

Entrenamientos en Ciberseguridad

Ramiro Pulgar

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



expertos en ciberseguridad...

ADN: Ramiro Pulgar

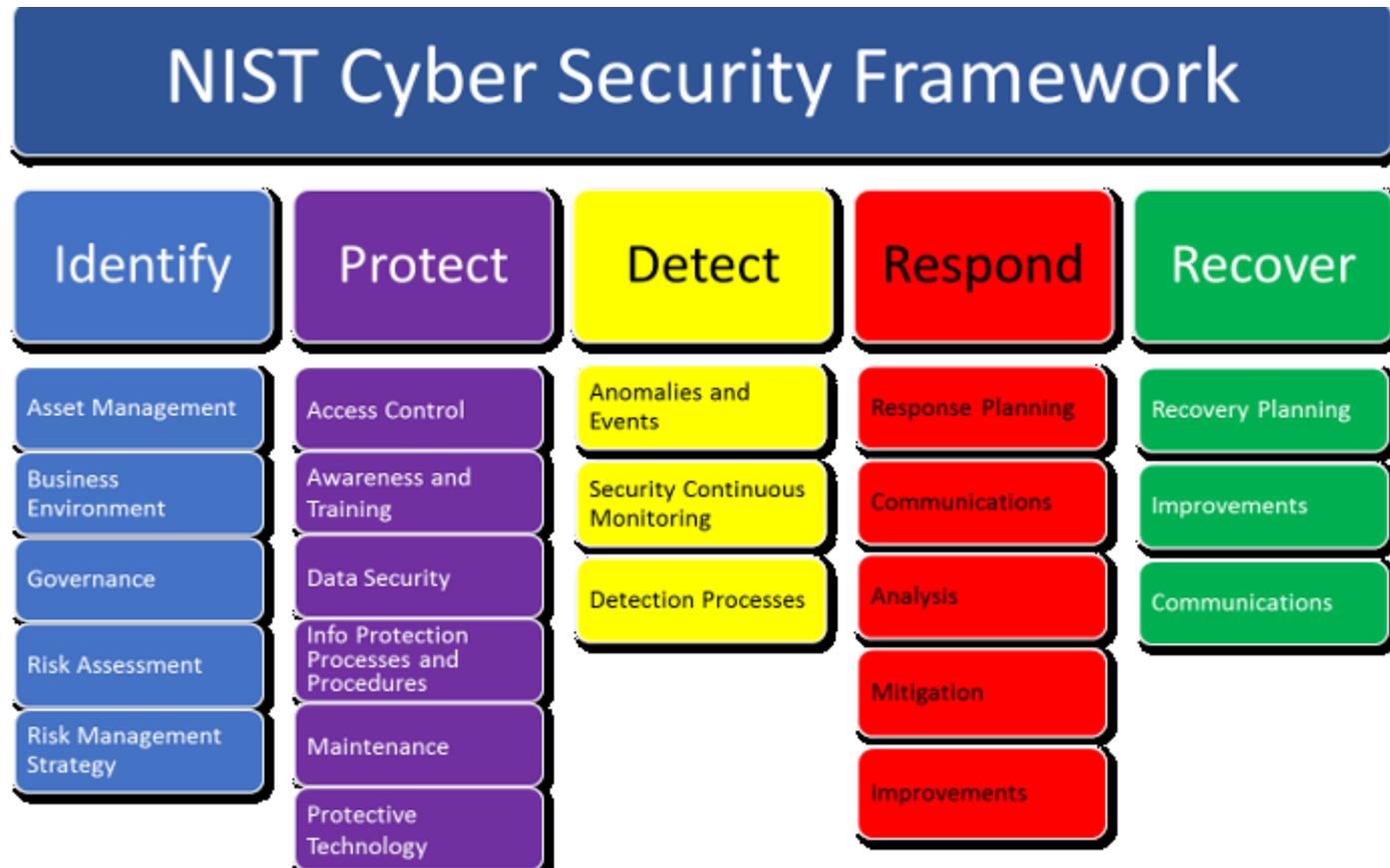
- Information Security Advisor & Pentester
- Arquitecto de TI
- Certificaciones:
 - EC-Council: LPT, CEH, ECSA, ECES, CHFI, ENSA, CEI, ECIH, CAST
 - Red Hat : RHC { SA, E }, ex Instructor / Examinador
 - ISO 27001 LA, LI, RM
 - Cybersecurity: CCSK, CSXF
- Miembro:
 - ISECOM (Gold)
 - ISACA
 - OWASP Ecuador 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

NIST Cybersecurity Framework



NIST 800-30

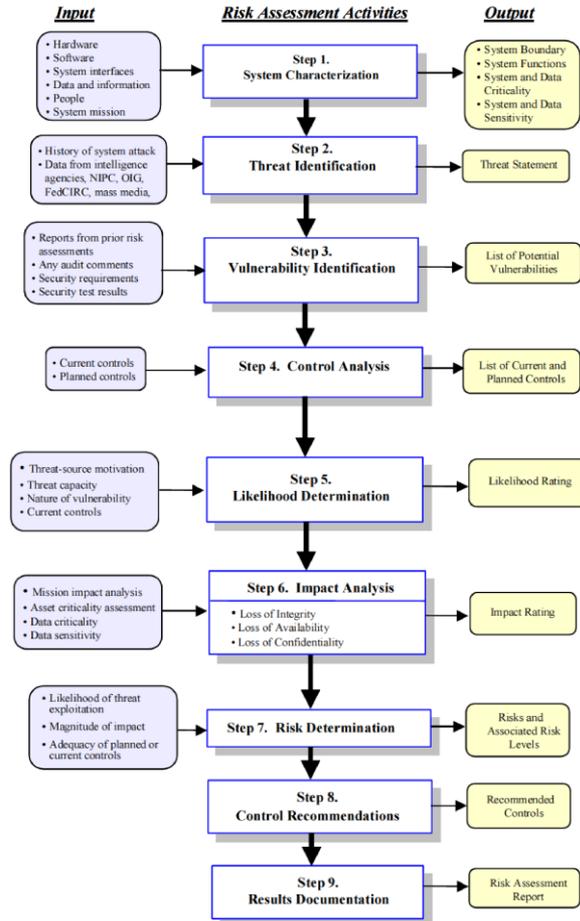
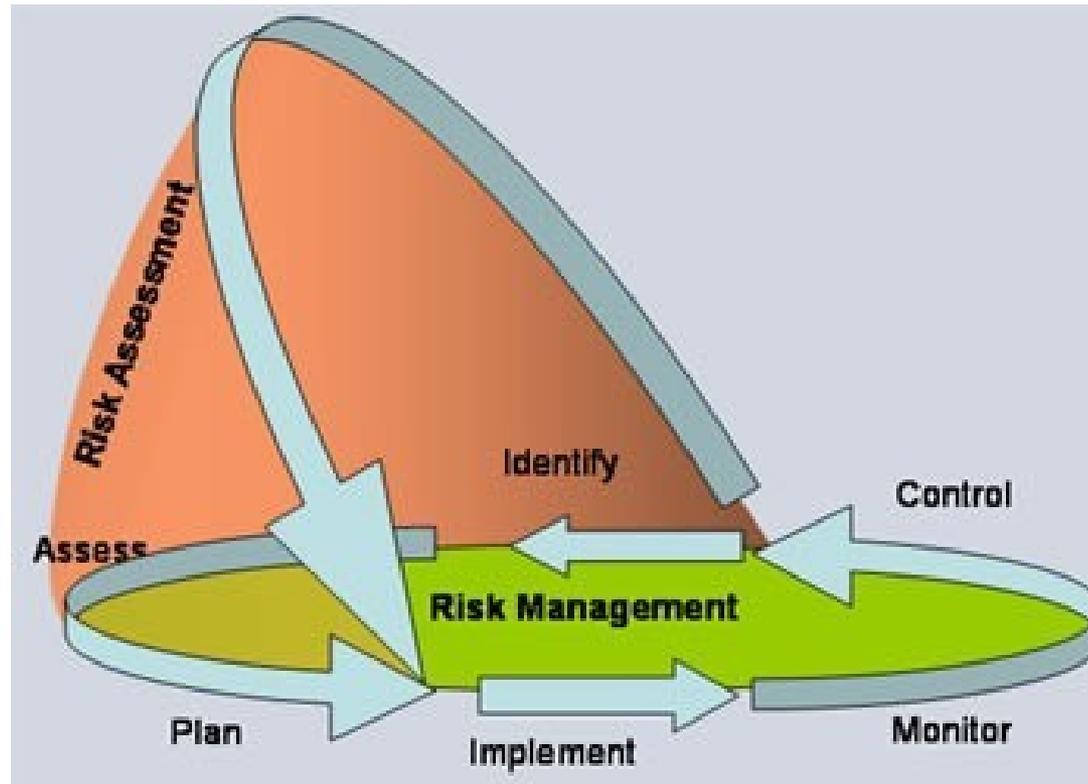
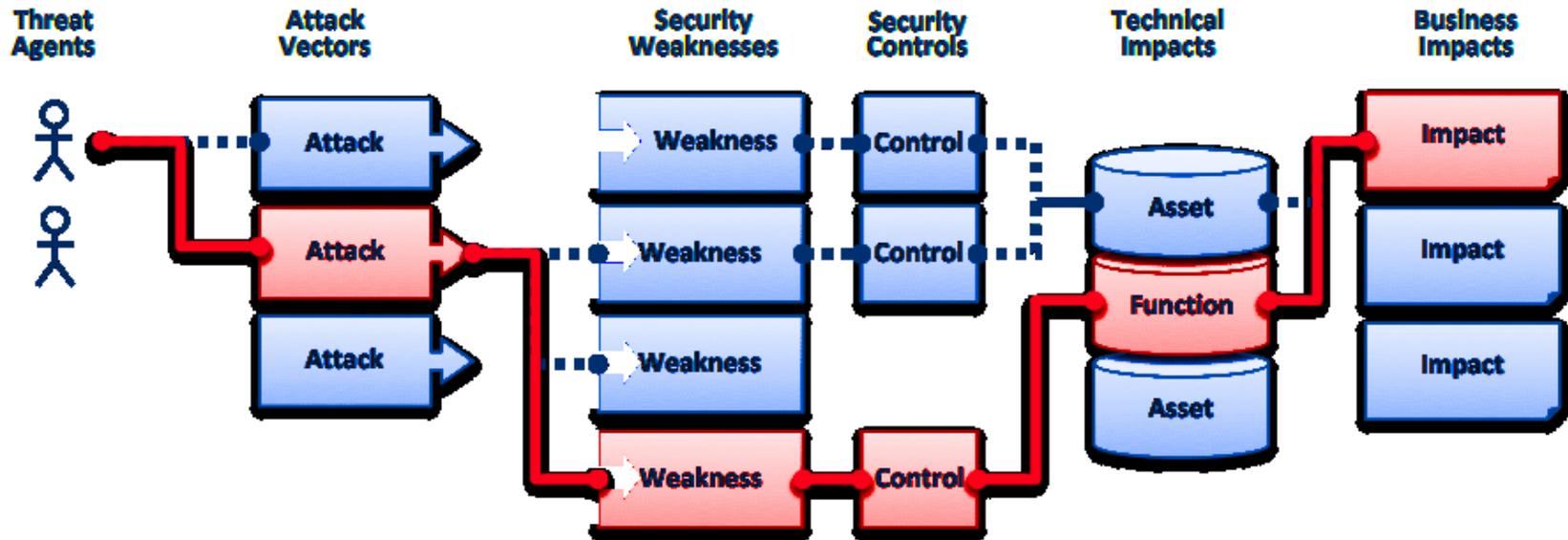


Figure 3-1. Risk Assessment Methodology Flowchart

Risk Management



Modelamiento de Amenazas



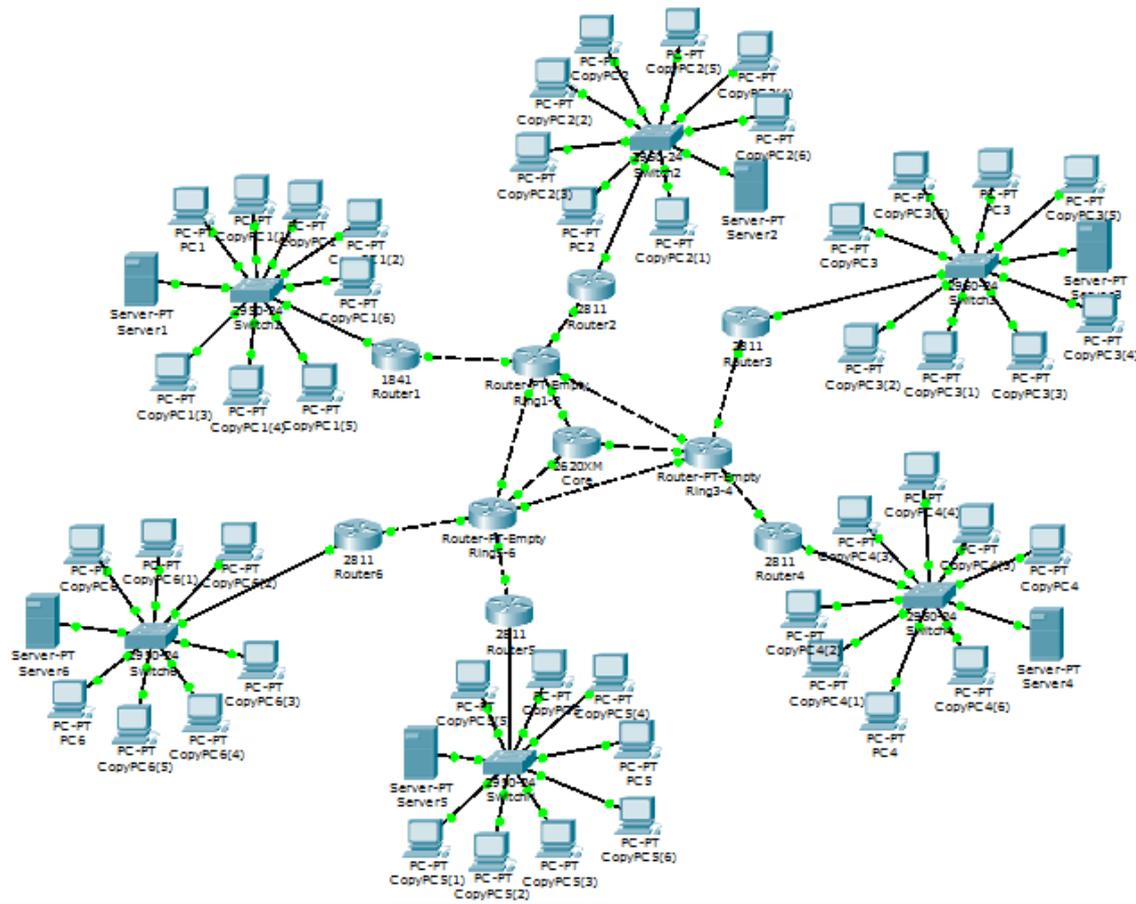
Cumplimiento



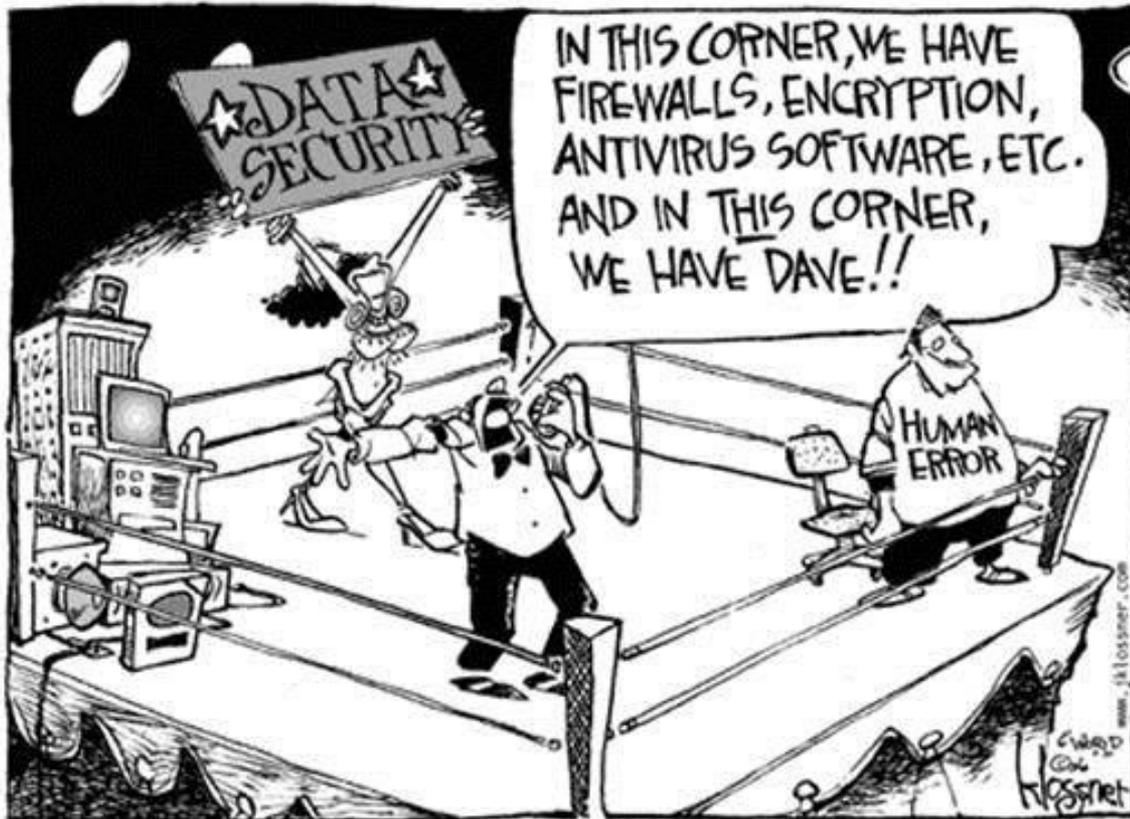
Complejidad de las redes



Complejidad de las redes



Complejidad de las Redes

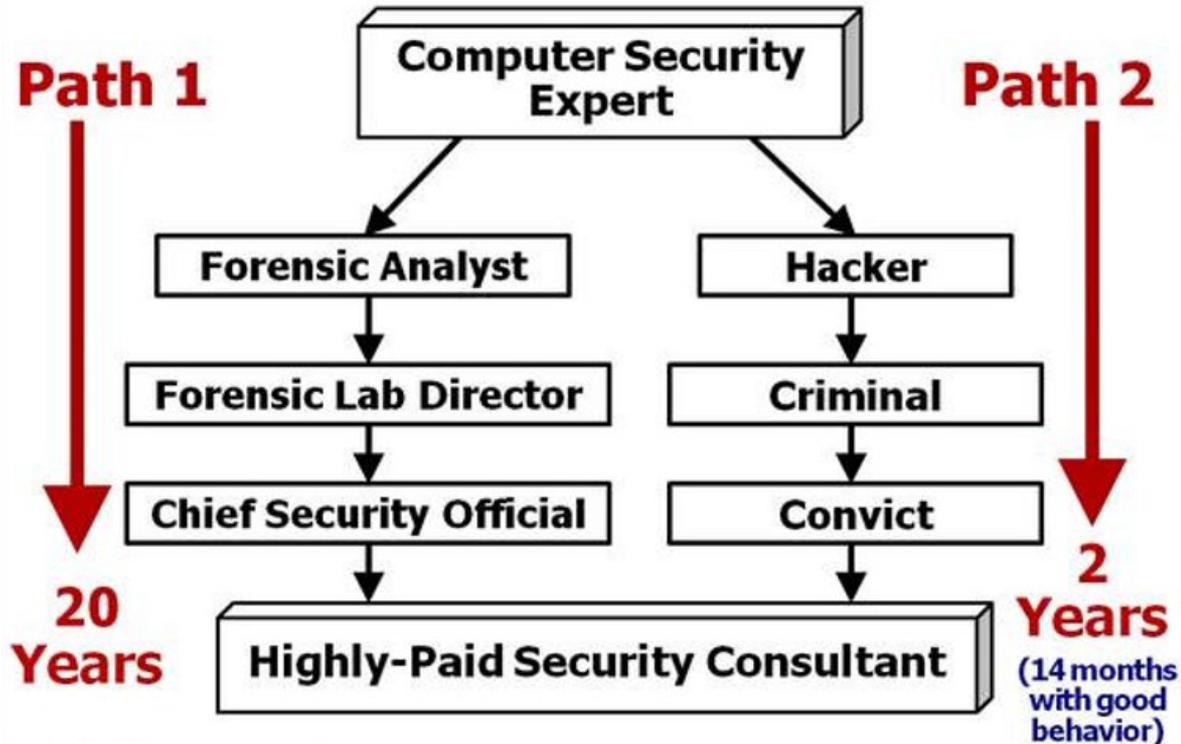


Complejidad de las Redes



Cómo ser famoso?

Computer Security Career Paths



Enfrento o no a los intrusos?



Enfrento o no a los intrusos?



Equipo azul vs Equipo Rojo



VS



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

Certificaciones

(ISC)²

CISSP[®]
Certified Information Systems Security Professional

CSSLP[®]
Certified Secure Software Lifecycle Professional

SSCP[®]
Systems Security Certified Practitioner

CAP[®]
Certified Authorization Professional

CCSP[®]
Certified Cybersecurity Professional

SANS



EC-Council

CCISO
Certified Chief Information Security Officer

CEH
Certified Ethical Hacker

ECIH
EC-Council Certified Incident Handler

LPT
Licensed Penetration Tester

ENSA
EC-Council Network Security Administrator

ECSP
EC-Council Certified Secure Programme

ECSA
EC-Council Certified Security Analyst

ISACA
Serving IT Governance Professionals

CISM
Certified Information Security Manager[®]
An ISACA[®] Certification

CRISC
Certified in Risk and Information Systems Control[®]
An ISACA[®] Certification

CGEIT
Certified in the Governance of Enterprise IT[®]



CHFI
Computer Hacking Forensic Investigator



CompTIA Advanced Security Practitioner CASP



Microsoft Certified Professional



Offensive Security OSWP

CSXP[™]
Certified Cybersecurity Practitioner

CISSP CISM
Certified Information Security Manager

CompTIA Security+[™]

CISCO CERTIFIED CCNP SECURITY

Certified CEH
Ethical Hacker

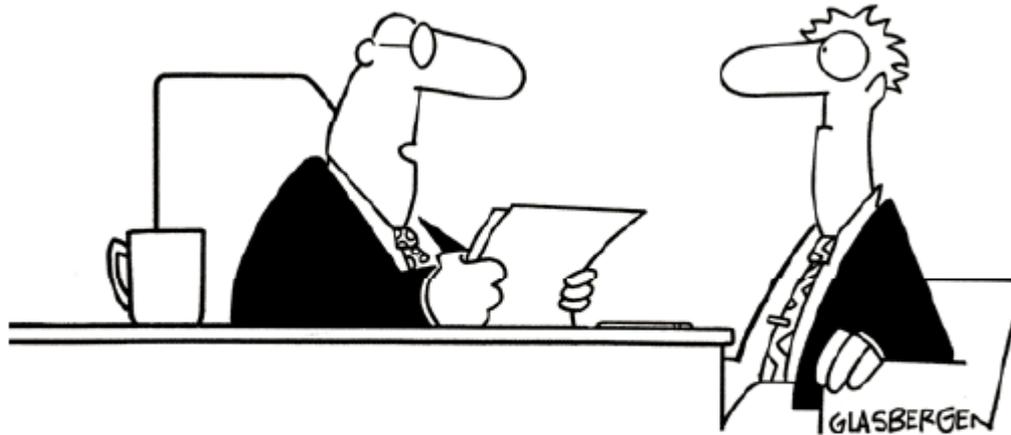


SSCP[®]



PREGUNTAS?

Copyright 2003 by Randy Glasbergen.
www.glasbergen.com



“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.”

Gracias!

Twitter/Skype: **@milovisho**

ramiro.pulgar@bluehatconsultores.com