Banca Electrónica Móvil

Alejandro Rodríguez Moreno

Subdirector de Auditoría Interna
Grupo Financiero Multiva

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS
50 años
1965 - 2015

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

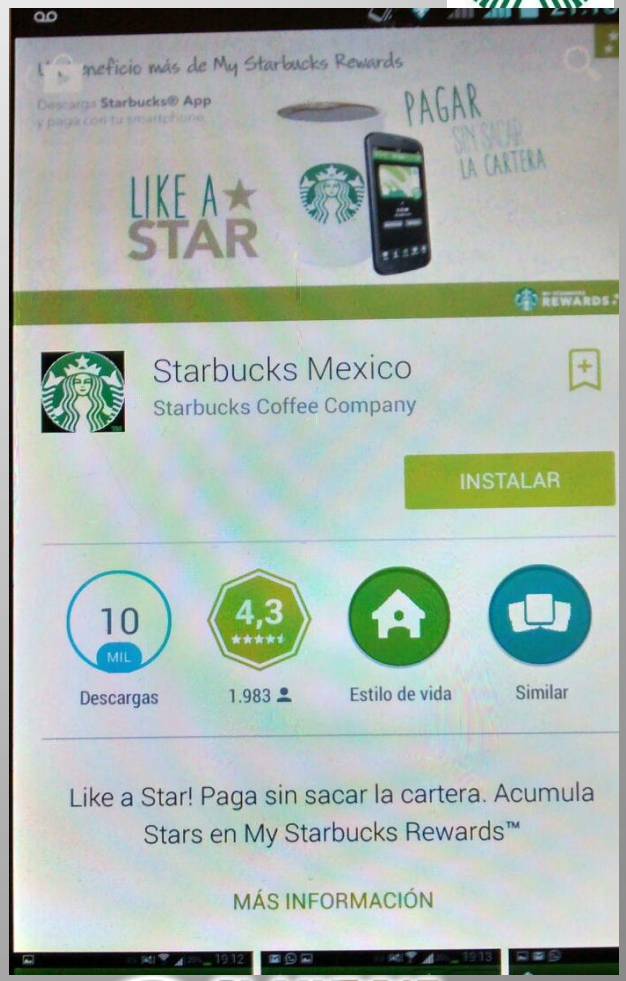
- ENTENDIMIENTO DE LA BANCA ELECTRÓNICA MÓVIL
- ASPECTOS DE SEGURIDAD
- ENFOQUE DEL AUDITOR DE TI
- FORENSIA DIGITAL

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 loyalti
- …

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

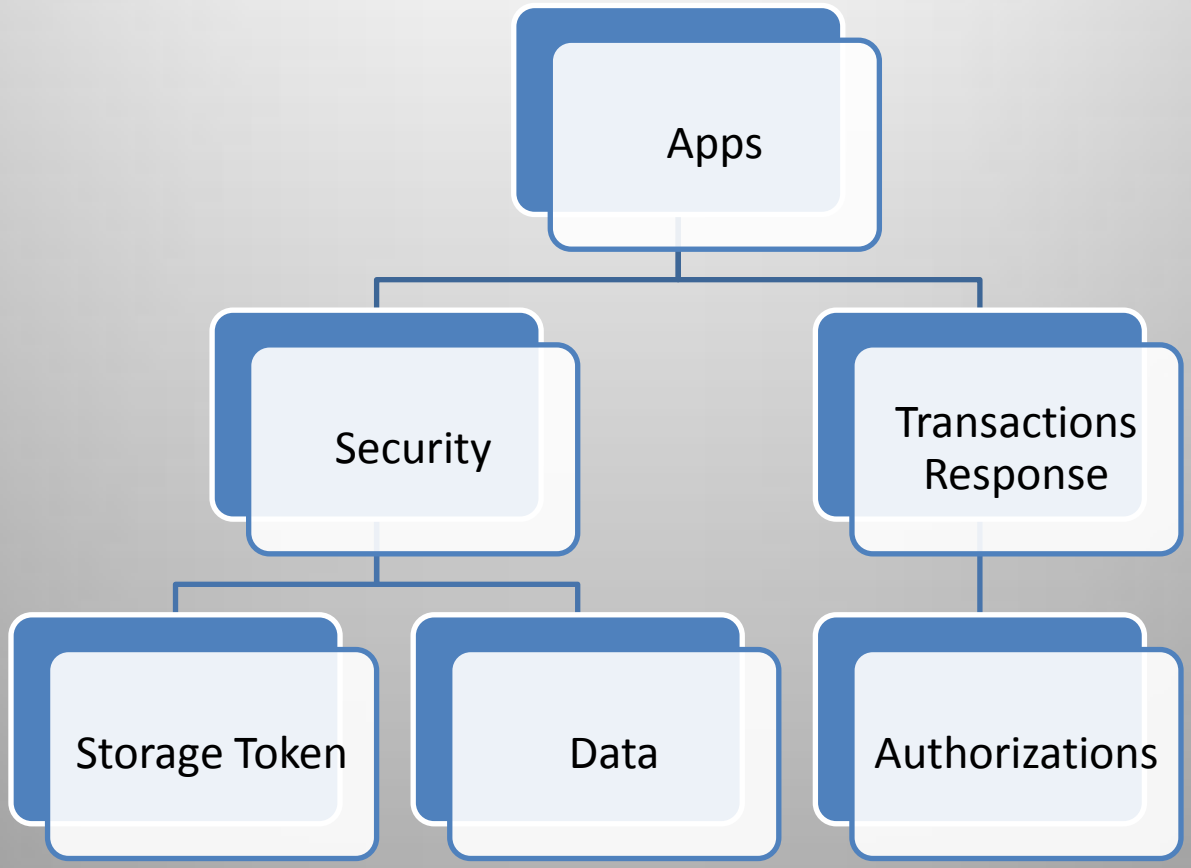
Feature Phones &

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 Applicaction
- 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)

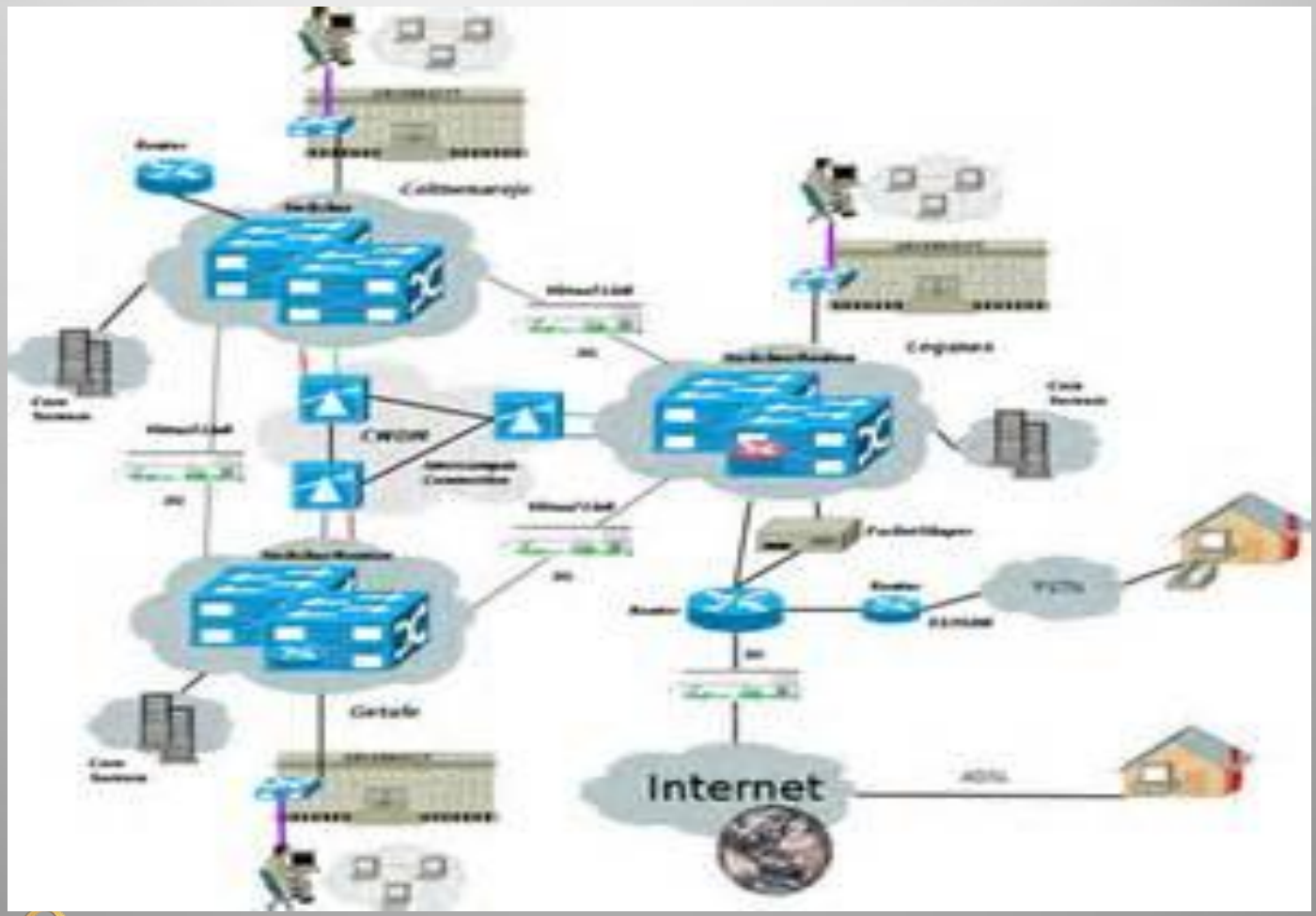
PARTICIPANTES EN UN PROYECTO DE BANCA ELECTRÓNICA Y CUMPLIMIENTO NORMATIVO

- **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…

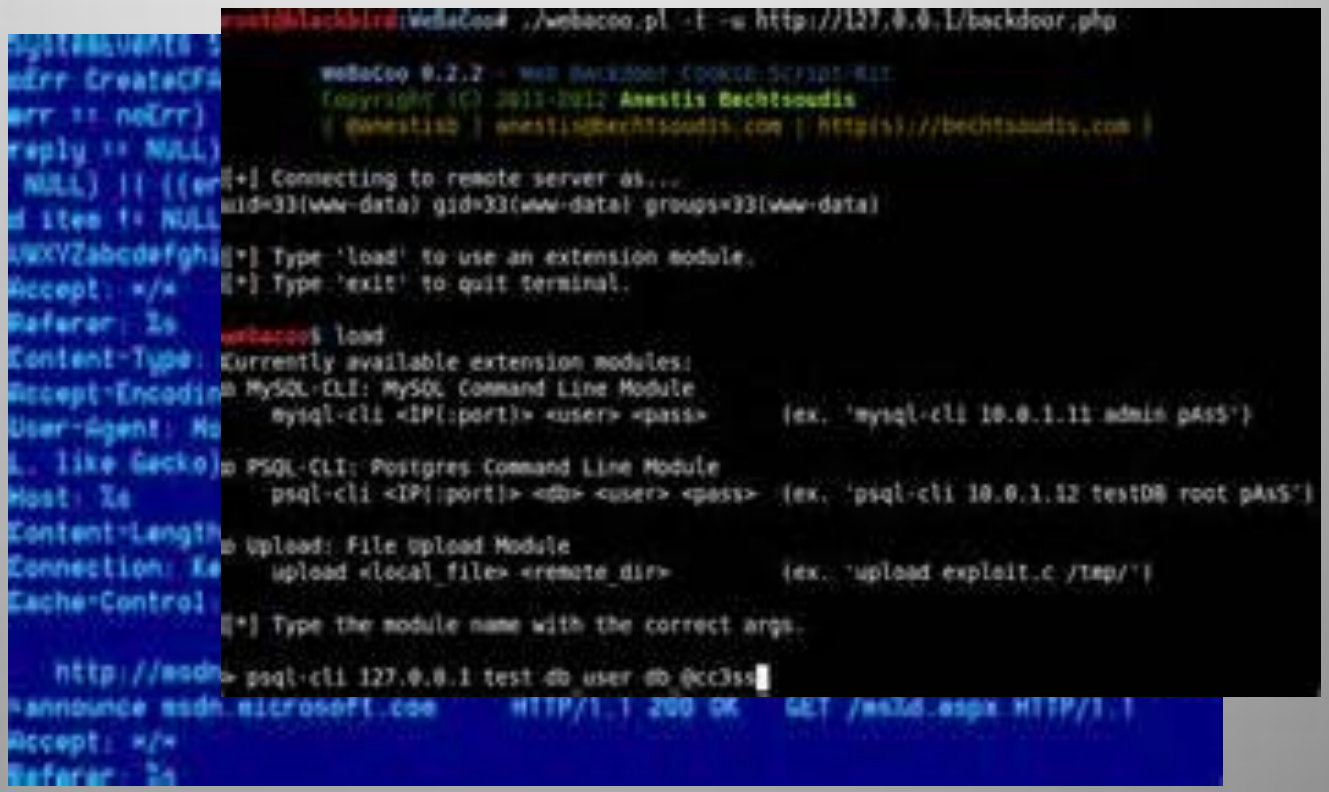
ANTES DE ESO…

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

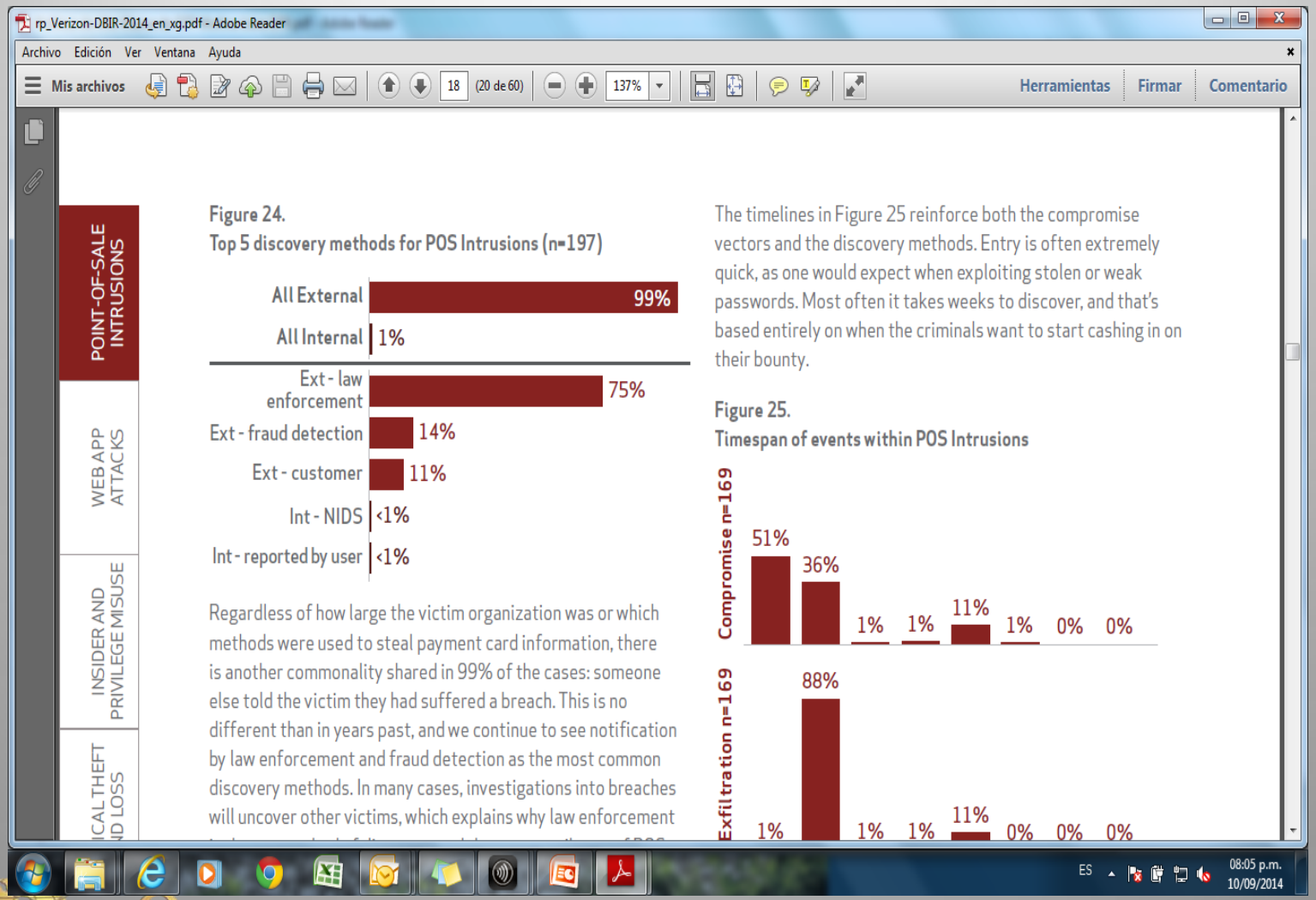
Enfocarse en temas como:

BACKDOOR EN VALIDACIÓN DE TOKENS -SEMILLAS

- IF .. Else..



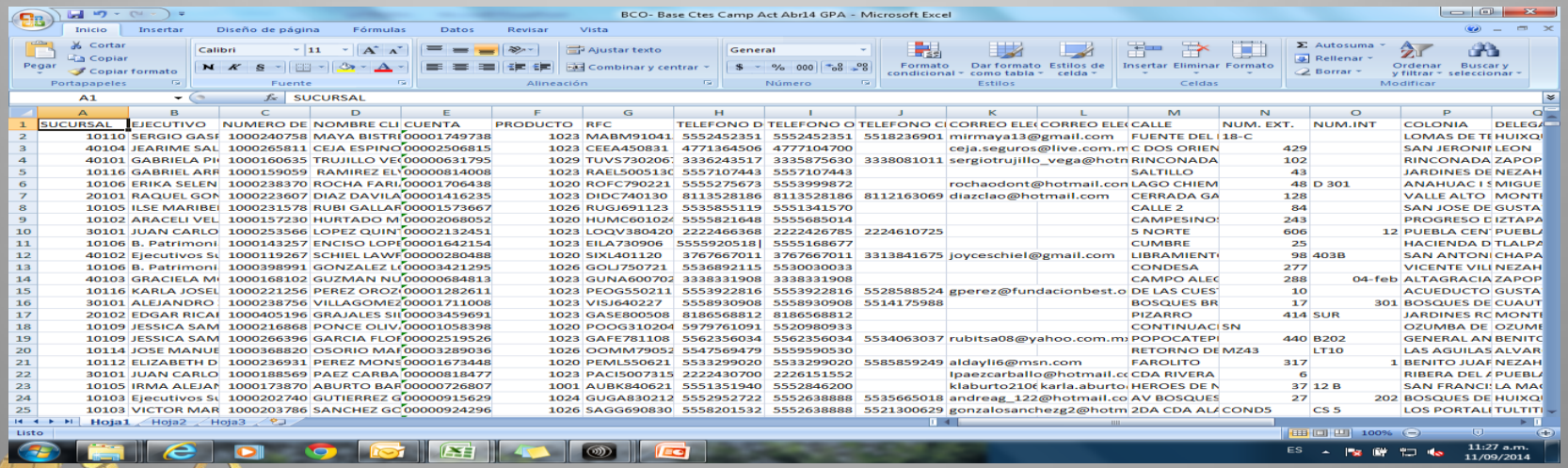
DISPOSITIVOS SENSIBLES, EJ. TPV´S



Fuente Verizon

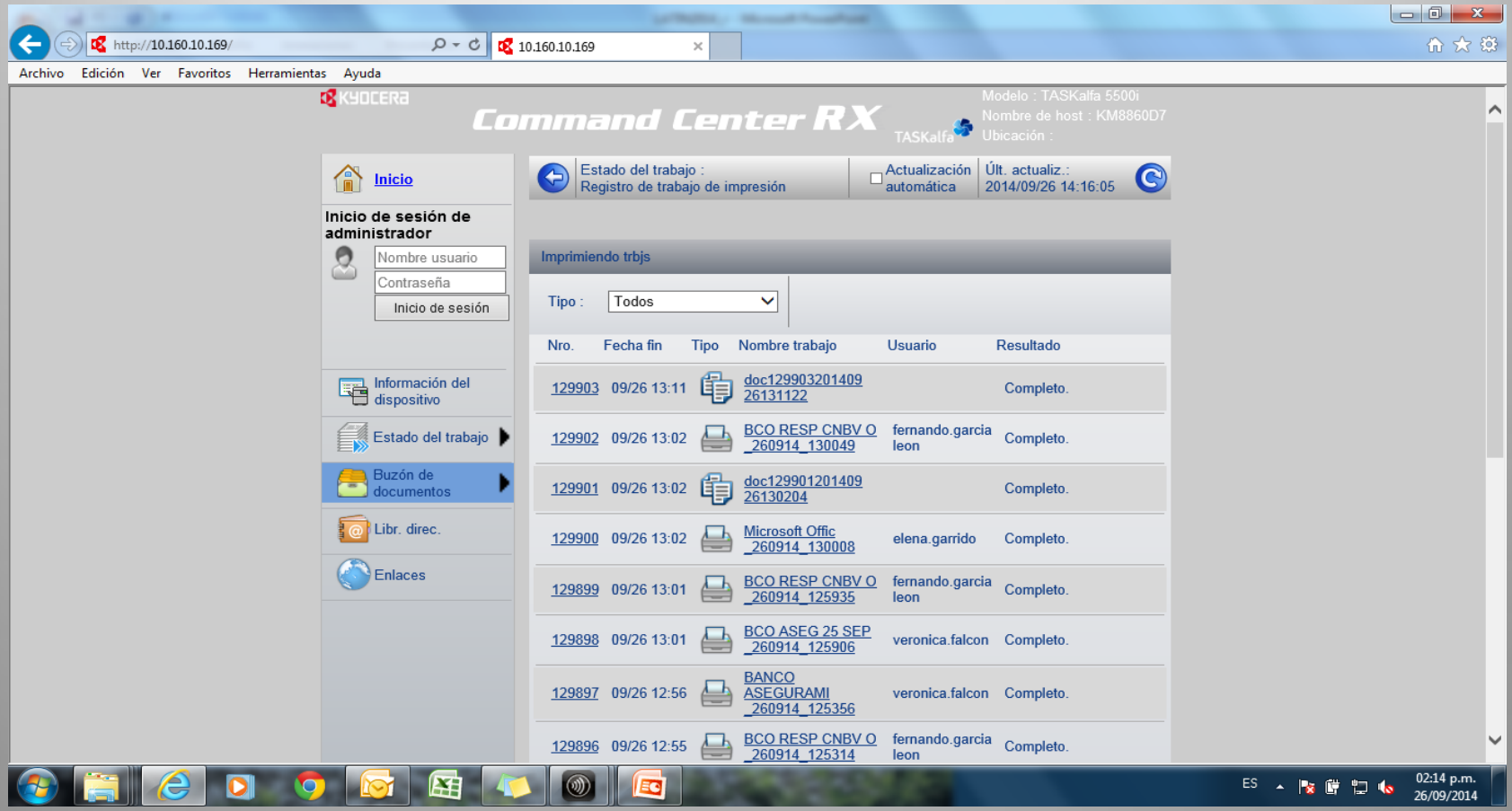
DISCOS DUROS

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



IMPRESORAS

– Que guardan?

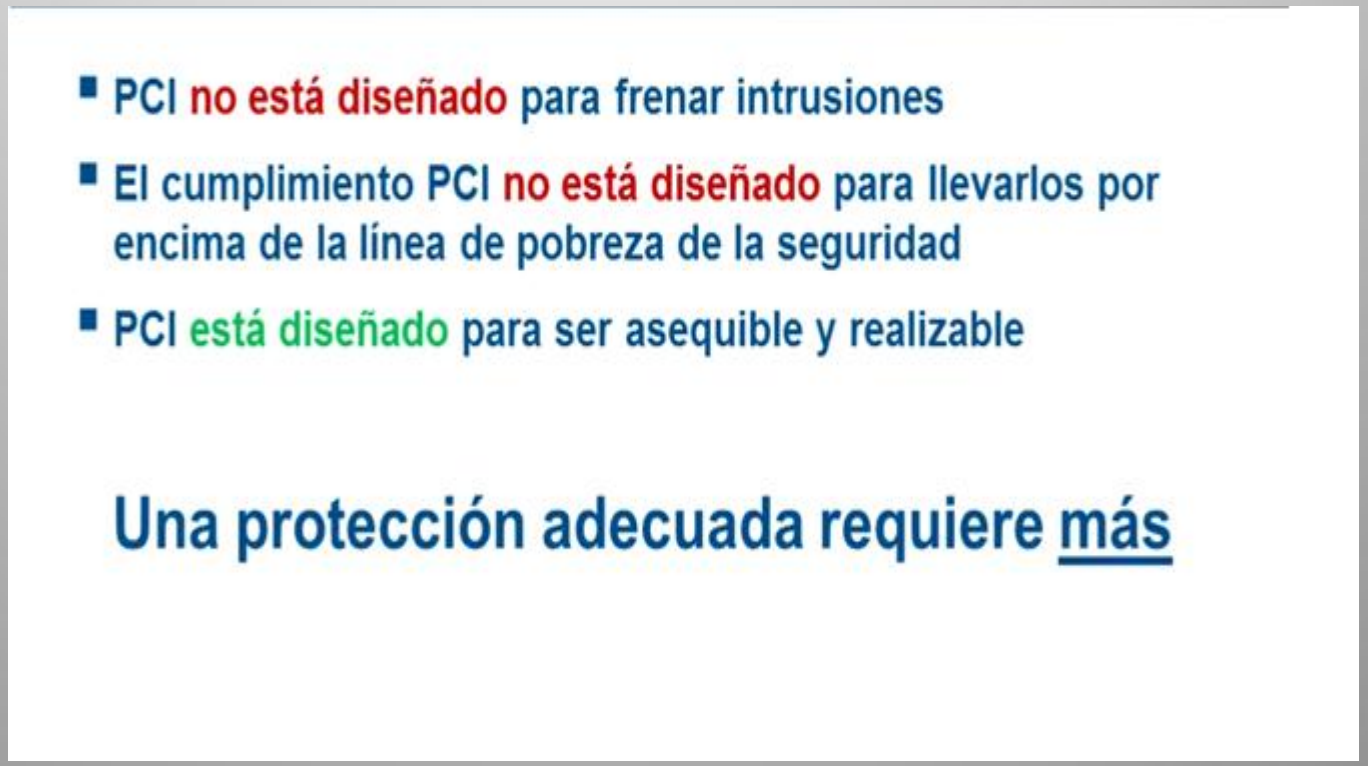


ERRORES OPERATIVOS?

- Quien los corrige?
- Queda una bitácora?

USO DE OTROS ESTÁNDARES

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



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

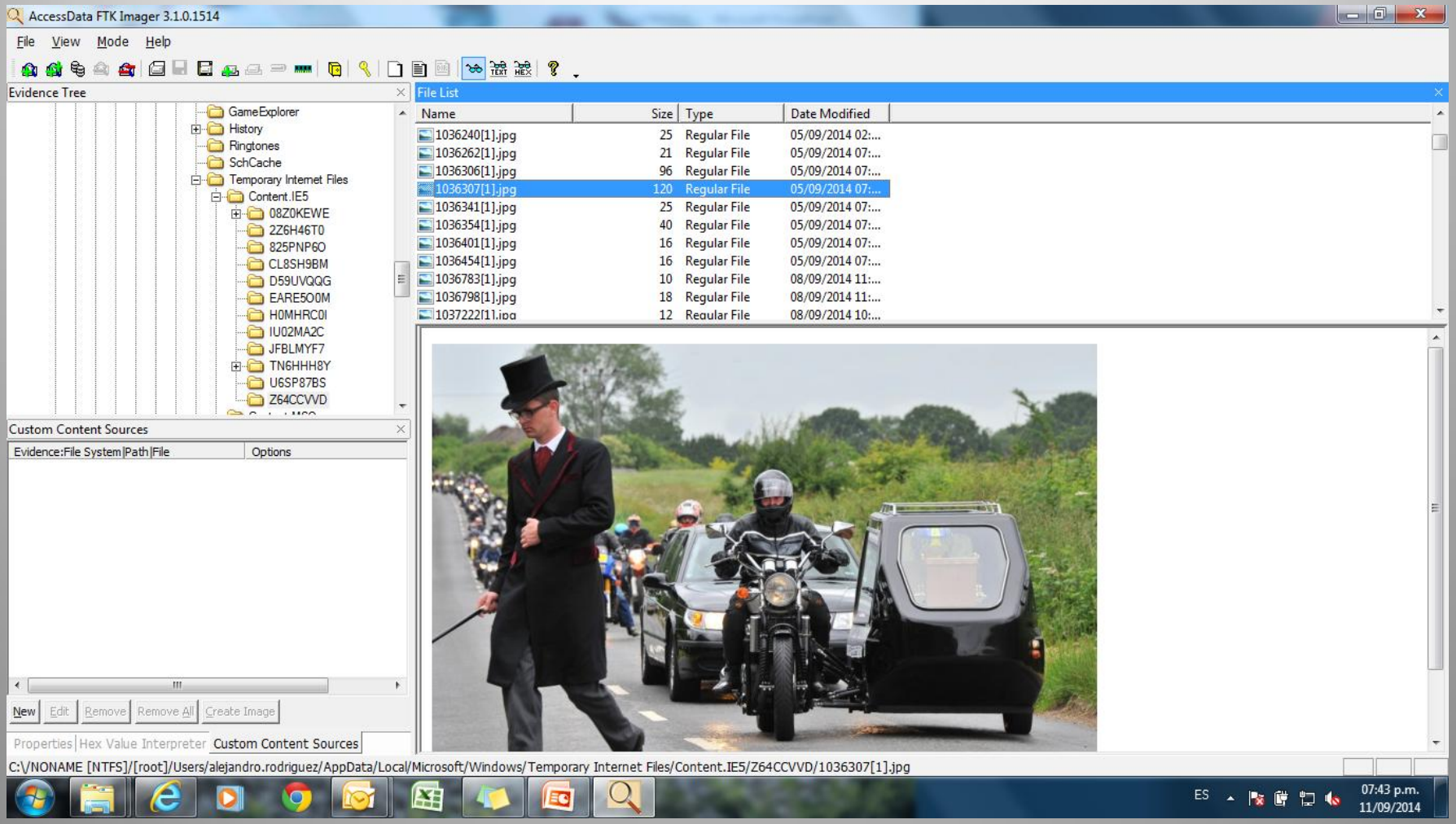
Fuente : SANS

FORENSIA DIGITAL

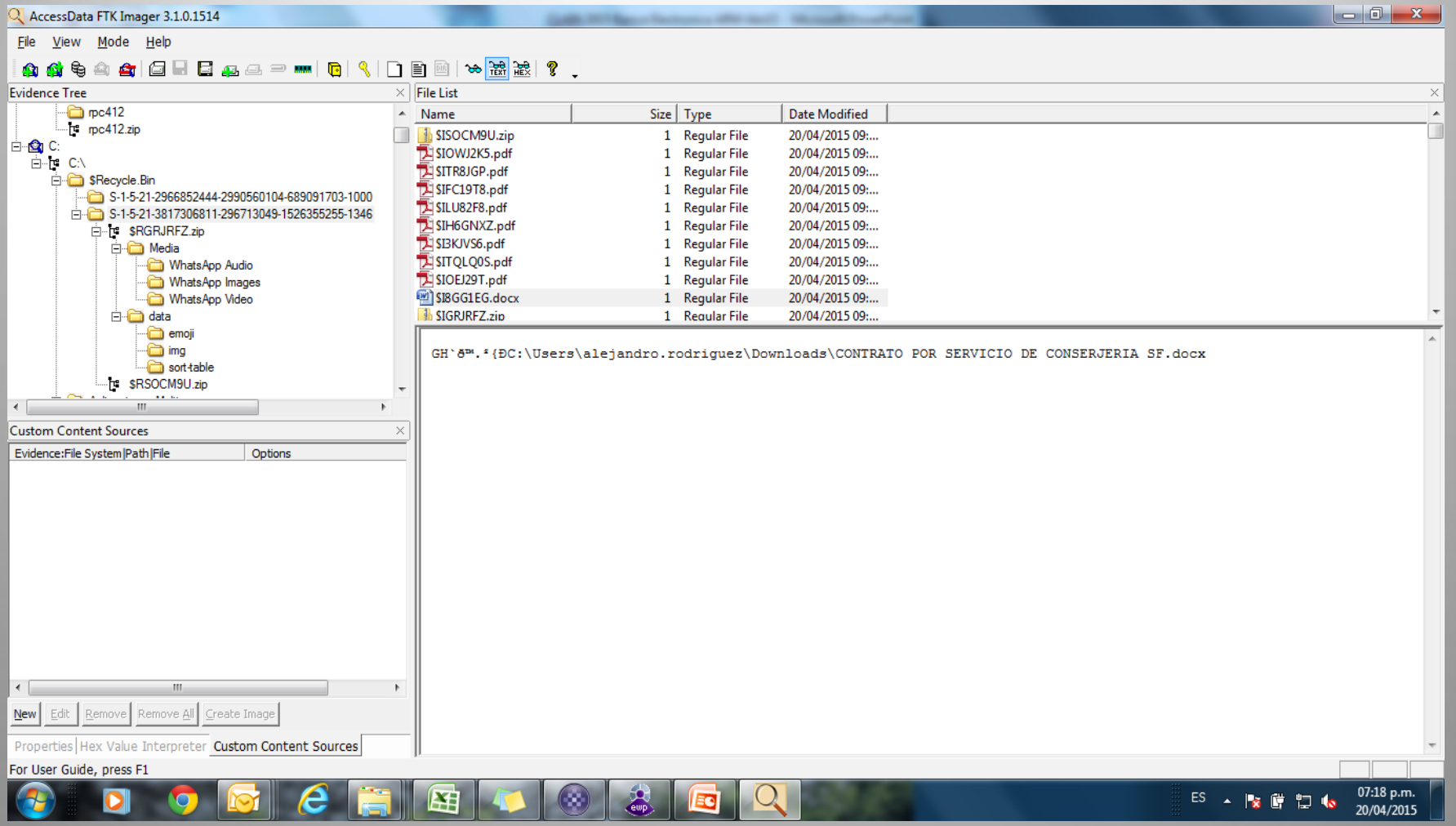
- Aún y con todo ello, se siguen presentando fraudes! SI..

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

FTK IMAGER



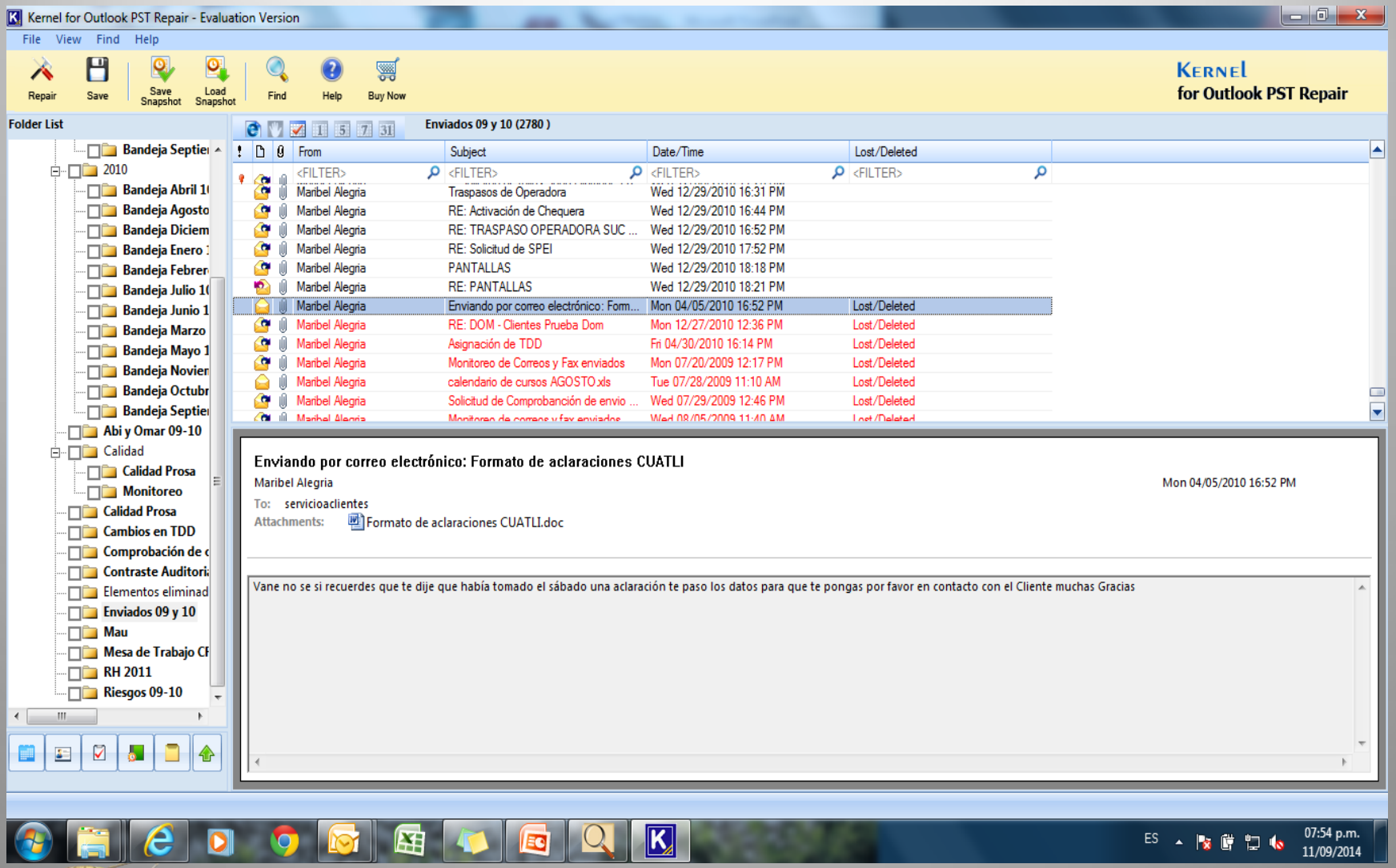
ARCHIVOS BORRADOS



FELABAN 50 años 1965 - 2015
FEDERACION LATINOAMERICANA DE BANCOS

CLAIN2015
XIX CONGRESO LATINOAMERICANO DE AUDITORIA INTERNA Y EVALUACIÓN DE RIESGOS

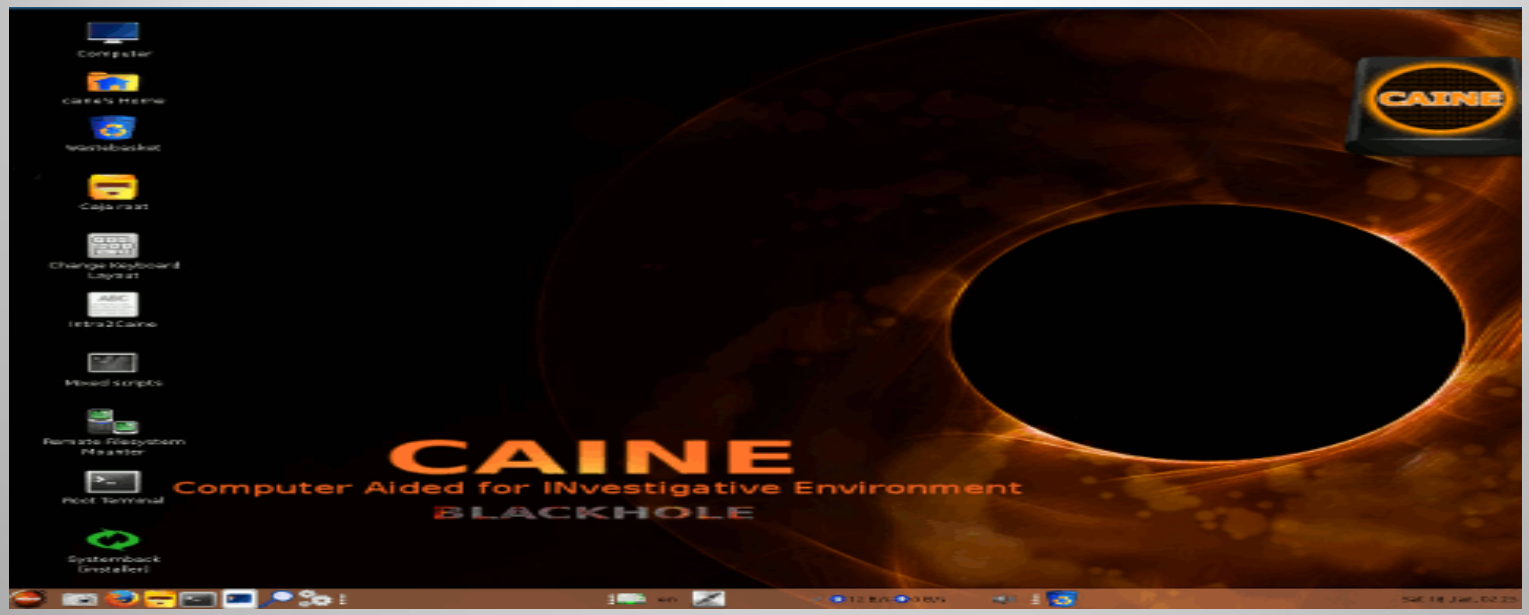
KERNEL OST/PST

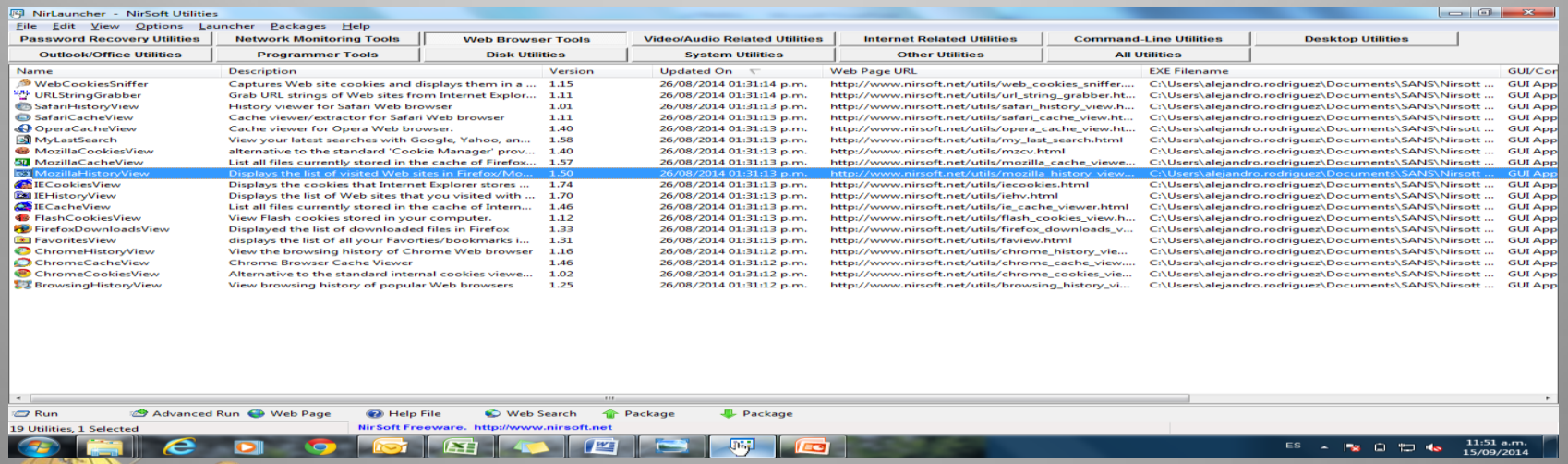


FELABAN 50 años 1965 - 2015

CLAIN2015 XIX CONGRESO LATINOAMERICANO DE AUDITORIA INTERNA Y EVALUACIÓN DE RIESGOS

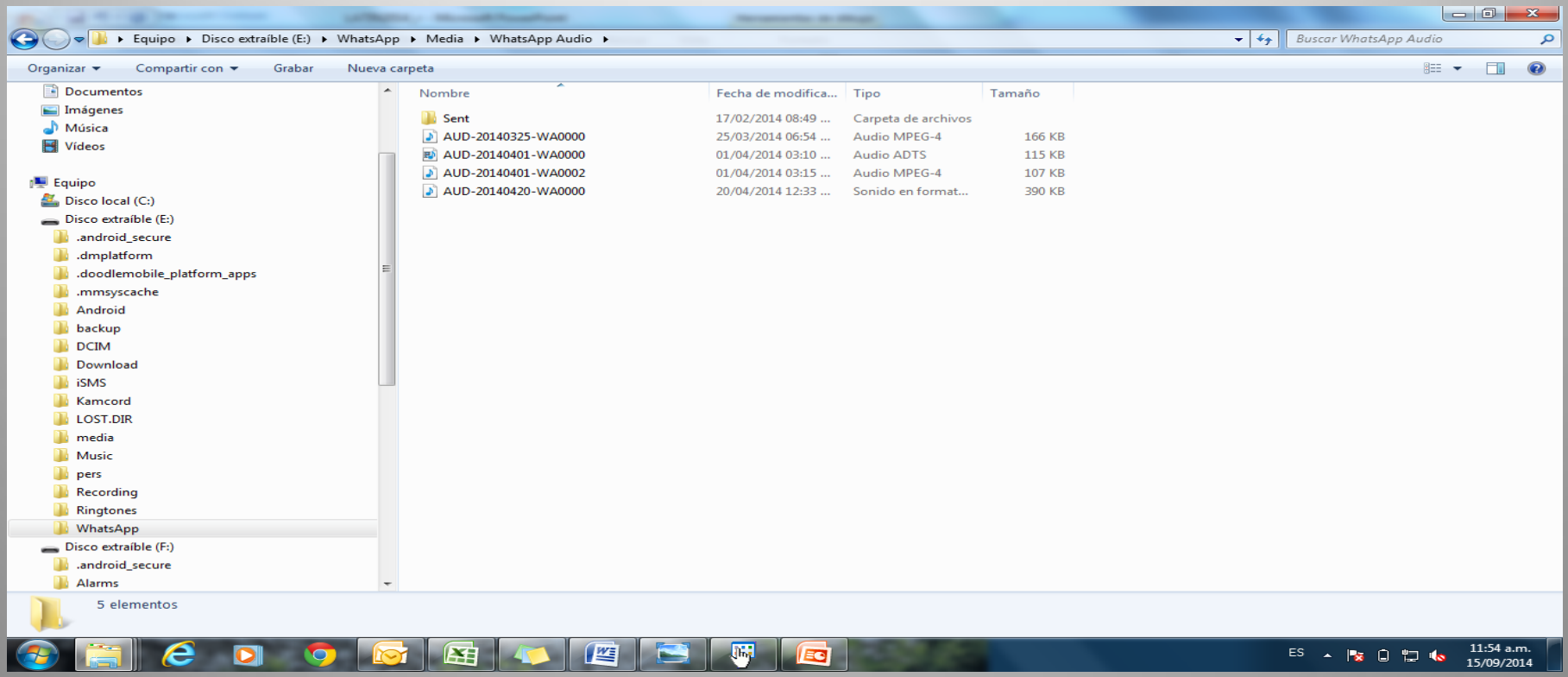
CAINE





OTRAS HERRAMIENTAS PARA MÓVILES

- **Cellebrite**
- **Katana**
- **ISO 27037:2012**



FELABAN 50 años 1965 - 2015
FEDERACION LATINOAMERICANA DE BANCOS

CLAIN2015
XIX CONGRESO LATINOAMERICANO DE AUDITORIA INTERNA Y EVALUACIÓN DE RIESGOS

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

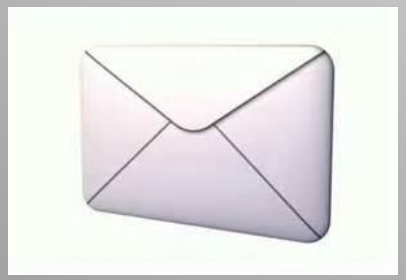
CONCLUSIONES FINALES

- 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!