

Carla Pérez Gavilán Del Castillo, A01023033

Prof. Ariel Lucién García

Introducción a Ingeniería en Tecnologías Computacionales

3 de octubre de 2018

### **Deloitte: Ciberseguridad**

En la actualidad la ciberseguridad es quizá una de los temas más alarmantes de las Tecnologías de la Información. Con muchas de las empresas siendo digitalizadas o automatizadas, no solo surgen los beneficios de mayor eficiencia o conectividad sino también el peligro de que un ciberataque pueda llegar a ser mucho más extenso y alcance a partes fundamentales de la empresa. Con este creciente riesgo, ha incrementado a la par la demanda de profesionistas que sepan de este tema, y puedan tomar medidas preventivas y reactivas a la misma. Deloitte como respuesta a esta amenaza ha construido un grupo de hackers que sea capaz de evaluar la seguridad de las empresas que los contratan e implementar medidas de seguridad para prevenir otros ataques. Tales como el cyber hunting o los hackeos de prueba (red team operations).

La ciberseguridad, muchas veces se subestima o prescinde de considerarla, por no ser un tema que ha adquirido importancia de manera inmediata. Con ataques al SPEI (Sistema Bancario Mexicano), a aerolíneas (como United Airlines), a la industria agropecuario, entre otras. Hoy en día las industrias manufactureras, aérea, automovilística e incluso la médica están entre las más susceptibles a ataques. Esto se debe a que han implementado nuevas tecnologías que a su vez han tenido un crecimiento acelerado: entre estas El Internet de las Cosas (*Internet of Things*), nanotecnología, biología digital, entre otras.

Los ciberataques hoy en día pueden no solo poner el riesgo la información sino que han tomado formas nuevas que pueden poner en riesgo la vida de muchas personas. Los ataques varían desde la ingeniería social con phishing (utilización de correos electrónicos para obtener contraseñas) a ransomware (pago por información retenida). Como medida preventiva las organizaciones han dispuesto de un CISO (Cyber Security Officer) que es un puesto dentro de la empresa que se encarga particularmente de prevenir y corroborar que la empresa esté preparada para sobrellevar este tipo de ataques.

Como profesionista de las Tecnologías de la Información la demanda por profesionistas competentes, llama a que exploremos y consideramos la ciberseguridad como una posible área de estudio. Hay mucho que desarrollar en esta área y su crecimiento exponencial llamará a gente preparada para enfrentar los nuevos retos que presente.

## OTRAS NOTAS:

- consultoría
- spei: ataque interbancario
  - la industria del cibercrimen: creciente
- ransomware:
- internet of things
- nanotecnología
- biología digital
- producción y control ubicuos
  - en controladores.
- manufactura de autos y de aviones
  - industria médica
    - vuelo de united
- información es protegida y/o definida contr al daño
- cyber threat hunting
  - sensores
- red team operations
  - cio
    - patrocinados por estado
      - profesionales
- presencia sin ser vistos
- manual canal
  - consejo de administración
- World Economic Forum: Suiza
- movimientos laterales
  - CNBV→
    - robo identidad
    - Ingeniería social: phishing, baiting, vishing, DD.
    - ransomware
    - robo de información
- eCrime
  - hacktivismo
- awareness, organizational goal, plan and roadmap
  - retail
  - ciencias de la salud
  - consumo/manufacturera
  - telecomunicaciones y transporte
  - comercio electrónica y pagos en línea
  - medios en línea
  - alta tecnología
- banco de chile
  - seguro: controles

- vigilante: ciberinteligencia, monitoreo
    - seguridad reactiva
    - seguridad preventiva
  - resiliente:
    - respuesta a los ciberataques
- Cyber Security Framework (CSF)
  - CISO: figura más demandada
    - Policía de la empresa
- control lord
- AML
- Ley de la prevención cibernética