Entrenamientos en Ciberseguridad

Ramiro Pulgar

Twitter/Skype: @milovisho
ramiro.pulgar@bluehatconsultores.com

BlueHat consultores

expertos en ciberseguridad...

ADN: Ramiro Pulgar

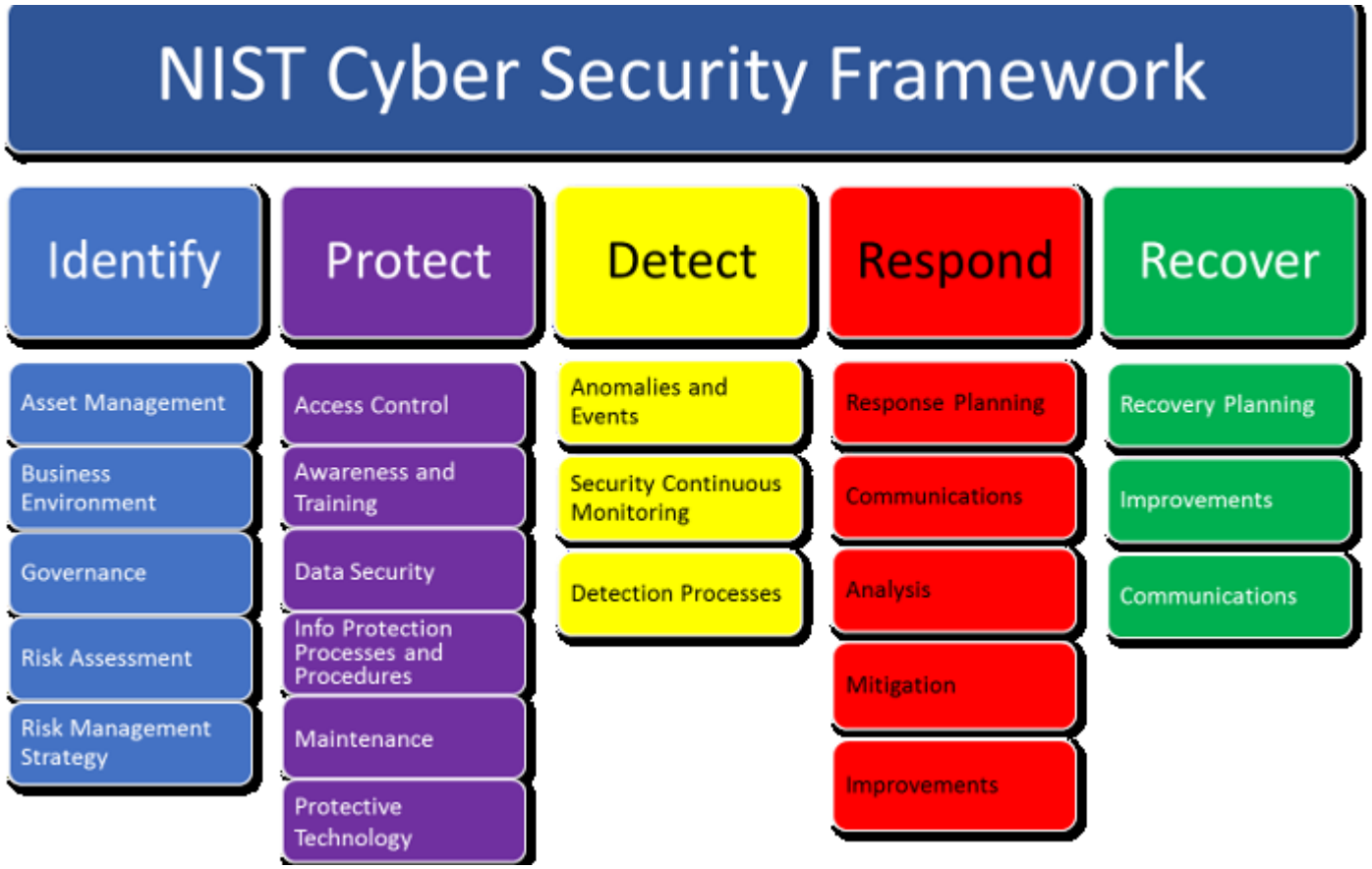
- Information Security Advisor & Pentester
- Arquitecto de TI
- Certificaciones:
  - EC-Council: LPT, CEH, ECSA, ECES, CHFI, ENSA, CEI, ECIH, CAST
  - Red Hat : RHC { SA, E }, ex Instructor / Examinador
  - ISO 27001 LA, LI, RM
  - Cybersecurity: CCSK, CSXF
- Miembro:
  - ISECOM (Gold)
  - ISACA
  - OWASP Ecuador Chapter Leader
  - ATM Industry Association
  - High Technology Crime Investigation Association
  - Association of Certified Fraud Examiners

Agenda

- NIST Cybersecurity Framework
- NIST 800-30
- Gestión de Riesgos
- Modelamiento de Amenazas
- Cumplimientos
- Complejidad de las redes
- Monitorear vs Analizar
- Equipo Azul vs Equipo Rojo

BLUE Hat consultores
expertos en ciberseguridad

NIST Cybersecurity Framework



NIST 800-30

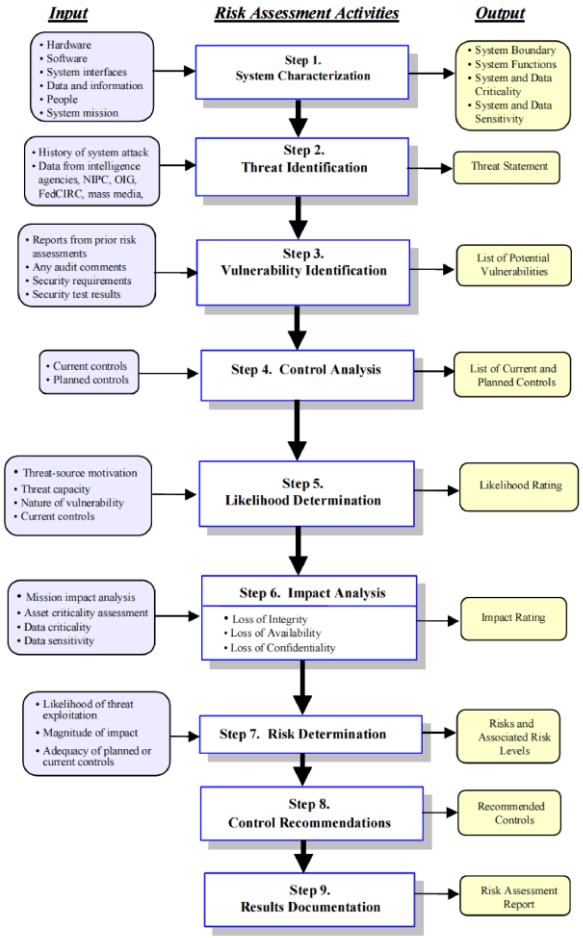
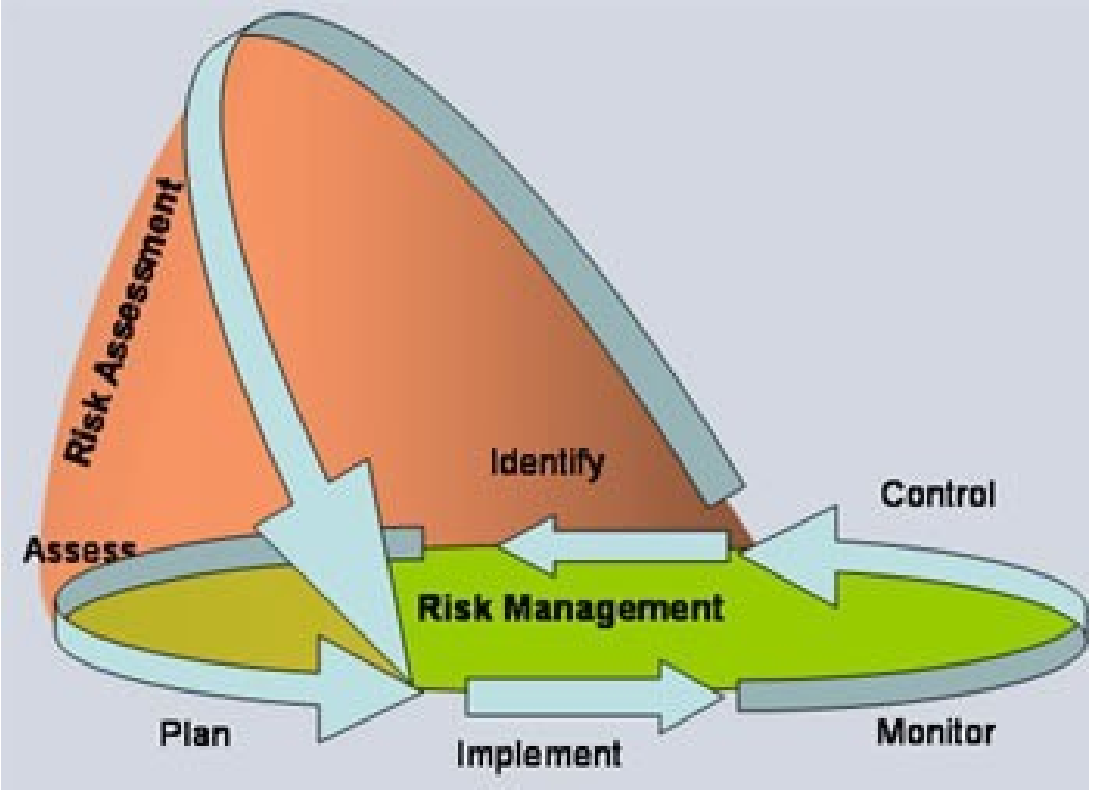
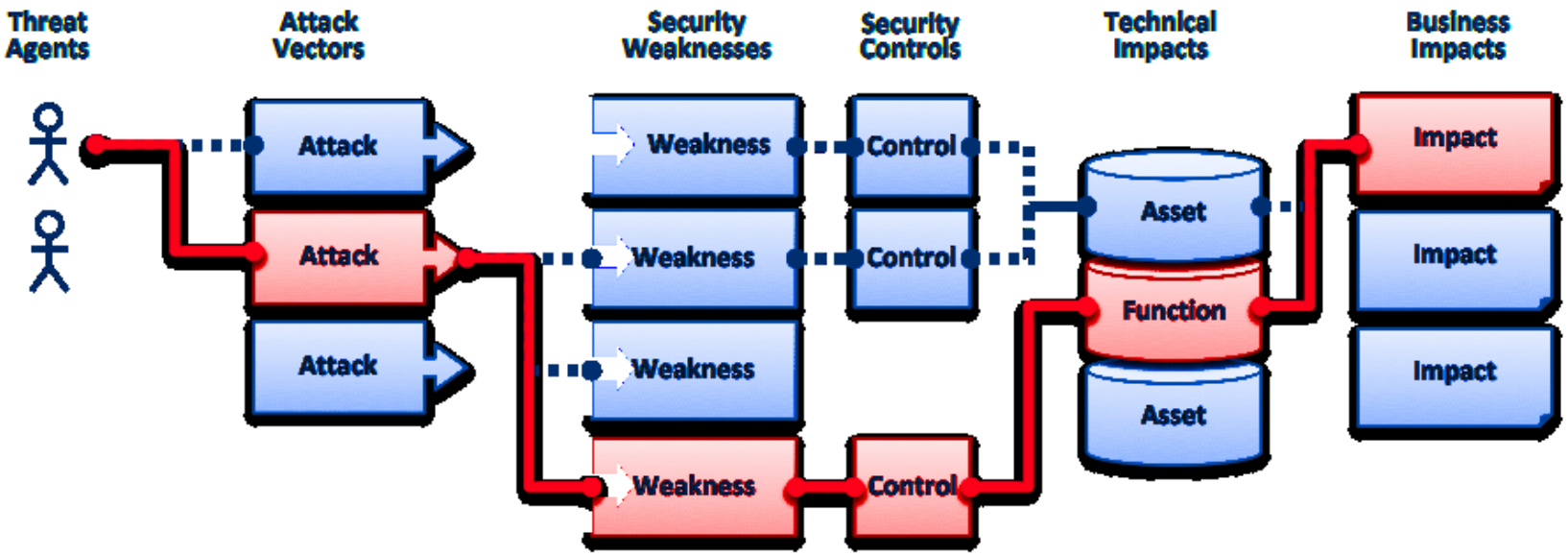


Figure 3-1. Risk Assessment Methodology Flowchart

Risk Management



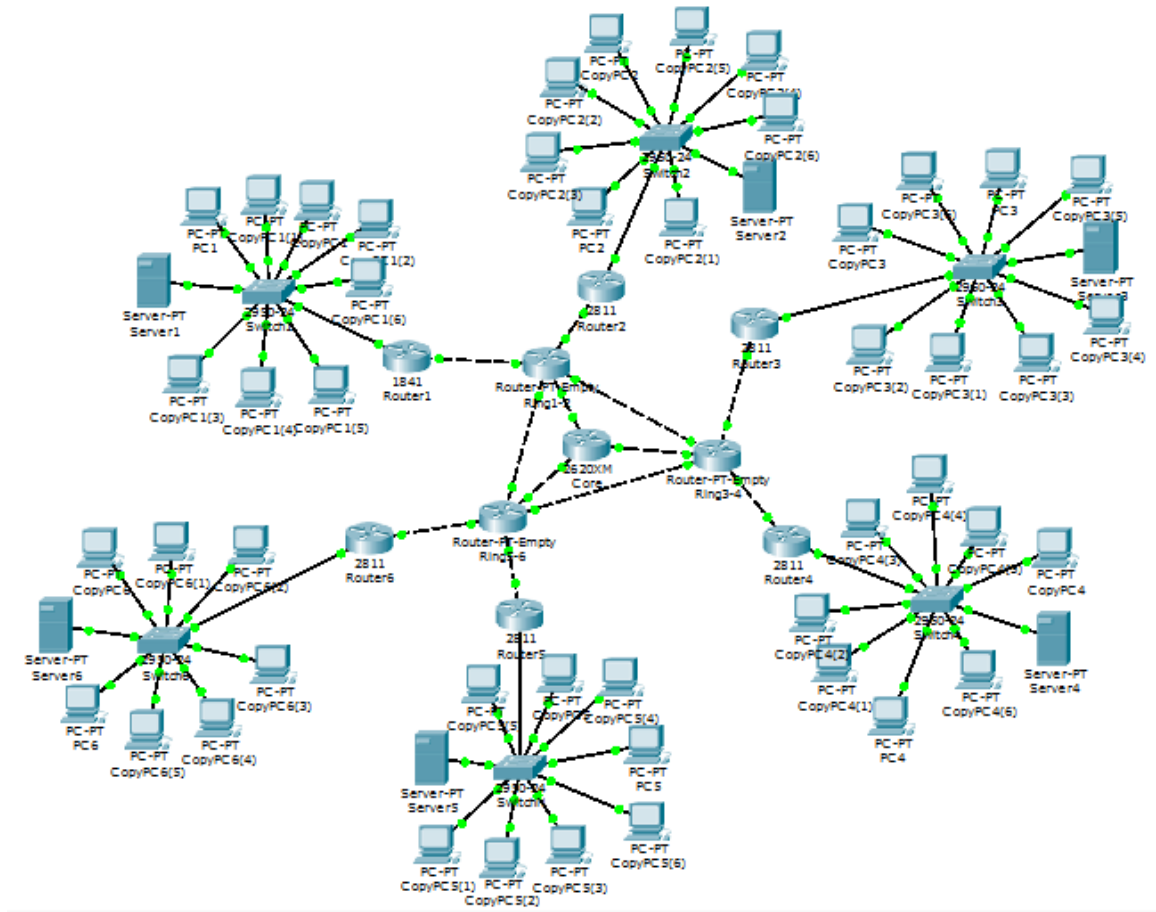
Modelamiento de Amenazas



Cumplimiento

Complejidad de las redes

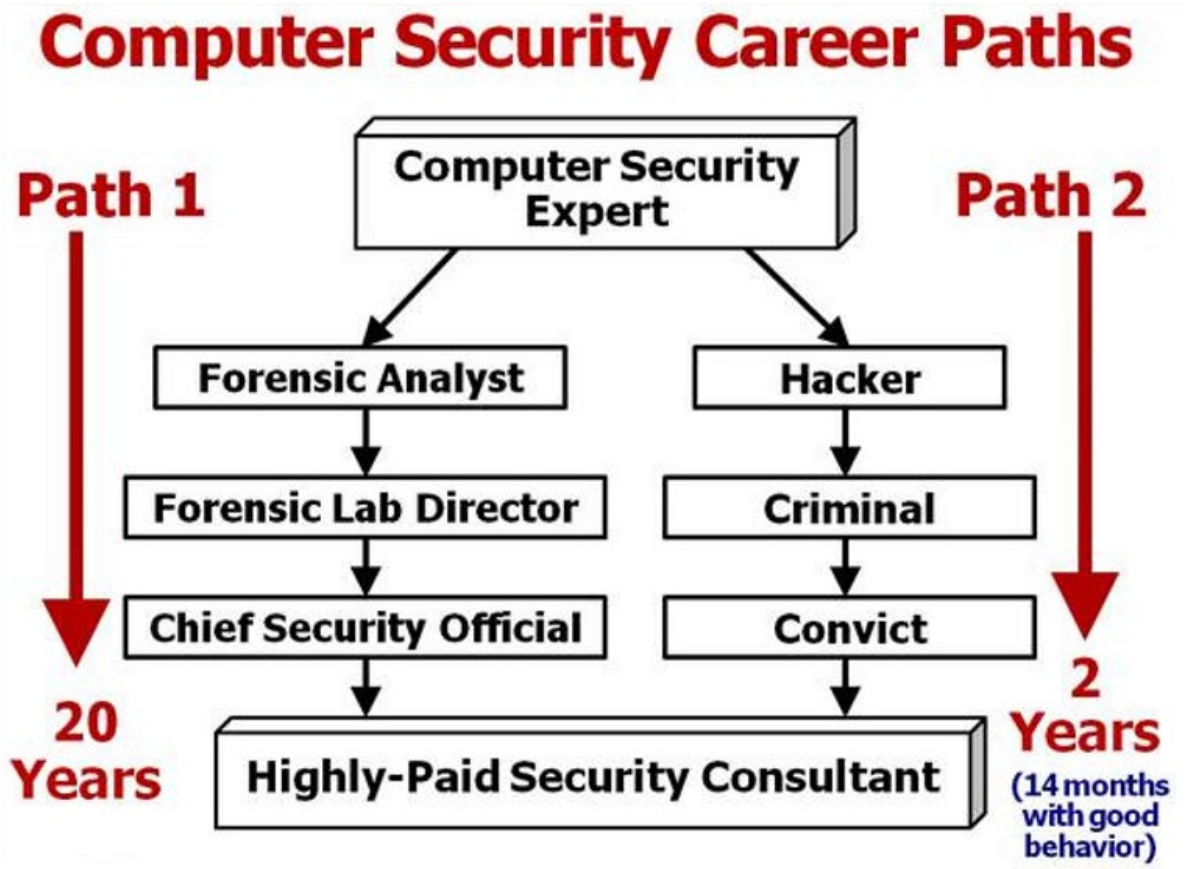
Complejidad de las redes



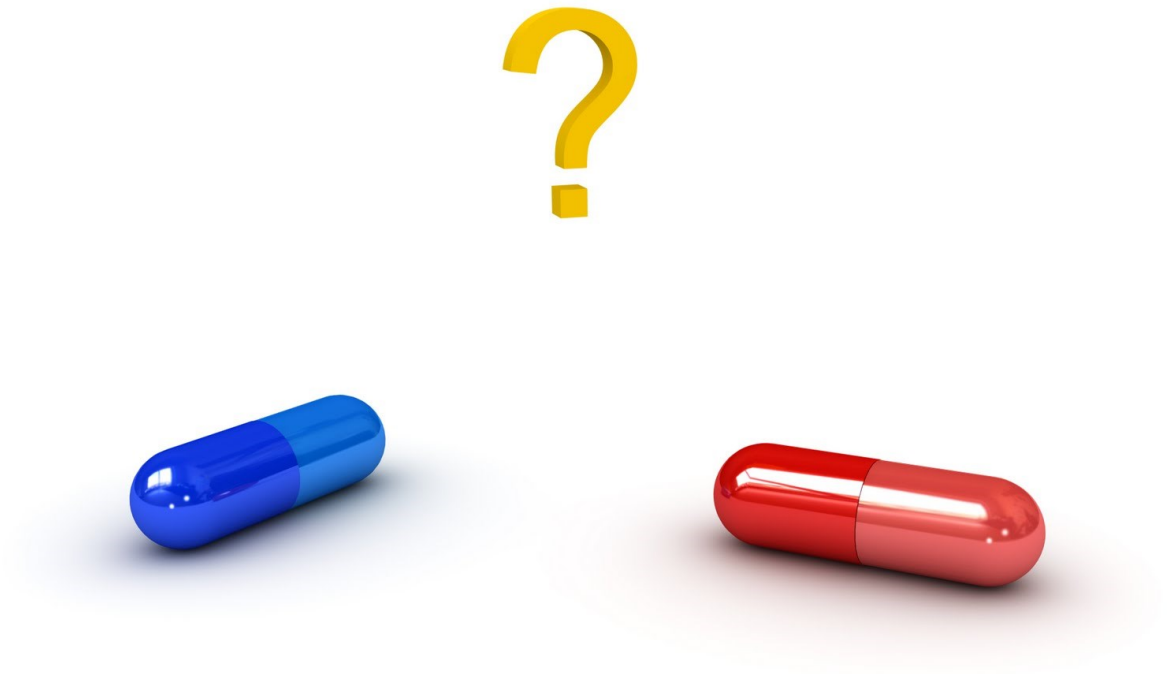
Complejidad de las Redes

Complejidad de las Redes

Cómo ser famoso?



Enfrento o no a los intrusos?



Enfrento o no a los intrusos?

BLUE Hat consultores
expertos en ciberseguridad

Equipo azul vs Equipo Rojo

VS

BlueHat consultores
expertos en ciberseguridad

Equipo azul vs Equipo Rojo

Equipo Rojo	Equipo Azul
Búsqueda de Información Crítica	Identificación
Escaneo de Redes y Evasión de IPS	Documentación detallada de cada ocurrencia
Intrusión de sistemas y Pivoting	Respuesta Inicial
Captura de tráfico y Robo de Sesiones	Comunicar el incidente
Denegación de Servicio	Contención
Intrusión a Aplicaciones	Estrategia de Respuesta
Intrusión a Wireless	Clasificación del Incidente
Ofuscación y Cifrado	Investigación del Incidente

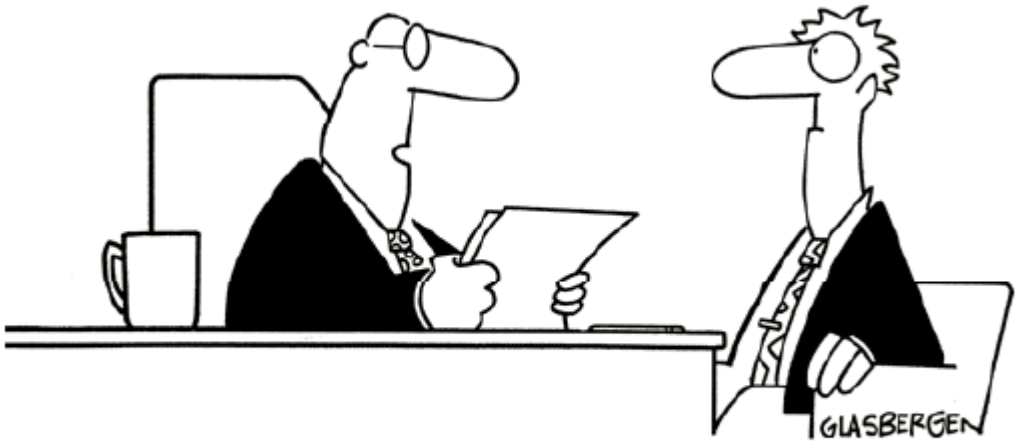
Equipo azul vs Equipo Rojo

Equipo Rojo	Equipo Azul
	Recolección de Datos
	Análisis Forense
	Protección de la Evidencia
	Notificación a Entes Externos
	Erradicación
	Recuperación
	Documentación técnica y ejecutiva
	Evaluación de Daños y Costos
	Revisión y Actualizaciones de Políticas de Respuesta ante Incidentes

BlueHat consultores
expertos en ciberseguridad

Certificaciones

PREGUNTAS?



"We're looking for someone who can help us crack down on identity theft. Fill out this application and don't forget to include your Social Security number, date of birth, phone number, home address and mother's maiden name."

BlueHat consultores
expertos en ciberseguridad

Gracias!

Twitter/Skype: @milovisho

ramiro.pulgar@bluehatconsultores.com