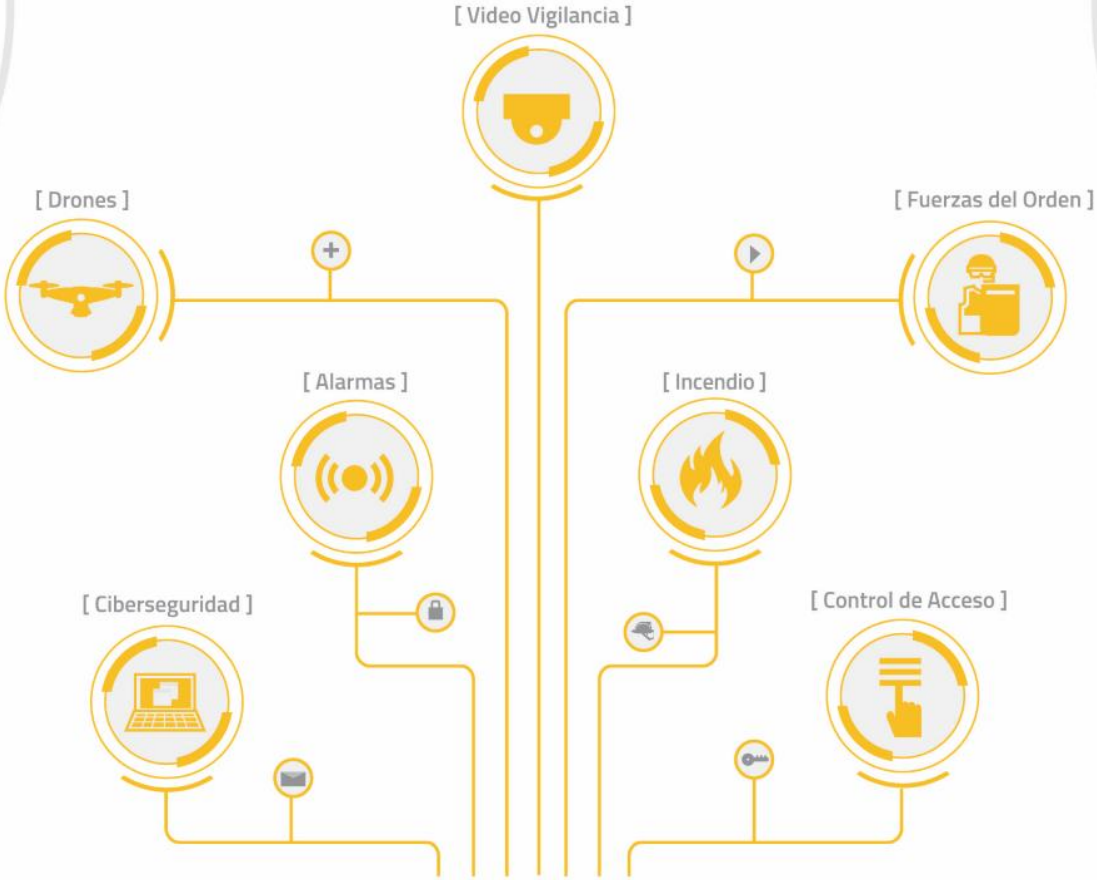


EXPO SEGURIDAD MÉXICO

7– 9 MAYO 2019

Ciudad de México

Centro Citibanamex

Patrocinadores Corporativos

AXIS COMMUNICATIONS

Hanwha Techwin

Powered by

ISC

Patrocinadores Fundadores

MAGOCAD

SYSCOM

Organizado por

Reed Exhibitions

La seguridad física y digital

¿Primas, hermanas, amigas o enemigas?

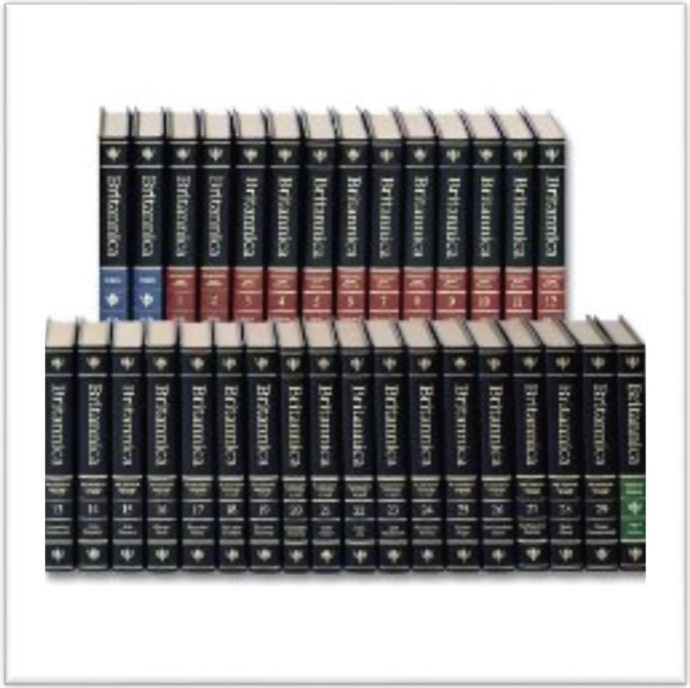
Juan Carlos Carrillo

@juan_carrillo

EXPO SEGURIDAD MÉXICO

Casandra

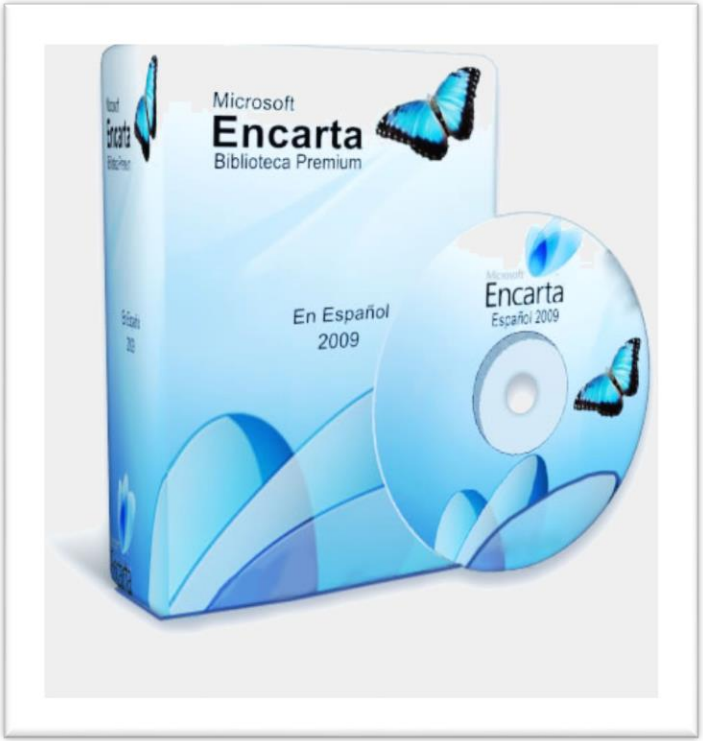
Físico vs Digital



En 1990, las ventas de la enciclopedia Britannica logro el record de ventas…

$650 millones de dólares

Físico vs Digital



- Una Enciclopedia *Britannica* se vendía desde $1,500 y hasta en $2,200 USD

- Una enciclopedia en CD-ROM se vendía desde $50 y hasta $70 USD

El cambio de paradigma

Robo físico

Robo digital

US largest card incident hacker has track record says Miami Herald

21 August 2009

As the fall-out in the Albert Gonzalez credit card hacking case - in which the card hacker was charged earlier this week with gaining unauthorized access to 130 million people's card details from major ...rchants - continues, the Miami Herald

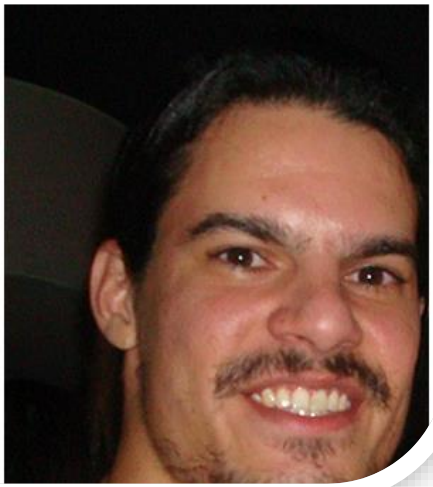
posts tagged 'Albert Gonzalez'

In Surprise Appeal, TJX Hacker Claims U.S. Authorized His Crimes

By Kim Zetter ✉ April 7, 2011 | 4:07 pm | Categories: Breaches, Hacks and Cracks, The Courts

Albert Gonzalez, the hacker who masterminded the largest credit card heists in U.S. history, is asking a federal judge to throw out his earlier guilty pleas and lift his record-breaking 20-year prison sentence, on allegations that the government authorized his years-long crime spree.

Gonzalez, 29, admitted last year that he and accomplices hacked into TJX, Office Max, Dave & Busters, Heartland Payment Systems and other companies to steal more than 130 million credit and debit card numbers, in what the government deemed the biggest computer crime case ever prosecuted in the United States. He's currently serving time at the Milan low-security federal prison in southeastern Michigan, with a release date in the year 2025.



EXPO SEGURIDAD MÉXICO

*La nueva **economia** de seguridad*

Crimen global en perspectiva

$56B
Mercado de robo de autos

$30B
Robo de Smartphones

$114B
Mercado de robo de tarjetas de credito

$85B
Mercado de cocaina

$400 Billones
Mercado global de cibercrimen

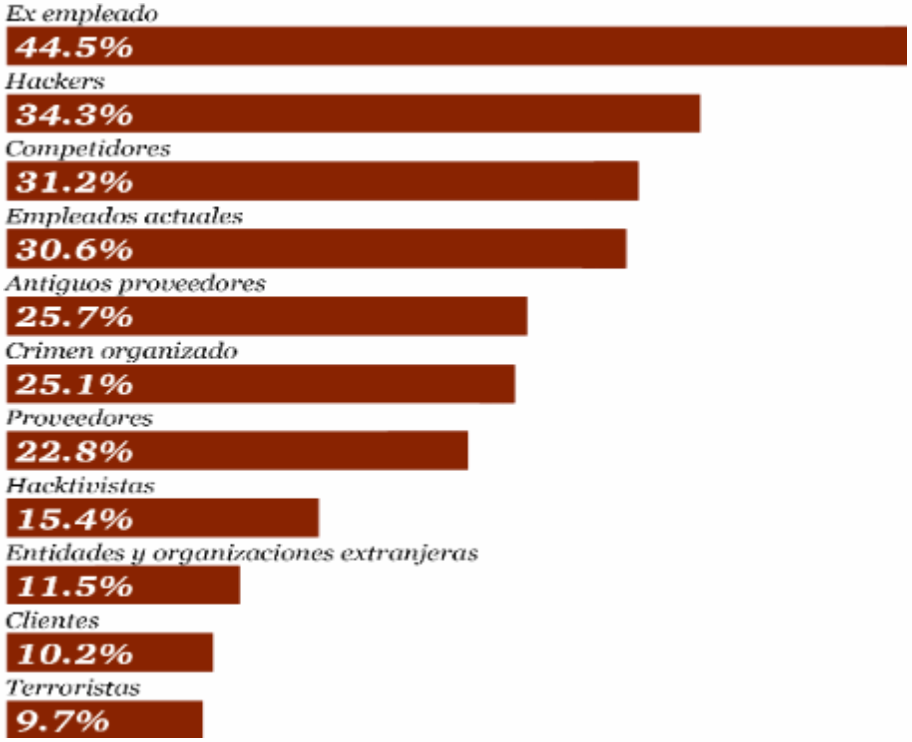
La principal fuente de los incidentes de seguridad es interno

En México

44%

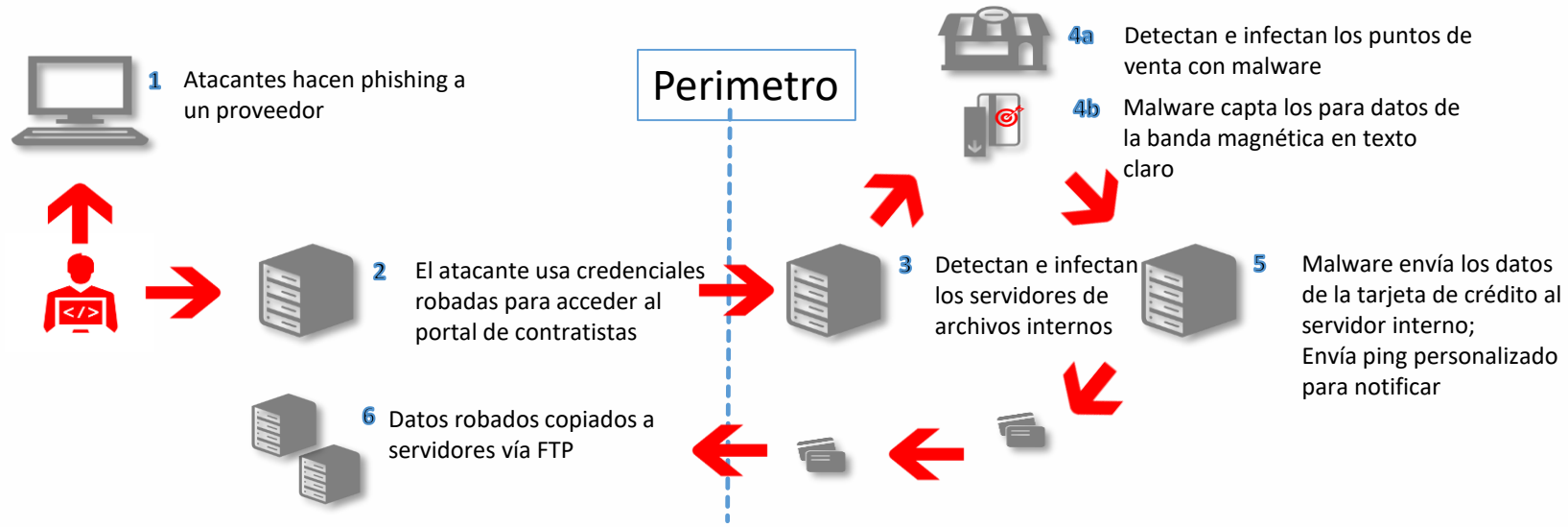
atribuyen estos incidentes a ex empleados

La principal fuente de incidentes de seguridad a **nivel global** se debe a empleados actuales

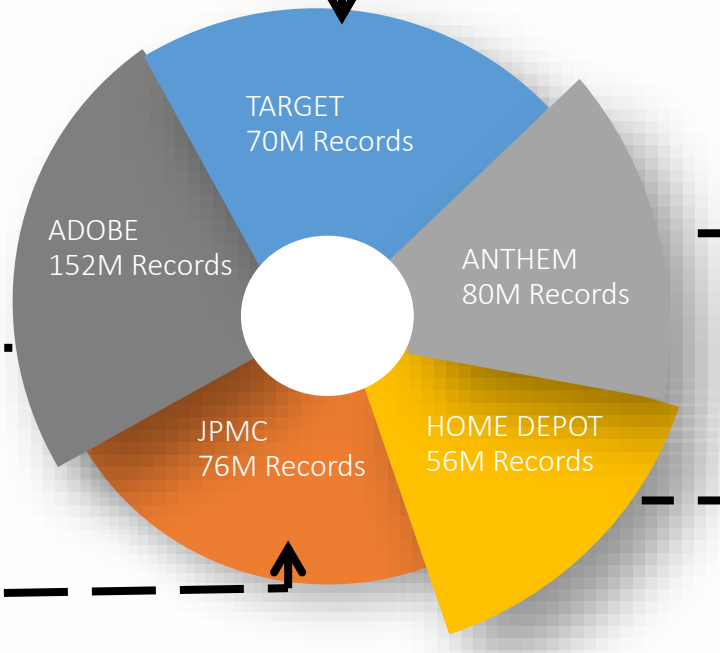


Anatomía de una
Fuga de información

110 millones de clientes afectados



¿Dónde estaban los errores?



Passwords por Default

Solución

Cambio de contraseña
Cada trimestre
Política de contraseñas
Seguras

Datos no cifrados

Solución

Cifrado del sistema
De archivos
Cifrado de las
Bases de datos

Credenciales Robadas

Solución

Autenticación de
Múltiples factores
Detección de fraude web

Passwords débiles

Solución

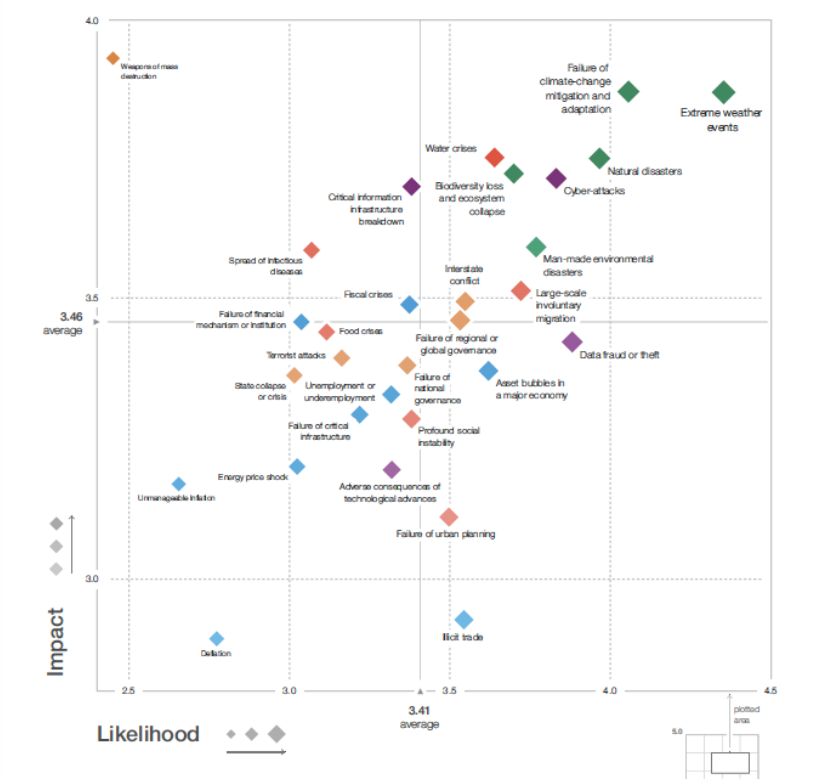
Autenticación de
Múltiples factores
Configuración y
Parches automatizados

Servidores no parchados

Solución

Autenticación de
Múltiples factores
Configuración y
Parches automatizados

EXPO SEGURIDAD MÉXICO



WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

The Global Risks Report 2019

14th Edition

Top 10 risks in terms of
Likelihood

1. Extreme weather events
2. Failure of climate-change mitigation and adaptation
3. Natural disasters
4. Data fraud or theft
5. Cyber-attacks
6. Man-made environmental disasters
7. Large-scale involuntary migration
8. Biodiversity loss and ecosystem collapse
9. Water crises
10. Asset bubbles in a major economy

Top 10 risks in terms of
Impact

1. Weapons of mass destruction
2. Failure of climate-change mitigation and adaptation
3. Extreme weather events
4. Water crises
5. Natural disasters
6. Biodiversity loss and ecosystem collapse
7. Cyber-attacks
8. Critical information infrastructure breakdown
9. Man-made environmental disasters
10. Spread of infectious diseases

Categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Source: World Economic Forum Global Risks Perception Survey 2018–2019.
Note: Survey respondents were asked to assess the likelihood of the individual global risk on a scale of 1 to 5, 1 representing a risk that is very unlikely to happen and 5 a risk that is very likely to occur. They also assess the impact on each global risk on a scale of 1 to 5 (1: minimal impact, 2: minor impact, 3: moderate impact, 4: severe impact and 5: catastrophic impact). See Appendix B for more details. To ensure legibility, the names of the global risks are abbreviated; see Appendix A for the full name and description.

EXPO SEGURIDAD MÉXICO

Top 5 Global Risks in Terms of Likelihood

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
1st	Asset price collapse	Asset price collapse	Storms and cyclones	Severe income disparity	Severe income disparity	Income disparity	Interstate conflict with regional consequences	Large-scale involuntary migration	Extreme weather events	Extreme weather events	Extreme weather events
2nd	Slowing Chinese economy (<8%)	Slowing Chinese economy (<8%)	Flooding	Chronic fiscal imbalances	Chronic fiscal imbalances	Extreme weather events	Extreme weather events	Extreme weather events	Large-scale involuntary migration	Natural disasters	Failure of climate-change mitigation and adaptation
3rd	Chronic disease	Chronic disease	Corruption	Rising greenhouse gas emissions	Rising greenhouse gas emissions	Unemployment and underemployment	Failure of national governance	Failure of climate-change mitigation and adaptation	Major natural disasters	Cyber-attacks	Natural disasters
4th	Global governance gaps	Fiscal crises	Biodiversity loss	Cyber-attacks	Water supply crises	Climate change	State collapse or crisis	Interstate conflict with regional consequences	Large-scale terrorist attacks	Data fraud or theft	Data fraud or theft
5th	Retrenchment from globalization	Global governance gaps	Climate change	Water supply crises	Mismanagement of population	Cyber-attacks	High structural unemployment or underemployment	Major natural catastrophes	Massive incident of data fraud/theft	Failure of climate-change mitigation and adaptation	Cyber-attacks

Los ciber ataques como probabilidad de riesgo

EXPO SEGURIDAD

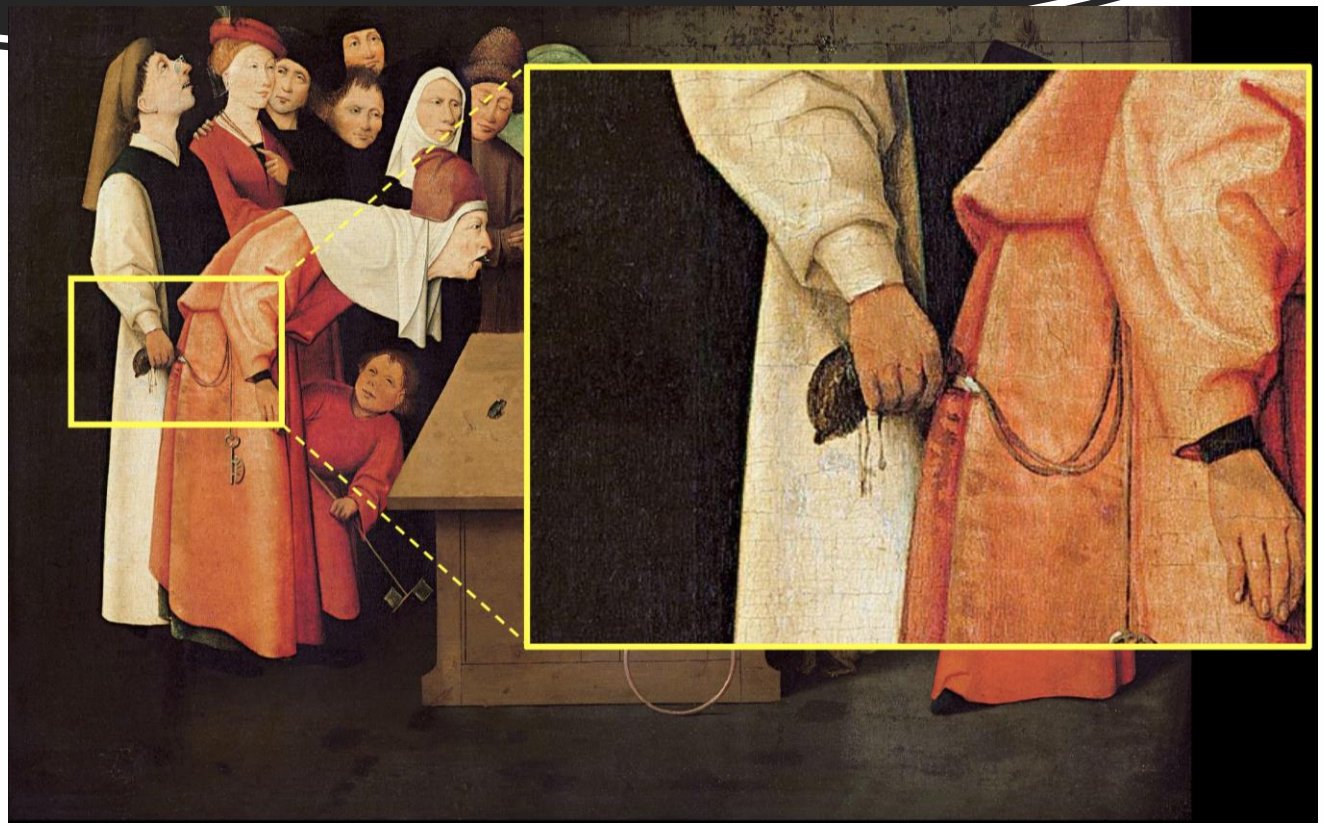
¿Puedes confiar en lo que “ves”?

EXPO SEGURIDAD

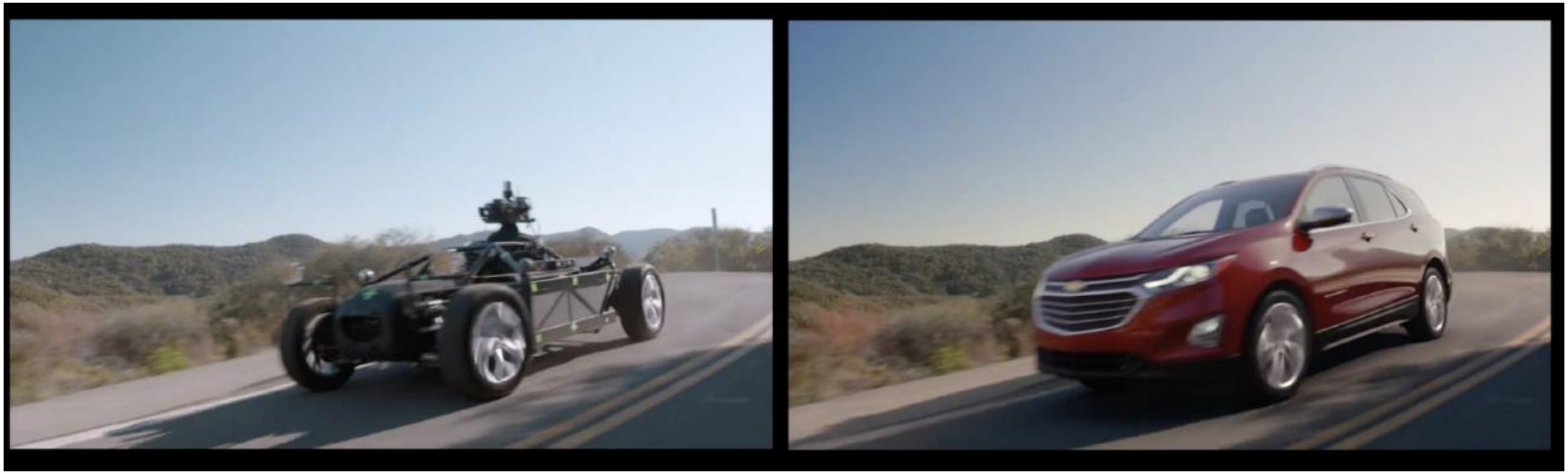
¿Puedes confiar en lo que “ves”?

La ilusión de lo que vemos NO es nueva

Ni la ilusión es nueva, ni los actores maliciosos



¿Qué es lo que estas “viendo”?




The Future
NEXT EXIT

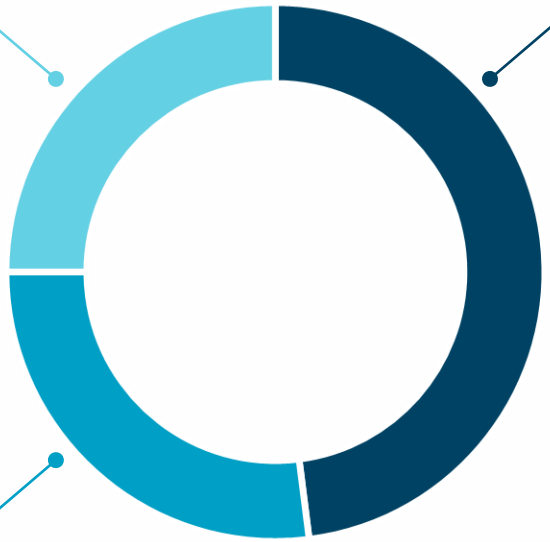
IBM Security

2018 Cost of a Data Breach Study: Benchmark research

https://www.ibm.com/security/data-breach

IBM

Causas de violaciones de datos



27%
Error Humano

48%
Ataque criminal

Fallas de los procesos del negocio

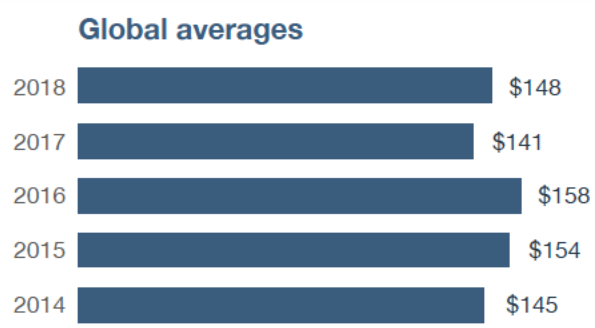
25%

Ponemon INSTITUTE

IBM

El costo de las fugas de información es cada vez mayor

- En promedio el costo de una brecha se incremento un 6.4%
- El costo por dato extraviado se incremento en un 4.8%
- El promedio de las bases de datos afectadas se incremento en un 2.2%



Ponemon INSTITUTE

IBM

Cuanto más rápido se pueda identificar y contener una violación de datos, más bajos es el costo

Por 4º año consecutivo, vemos la relación entre la rapidez con la que una organización puede identificar y contener los incidentes de violación de datos y las consecuencias financieras.

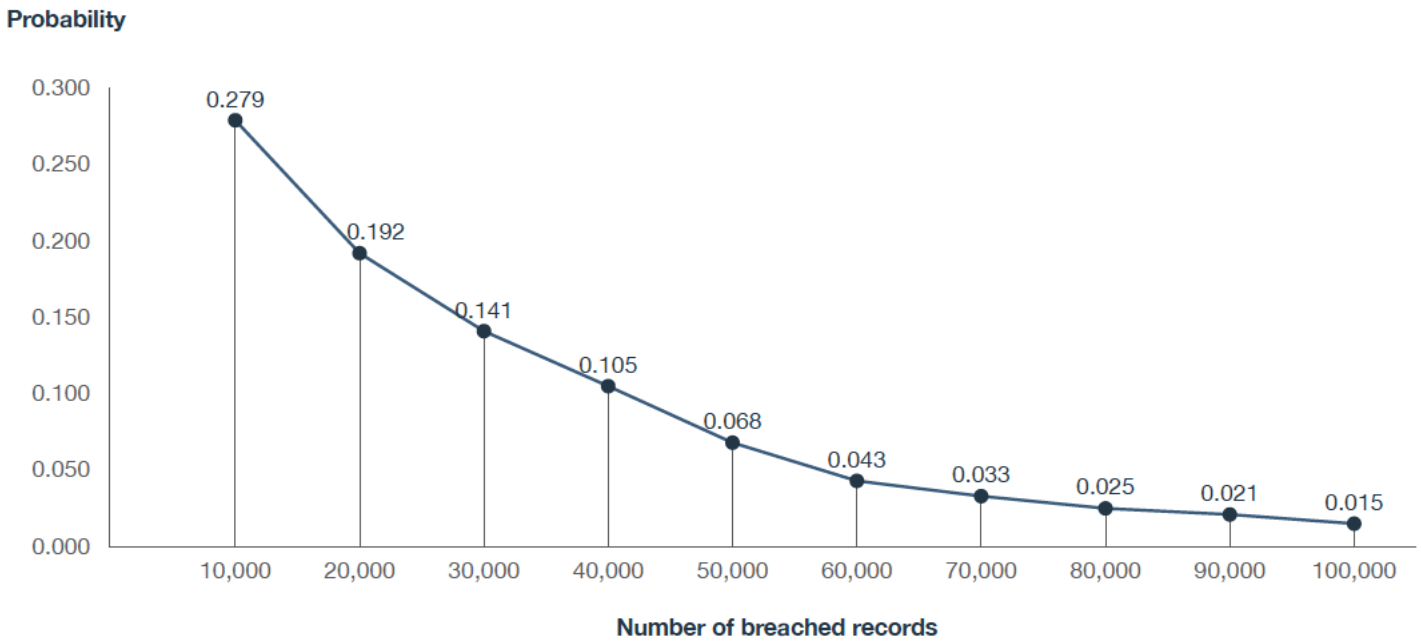
El tiempo promedio para identificar una brecha (MTTI) es de 197 días, y el tiempo promedio para contener (MTTC) es de 69 días.

El tiempo de identificación como el de contención es más alto para ataques maliciosos y criminales; y mucho más bajos para las brechas de datos causadas por un error humano.

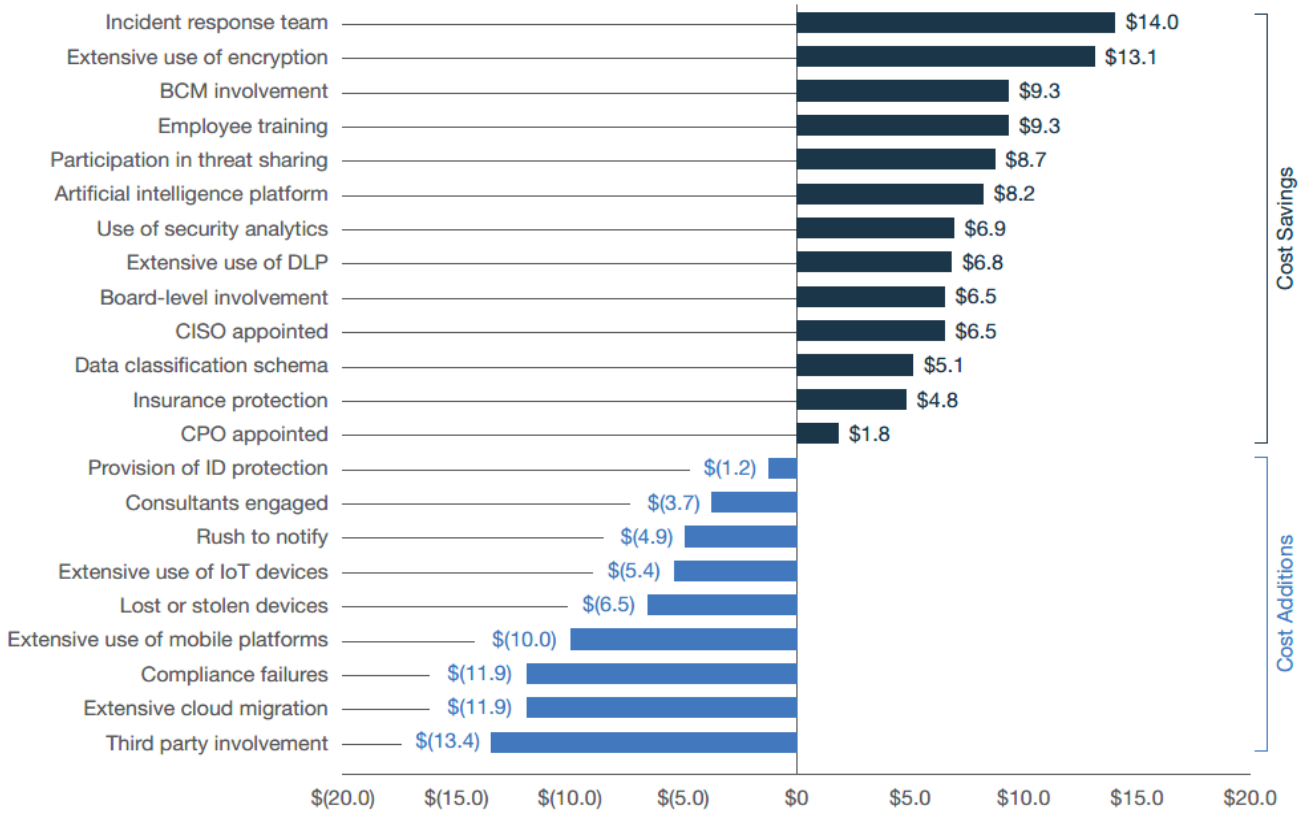
Las compañías que identifican una brecha en menos de 100 días ahorraron más de $1 millón de USD en comparación con las que tardan más de 100 días.

Las empresas que contienen una brecha en menos de 30 días gastan $1 millón de USD menos que aquellas que tardan más de 30 días en resolverse.

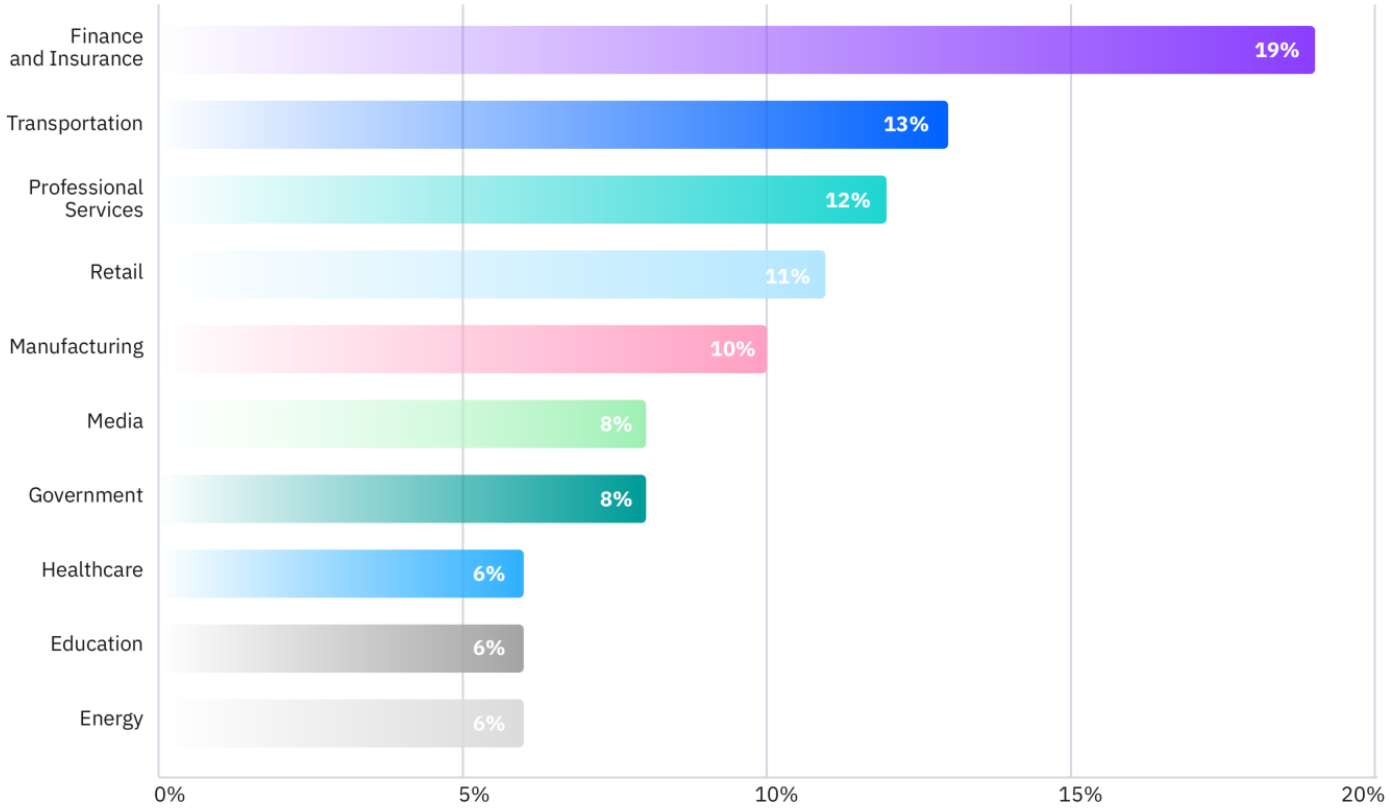
Cuanto más grande es la brecha, menor posibilidad de quela organización tenga otra brecha en los próximos 24 meses



Factores que tienen impacto en el costo



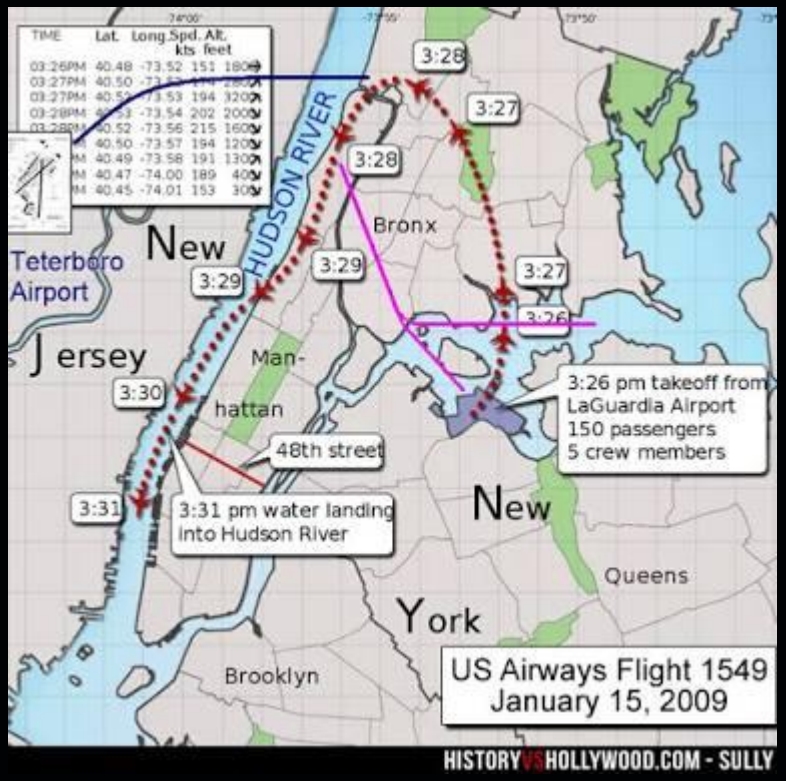
Industrias atacadas frecuentemente



No fracasa el que sufre un ataque de seguridad, es parte del juego, fracasas si no tienes capacidad de respuesta

- Charles Blauner
  - CISO, Citigroup

Sully y la respuesta a incidentes



- Sully, al momento del incidente tenia 58 años, 19,663 horas de vuelo
- Su copiloto tenia 49 años, 15,643 horas de vuelo
- Las 3 azafatas tenían 38, 28 y 26 años de experiencia
- Todos recibían su capacitación anual para emergencias

6 pasos para fortalecer el plan de respuesta a incidentes

Obtener apoyo de la alta dirección

- Un plan de respuesta a incidentes no solo se aplica a TI y seguridad.

Conocer los riesgos

- Conocer el impacto para la organización, como la interrupciones en la producción, productos defectuosos o brechas de terceros.

Definir roles y responsabilidades

- Todos deben conocer su responsabilidad en caso de un incidente de seguridad.
- Definir un grupo predefinido de especialistas en respuesta, conocido como equipo de respuesta a incidentes de seguridad informática (CSIRT).
- Además de los expertos en seguridad, este equipo debe incluir representantes de la administración y otras unidades de negocios.

Determinar los canales de comunicación

- Definir los canales de comunicación relevantes.
- Establecer pautas sobre qué detalles deben comunicarse a TI, la administración superior, los departamentos relevantes, los clientes afectados y el público.

Reglas de compromiso

- Los pasos de respuesta a incidentes deben seguir una estructura y metodología claras, como el marco de respuesta a incidentes de 6 pasos de SANS.

Entrenar el Plan

- Realizar ejercicios de mesa y los libros de ejecución.
- Realizar un simulacro regular del flujo de respuesta.
- Unirse a grupos de discusión y compartir prácticas exitosas con otros equipos.

https://www.securitylearningacademy.com

Most Visited | Elevate It | Mail | IBM WebEx | Key Tools and Links | IBM Press Releases | Bluemine | GDPR Sales | My Career Tools | Interview The IBM ... | X-Force Exchange

IBM Security **Learning Academy**

Prepare to outthink security threats

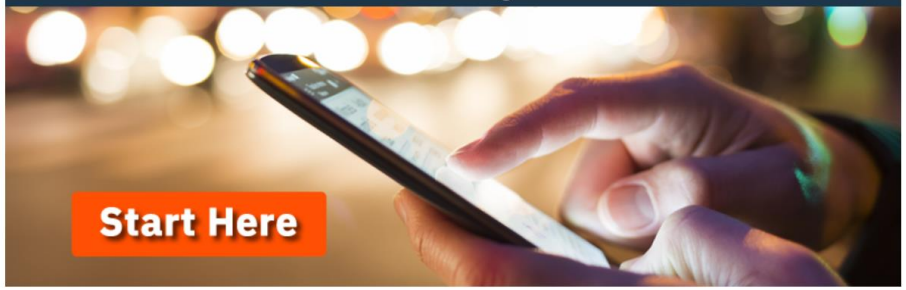
Join the IBM Security Client Success group on LinkedIn

Hear from IBM Security Support executives
Get the latest Support resources, and more

Join the group!

View our Complete Catalog

New to the Academy? Learn how to navigate here!



Learn About Translated Courses

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Juan Carlos Carrillo

T:+52 1 55 3106 7035

@juan_carrillo

IBM