1º Reunión: CICLO DE CAPACITACIÓN Y CONCIENTIZACIÓN EN CIBERSEGURIDAD DOCUMENTAL. CPCECABA, CABA, 2017.

Introducción a la seguridad de la información en los registros contables.

Diego Sebastian Escobar.

Cita:

Diego Sebastian Escobar (Mayo, 2017). *Introducción a la seguridad de la información en los registros contables. 1º Reunión: CICLO DE CAPACITACIÓN Y CONCIENTIZACIÓN EN CIBERSEGURIDAD DOCUMENTAL. CPCECABA, CABA.*

Dirección estable: https://www.aacademica.org/escobards/6

ARK: https://n2t.net/ark:/13683/ptuD/t5b

CICLO DE CAPACITACIÓN Y CONCIENTIZACIÓN EN CIBERSEGURIDAD DOCUMENTAL

1º Reunión: Introducción a la seguridad de la información en los registros contables.

Exposición

Dr. C.P. y L.A. Diego Sebastián Escobar

Coordinación

Dra. C.P. Silvia Gladys Iglesias

consejo
Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires

Introducción a la problemática de la información digital

Documentos Digitales

Problemas

Cómo determinar al autor

Fácilmente alterable

Puede ser objeto de repudio

No permite reemplazar al papel en todas sus formas.

Principios de la Seguridad de la Información

Integridad

- La integridad de la información es la característica que hace que su contenido permanezca inalterado, a menos que sea modificado por personal autorizado.

Disponibilidad

- La disponibilidad de la información es su capacidad de estar siempre disponible en el momento que la necesiten, para ser procesada por las personas autorizadas.

Confidencialidad

- La confidencialidad de la información es la necesidad de que sólo tenga acceso a ésta personas autorizadas.

Incidentes de seguridad de la información

Incidente

Cualquier evento que afecte la disponibilidad, integridad y/o confidencialidad de la información

	INTERNO	EXTERNO
Malicioso	*Un empleado enojado destruye un documento importante.*	*Un atacante realiza un ataque de denegación de servicio contra el sitio web de la organización.*
Involuntario	*Un empleado pierde un dispositivo USB donde había copiado información confidencial de la empresa.*	*Un exceso de visitas a un sitio web hace que este deje de funcionar y se pierda la disponibilidad.*

Amenazas que acechan la seguridad de la información.

Fraudes a través de engaños y robo de información

A – Fraude a través de "Ingeniería Social"

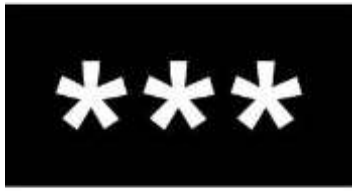
Ingeniería Social

Utilización de habilidades sociales para manipular el accionar de una persona

Distintos medios para engañar y comprometer la seguridad de la empresa

Correos falsos

Llamados telefónicos falsos



Códigos maliciosos

¿Qué debo hacer?

B - Robo de información

Uno de los mayores problemas en una organización

Robo de información sensible

Incidente generado por

- ✗ Un mal accionar de las personas
- ✗ Una acción maliciosa

Se puede dar a través de

- ✓ Medios digitales

- ✓ Material físico

¿Qué debo hacer?

B - Robo de información

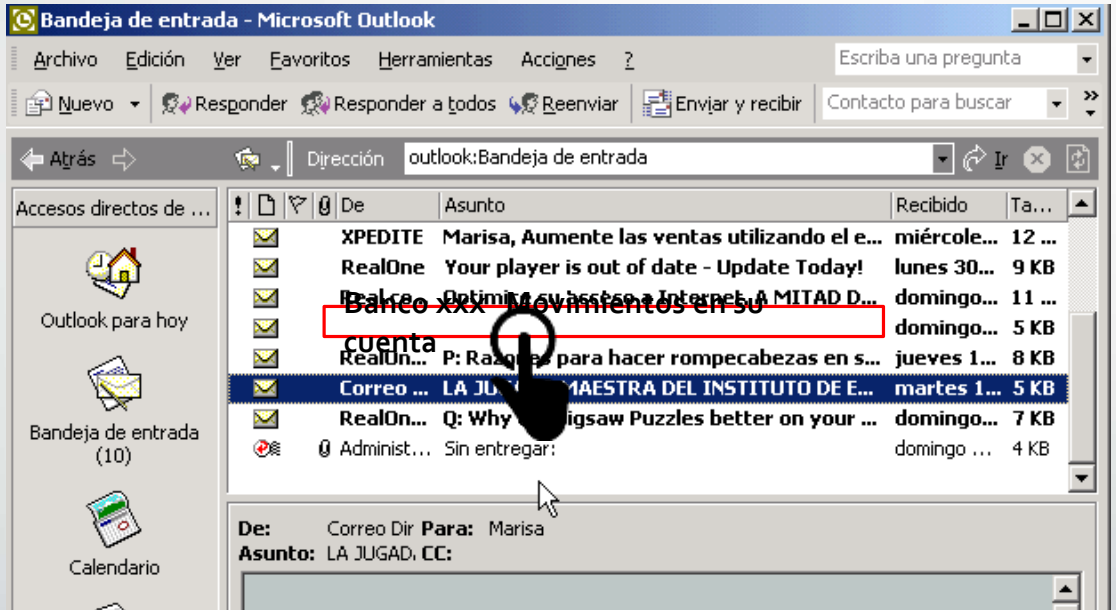
El peligroso juego que roba datos personales en Facebook

Se trata de "¿A qué famoso te pareces?" de la aplicación Vonvon. El mismo utiliza información del perfil de los usuarios para propósitos de marketing, que no explica antes de ser utilizado.

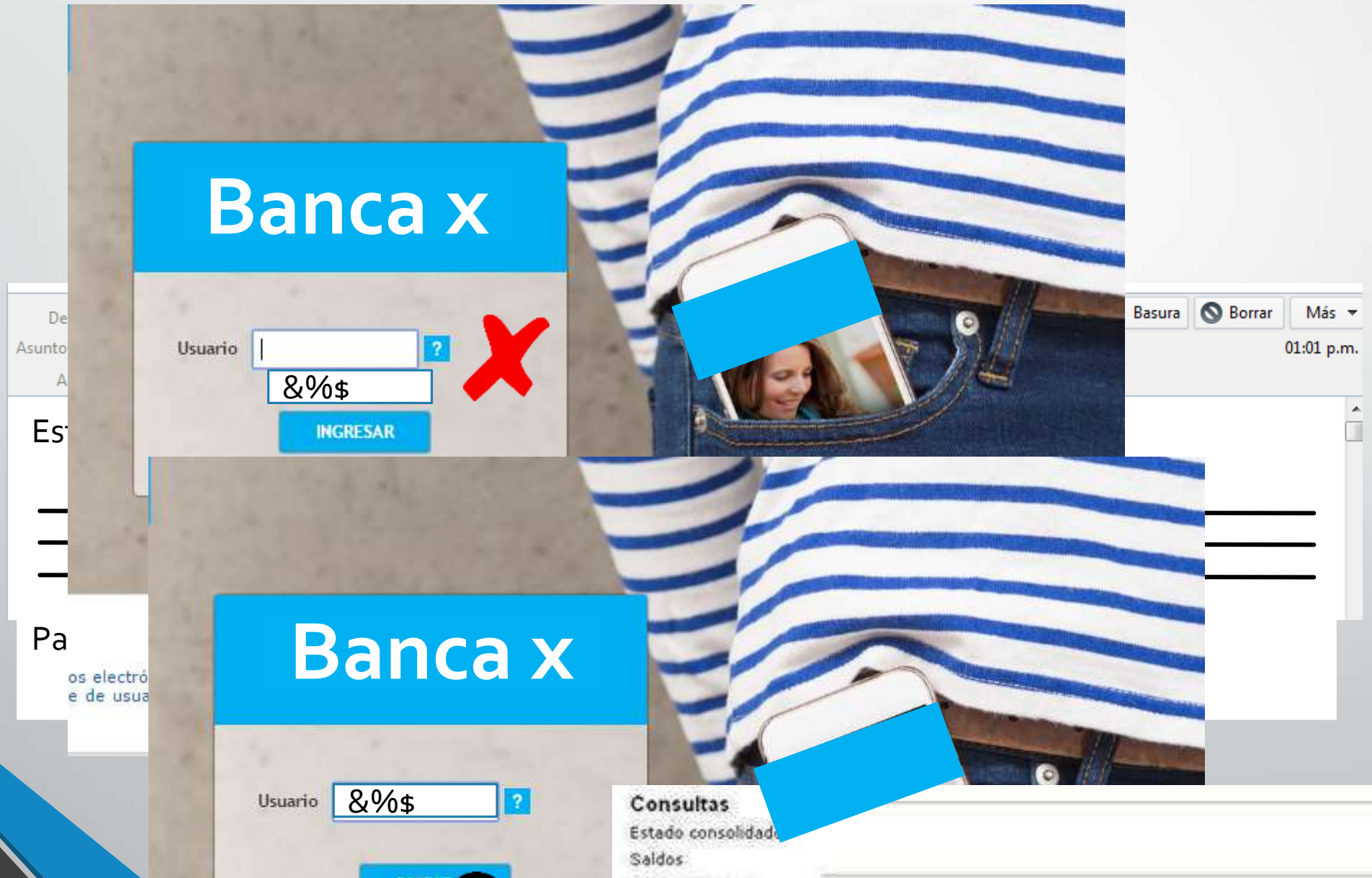
C - Phishing

Phishing

Busca obtener usuarios y claves de acceso a sitios con información sensible



C – Phishing: Captura de Credenciales a través de Correos Electrónicos



C – Phishing: Captura de Credenciales a través de Correos Electrónicos

De **Banco xxx**
Asunto Movimientos en su
A Yo

Archivar | Basura | Borrar | Más
01:01 p.m.

El correo electrónico no fue enviado por nuestro banco

Estimado:

Para verificar sus datos, haga clic aquí: http://www.bancoxxx.com

No brindó un canal seguro (https://)

Prestar atención a esos "detalles importantes"

D – Vishing y Smishing

Vishing

El Vishing es una práctica criminal fraudulenta en la cual se hace uso del servicio de telefonía y la ingeniería social para engañar personas y obtener información financiera o información útil para el robo de identidad

Smishing

El Smishing es similar pero en este caso lo que nos llega es un mensaje de texto mediante el cual se nos invita a enviar nuestro usuario y clave para validar una falsa información.

Amenazas que acechan la seguridad de la información.

Malware

E - Malware

Virus informáticos → No son la única amenaza existente

Nuevas variantes

↓

"Malware" o "Código Malicioso"

↓

Categoría que engloba todos los tipos de códigos informáticos maliciosos

Finalidad

↓

Causar un daño al software o hardware de nuestro equipo informático

↓

- ✓ Modificar información
- ✓ Destruir información
- ✓ Robar información

E - Malware – Caso Telefónica

Clarín | Tecnología

12/05/2017 - 11:01 | Clarin.com | Tecnología

Seguridad informática

Ransomware: qué es y cómo se propaga el virus que atacó a Telefónica

Este software malicioso tiene la capacidad de camuflarse dentro de archivos adjuntos o videos de sitios de dudoso origen.

Ransomware: el ciberataque masivo llegó ahora a China, Japón, Indonesia y Tailandia

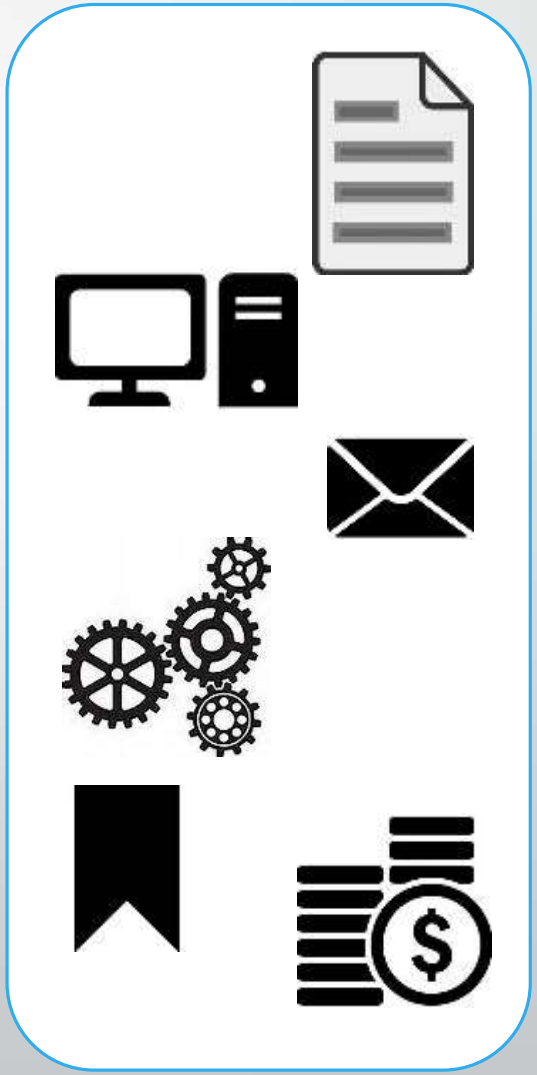
En la segunda oleada, el virus que infecta computadores y roba información de todo el mundo golpeó Asia

El ciberataque a nivel internacional que se produjo el viernes pasado afectó enChina durante el fin de semana a unas 30.000 organizaciones y empresas.

E - Malware

Efectos de los códigos maliciosos

- ✓ Causar daño al Hardware o Software
- ✓ Alterar y causar pérdida de información
- ✓ Afectar la disponibilidad de sistemas y servicios
- ✓ Afectar la productividad
- ✓ Afectar la imagen de una organización o de una persona
- ✓ Causar pérdidas económicas



E - Malware

Aspectos en común

- ✓ Tienen una técnica para infectar un sistema informático y ocultarse
- ✓ Tienen como objetivo determinados tipos de archivos
- ✓ Atacan a un sistema informático particular

E - Malware

Virus

- ✓ Está oculto dentro de otro archivo ejecutable útil e inofensivo
- ✓ Requiere que el usuario lo ejecute para desplegar su rutina maliciosa

Gusano

- ✓ No requiere de ningún archivo ejecutable que lo contenga o lo porte, existe en sí mismo y es autónomo.
- ✓ Infectan sistemas y se reproducen muy velozmente

Troyano

- ✓ Se esconde dentro de un programa útil para el usuario, pero oculta las peores intenciones

E - Malware

Keyloggers

- ✓ Permite registrar todas las pulsaciones que un usuario haga sobre el teclado de un equipo infectado y documentarlas en un archivo para su posterior lectura

Hoaxes

- ✓ Son engaños que llevan al usuario a creer que está infectado con un virus, cuando en realidad están haciendo referencia a un archivo crítico para el funcionamiento del sistema operativo
- ✓ Le piden al usuario que lo elimine, causándole un daño irreparable al sistema que lleva a la pérdida de información

Botnets o Redes Robots

- ✓ Estas redes se utilizan para robar información, atacar la disponibilidad de grandes sistemas y enviar cantidades industriales de spam

Amenazas que acechan la seguridad de la información.

Robo, rotura o pérdida de los soportes

Cuidado de la información almacenada en dispositivos móviles

Permiten el acceso a la información en todo momento

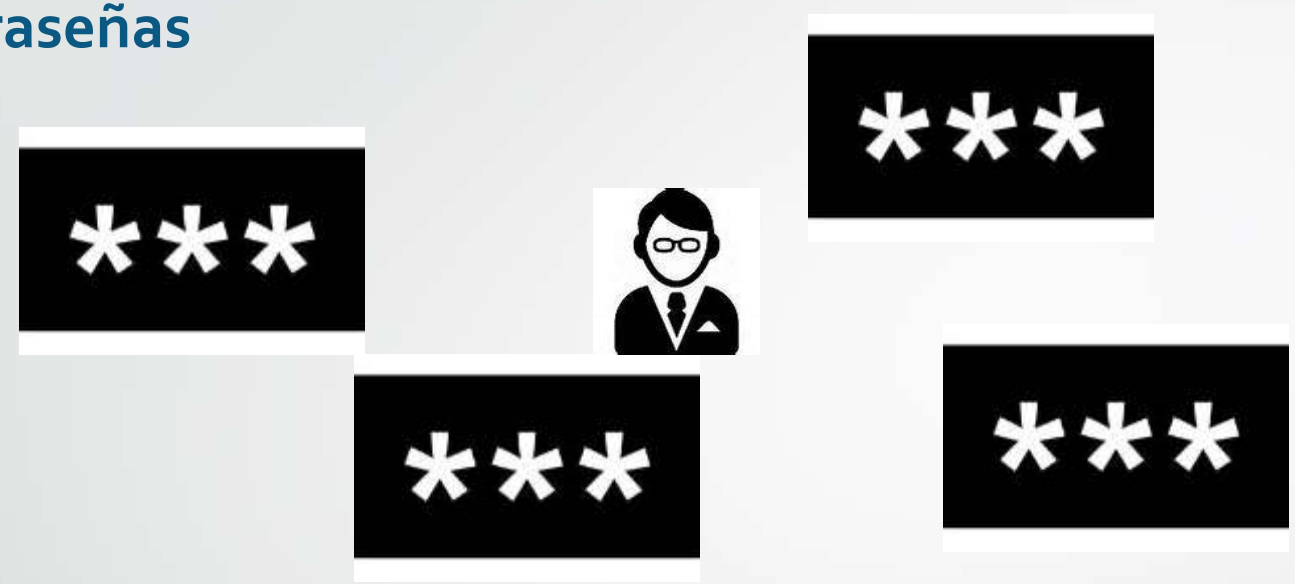
¿Qué pasa si se pierde o es robado el teléfono de la empresa?

Debemos ser proactivos y disminuir el impacto/riesgo.

¿Qué debo hacer?

Recomendaciones

Recomendaciones para la selección de contraseñas



Una **contraseña débil** puede significar el acceso a información confidencial o a un sistema por parte de un atacante o un código malicioso

Las contraseñas deben ser:
- ✓ Fuertes
- ✓ Fáciles de recordar
- ✓ Difíciles de descifrar

Recomendaciones de seguridad en el uso del correo electrónico

Correo electrónico corporativo

Se utiliza como fuente de comunicación de la empresa

Se debe evitar su exposición en Internet

La exposición de nuestra dirección de correo electrónico en internet aumenta la posibilidad de:

- ✓ Un ataque de *phishing*
- ✓ Un aumento de correo no deseado

Correos de origen dudoso

Los datos pueden ser enviados al atacante

¿Qué debo hacer?

Recomendaciones sobre manipulación de documentación fuera del lugar de trabajo

Muchos empleados se llevan el trabajo al hogar

El equipo desde el que se trabaje puede encontrarse expuesto en una red que no está debidamente controlada

Tomar medidas

- ✓ Contar con un software antivirus
- ✓ Tener el sistema operativo actualizado al día de la fecha
- ✓ Respetar las políticas de seguridad de la organización
- ✓ Cuando se lleva documentación y papeles de importancia, tener cuidado en lo que respecta al robo, hurto o extravío de los mismos en lugares públicos o en el hogar
- ✓ Manipular los documentos teniendo en cuenta el nivel de confidencialidad que requieren
- ✓ Al utilizarse dispositivos de almacenamiento USB o memorias, realizar un análisis con un antivirus

Malware – ¿Cómo Prevenirnos?

- No descargar contenido multimedia de las redes P2P

- No ingresar a sitios Web no confiables o no permitidos por la organización

- Mantener el antivirus actualizado

Malware – ¿Cómo Prevenirnos?

- No ejecutar archivos adjuntos de procedencia dudosa o desconocida.
- No hacer clic en enlaces, a menos que sepamos con certeza a dónde llevan.
- No insertar dispositivos de almacenamiento (CD's, DVD's, pendrives, celulares, etc) de origen desconocido en la PC
- No instalar software que no esté aprobado por la organización

Buenas prácticas

INFORMACIÓN PERSONAL	Evitar compartir información con personas no autorizadas a acceder a la misma
ACCESO A SITIOS DE DUDOSA REPUTACIÓN	Evitar el acceso a sitios de dudosa reputación
CONTRASEÑAS ROBUSTAS	Utilizar contraseñas fuertes
DESCARGA DE APLICACIONES NO CONOCIDAS	Evitar la descarga de aplicaciones no conocidas que podrían ser *malware*
ACCESO A SITIOS DUDOSOS	Evitar el ingreso de información en sitios dudosos que podrían implementar un ataque de *phishing*
REPORTAR INCIDENTE DE SEGURIDAD	Reportar cualquier sospecha de un incidente de seguridad para la organización

Buenas prácticas desde la perspectiva del empleado

POLÍTICAS DE SEGURIDAD	Leer y respetar las políticas de seguridad de la empresa
BLOQUEO DE SESIÓN DISPOSITIVOS CORPORATIVOS	Bloquear la sesión cuando se abandona el puesto de trabajo
DESTRUIR DOCUMENTOS	Destruir documentos impresos sensibles antes de arrojarlos a la basura.
NO DIVULGACIÓN DE CONTRASEÑAS	No compartir contraseñas personales y laborales.

Conclusión

Proteger la información confidencial de la organización = Proteger el negocio

Utilización de las tecnologías para la seguridad
+
Educación de los usuarios

Proteger los activos de información del negocio

Cualquier incidente de seguridad podría impactar
- ✓ En la imagen de la organización
- ✓ En la confianza de los clientes
- ✓ En la continuidad del negocio
- ✓ En incumplimiento de normativas legales/regulatorias

La **seguridad corporativa** otorga un valor agregado

¡Muchas gracias!