Seguridad Integral de la Información.

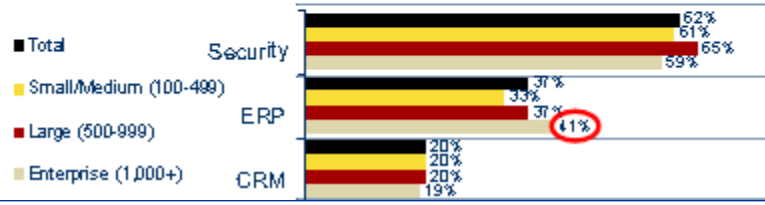
Telefónica del Perú
VP Empresas
Fecha: Marzo de 2010

Cesar.farro@t-empersas.com.pe
BSI Lead Auditor, GIAC GSNA y GFWA - SANS Local Mentor Program
Product Manager de Seguridad TI

0 El Mercado de la Seguridad:

Needs and Opportunities

QUESTION: Of the following IT solutions, please specify what type of IT Investments your organization will make within the next 12 months.



	1st Investment Area	2nd Investment Area	3rd Investment Area
Security	Antivirus	Antispam	Firewall / VPN
ERP	Finance / Accounting	Procurement	Purchase / Stock Management
CRM	Contact center / Customer Service	Marketing	CRM Analytics

Fuente: IDC, Latin America IT Spending by Company Size special presentation for Telefonica
September 2nd 2009

Needs and Opportunities

Latin America All Markets:
1) Security
2) ERP
3) CRM

ARGENTINA:
1) Security
2) ERP
3) Collaborative App.

COLOMBIA:
1) Security
2) ERP
3) Mobile Enterpise Sol.

VENEZUELA:
1) Security
2) ERP
3) BI

BRAZIL:
1) Security
2) ERP
3) Virtualization

MEXICO:
1) Security
2) ERP
3) Collaborative applications

CHILE:
1) Security
2) ERP
3) Mobile Enterpise Sol.

PERU:
1) Security
2) ERP
3) BI

Needs and Opportunities

Latin America All Markets:
1) Security
2) ERP
3) CRM

FINANCE(*):
1) Security
2) Collaborative App.
3) Virtualization

COMMERCE:
1) Security
2) ERP
3) Collaborative App.

MANUFACTURING:
1) Security
2) ERP
3) BI

TELECOM(*):
1) Security
2) CRM
3) ERP

RESOURCES(*):
1) Security
2) ERP
3) Supply Chain

PUBLIC SECTOR(*):
1) Security
2) ERP
3) Virtualization

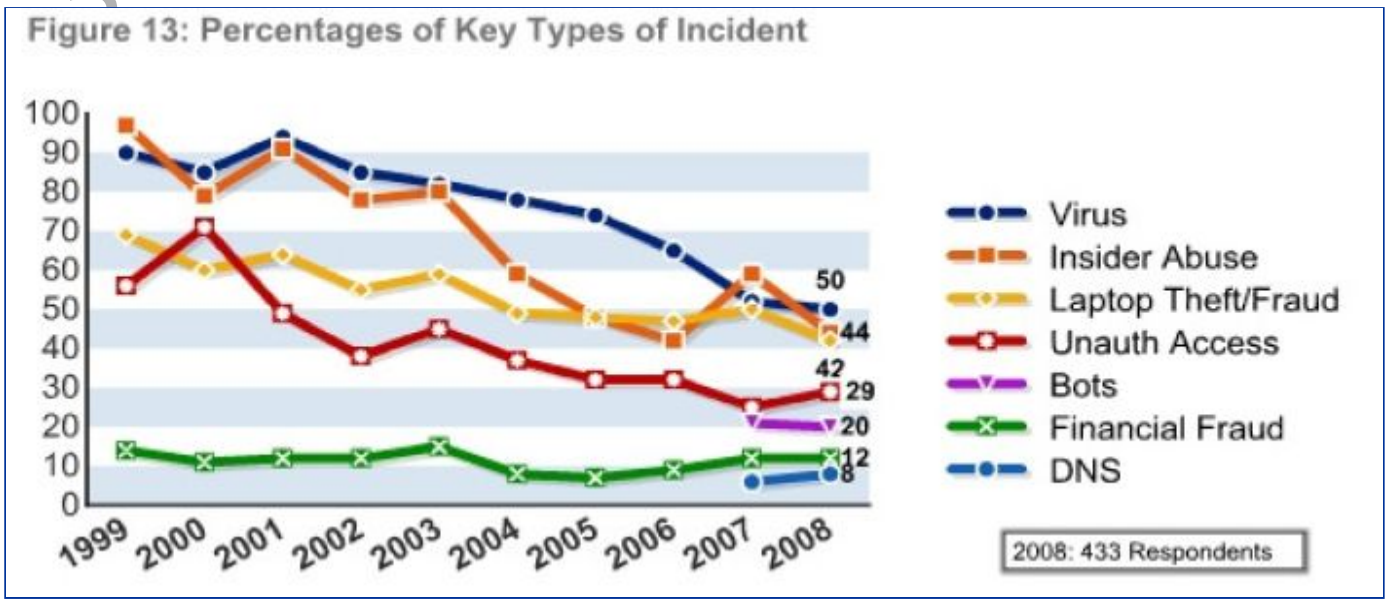
SERVICES:
1) Security
2) ERP
3) CRM

Requerimientos Legales en Latin America:

IDC Analyze the Future

Fuente: IDC, Latin America IT Spending by Company Size Special presentation for Telefonica September 2nd 2009

Estadísticas en Incidencias de Seguridad



Latest Threats

1	09-23-09 W32.Lafee
1	09-22-09 Trojan.Opachki
1	09-21-09 Trojan.Bredolab!gen
1	09-21-09 Trojan.Wampyr!inf
1	09-19-09 Infostealer.Bzup.B

More...

Latest IDS Signatures

Cisco IPS NEW	23Sep09	S437
Juniper IDP DI NEW	22Sep09	#1508
Sourcefire IPS NEW	21Sep09	SEU 265
Proventia	11Sep09	29.091
IntruShield	09Sep09	5.1.27.12
Symantec IPS	17Jun09	v108

The most expensive computer security incidents were those involving financial fraud…

…with an average reported cost of close to $500,000 (for those who experienced financial

Virus incidents occurred most frequently…

…occurring at almost half (49 percent) of the respondents' organizations.

Almost one in ten organizations reported they'd had a Domain Name System incident…

…up 2 percent from last year, and noteworthy, given the current focus on vulnerabilities in DNS.

Latest Tool Versions

Nmap NEW	17Sep09	5.0
Snort NEW	16Sep09	2.8.5
Nessus NEW	15Sep09	4.0.2
Wireshark NEW	15Sep09	1.2.2
Kismet	24Juny09	09-06R1
Cain & Abel	27May09	4.9.31
Metasploit	19Nov08	3.2

2008 CSI Computer Crime and Security Survey

Robo de datos y tarjetas de crédito:

Caso,Cadena de Tiendas TJX robo de Tarjetas de Créditos (Mayo 2007):

Un robo de los datos de 45,7 millones de tarjetas de crédito de los clientes

Clientes de las ocho cadenas con las que opera TJX en Estados Unidos, Puerto Rico, Canadá, el Reino Unido, Irlanda -en estos dos últimos países opera 210 tiendas- han sido afectados por el robo de hasta un centenar de archivos con la información y perpetrado por 'piratas' informáticos.

Caso, Manipulación de “SCADA” System (Sep

PACIFIC ENERGY

Un ex consultor de TI de una empresa de exploración de petróleo y gas se declaró culpable de la manipulación de los sistemas informáticos de la empresa los sistemas se utilizan para controlar a gran escala de los sistemas industriales en las plantas de fabricación, servicios públicos y la industria química,*

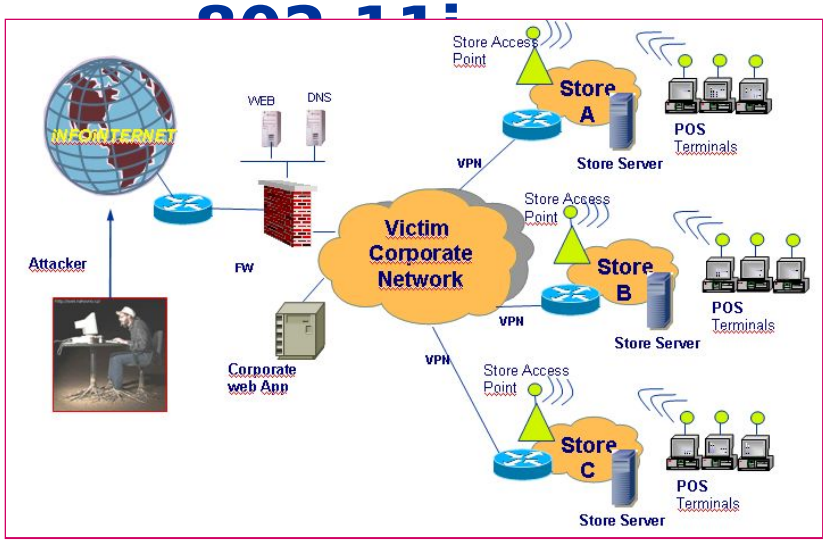
* Fuente: http://www.networkworld.com/news/2009/092309-contractor-pleads-guilty-to-scada.html

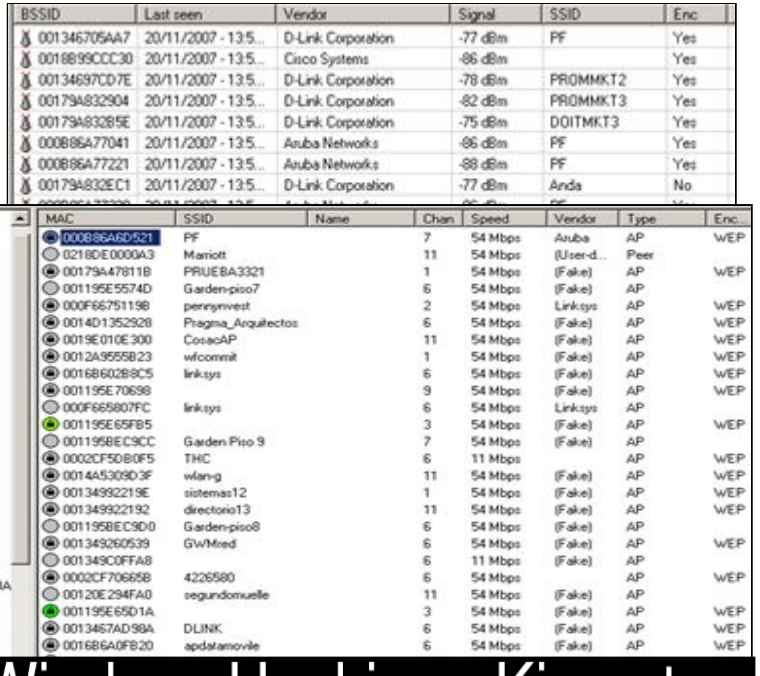
Caso,Transbank. Santiago de Chile (Sep 2007).

Clonó tarjetas y robó 160 millones

Una estafa por cerca de 160 millones de pesos y el robo de una base de datos de 19 mil 195 clientes bancarios imputan al ingeniero civil informático Javier Eduardo Cárdenas Foitzick (43).

0 Wireless LAN: 802.11 a/b/g y





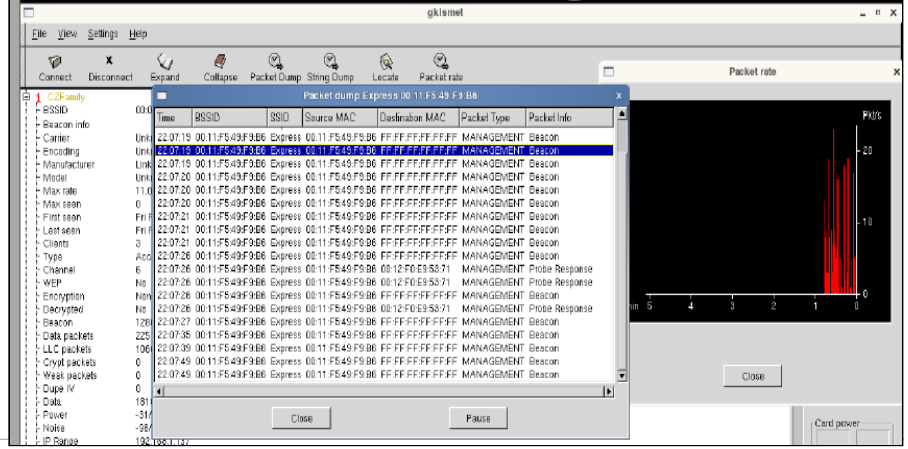
NIST National Institute of Standards and Technology
Information Technology Laboratory

Guide to Securing Legacy IEEE 802.11 Wireless Networks (SP800-48 Rev. 1 Jul 20

Table 3-1. Major Threats Against Network Security

Threat Category	Description
Denial of Service	Attacker prevents or limits the normal use or management of networks or network devices.
Eavesdropping	Attacker passively monitors network communications for data, including authentication credentials.
Man-in-the-Middle	Attacker actively impersonates multiple legitimate parties, such as appearing as a client to an AP and appearing as an AP to a client. Allows attacker to intercept communications between an AP and a client, thereby obtaining authentication credentials and data.
Masquerading	Attacker impersonates an authorized user and gains certain unauthorized privileges.
Message Modification	Attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
Message Replay	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
Misappropriation	Attacker steals or makes unauthorized use of a service.
Traffic Analysis	Attacker passively monitors transmissions to identify communication patterns and participants.

Wireless Hacking : Kismet



Recomendaciones del uso de

National Institute of Standards and Technology
Information Technology Laboratory

Guide to Securing Legacy IEEE 802.11 Wireless Networks (SP800-48 Rev. 1 Jul 2008)

Recommendations

should be implemented to provide the needed security. Because of the serious security flaws in the legacy IEEE 802.11 standard, NIST recommends that organizations with existing legacy IEEE 802.11 WLAN implementations develop and implement migration strategies to move to IEEE 802.11i, which offers better security.

Fuente:

PCI Payment Card Indus_v1-1.pdf
Version 1.2

PCI Security Standards Council

Requisitos de las DSS de la PCI	Procedimientos de prueba
4.1.1 Asegúrese de que las redes inalámbricas que transmiten datos de los titulares de las tarjetas o que están conectadas al entorno de datos del titular de la tarjeta utilizan las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) a los efectos de implementar cifrados sólidos para la autenticación y transmisión. ▪ *En el caso de nuevas implementaciones inalámbricas, se prohíbe la implementación WEP después del 31 de marzo de 2009.* ▪ *En el caso de actuales implementaciones inalámbricas, se prohíbe la implementación WEP después del 30 de junio de 2010.*	4.1.1 En el caso de redes inalámbricas que transmiten datos de los titulares de las tarjetas o que están conectadas al entorno de datos del titular de la tarjeta, controle que utilicen las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) a los efectos de implementar cifrados sólidos para la autenticación y transmisión.

de los tarjetahabientes,
ed Access (WPA o
mente del protocolo
ad y el acceso a una red
hacer lo siguiente:
104 bits y un valor de
s (WPA o WPA2), VPN, o
ma automática) si la
os en el personal con acceso a las claves.
- Restringir el acceso basándose en la dirección de código de acceso de medios (MAC).

Fuente:

Department of Defense (DoD) of U
http://iase.disa.mil/stigs/stig/wireless-stig-v5r1-final20feb07.pdf

DEPARTMENT OF DEFENSE · UNITED STATES OF AMERICA

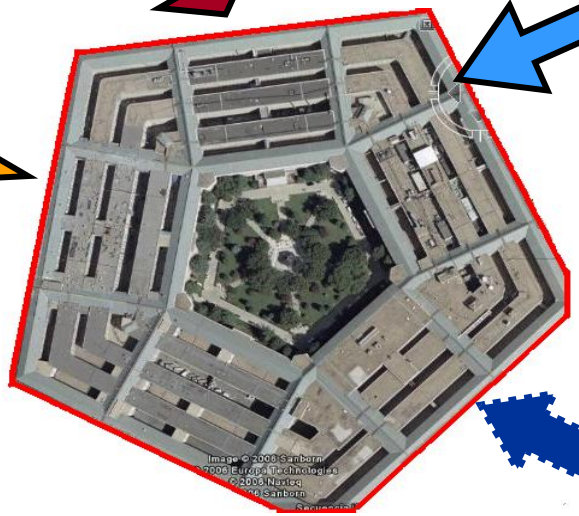
2.2.3.4 WEP and WPA

WEP and WPA are both "legacy" WLAN security protocols that were part of the IEEE 802.11 standard prior to the release of IEEE 802.11i. Although most consumer WLAN products and some enterprise WLAN systems continue to support these protocols, neither protocol meets DoD security requirements and will not be used in DoD.

De quienes nos debemos proteger:

Defacement Web
Denial of Service
SQL Injection
Phishing
Trafico desde Internet
Virus
SPAM-Bombing
XSS, Cross Site Scripting
Malware

WLAN, LAN
MITM
Robo de Info
Proveedores
XSS- Cross Site Scripting
Denial of Service
SQL Injection
Acceso Desautorizado
Inundación Tráfico



Información hablada
Información impresa
Acceso a los Sistemas
Robo de Información.
Empleados Internos
Manejo de Dispositivos Moviles: CDs, USB, HD.
Acceso a la red: LAN, WLAN, WAN
Acceso directo :
-Base de Datos
- File Server
- Unidad de Backup

Amenazas:

Tormentas
Huracán,
Desastres,
Terremotos,
Vandalismo.

Estrategia de protección: “Defense in Depth”

Es una estrategia práctica utilizada para proteger la información de las empresas basado en la IATF [1]. Seguridad en Profundidad es una estrategia basada en crear capas de protección para un sistema en un entorno

[1] IATF : Information Assurance Technical Framework – Chapter 2

La estrategia recomienda un balance de los siguientes puntos, para su implementación en el aseguramiento de la infraestructura tecnología de las empresas :

- **Capacidad de Protección**
- **Costo**
- **Performance**
- **Operación**

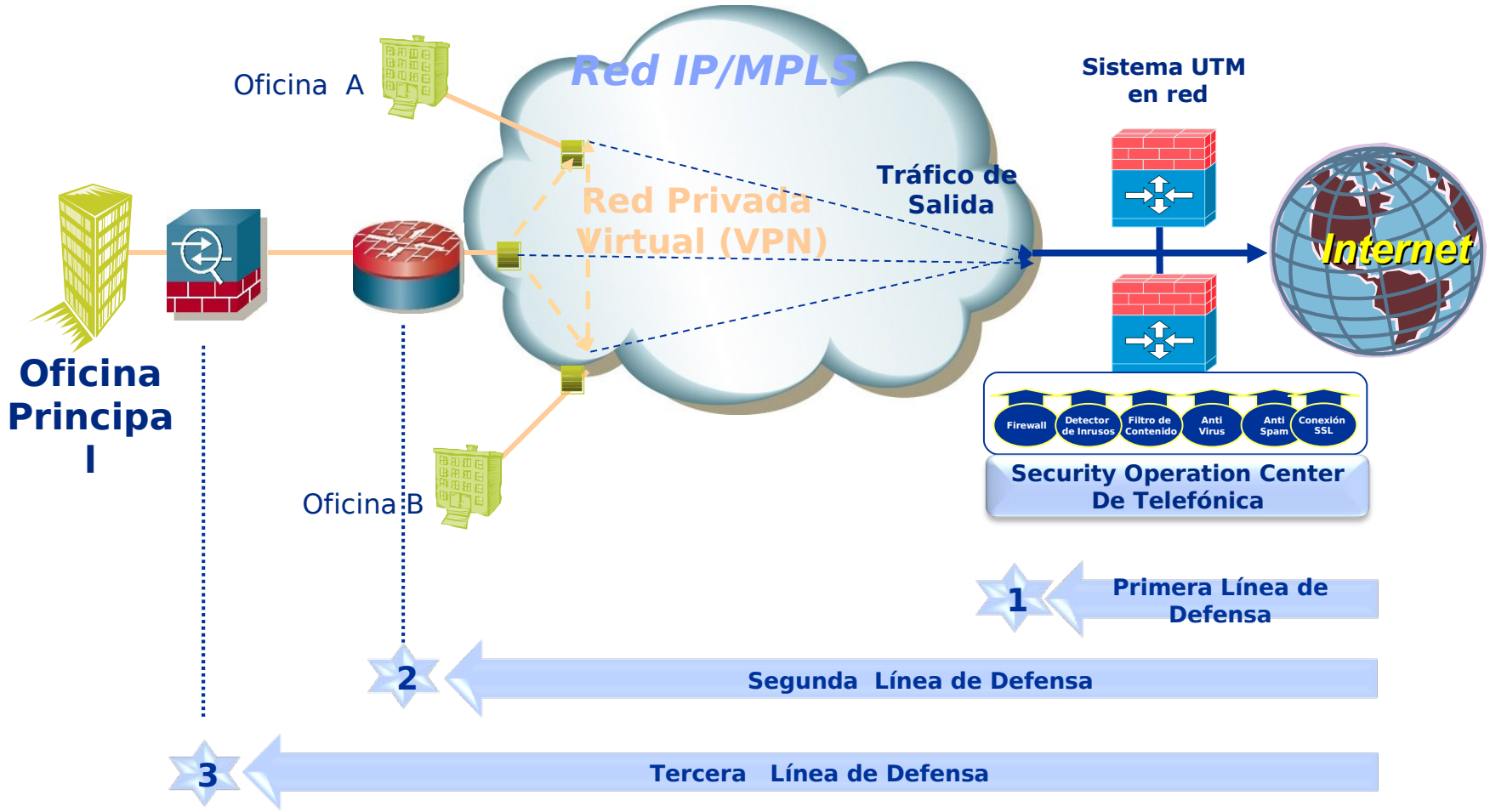
[1] IATF : Information Assurance Technical Framework – Chapter 2

Fuente:

http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Estrategia de protección

"Defense in Depth"



11 Regulación: Sector Go

-- **Presidencia Consejos de Ministros (**

- **NORMA TECNICA PERUANA "NTP-ISO/ IEC 17799-2007 EDI":**

  -**Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información.**
  - **RESOLUCIÓN MINISTERIAL No 246-2007-PCM (22Agosto,2007).**

- **Creación del Grupo de Trabajo denominado Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (Pe-Cert)- Resolución Ministerial No 360-2009-PCM (19Ago09).**

- **La Norma NTP-ISO/IEC 17799-2007 EDI debe ser incluida dentro de los planes operativos informáticos, y es de carácter "obligatorio" para todas las instituciones públicas de todos los niveles del Gobierno, Gobierno Central, Regional, Municipalidades y Entidades Constitucionalmente Autónomas. (JNE, Reniec, Poder Judicial, Congreso de la República, ONPE, Tribunal Constitucional, Defensoria del Pueblo).**

1 2 Regulación Sector Financiero a nivel Perú

- **CIRCULAR No G-140-2009: (Gestión de la seguridad de la información):**
  - **Objetivo: Las empresas deberán establecer, mantener y documentar un sistema de gestión de la seguridad de la información (SGSI: Sistema de Gestión de Seguridad de la Información), se toma como referencia estándares ISO 27001 e 17799.**
  - **Vigencia: Para su cumplimiento un plazo de adecuación hasta el 31 de marzo de 2010. Para las AFP, En un plazo que no excederá de noventa (90) días calendario de haberse publicado la presente Circular.**

-http://www.sbs.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=0&JER=105

CIRCULAR Nº G- 139 -2009: (Gestión de la continuidad del negocio):

- **Objetivo : Dot pacidad de mantener, o de ser el caso r procesos de negocio dentro de un al**
- **Vigencia: Par zo de adecuación hasta el 31 de marzo de**

-http://www.sbs.gob.pe/ &PFL=0&JER=105

Telefónica del Perú

Procesos: Interacción directa con la comunidad internacional

Phishing

Ataque de ingeniería social, suplantando la identidad de una empresa de “confianza” se solicita información sensible del usuario.

Cadena de producción de esta “Industria” floreciente

¿Es fácil hacer “Phishing” ?

- **No existen Barreras de entrada**
- **Bajo Riesgo**
- **Altos Beneficios**