Convergencia de la seguridad

agosto de 2011

Antonio Rodríguez
Alfredo Reyes

Agenda

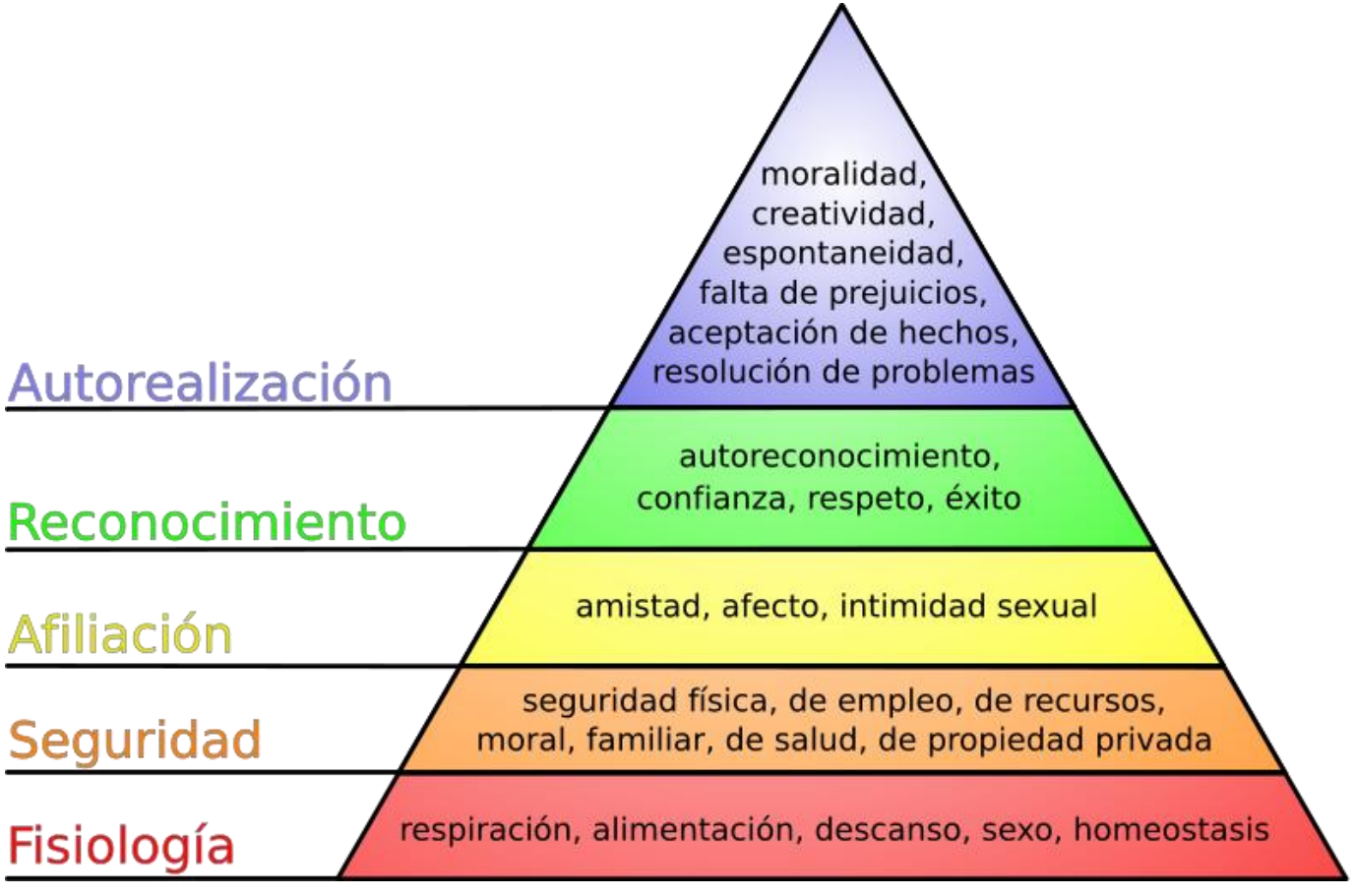
- Conceptos de seguridad e inseguridad.
- Prevención del fraude. Dos casos de convergencia.
- La convergencia
- Cómo se converge!

Qué se entiende por seguridad?

Confianza que nace de la sensación de ausencia de peligro.

En realidad es un estado de ánimo, una sensación, una cualidad intangible.

Jerarquía de necesidades de Maslow (Abraham)



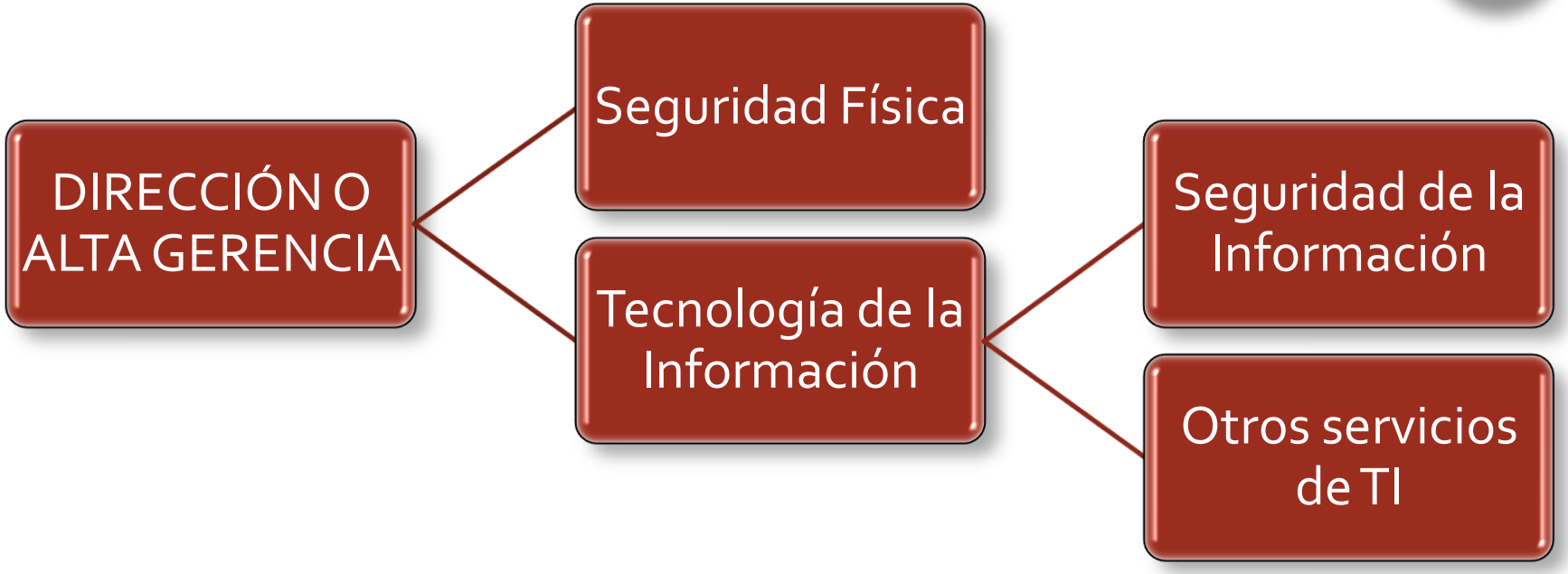
Dónde están los inicios de la convergencia?

Qué áreas deben ser protegidas?

- **La tecnología como parte de los medios o dispositivos utilizados para atender la seguridad física.**

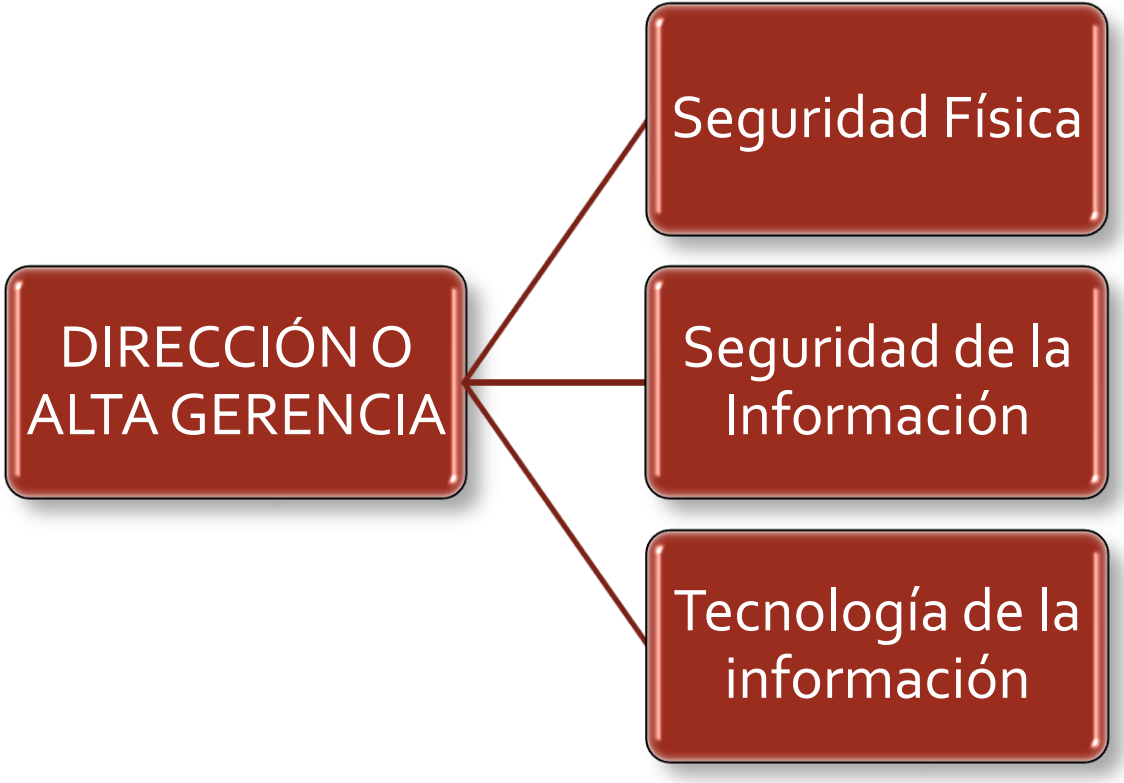
- **La tecnología como parte de los bienes a proteger.**

Cómo se han estructurado las organizaciones para darse seguridad?



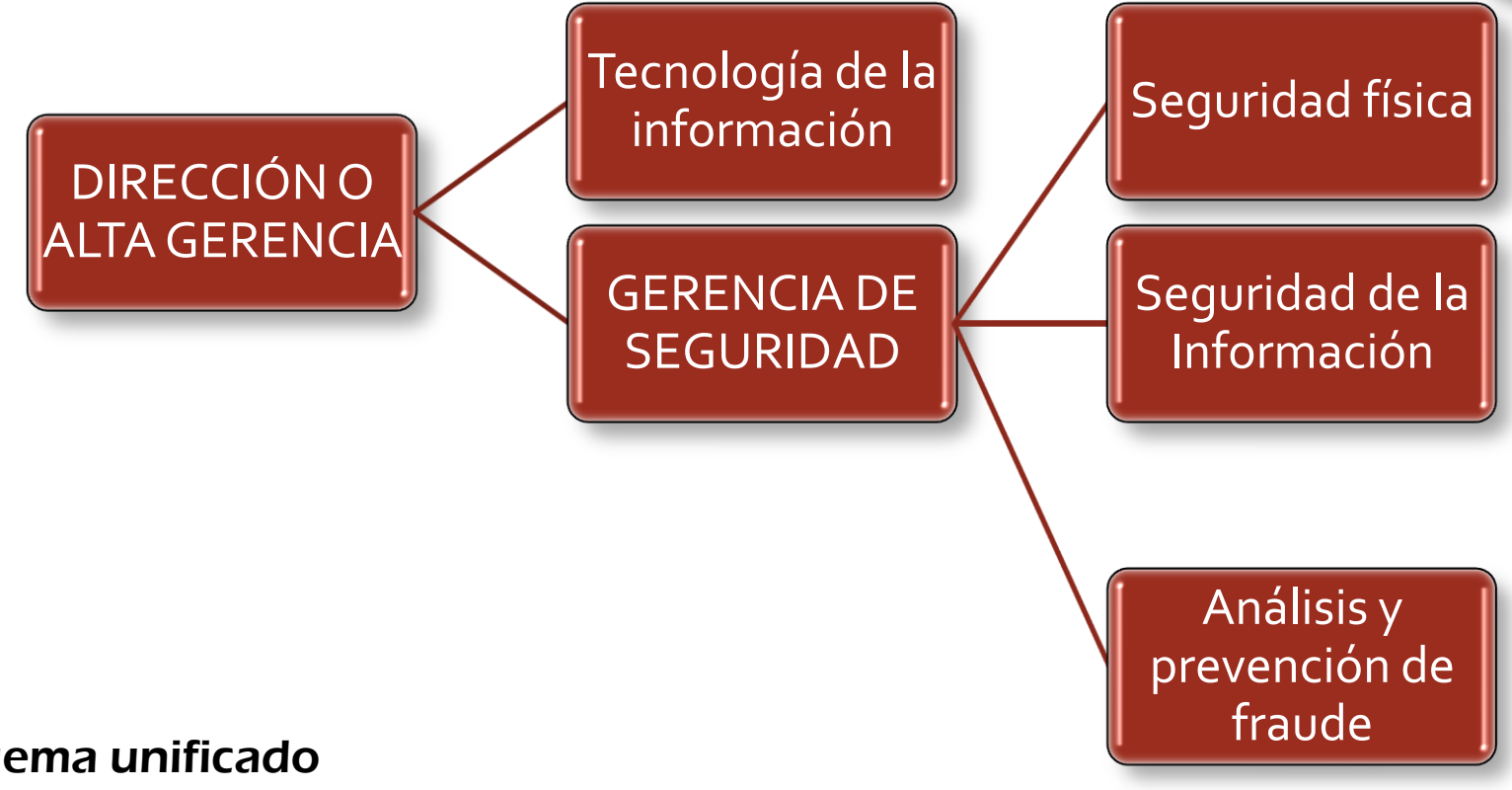
Esquema integrado

Cómo se han estructurado las organizaciones para darse seguridad?



Esquema independiente

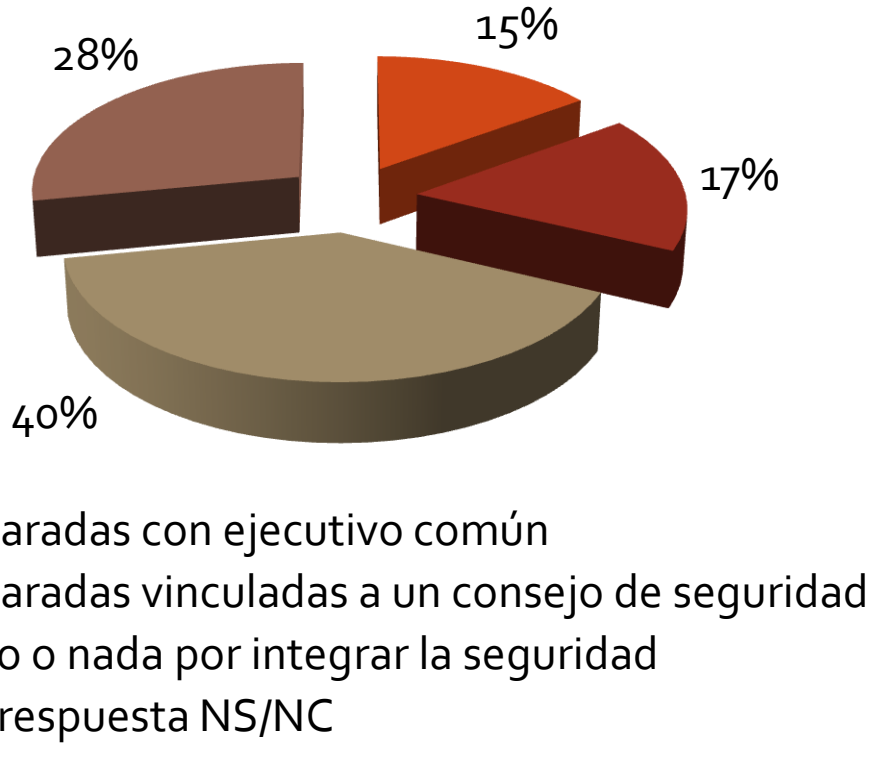
Cómo se han estructurado las organizaciones para darse seguridad?



Esquema unificado

Cómo está integrada la seguridad en las empresas hoy?

Integración de la seguridad



Deloitte 2009

De qué se han venido preocupando las organizaciones?

En 1970: Personas, edificios, productos, maquinaria.

En 1980: La tecnología como medios para atender la seguridad física y lo de 1970.

En 1990: La tecnología como medios a proteger y lo anterior.

En 2011: Información, información, ... y todo lo de los '70, '80 y '90.

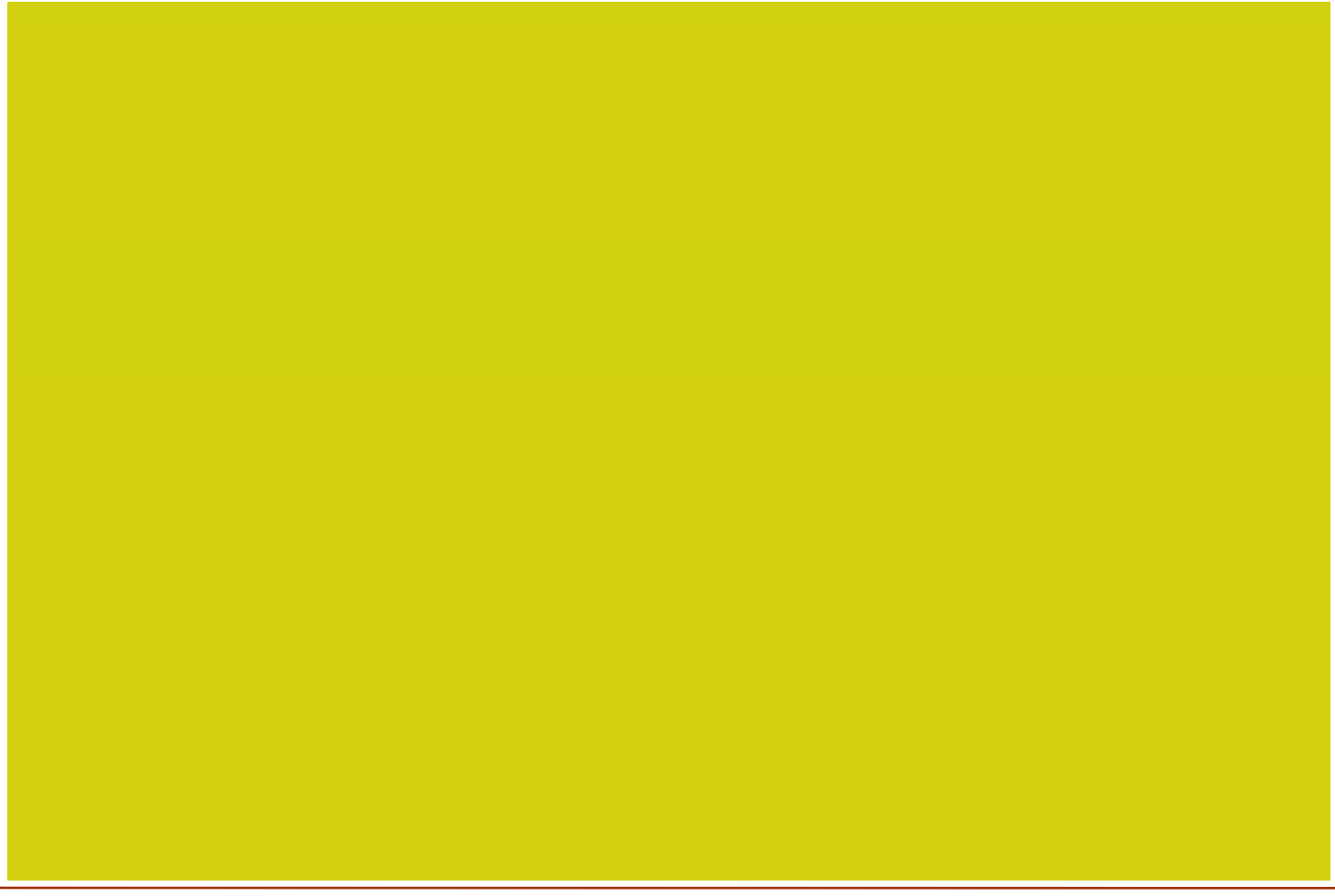
LA INFORMACIÓN: ACTIVO CADA VEZ MÁS CRÍTICO.

Cada vez hay más dependencia de los activos físicos en activos más intangibles, como la información y los sistemas que la tratan.

¿Cómo se controla hoy el acceso a nuestras oficinas?

Dónde están los riesgos?

Qué es lo que más falla en materia de seguridad?



Fraude: definición

Por fraude entendemos un acto voluntario por el que una persona o grupo de personas, consejeros, directivos o empleados y/o terceras partes, emplean algún tipo de engaño para obtener un beneficio o ventaja injusta o ilegal, con perjuicio para la empresa. (Deloitte)

Association of Certified Fraud Examiners (ACFE) - 2010 Report to the Nations

- Según la encuesta 5% de las ganancias se pierden por fraude. A nivel mundial la cifra asciende a: 2.900.000.000.000 (2.9 trillones).
- Fuente:

http://www.acfe.com/rttn/2010-rttn.asp

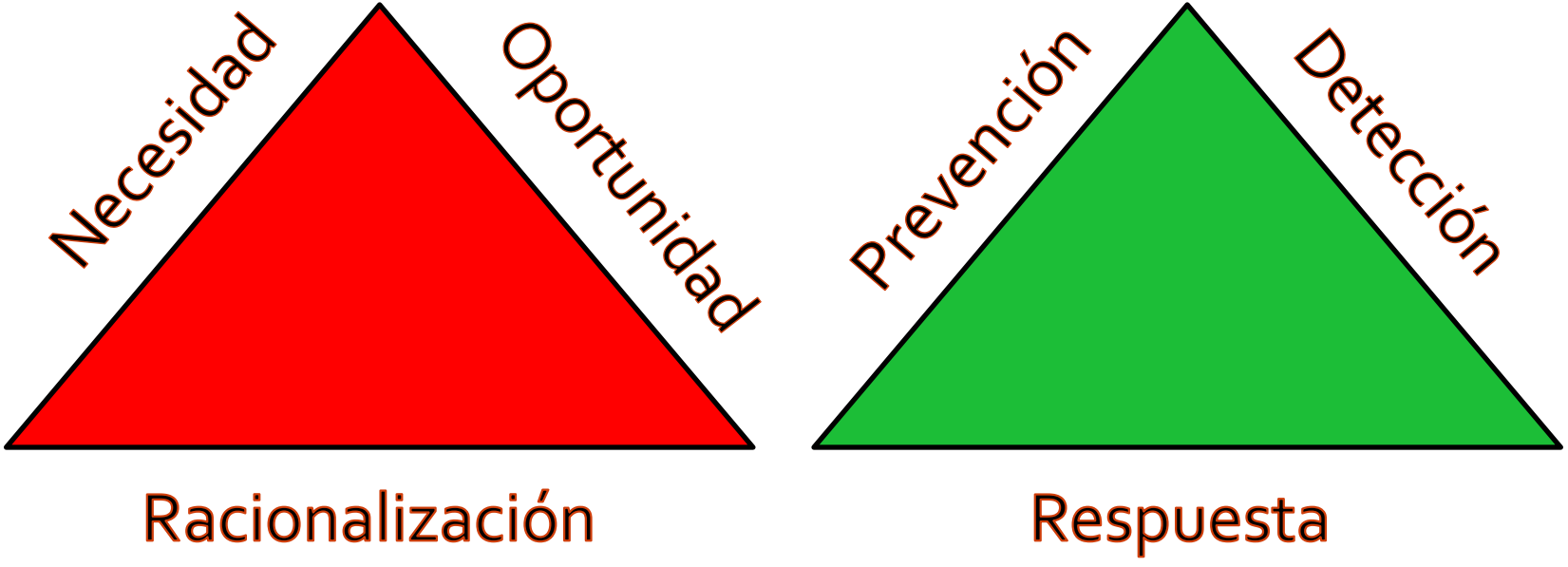
Cuánto cuesta cometer un fraude?

Con información de: press.pandasecurity.com

Producto Precio aproximado en Internet:

- Datos de tarjetas de crédito De $2 a $90 USD
- Tarjetas de crédito (físicas) Desde $190 USD
- Clonadores de tarjetas De $200 a $1,000 USD
- Cajeros automáticos falsos Hasta $35,000 USD
- Datos de acceso bancario validados De $80 a $700 USD
- Transferencias bancarias y cambio de cheques De 10% a 40% del monto
- Datos de acceso a plataformas de pago y tiendas *online* De $80 a $1,500 USD
- Compras y envíos ilegales de productos De $30 a $300 USD, dependiendo del "proyecto"
- Renta de servidores para envío de *spam* Desde $15 USD
- Renta de servidores SMTP De $20 a $40 USD por trimestre
- Renta de VPN para esconder identidad $20 USD por trimestre

Los triángulos del fraude



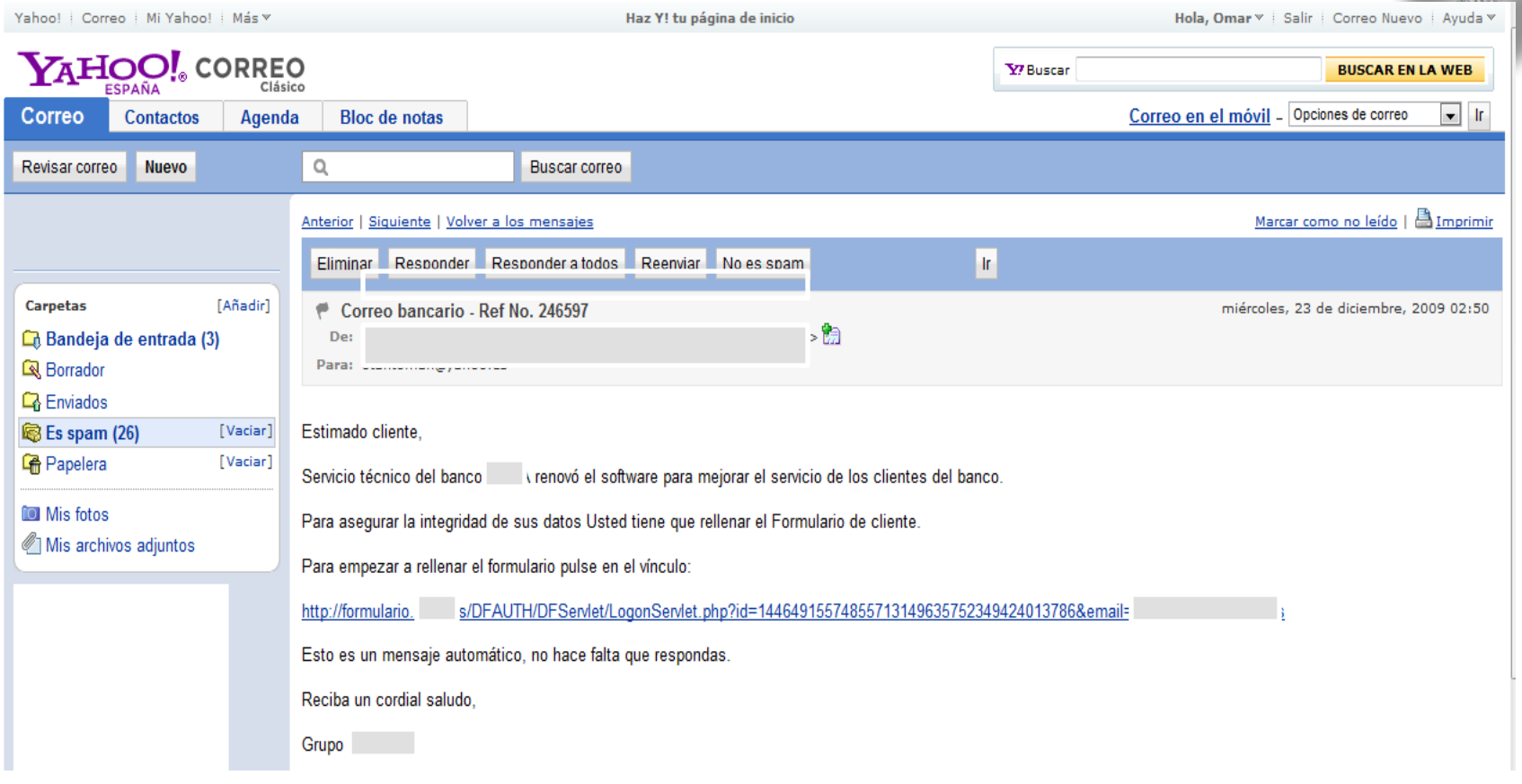
Caso 1: phishing + ingeniería social

Año 2008: Algunos clientes reclaman por movimientos no reconocidos a través de la plataforma de e-banking. En particular uno de ellos denuncia haber recibido en su cuenta una transferencia que no reconoce como originada en su giro comercial.

Phishing
Cuando nos intentan "pescar" con cualquier tipo de engaño para que facilitemos nuestras claves, o cualquier otro dato.

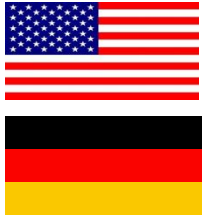
Ingeniería social
Agrupa a las conductas útiles para obtener información de las personas.

Phishing: un ejemplo real



La maniobra

Otros orígenes de las IP utilizadas para el ataque



Phishing

Usuario y password

Resultado del fraude

Ing. social

P.C. DEL DAMNIFICADO

E-bank

CUENTA DE DESTINO
(Mula o peón)

Un caso de skimming o clonación de tarjeta

PORTADA | EDICIÓN IMPRESA | CLASIFICADOS

Entrar con Facebook | Iniciar Sesión

EL OBSERVADOR .com.uy

20 de Mayo 2011 Actualizado: 20:29:21

MONTEVIDEO
T 21 | H 64%
+ AMPLIAR

BUSCADOR
buscar

PORTADA
CADUCIDAD
NACIONAL
ECONOMÍA
AGRO
MUNDO
DEPORTES
TECNOLOGÍA
SALUD
ESPECTÁCULOS
ESTILO
OPINIÓN
MULTIMEDIA

Añadir un tag...

SIGNO DEL MES
Tauro
Excelente semana. Mercurio y Venus ingresan a su signo generando una revolución energética que le ayudará a poner las cosas en su lugar.
+ AMPLIAR

Feedback

ACTUALIDAD - SEGURIDAD

Denuncian clonación de tarjetas de débito y retiro de dinero

Varios usuarios de tarjetas de débito que funcionan en la red de cajeros automáticos [redacted] sufrieron retiros de dinero en sus cuentas bancarias este fin de semana

+ - 14.03.2011, 19:05 hs

Texto: -A / A+

COMPARTE ESTA NOTICIA
Tweet
Envíala por email
Más Opciones
Imprímela

NOTICIAS RELACIONADAS
Se normalizan cajeros automáticos
Largas filas en cajeros
Tres policías a prisión por estafas con tarjetas de crédito
Varios procesados por estafas con tarjetas de crédito

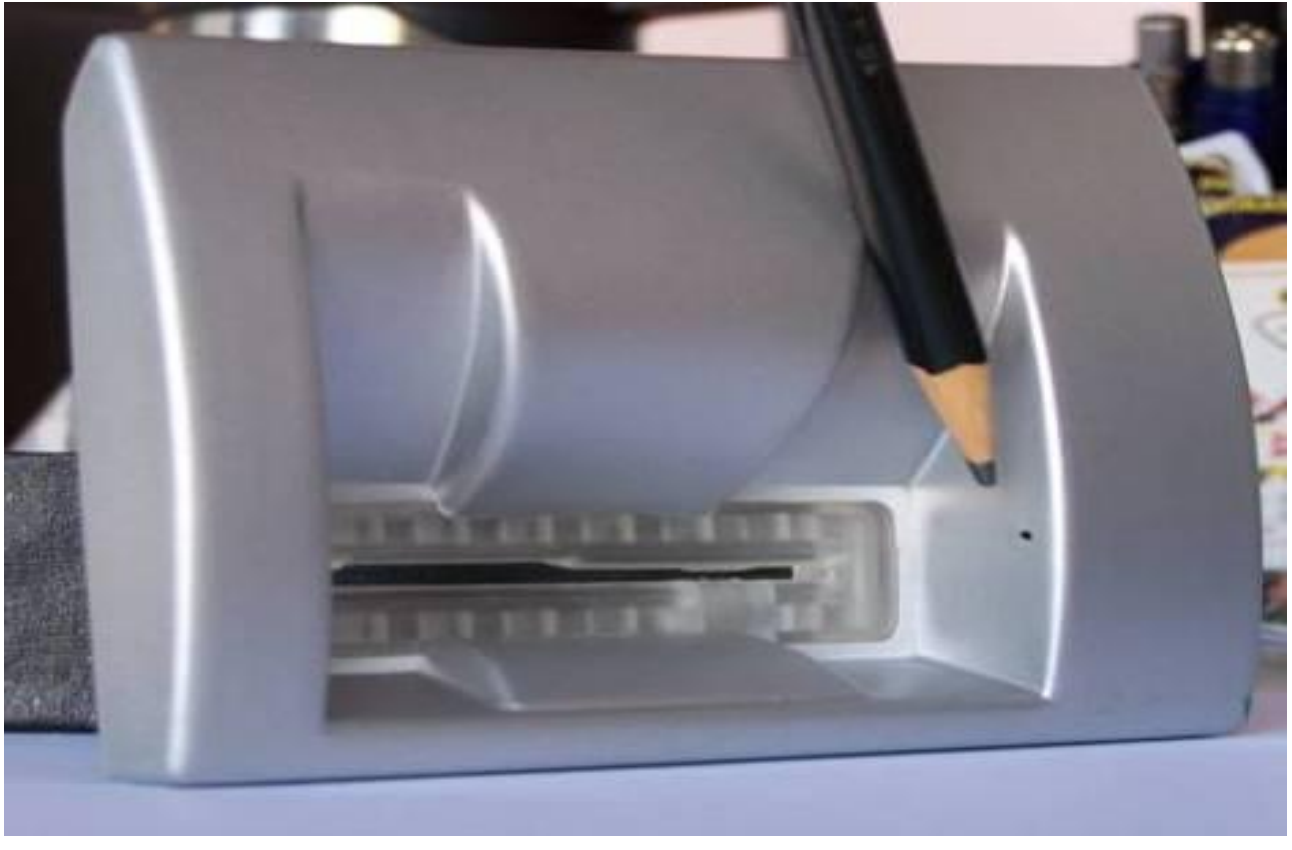
MAS LEÍDAS | MÁS COMENTADAS | MÁS COMPARTIDAS

Esta vida es de regalo: todo lo que estoy viviendo es de

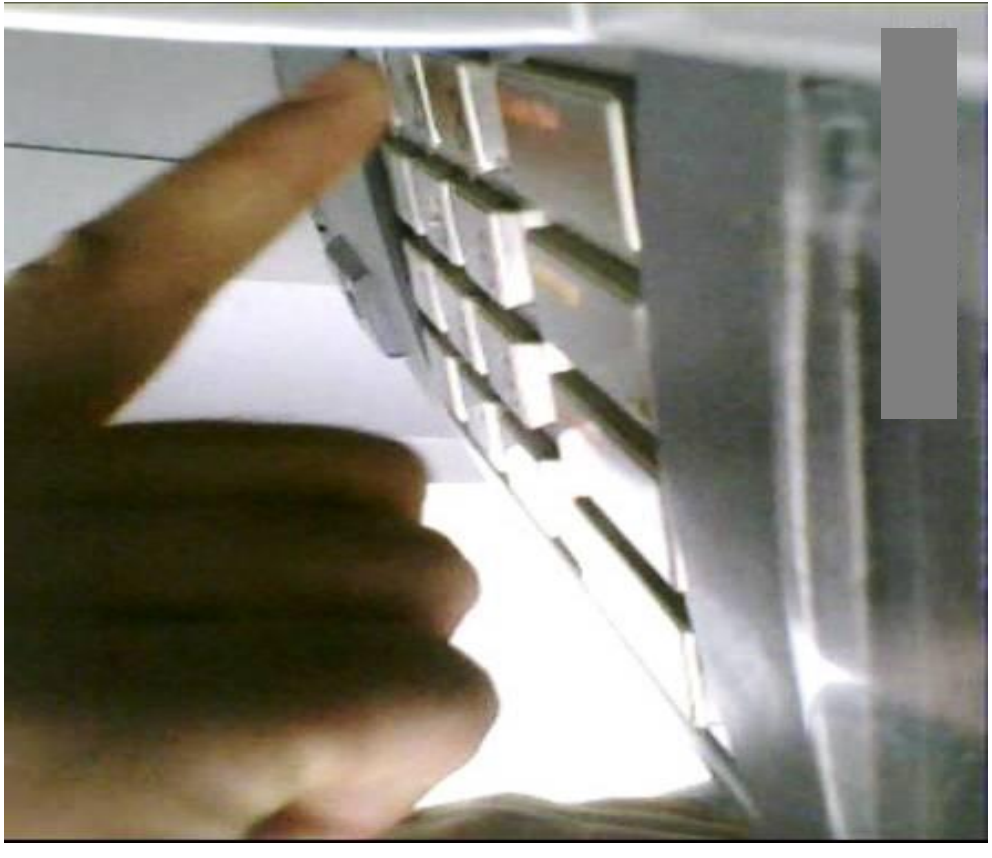
Internet | Modo protegido: desactivado

125%

Dispositivo de clonación



Vista de la cámara



Es el uso combinado de métodos y técnicas de protección tanto físicas como lógicas para salvaguardar un bien.

En otras palabras: es utilizar todas la herramientas posibles para proteger un bien sin importar si el bien o los medios utilizados pertenecen al mundo físico o lógico.

Qué es lo que converge?

- **Seguridad física**
  - ✓ Protección de personas
  - ✓ Protección de bienes
- **Seguridad lógica**
  - ✓ Protección de información
  - ✓ Protección de sistemas
  - ✓ Protección de redes
- **Continuidad del negocio**
- **Gestión de riesgos**
- **Seguridad legal**
- **Prevención del fraude**

En realidad convergen las diferentes formas de seguridad?

Convergencia (Concepto de 1997)

Es la cooperación formal de las diferentes funciones de seguridad de una organización y su integración, complementándose.

Objetivo

Proteger de la mejor forma posible los activos de la organización respecto de cualquier amenaza que les pueda causar daño, sin importar el origen.

La seguridad es una cadena

Un atacante nos dañará de la forma más sencilla para él, ya sea física, lógica o legal.

Qué no es convergencia?

Unificar varios departamentos de seguridad en un área común sin ir más allá.

Forzar una reunión mensual entre las áreas de seguridad física y lógica, sin buscar los puntos en común o los complementos.

Darle un arma a los analistas de seguridad lógica y la administración de infraestructura de SI a analistas de seguridad física.

Dedicarse a mezclar controles lógicos y físicos sin buscar la complementación.

Qué catalizadores hay para converger?

Convergencia tecnológica

Control de acceso y presencia – Cámaras IP, detectores de intruso.

Convergencia de la comunidad

Hasta el año 2005 las organizaciones que aglutinaban a miembros con diferentes funciones de seguridad no tenían relación entre sí.

Convergencia en la educación

Cada vez más habitualmente los masters en Dirección de Seguridad Física incluyen referencias a la SI. A su vez referencias de SI hablan también de seguridad física o legal (ISO 27001-2)

Como resultado de la convergencia tecnológica, las amenazas contra los activos de una organización también convergen.
Sino veamos:

Escenario

Un ataque que combine elementos físicos y lógicos contra una organización.

Ejemplo

Una amenaza de bomba dispuesta en un edificio, combinada con el bloqueo remoto de la red de semáforos mediante una negación de servicio.

"Lo más extraordinario de Internet es que ahora todo el mundo está conectado con los demás...

Lo más terrible de Internet es que ahora todo mundo está conectado con los demás."

Entonces, por qué converger?

- Hay una expansión del ecosistema empresarial y crece la complejidad de las organizaciones.
- Hay una globalización en la relación entre organizaciones, proveedores, clientes, partners.
- Hay una pérdida del perímetro de seguridad dado que en el mundo globalizado aparecen amenazas globales.

Entonces, por qué converger?

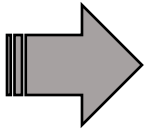
- La complejidad creciente de las organizaciones hace que aparezcan nuevas amenazas.
- Nuevas normativas, estándares y leyes que tratan la seguridad de una forma integral.
- Cumplimiento complejo que exige la unificación de diferentes puntos de vista de la seguridad.
- Nueva práctica de gestión unificada.
- Por sobre todo más y mejor seguridad!

Esto no significa que busquemos personal multidisciplinario a nivel técnico, sino a nivel de gestión.

Es así que las organizaciones buscan un Director de Seguridad que sea un gestor del riesgo GLOBAL.

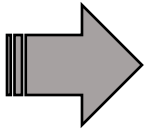
Camino de la convergencia

- **Beneficios**



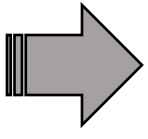
  - Alineación de la seguridad con el negocio.
  - Director de seguridad como referencia única.
  - Personal de seguridad versátil.
  - Reducción de costos.

- **Condiciones**



  - Apoyo de la Dirección y de la Alta Gerencia.
  - Encontrar ese Director de Seguridad.
  - Buen equipo de trabajo.
  - Un Plan de Trabajo.

- **Obstáculos**



  - Diferencias culturales.
  - Áreas de conocimiento diferentes.
  - Pérdida de control.
  - Factores políticos.

Por ejemplo en indicadores de gestión:

- Capacitación
- Concientización
- Protección de firewalls
- Las dudas de los usuarios cuando se enfrentan a problemas.

El tratamiento de nuevas disposiciones como las leyes 18.381, 18.331 y comunicado de la UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES en resolución relativa a video vigilancia de fecha 30.7.2010

Cómo debe ser el Gerente se Seguridad?

Intentar definir los conocimientos y experiencia que debería tener un Gerente de Seguridad es difícil. Además de su formación y experiencia, cada Gerente tiene su propia personalidad y competencias que le hacen siempre diferente a los demás.

Diferentes perfiles son adecuados para diferentes empresas, ya que los retos son diferentes también.

Debe si tener poder decisivo sin titubeos.

Extremada objetividad.

Firmeza, resiliencia.

Querer lo que se hace.

Ser negociador por excelencia.

No tener exceso de confianza.

La inseguridad no distingue lo físico de lo lógico. Quienes la aprovechan tampoco. Por tanto no distingamos nosotros la protección. Debemos proteger lo crítico por igual.

El lenguaje lógico en situaciones emocionalmente límites no funciona, la memoria tampoco. Planificar es prevenir.

En seguridad cuando aprendimos las respuestas, nos cambiaron las preguntas.

En seguridad no debemos confundir rapidez con apuro.

Es lo mismo apuro que rapidez?

Muchas gracias!

Fuentes:

- IV seminario internacional de prevención de fraude en el sistema financiero. José Marangunich
- Carlos Blanco Pasamontes. Director Eulen Seguridad.
- Felaban – Celaes
- Antonio Villalón. STC (sistemas tecnológicos y comunicaciones)
- Prismamx.com – Lic. Carlos Ramírez
- Manual cism
- Wikipedia
- Antonio Rodríguez
- Alfredo Reyes

antonio.rodríguez@brou.com.uy
alfredo.reyes@brou.com.uy