Principios básicos de la ciberseguridad

Sobre mí

Santiago de Diego

Doble grado en matemáticas e ingeniería informática (Universidad de Granada)

Certificación CPHE

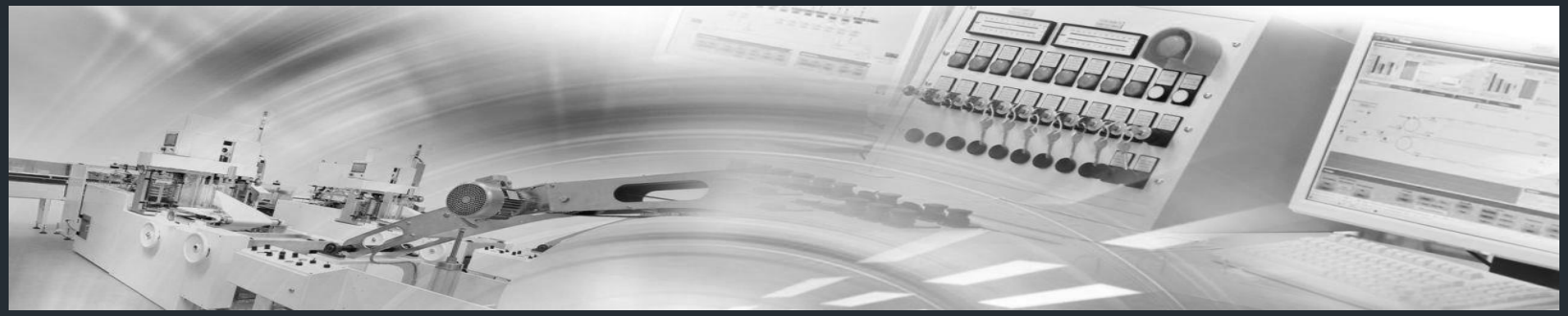
Máster en Ciberseguridad (UNIR)

Cybersecurity Researcher en Tecnalia Research & Innovation

Temas de investigación actualmente:

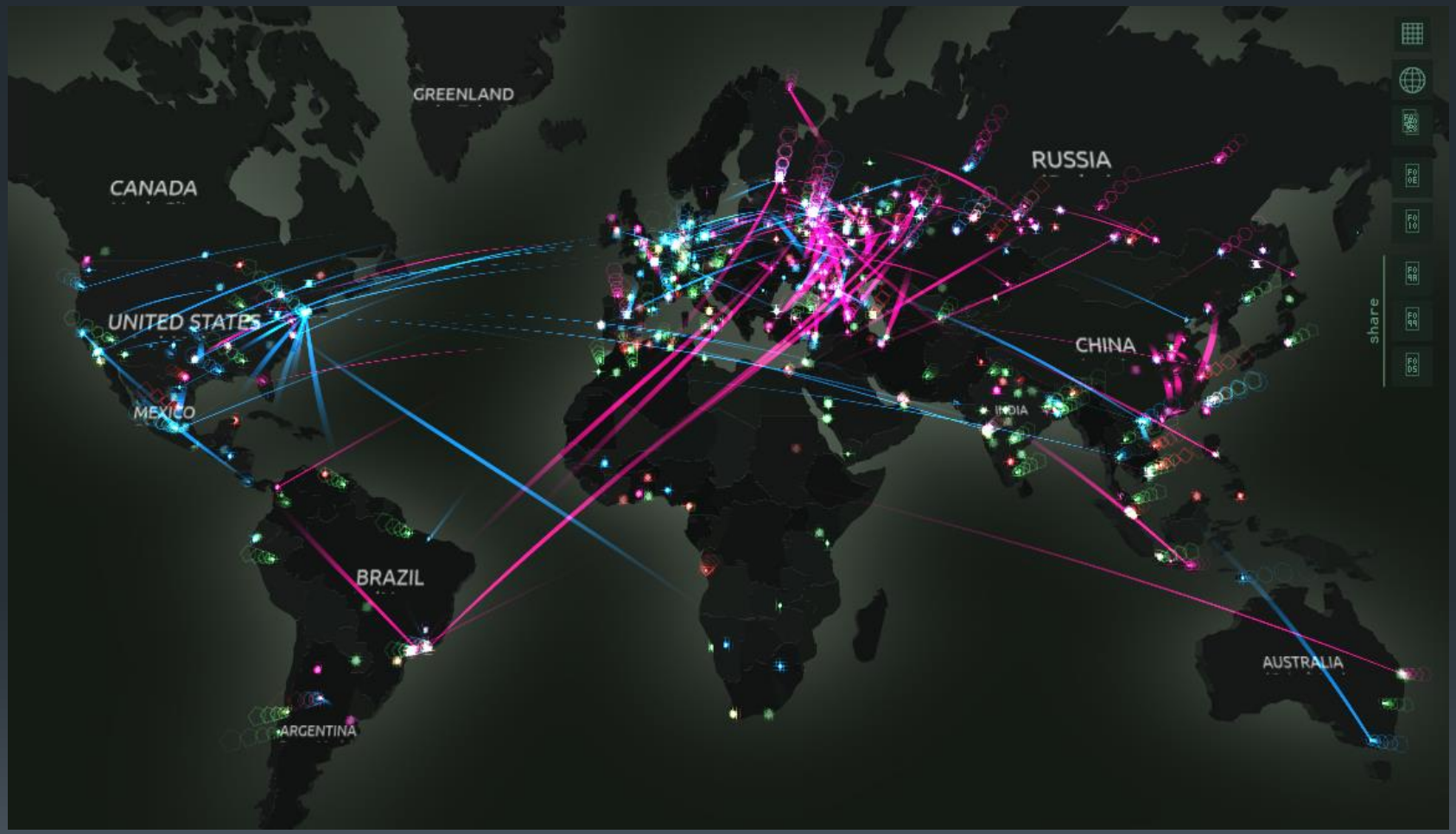
- Tecnologías Blockchain
- Ciberseguridad en dispositivos Smart Grid

www.linkedin.com/in/santiago-de-diego-226455ba/



- Introducción
- Breve Perspectiva histórica
- Ciberseguridad en el mundo actual
- Qué es la ciberseguridad?
  - Definiciones básicas
  - Importancia de la ciberseguridad
  - Objetivos principales
  - Entidades implicadas
  - Conceptos

Mapa de ciberamenazas en tiempo real



https://cybermap.kaspersky.com/es/

Claves

- PRIMERA
  - Las amenazas con origen en los propios estados, así como la profesionalización de la delincuencia en el ciberespacio, constituyen los mayores peligros.

Claves

- SEGUNDA
  - El impacto potencial en los sistemas de información víctimas de los ciberataques se está incrementando a medida que lo hace la digitalización de la sociedad.

Claves

- TERCERA
  - Los problemas derivados del software no-actualizado..

https://static.securityintelligence.com/uploads/2017/05/Wcry_note.png

Claves

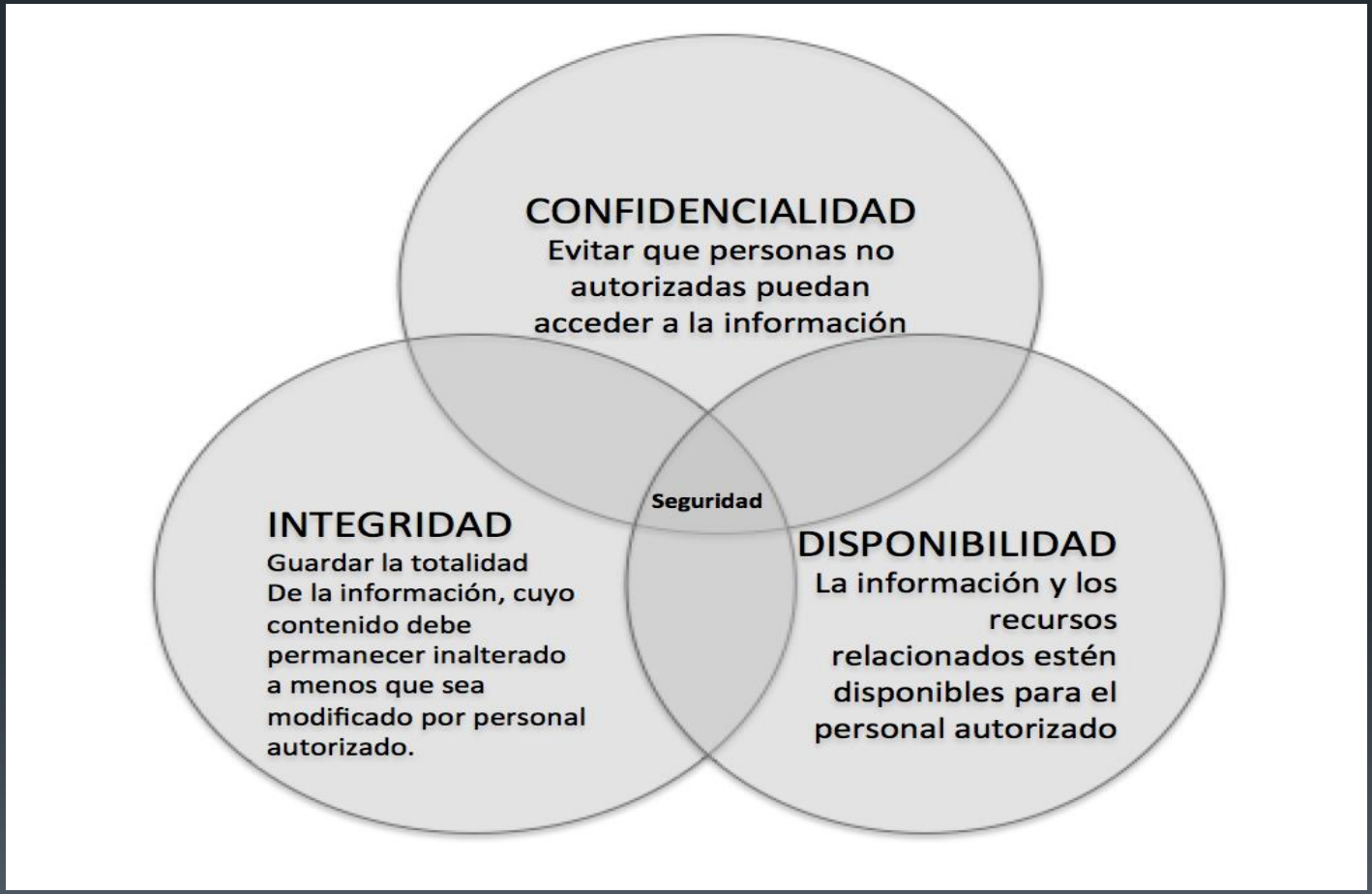
- CUARTA
  - Los problemas de privacidad derivados de la recolección masiva de datos (Big Data).

La privacidad en la era del big data

Definiciones básicas

- CIBERSPACIO: Puede decirse que el ciberespacio es una realidad virtual. No se trata de un ámbito físico, que puede ser tocado, sino que es una construcción digital desarrollada con computadora
- CIBERGUERRA: Conflicto en el Ciberespacio.
- CIBERDEFENSA: Conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición.
- CIBERSEGURIDAD: Conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propia y negarlo a terceros.
- CIBERCRIMEN: Acción criminal en el ciberespacio.
- CIBERTERRORISMO: Acción terrorista en el ciberespacio.

Objetivos principales



Entidades implicadas

- Desarrolladores de software.
- Integradores de soluciones.
- Fabricantes de productos.
- Usuarios finales u organizaciones.
- Organismos certificadores.
- Administradores de sistemas y de seguridad.

Conceptos

- Vulnerabilidad
- Política de seguridad

- Amenaza
- Ataque

Vulnerabilidad

- Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible.

- Pueden tener distintos orígenes: fallos de diseño, errores de configuración o carencias de procedimientos.

  Inyección de código sql.

- Por sí sola, no causa daño alguno, pero posibilita que se materialice una amenaza sobre el activo afectado.

Ejemplo de vulnerabilidad

JAN 30TH, 2015

GHOST: nueva vulnerabilidad crítica de Linux

Investigadores de la empresa de seguridad Qualys han descubierto un severo agujero de seguridad en la librería GNU C de Linux (glibc). Esta vulnerabilidad, llamada GHOST (CVE-2015-0235), permitiría a hackers tomar control remoto de cualquier sistema sin siquiera conocer usuarios o contraseñas.

Para utilizar la vulnerabilidad, el atacante sólo tiene que producir un *buffer overflow* enviando un hostname inválido a alguna aplicación que realice resolución DNS. La vulnerabilidad permitirá al atacante ejecutar cualquier tipo de código o comandos con los mismos permisos del usuario que ejecuta la aplicación afectada. En resumen, una vez que el atacante utilizó la falla GHOST pueden tomar control del sistema.

GHOST

Políticas de seguridad

- Conjunto de reglas y prácticas que definen y regulan los servicios de seguridad de una organización o sistema.
- Protege los recursos críticos de amenazas latentes en el entorno.
- Garantiza la seguridad de los sistemas de información.
- Disminuye los riesgos de pérdida, manipulación o indisponibilidad de la información.
- Asegura el cumplimiento de los objetivos de la organización.

Normativas

- ISO/IEC 27001 (Seguridad de la Información)
  - Norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.
  - Permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.
  - Supone una diferenciación respecto al resto de organizaciones.
- ISA/IEC-62443, etc

Amenaza

- Violación de la seguridad en potencia.
- Puede materializarse al explotar una vulnerabilidad para causar una infracción de la seguridad.
- Dicha infracción de la seguridad puede provocarse:
  - Intencionadamente: ataque
  - Inintencionadamente: desastre natural o negligencia.
- Desde el punto de vista de una organización pueden ser tanto internas como externas.

Amenaza …

- Según la Agencia de Seguridad de Estados Unidos, por cada compañía que sabe que está siendo hackeada, existen otras 100 que desconocen que sus sistemas han sido comprometidos …

Ataque

- Acto intencionado y deliberado que viola la política de seguridad de un sistema.

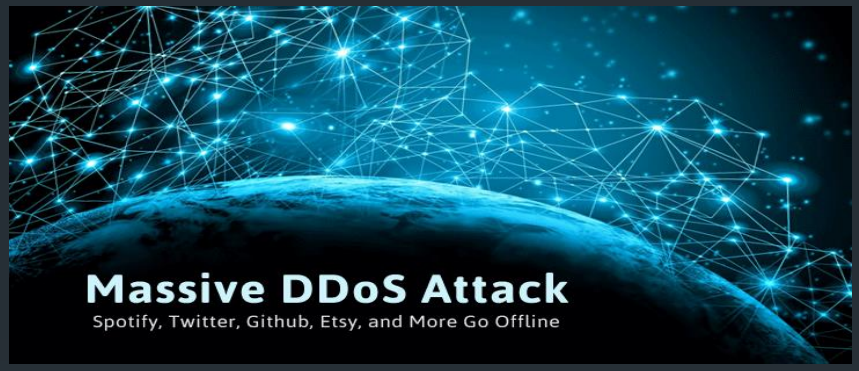
- Puede ser:

  - Activo: Altera el sistema, recursos u operaciones.

  - Pasivo: Intenta aprender o utilizar información del sistema, pero no afecta al propio sistema, ni a su funcionamiento.

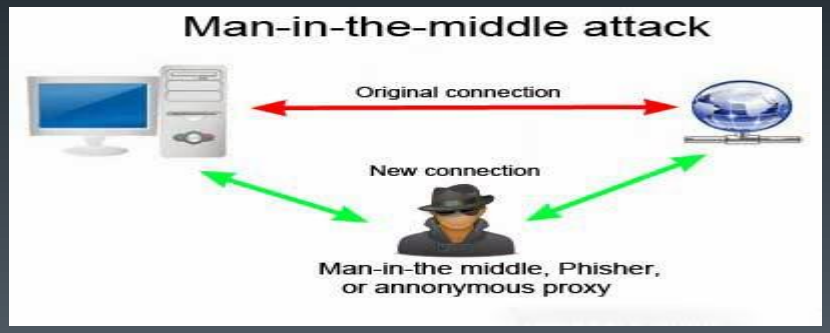
Ejemplos de ataques

- Denegación de servicio -> DyN (Octubre 2016)



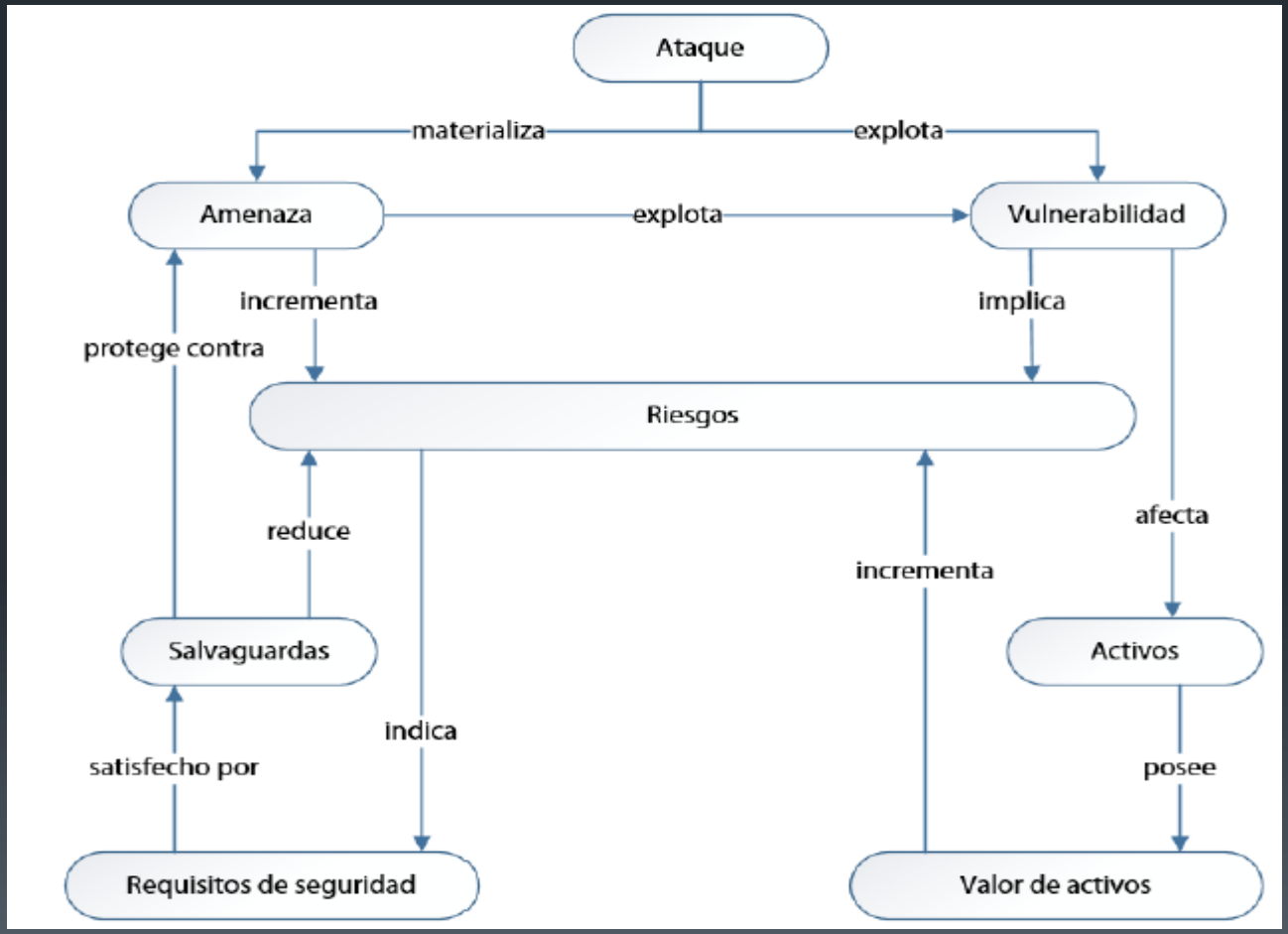
Ataque DDoS a Dyn

- Man in the middle.



Heartbleed

Resumen


Ataque
materializa
explota
Amenaza
explota
Vulnerabilidad
incrementa
implica
protege contra
Riesgos
reduce
afecta
incrementa
Salvaguardas
Activos
indica
satisfecho por
posee
Requisitos de seguridad
Valor de activos

REFERENCIAS

- Ciberseguridad y protección de la información
- Ingeniería del software y ciberseguridad