Seguridad de la Información en Instituciones Financieras: una perspectiva de riesgo

Congreso Internacional de Finanzas y Auditoría

Ing. José Luis Antigua D. (jose.antigua@bdo.com.do)
Director Riesgos y Tecnología
BDO Dominicana
21 Julio 2012

CONTENIDO

- TITULARES
- CIFRAS IMPORTANTES
- LA SEGURIDAD DE LA INFORMACIÓN
- COSO-ERM
- MÉTODOS COMUNES DE ATAQUE
- ¿QUÉ HACER?

TITULARES

INVESTMENT BANKING | MARCH 14, 2011, 6:09 AM | 69 Comments

Bank of America Unit Tried to Hide Foreclosure Information, Hackers Say

s Anonymous
Monday provided

NOTICIAS | 16 JUL | POR FEDERICO MÉNDEZ

"Hackeos" son el 60% de delitos de alta tecnología

Un 30% a

TECNOLOGÍA Y TELECOMUNICA | 01 MAR | 1 | POR ING. HIDDEKEL MORRISON, MBA

Tarjetas de Crédito Tecnología insegura en República Dominicana

AUGU

How Hackers Snatch Real-Time Security ID Numbers

By SAUL HANSELL

Thieves Found Citigroup Site an Easy Entry

El
cie

ty system — but the

FM
La

Ra

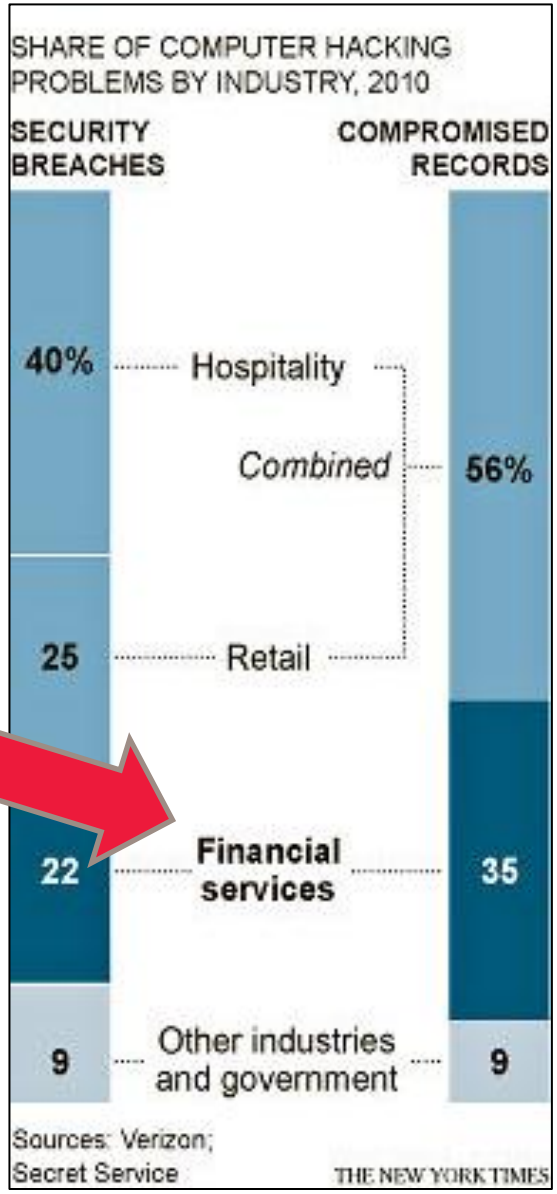
FRAUDES

Bancos se ponen alertas por clonación de tarjetas

EMPRESAS HAN TENIDO QUE CAMBIAR TODOS LOS PLÁSTICOS DE EMPELADOS

CIFRAS DEL SECTOR

En el 2010, el 35% de los ataques de hackers se hacía directamente al sector financiero.



Verizon, 2010

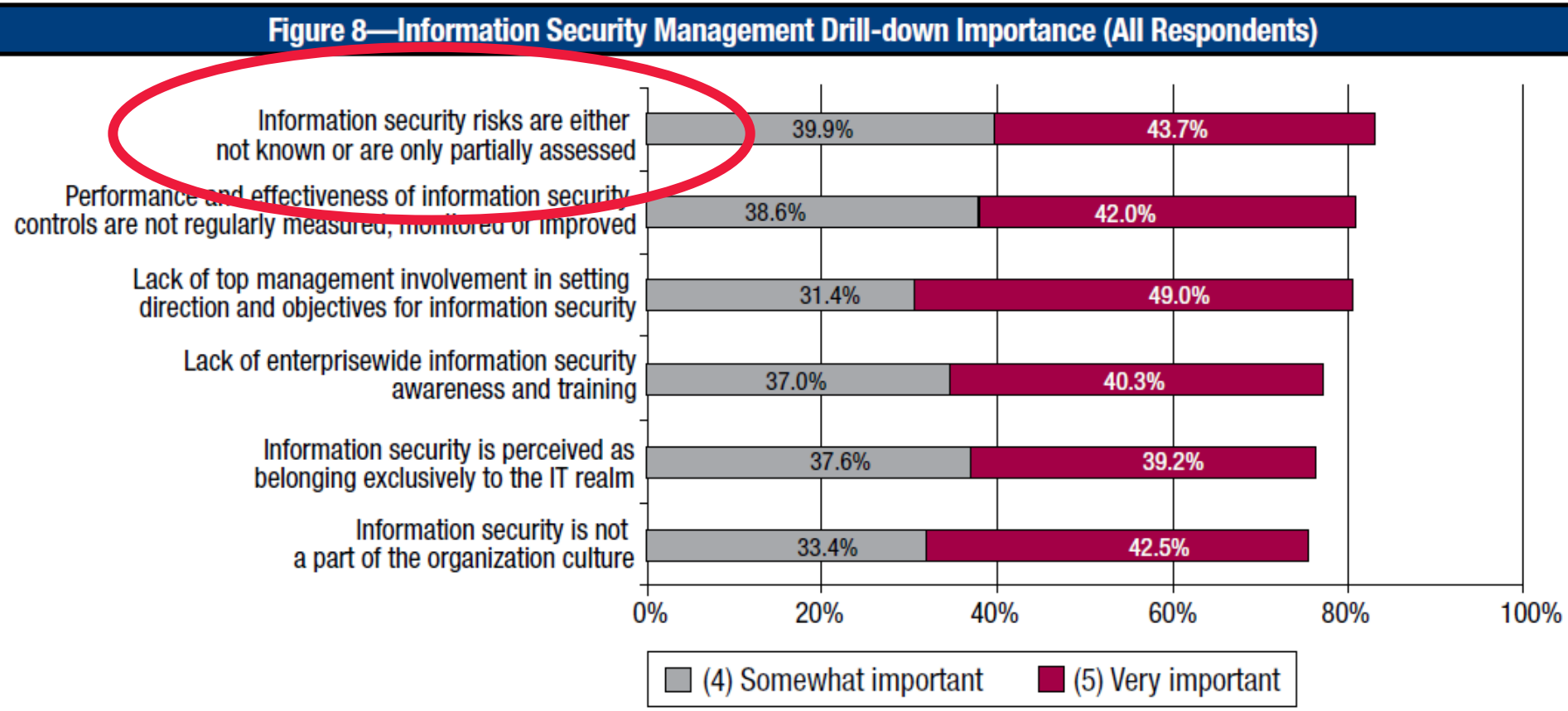
CIFRAS DEL SECTOR

Reclamaciones recibidas por la SIB (últimos dos años)

«Transacciones Fraudulentas» está en el «Top 10» de causas de reclamaciones

SIB, 2012

CIFRAS DEL SECTOR



ISACA, 2011

Seguridad de la Información

Es un componente esencial del gobierno corporativo y la gerencia que afecta todos los aspectos de los controles de la entidad.

Su administración es el conjunto de prácticas encaminadas a:

- salvaguardar los activos de la empresa
- Asegurar disponibilidad continua
- Preservar la confidencialidad
- Asegurar la integridad

Elementos Claves Sistema de Administración de Seguridad de la Información

- Compromiso y Apoyo de la Gerencia
- Políticas y Procedimientos
- Organización
- Conciencia y Educación sobre Seguridad
- Monitoreo
- Administración de Incidentes

ISACA 2010

¿HA ESCUCHADO ESTO ALGUNA VEZ?

Discusión sobre violaciones comunes a las normas de seguridad en el día a día

Existen violaciones a diario…

«La Administración de la Seguridad de la Información es un reto afecta y debe ocupar a todos»

Recordemos COSO-ERM

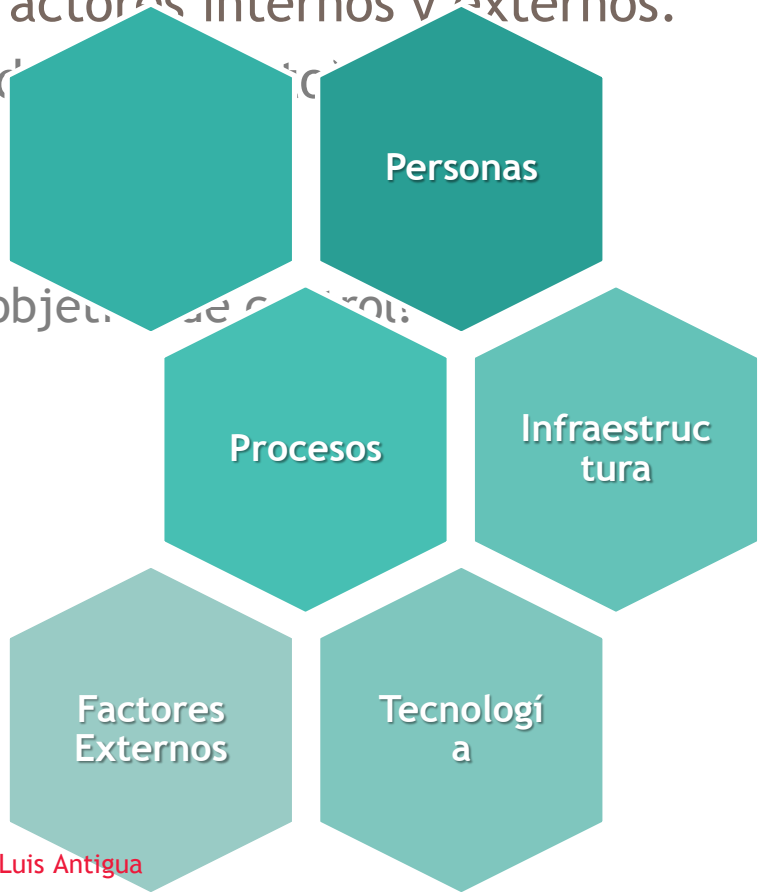
"… un proceso, efectuado por la junta directiva de una entidad, la gerencia u otro personal, aplicado en la definición de la estrategia y a través del la organización, diseñado para identificar eventos potenciales que puedan afectar a la entidad, y para administrar los riesgos que se encuentran dentro de su apetito por el riesgo, para proveer una seguridad razonable con respecto al logro de los objetivos de la entidad."

The Committee of Sponsoring Organizations oh the Treadway Commission

Recordemos COSO-ERM

Componentes COSO-ERM

- **Identificación de eventos** (vulnerabilidades y amenazas) por proceso u objetivo, considerando factores internos y externos.
- Evaluación de riesgos (probabilidad
- Respuesta a riesgos
- Actividades de control
  - ¿Cómo definir adecuadamente un objet
  - Definición de Excepciones
- Información y Comunicación
- Monitoreo



Informe COSO-ERM, 2004

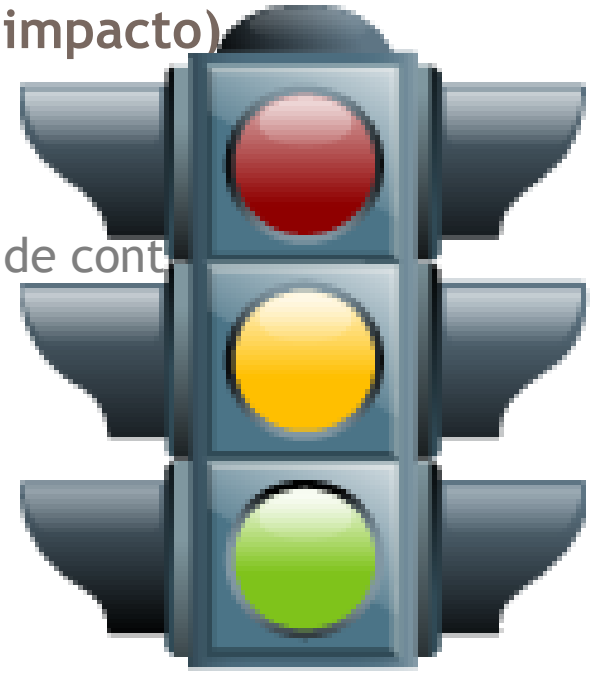
Componentes COSO-ERM

- Identificación de eventos (vulnerabilidades y amenazas) por proceso u objetivo, considerando factores internos y externos.
- **Evaluación de riesgos (probabilidad por impacto)**
- Respuesta a riesgos
- Actividades de control
  - ¿Cómo definir adecuadamente un objetivo de cont
  - Definición de [illegible]
- Información y Comunicación
- Monitoreo

Alto

Medio

Bajo



Informe COSO-ERM, 2004

Componentes COSO-ERM

- Identificación de eventos (vulnerabilidades y amenazas) por proceso u objetivo, considerando factores internos y externos.
- Evaluación de riesgos (probabilidad por impacto)
- **Respuesta a riesgos**
- Actividades de control
  - ¿Cómo definir adecuadamente un objetiv
  - Definición de Excepciones
- Información y Comunicación
- Monitoreo

***Informe** COSO-ERM, 2004*

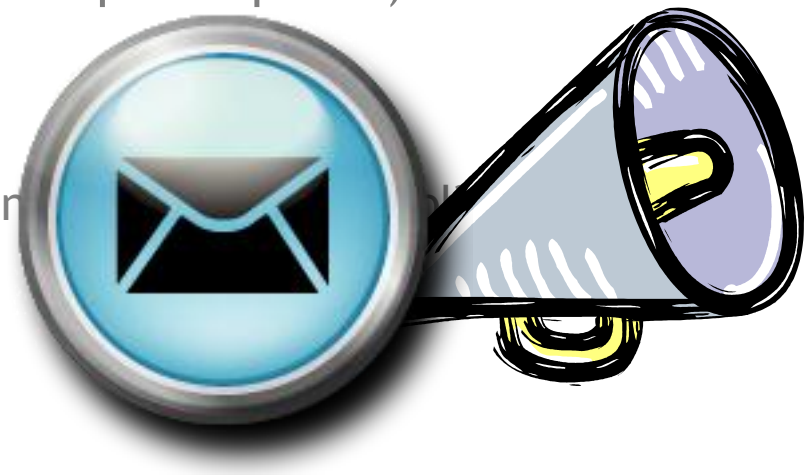
Planificación

- Identificación de eventos (vulnerabilidades y), por proceso u objetivo, considerando factores in
- Evaluación de riesgos (probabilidad por imp
- Respuesta a riesgos
- **Actividades de control**
  - ¿Cómo definir adecuadamente un objetivo de control?
- Información y Comunicación
- Monitoreo

***Informe** COSO-ERM, 2004*

Planificación

- Identificación de eventos (vulnerabilidades y amenazas) por proceso u objetivo, considerando factores internos y externos.
- Evaluación de riesgos (probabilidad por impacto)
- Respuesta a riesgos
- Actividades de control
  - ¿Cómo definir adecuadamente un
- **Información y Comunicación**
- Monitoreo



***Informe** COSO-ERM, 2004*

La Banca: el escenario ideal

- Dinero (no sólo físico)
- Personas (internas y externas)
- Tecnología (constante demanda)

Métodos Comunes de Ataque

Ingeniería Social:

Uso de las relaciones / comportamiento humano para llegar a un objetivo.

Veamos un ejemplo…

Métodos Comunes de Ataque

Virus:

Programa que se instala en un equipo y se difunde masivamente a través de los medios disponibles. Su objetivo podría ser dañar o capturar información del huésped.

Caso New York Times…

Métodos Comunes de Ataque

Phishing:

Forma de Ingeniería Social basada en el engaño (usurpación de identidad empresarial principalmente) a través de páginas, correos, entre otros.

Ejemplo página web Banco…

¿Qué hacer ante la realidad?

- Administración de Riesgos
  - Foco en Personas y Tecnología
- Controles mínimos entidades financieras:
  - Proveedores
  - Control Cambios
  - **Seguridad**
  - Gobierno TI
  - Continuidad Negocios

Existen alternativas…
Estándares y Marcos de Seguridad

- **ISO 27000** (Seguridad de la Información)
- **COBIT** (Gobierno de TI; Incluye Objetivos de Control de Seguridad)
- **PCI** (estándar de seguridad enfoque Tarjetas Crédito)

Existen alternativas…
Herramientas Tecnológicas

- Software para Administrar Riesgos (Desde Levantamiento hasta Seguimiento)

- Software para Análisis y Monitoreo de Transacciones

Existen alternativas…
Modelo de capacidad de Análisis: MCAA

Desarrollado en base a experiencia en más de 15,000 empresas a nivel mundial, para ayudar a evaluar más claramente el nivel análisis de datos en auditoría, planificar y comunicar lo que se debe hacer

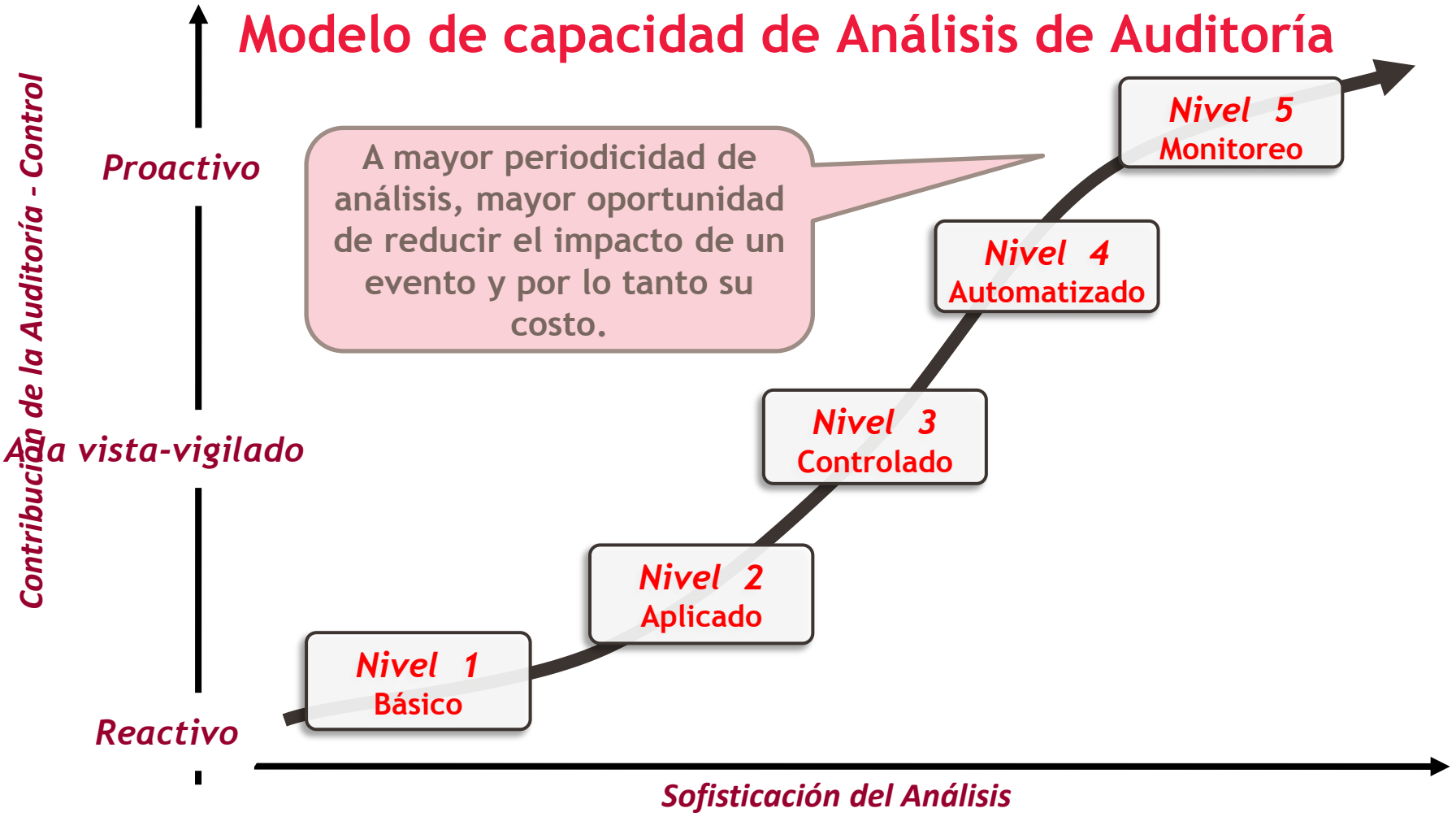
Hecho para obtener mayores beneficios y administrar riesgos en términos de:

- Personas
- Tecnología
- Procesos

Revolucionar el enfoque tradicional de la auditoría (de reactivo a proactivo)

Cinco niveles a través de los cuales auditoría interna puede ampliar su uso de análisis

Existen alternativas…



Existen alternativas…
Tips Seguridad de la Información

- No comparta sus claves ni tarjetas de acceso
- No suministre información confidencial sin confirmar la identidad del solicitante
- No acceda a los vínculos de correos con ofertas o tarjetas de felicitación
- Cambie periódicamente su contraseña; utilice frases y combinaciones de letras y números
- Nunca deje abierta su sesión de trabajo
- Capacítese y capacite a su personal constantemente

Preguntas