bandeja Enero
  - Bandeja Febren
  - Bandeja Julio 11
  - Bandeja Junio 1
  - Bandeja Marzo
  - Bandeja Mayo 1
  - Bandeja Novier
  - Bandeja Octubr
  - Bandeja Septie...
- Abi y Omar 09-10
- Calidad
  - Calidad Prosa
  - Monitoreo
- Calidad Prosa
- Cambios en TDD
- Comprobación de c
- Contraste Auditori
- Elementos eliminad
- Enviados 09 y 10
- Mau
- Mesa de Trabajo CF
- RH 2011
- Riesgos 09-10

Enviados 09 y 10 (2780)

From	Subject	Date/Time	Lost/Deleted
<FILTER>	<FILTER>	<FILTER>	<FILTER>
Maribel Alegria	Traspos de Operadora	Wed 12/29/2010 16:31 PM	
Maribel Alegria	RE: Activación de Chequera	Wed 12/29/2010 16:44 PM	
Maribel Alegria	RE: TRASPASO OPERADORA SUC ...	Wed 12/29/2010 16:52 PM	
Maribel Alegria	RE: Solicitud de SPEI	Wed 12/29/2010 17:52 PM	
Maribel Alegria	PANTALLAS	Wed 12/29/2010 18:18 PM	
Maribel Alegria	RE: PANTALLAS	Wed 12/29/2010 18:21 PM	
Maribel Alegria	Enviando por correo electrónico: Form...	Mon 04/05/2010 16:52 PM	Lost/Deleted
Maribel Alegria	RE: DOM - Clientes Prueba Dom	Mon 12/27/2010 12:36 PM	Lost/Deleted
Maribel Alegria	Asignación de TDD	Fri 04/30/2010 16:14 PM	Lost/Deleted
Maribel Alegria	Monitoreo de Correos y Fax enviados	Mon 07/20/2009 12:17 PM	Lost/Deleted
Maribel Alegria	calendario de cursos AGOSTO.xls	Tue 07/28/2009 11:10 AM	Lost/Deleted
Maribel Alegria	Solicitud de Comprobación de envío ...	Wed 07/29/2009 12:46 PM	Lost/Deleted
Maribel Alegria	Monitoreo de correos y fax enviados	Wed 08/05/2009 11:40 AM	Lost/Deleted

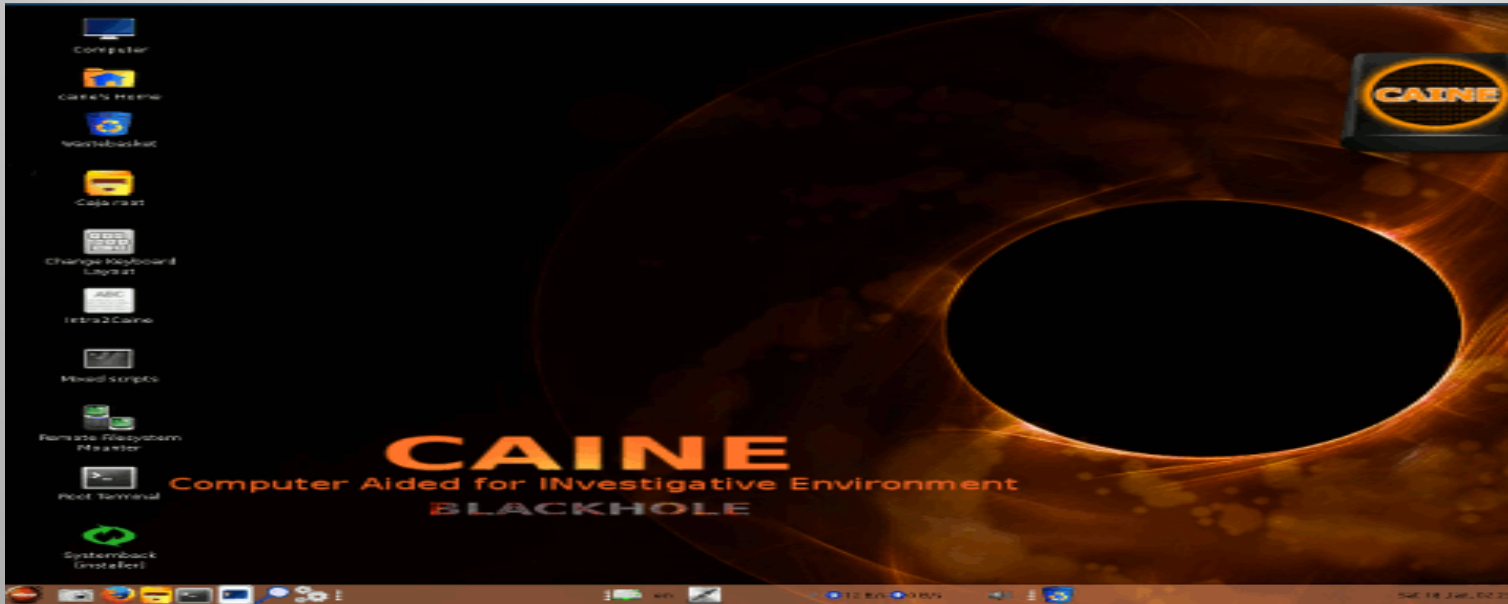
**Enviando por correo electrónico: Formato de aclaraciones CUATLI**  
 Maribel Alegria  
 To: servicioclientes  
 Attachments: Formato de aclaraciones CUATLI.doc  
 Mon 04/05/2010 16:52 PM

Vane no se si recuerdes que te dije que había tomado el sábado una aclaración te paso los datos para que te pongas por favor en contacto con el Cliente muchas Gracias

ES 07:54 p.m. 11/09/2014



# CAINE



NirLauncher - NirSoft Utilities

File Edit View Options Launcher Packages Help

Outlook/Office Utilities	Programmer Tools	Disk Utilities	System Utilities	Web Page URL	EXE Filename	GUI/Cor
WebCookiesSniffer	Captures Web site cookies and displays them in a ...	Version	Updated On	http://www.nirsoft.net/utis/web_cookies_sniffer...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
URLStringGrabber	Grab URL strings of Web sites from Internet Explor...	1.15	26/08/2014 01:31:14 p.m.	http://www.nirsoft.net/utis/url_string_grabber.ht...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
SafariHistoryView	History viewer for Safari Web browser	1.01	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/safari_history_view.h...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
SafariCacheView	Cache viewer/extractor for Safari Web browser	1.11	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/safari_cache_view.ht...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
OperaCacheView	Cache viewer for Opera Web browser.	1.40	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/opera_cache_view.ht...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
MyLastSearch	View your latest searches with Google, Yahoo, an...	1.58	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/my_last_search.html	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
MozillaCookiesView	alternative to the standard 'Cookie Manager' prov...	1.40	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/mzcv.html	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
MozillaCacheView	List all files currently stored in the cache of Firefo...	1.57	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/mozilla_cache_view...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
MozillaHistoryView	Displays the list of visited Web sites in Firefox Vie...	1.50	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/mozilla_history_view...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
IECookiesView	Displays the cookies that Internet Explorer stores ...	1.74	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/iecookies.html	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
IEHistoryView	Displays the list of Web sites that you visited with ...	1.70	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/iehv.html	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
IECacheView	List all files currently stored in the cache of Intern...	1.46	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/ie_cache_viewer.html	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
FlashCookiesView	View Flash cookies stored in your computer.	1.12	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/flash_cookies_view.h...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
FirefoxDownloadsView	Displayed the list of downloaded files in Firefox	1.33	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/firefox_downloads_v...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
FavoritesView	displays the list of all your Favorites/bookmarks l...	1.31	26/08/2014 01:31:13 p.m.	http://www.nirsoft.net/utis/faview.html	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
ChromeHistoryView	View the browsing history of Chrome Web browser	1.16	26/08/2014 01:31:12 p.m.	http://www.nirsoft.net/utis/chrome_history_vie...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
ChromeCacheView	Chrome Browser Cache Viewer	1.46	26/08/2014 01:31:12 p.m.	http://www.nirsoft.net/utis/chrome_cache_view...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
ChromeCookiesView	Alternative to the standard internal cookies view...	1.02	26/08/2014 01:31:12 p.m.	http://www.nirsoft.net/utis/chrome_cookies_vie...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App
BrowsingHistoryView	View browsing history of popular Web browsers	1.25	26/08/2014 01:31:12 p.m.	http://www.nirsoft.net/utis/browsing_history_vl...	C:\Users\alejandro.rodriguez\Documents\SANS\Nirsott ...	GUI App

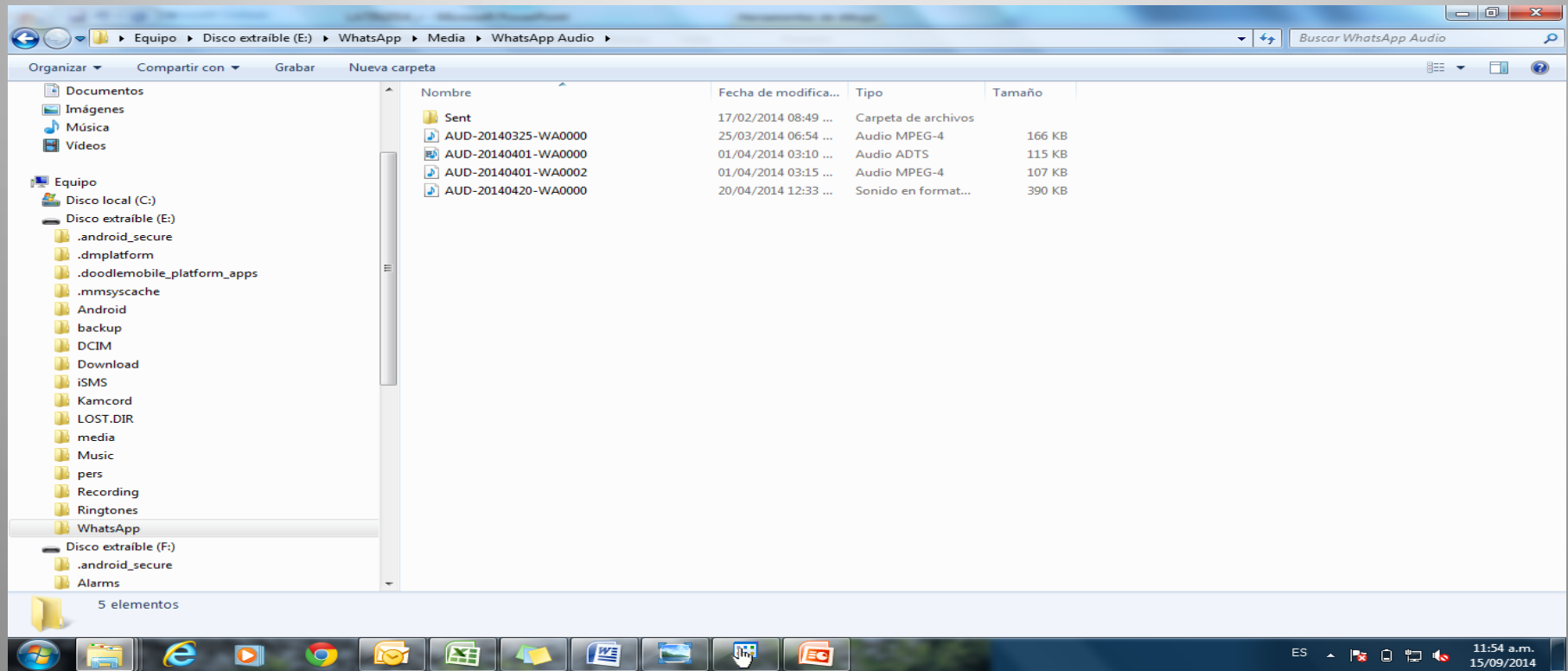
Run Advanced Run Web Page Help File Web Search Package Package

19 Utilities, 1 Selected NirSoft Freeware. http://www.nirsoft.net

ES 11:51 a.m. 15/09/2014

# OTRAS HERRAMIENTAS PARA MÓVILES

- Cellebrite
- Katana
- ISO 27037:2012



# ENCUESTA

- **Estamos listos para las nuevas tecnologías Móviles?**
- **Si, por que..**
- **Estoy capacitándome constantemente**
- **Conozco el entorno tecnológico puesto que Sistemas me invita a sus Comités de Sistemas**

# ENCUESTA...

- Participo en el momento de ver la seguridad y riesgos de un proyecto tecnológico.
- Tenemos instalado algún sistema de Monitoreo? Sin ser responsables, claro ej. WebSense

## CONCLUSIONES FINALES

- Entender siempre el entorno de Negocio, operativo y Tecnológico
- Revisiones integrales Diversifiquen el conocimiento (forensia, etc.)
- Uso de normas/ estándares locales
- No guardar información sensible ya utilizada

# CONTACTO

**Alejandro Rodríguez M.**



**@alexrdz41**



**alejandro.rodriguez@multiva.com.mx**  
**educacion.isaca@gmail.com**



¡Muchas Gracias  
por su atención!