POLI
POLITÉCNICO GRANCOLOMBIANO
INSTITUCIÓN UNIVERSITARIA

CYBERSECURITY DAYS

Del **24** al **26** de octubre de **2018**

La información es un arma muy poderosa, que no caiga en manos equivocadas.

Ciberseguridad, muchos enfoques y dudas por resolver

Jeffrey Steve Borbón Sanabria MsC.
Tutor virtual Politécnico Grancolombiano
2018

Algunas definiciones de Ciberseguridad

NIST:

“The ability to protect or defend the use of cyberspace from cyber attacks”

ISO:

“protection of privacy, integrity, and accessibility of data information in the Cyberspace”

ISACA:

“The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems”

GARTNER:

“Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries.”

Algunas definiciones de Ciberseguridad

ENISA:

“Cybersecurity covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents. Considering the different types of components of the cyber space.”

Ciberespacio

Ciberataques

Ciber….

Aquí aparecen las dudas

- ¿No es la misma seguridad de la información?
- ¿Y por ciberespacio a qué nos referimos?
- ¿Perdemos lo que teníamos implementado antes?
- ¿Otra norma más a implementar?

Seguridad de la información vs Ciberseguridad

- Diversos enfoques plantean que uno contiene a la otra y viceversa.

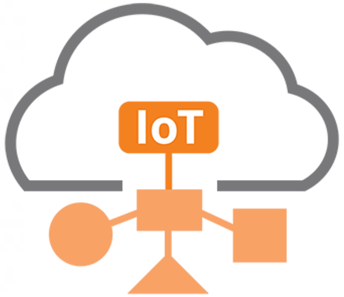
- Algunas consideraciones indican que seguridad de la información se encarga de la información análoga, seguridad informática de la digital y ciberseguridad de la digital en el ciberespacio

- Pensemos en la idea de una evolución basada en los retos actuales.

Evolución que significa más por proteger

- **Modelo de seguridad de la información**
- **Sistema de gestión de seguridad**

Políticas – Procedimientos
Controles – Riesgos gestionados
Gestión de incidents – Cultura - Etc



GESTIÓN DE RIESGOS

Los riesgos también aumentan, no sólo en cantidad, también se presentan amenazas igual y más elaboradas.

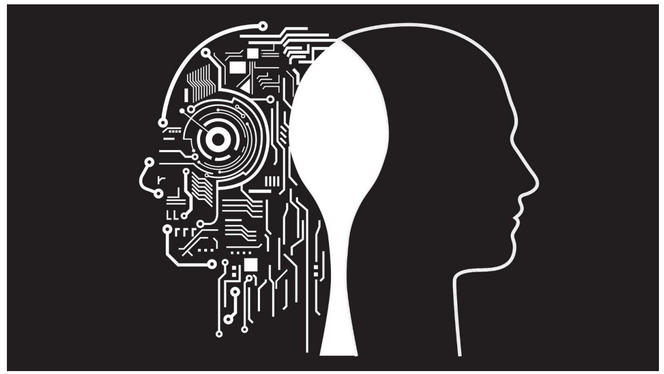
Necesidades con este cambio de alcance

- Conocimiento de cómo se encuentra expuesta la organización hacia afuera.
- Tecnologías y controles con capacidades complementarias y mayor alcance/visibilidad
- Capacidad de detectar, controlar y ser necesario, atacar (para defender)
- Desarrollo de habilidades técnicas en temas en auge (para entender y de ser posible participar en implementar)

Habilidades no técnicas a desarrollar

Estrategia – Defensa - Ataque

Diplomacia y relacionamiento externo



Abstraerse de lo técnico

Habilidades técnicas a desarrollar

- Análisis de malware
- Análisis forense
- Hacking
- Desarrollo seguro (nuevas tendencias)
- Redes (Nuevos protocolos y medios de comunicación)
- Infraestructura (ya no sólo servidores)
- Machine learning
- Hardware seguro
- Gestión de identidades
- Consumo de servicios Web
- Antifraude
- Conocimiento legal
- Entre muchas otras…

Materiales, guías y otros de apoyo

- NIST Cybersecurity Framework (v1.1)
https://www.nist.gov/cyberframework/framework
- Guías National Cyber Security Center (UK)
https://www.ncsc.gov.uk/smallbusiness
- Estrategias europeas para ciberseguridad (por país)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map
- Normas especializadas por sector
NERC – ISA 99 – Etc
- ISO 27032* (A la fecha se encuentra desactualizado)

GRACIAS

POLI
POLITÉCNICO GRANCOLOMBIANO
INSTITUCIÓN UNIVERSITARIA