ISO 27032

Gestión de Riesgos de Ciberseguridad

whoami

- **Una fork en GitLife que seguro será mucho mejor software!**
  - **Padre** [no mucho ultimamente :-( ]
- **cat /dev/sec | grep * >> /dev/mind**
  - **Curioso**, navegante empedernido
- **hexdump /tmp/life/* >> /dev/mind**
  - **Nerdo** [sí, para mí “nerdo” es un cumplido…]

- Certificaciones: **CISA** (*ISACA*), **PCI-P** (PCI-SSC), CCNP Security, ...
- Experiencia: IBM, CERTuy, Deloitte...
  - “*wc -l ~/.history*” da un número más grande de lo que quiero reconocer...
- Docente en Universidad ORT del Uruguay
- Actualmente Socio Director de **Krav Maga Hacking**
  - Pentesting, Consultoría, Entrenamientos

¿Porqué ISO 27032?

- Guía de Buenas Prácticas en Ciberseguridad, considerando todo el Ciberespacio (Equipamiento de red, Software, Interconexión de redes, Personas, Servicios de Internet)

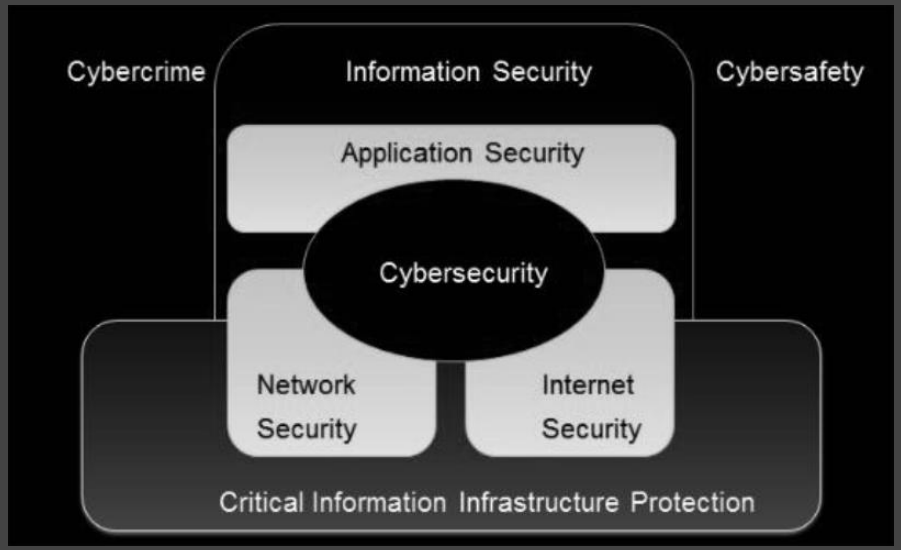
- Explicación de la relación entre Ciberseguridad, Seguridad Informática y Seguridad de la Información.

- Un marco de referencia para la toma de decisiones para la resolución de temas relacionados a la ciberseguridad

- La organización no es certificable bajo ISO 27032 pero puede alinear sus análisis y buenas prácticas a la misma.

Protección del Ciberespacio y activos de las organización y de los usuarios:

- Herramientas de seguridad
- Políticas
- Conceptos de Seguridad
- Controles implementados
- Guías y Estándares
- Gestión de Riesgos
- Entrenamientos
- Buenas Prácticas
- Tecnologías implementadas
- Seguridad de activos digitales

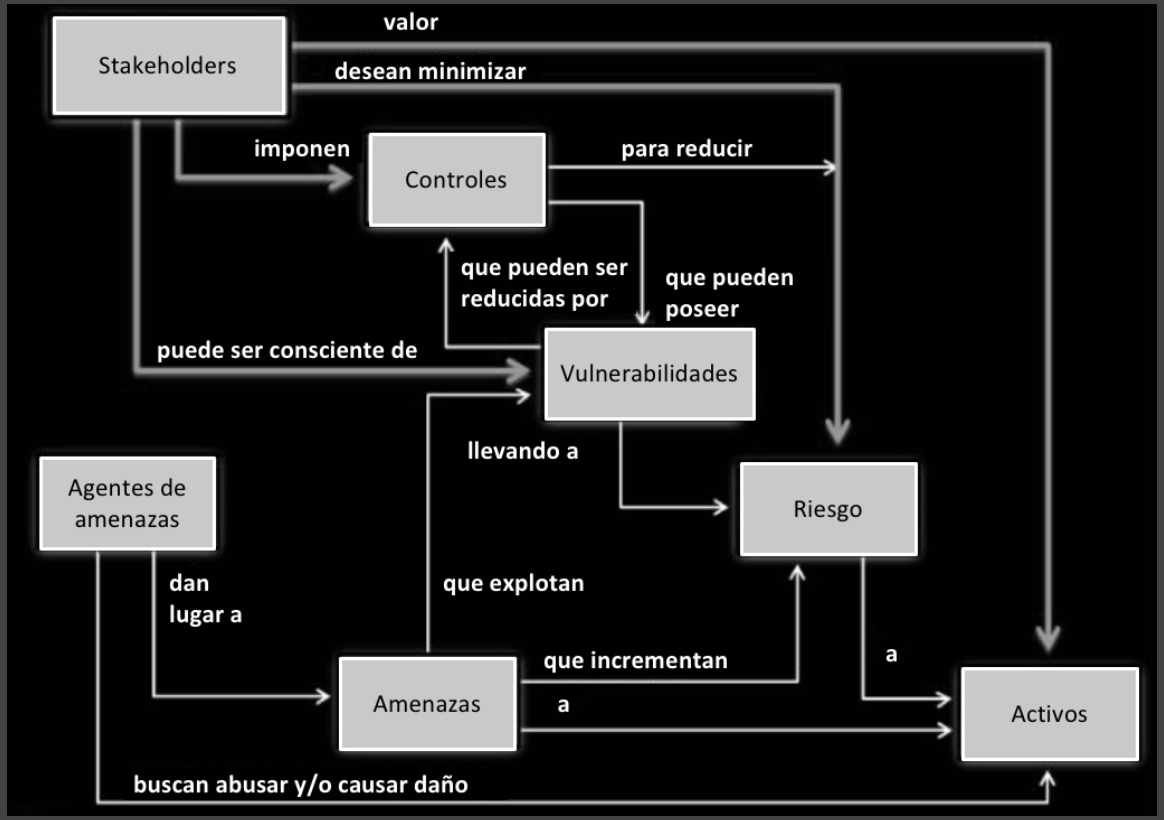


Activos (ISO 27032 8.1)

Cualquier cosa que tenga valor para las personas o la organización

- Software
- Información
- Activos físicos (PC, laptops, servidor, etc)
- Servicios
- Personas, su formación, sus capacidades y experiencia
- Intangibles como la imagen o la reputación

Conceptos y Relaciones



Gestión de Riesgos (ISO 27032 11.2)

Los objetivos de la Gestión de Riesgos de Ciberseguridad son:

- Brindar protección de seguridad a todo el ciberespacio dentro de la organización
- Planificar la resolución de incidentes
- Gestionar Crisis
- Educar y Asesorar a la alta gerencia en temas de Ciberseguridad y Riesgos de Ciberseguridad
- Compartir de forma correcta, en tiempo , relevante y exacta la información de amenazas a fuerzas de seguridad, legales y tomadores de decisiones.

Gestión de Riesgos (ISO 27032 11.2) [cont.]

Los objetivos de la Gestión de Riesgos de Ciberseguridad son:

- Gestionar riesgos en forma coordinada con proveedores de productos, servicios y establecer correctos mecanismos de comunicación y coordinación ante eventos o incidentes.
- Comprender el nivel de riesgos de ciberseguridad y seleccionar los controles para proporcionar un nivel aceptable de riesgo
- Es un trabajo continuo, no una actividad puntual y estática
- Aplicada a todas las tecnologías de la organización
- Ciberseguridad debe ser responsabilidad de la Alta Gerencia / Directorio

Ataque Interno (ISO 27032 9.4.2)

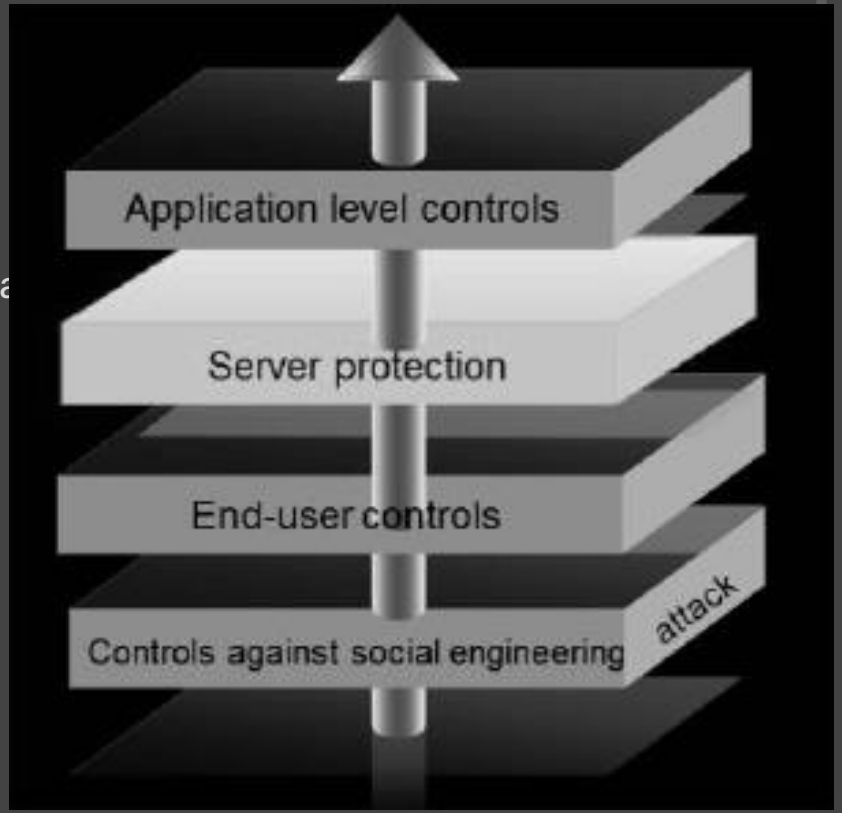
- Generados por empleados, proveedores o atacantes que han logrado acceso a la red interna
- Puede ser con acceso físico o remoto no autorizado o a través de personas con acceso físico a la red

Ataque Externo (ISO 27032 9.4.3)

- Atacantes externos a infraestructura, aplicaciones, servicios o cualquier activo
- Escaneos de puertos automatizado
- Ataques de Denegación de Servicio
- P2P (Peer to Peer Apps)
- Ataques de tipo Buffer Overflow que permiten por ejemplo ejecución remota de código
- IP Spoofing
- Phishing
- Malware, Gusanos
- Exploits de día 0
- Exploits ante vulnerabilidades conocidas

Controles (ISO 27032 12)

- Aplicaciones
  - Validación, Cookies, Revisión de Código
  - Autenticación, Políticas, Scripts, Sesiones
- Servidores
  - Guías y estándares de instalación y configura
  - Parches, Testing, Monitoreo y Backups
- Usuario Final
  - Parches, Antivirus, Seguridad Web y Email
  - Firewall e IPS personal, Educación continua
- Personas
  - Educación continua
  - Campañas de Security Awareness



Recomendaciones Estratégicas

- Entrenamientos continuos y medibles de educación para toda la organización
- Adoptar ISO 27032 como Buenas Prácticas en Ciberseguridad
- Incorporar en la gestión de riesgos basada en ISO 27005 los aspectos identificados en los riesgos detectados a nivel de Ciberseguridad en el assessment, considerando los controles ISO 27032.
- Revisión de política de parches, configuraciones por defecto y protocolos
- Implementar un plan o programa de protección de datos especialmente para datos fuera de servidores

Proyectos de Mejora Continua

- Implementar Scanner de Vulnerabilidades Automatizado tanto externo como interno, alineado a un plan de gestión de vulnerabilidades y parches
- Implementar un plan de gestión de incidentes de ciberseguridad y evaluar la creación o contratación de servicios de SOC y CSIRT.
- Activación de IPS a nivel de red y estaciones de trabajo (PC, laptops, servidores)
- Implementar Lista Blancas de Aplicaciones en servidores críticos
- Revisión de política de parches, configuraciones por defecto y protocolos
- Evaluar implementación de soluciones para prevención de fuga de información

Conclusiones

- Adopción de buenas prácticas internacionales
- Correcta gestión de riesgos contemplando ciberseguridad
- Apoyo de la alta gerencia en aspectos de ciberseguridad
- Colaboración ante incidentes
- Capacitación y concienciación
- Procesos de mejora continua implementados y efectivos

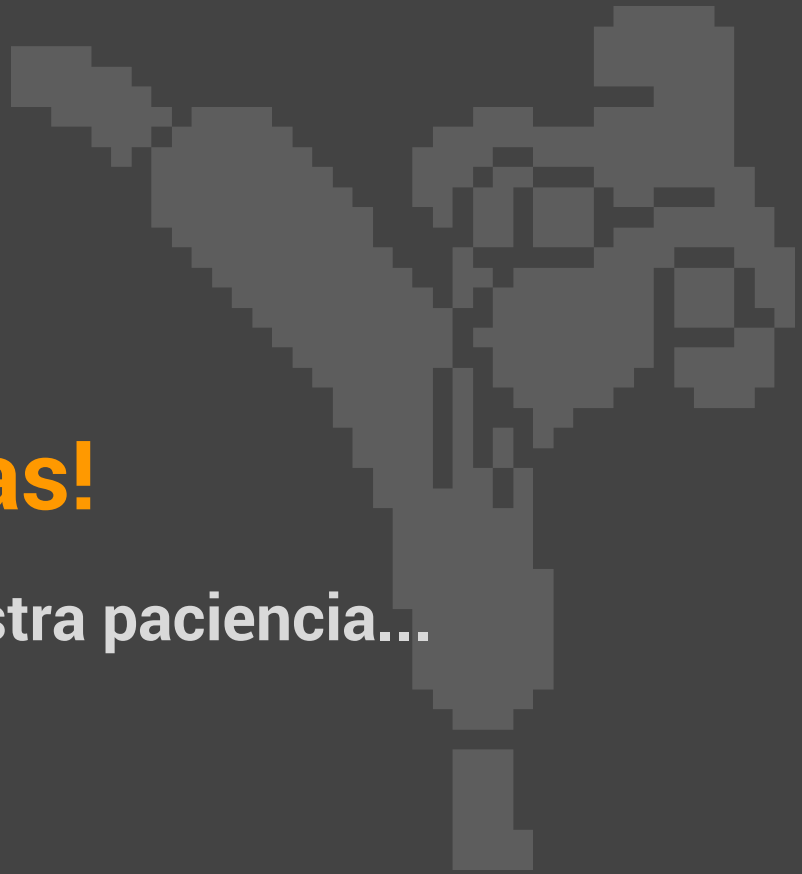
Disclaimer

Nada nuevo bajo el sol...

Referencias

- Google search: wannacry
  - :-P

¿Preguntas?



¡Gracias!

En particular por vuestra paciencia...