Security A(r)t Work

www.securityartwork.es
www.s2grupo.es

S2 GRUPO

Protección de Infraestructuras Críticas

Antonio Villalón
Director de Seguridad
avillalon@s2grupo.es

AENOR ER Empresa Registrada UNE-EN ISO 9001 ER-0343/2008
AENOR ER Seguridad Información UNE-ISO/IEC 27001 SI-0002/2006
AENOR ER Gestión Servicios TI UNE-ISO/IEC 20000-1 STI-0001/2011
AENOR ER Gestión I+D+i UNE 166002 IDI-0066/2010

Contenidos

- Algunas reflexiones…
- Seguridad… ¿lógica?
  - Mitos y realidades.
- Unos ejemplos.
- PIC en España.
- Conclusiones.

¿Protección de IICC?

¿Protección de IICC?

¿Qué sigue igual que hace 800 años… o más?

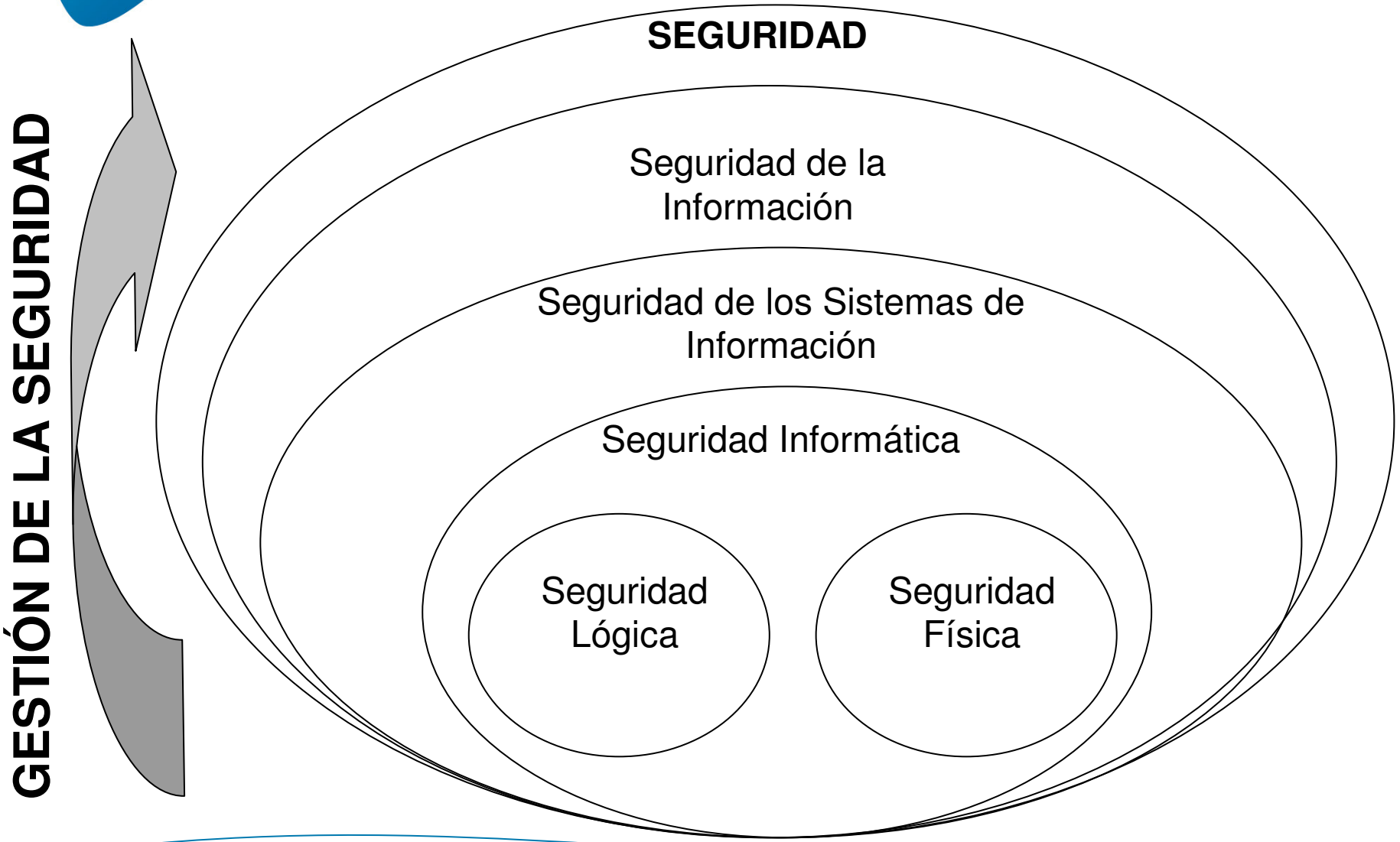
- Los pueblos (reinos, califatos, imperios… actualmente estados) NECESITAN proteger sus infraestructuras críticas…
  - Manantiales, depósitos de grano… o centrales nucleares.
- … y lo hacen (o lo intentan) en múltiples frentes…
- …con o sin LPIC.
- Los enemigos ATACAN esas infraestructuras críticas con dos objetivos primarios:
  - DESTRUCCIÓN (o degradación).
  - CONTROL.

¿Protección de IICC?

¿Qué ha cambiado en este tiempo? **LA TECNOLOGÍA**

- Beneficios indiscutibles en nuestras vidas, pero con contraprestaciones:
- Para **nosotros**:
  - Más necesidades básicas y por tanto más infraestructuras críticas
    - Electricidad, TIC, espacio, nuclear…
  - Más interdependencias entre ellas.
- Para un **enemigo**:
  - Más objetivos potenciales.
  - Más formas de ataque en todos los ámbitos…
    - … entre ellos, los relacionados con seguridad lógica.

Seguridad lógica



Seguridad lógica

- Medidas de seguridad (Resolución, de 15 de noviembre de 2011, de la Secretaría de Estado de Seguridad):
  - Organizativas o de gestión.
  - Operacionales o procedimentales.
  - De protección o técnicas.
    - Prevención y detección.
      - Medidas y elementos de seguridad física y electrónica.
      - **Medidas y elementos de seguridad lógica.**
      - Otros.
    - Coordinación y monitorización.
- Seguridad "lógica": salvaguardas lógicas… y todo lo demás.
  - Organización y gestión de la seguridad.
  - Respuesta ante incidentes.
  - Protección tecnológica.
  - Seguridad de la información.
  - …

Seguridad lógica: mitos

Responsabilidad de "Informática"

- ¿Qué leemos aquí?
  - Seguridad **lógica** vs. **Seguridad** lógica.
  - Seguridad **informática** vs. **Seguridad** informática.
  - Seguridad **tecnológica** vs. **Seguridad** tecnológica.
  - Seguridad **de la información** vs. **Seguridad** de la información.
- ¿Se habla en la legislación del "*Departamento de Informática*" o del "*Responsable de seguridad lógica*"?
- Separemos…
  - Informática vs. Seguridad.
  - Responsabilidad vs. Operación.

Seguridad lógica: mitos

Seguridad "de los ordenadores"

- Algo más que "ordenadores":
  - Sistemas SCADA.
  - Elementos de seguridad "tradicional": CRA, videovigilancia, controles de acceso…
  - …y otros "ordenadores": *tablets*, *smartphones*… INFORMACIÓN, en definitiva.
- Impacto de la tecnología en el negocio.
- La información como activo crítico.

Seguridad lógica: mitos

El riesgo no existe

- El impacto es alto
  - Dependencia de la tecnología (informática, electrónica…).
- ¿Y la probabilidad? Creo que también alta…
  - Superficie de ataque.
  - Riesgo para el atacante.
  - Impacto potencial.
  - …
- Escenarios con alta probabilidad y alto impacto.
  - R = P x I, ¿no?
  - **Alto riesgo.**

Seguridad lógica: realidades

- Los ataques tecnológicos a IICC son hoy en día una realidad.
  - No hablamos de ciencia ficción.
  - Alto impacto.
- Mismos objetivos principales que hace 800 años:
  - Destrucción/degradación.
  - Control.
- Rara vez hablamos de nuevos ataques.
  - Ataques clásicos cometidos a través de otros medios…
  - …con un problema añadido: estos nuevos medios NO sustituyen a los anteriores, sino que se añaden a ellos.
  - Quitemos el prefijo “ciber”.
    - Ciberdelincuencia, ciberguerra, ciberespionaje, ciberamenazas…

Seguridad lógica: realidades

- ¿**Qué** persigue un atacante?
  - Destrucción o degradación.
    - Denegación de servicio (DoS).
  - Control.
    - Alteración.
    - Robo de información.
- ¿**Quién** nos ataca?
  - Delincuentes.
    - Mafias.
    - Grupos terroristas.
    - …
  - Enemigos.
    - Estados.
    - Empresas.
    - …

Seguridad lógica: realidades

- ¿**Cómo** lo hacen?
  - Ataques generalistas, dirigidos o no.
  - Ataques específicos, dirigidos.
    - Amenazas persistentes avanzadas (APT).

- ¿**Dónde** nos pueden dañar?
  - Sistemas de control (destrucción, degradación, alteración).
  - Sistemas informáticos y de comunicaciones (todo lo anterior… y robo de información).

- ¿**Cuándo** nos pueden atacar?
  - Ahora mismo.

Seguridad lógica: realidades

- ¿**Por qué** un ataque lógico/tecnológico?
  - Conexión de sistemas a la red.
    - Sistemas generalistas.
    - Sistemas de control.
  - Impacto para el atacado.
    - Potencialmente alto…
    - …en especial, combinado con otros ataques.
  - Riesgo para el atacante.
    - Bajo (en especial si lo comparamos con otros ataques).
  - Otros factores, por ejemplo psicológicos.
    - Entendemos la bomba, pero no el ataque lógico…

Un ejemplo: STUXNET

- Malware dirigido a sistemas de control industrial de SIEMENS, descubierto en **junio de 2010**.
  - Sabotaje de variadores de frecuencia…
  - …solo los usados para enriquecer Uranio…
  - …y sólo los de ciertas empresas.
- Ataque dirigido, complejo y sofisticado.
  - Conocimientos elevados de informática.
  - Conocimientos elevados de sistemas SCADA.
  - Conocimientos elevados del proceso nuclear.
- Afecta al sistema (PLC) pero el operador no observa nada raro.
  - Resultado: uranio enriquecido de calidad deficiente.
- **Impacto:** retraso del programa nuclear iraní.
- **Creador:** desconocido.

Un ejemplo: DUQU

- Malware descubierto en **septiembre de 2011** y cuyo objetivo es el robo de información…
  - …útil para organizar ataques posteriores contra ICS.
- Ataque dirigido, complejo y sofisticado.
  - Muy similar a STUXNET en algunos puntos.
- Ataque pasivo (al menos inicialmente).
  - Podría alterarse el código para dañar sistemas.
- **Impacto:** desconocido (Irán reconoció contaminaciones).
- **Creador:** desconocido (¿los mismos que crearon STUXNET?).

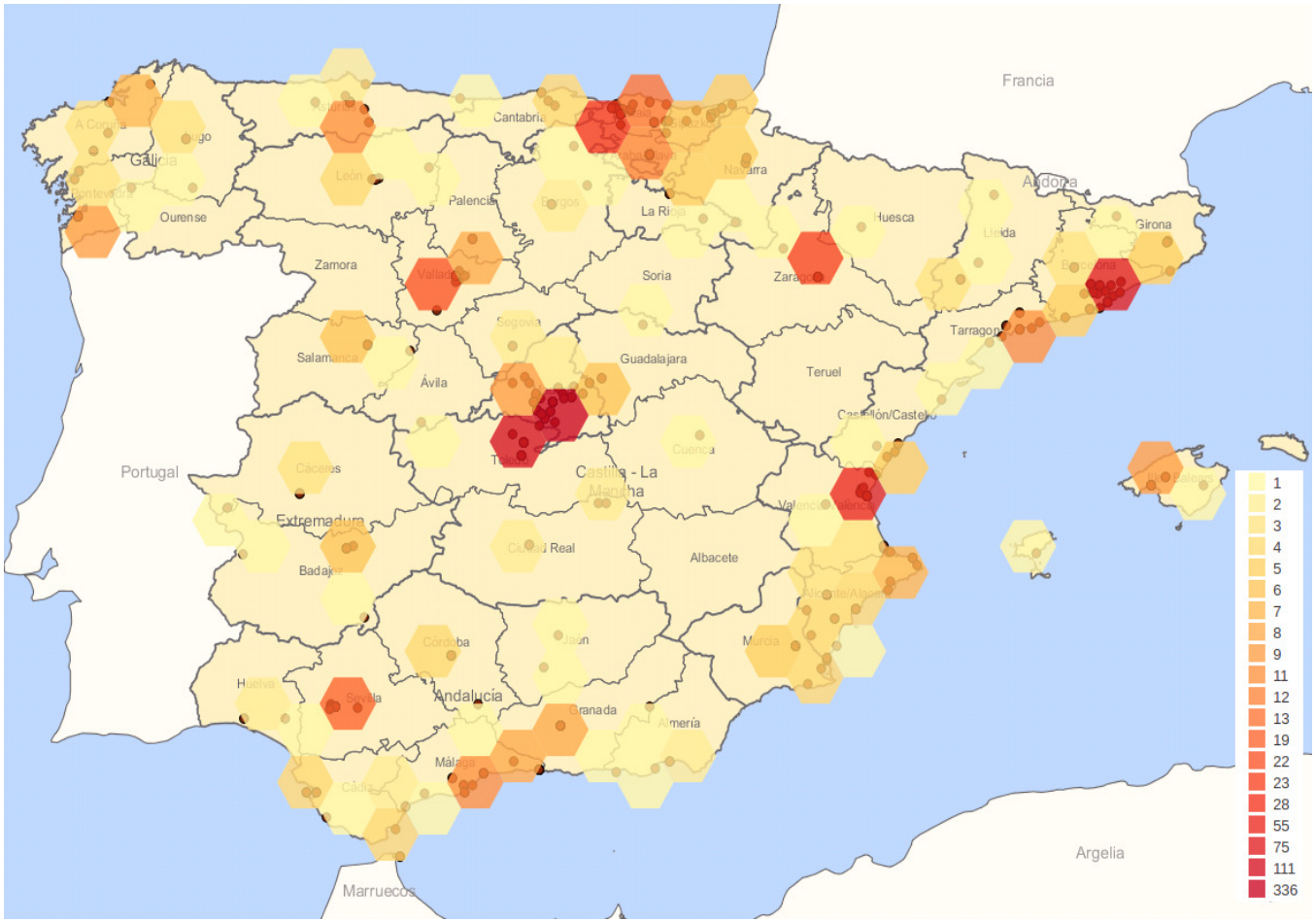
Un ejemplo: FLAME

- Malware descubierto en **mayo de 2012** cuyo objetivo es el robo de información…
  - ¡…activo desde febrero de 2010!.
- Ataque complejo y sofisticado.
  - Descrita como la mayor herramienta de espionaje descubierta hasta el momento.
    - Veinte veces más complejo que STUXNET.
    - Hasta diez años para analizar el malware por completo.
  - Puede espiar cualquier entorno donde se disemine.
- Ataque pasivo: espionaje.
- Contaminaciones principalmente en Oriente Medio.
- **Impacto:** desconocido.
- **Creador:** desconocido.

PIC en España

- Esto está sucediendo ahora mismo…
  - …y más ataques que no saltan a los medios generalistas…
  - …y más aún que desconocemos.
- ¿Y en España? Informe Técnico sobre PIC (junio 2012).
  - Análisis generalista, no dirigido.
  - Pruebas no hostiles (*information gathering*).
  - Herramientas NO avanzadas.
- Resumen:
  - Acceso potencial a unos 1.000 entornos de control.
  - Acceso potencial a unos 100 elementos adicionales ubicados en IICC.
  - Demasiados entornos inseguros.
    - Algunos sectores más que otros.

PIC en España



PIC en España

- Problemática: **falta de percepción del riesgo** (entre otros).
  - Desconocimiento.
  - Comodidad.
  - Inseguridad por defecto.
- Líneas de trabajo.
  - Eliminar el desconocimiento.
  - Primar seguridad frente a comodidad.
  - Exigir y mantener sistemas seguros.
- ¿Cómo?
  - Concienciación, concienciación y más concienciación…
  - …de **todos** los actores… empezando por el Departamento de Seguridad, con su Director al frente.

PIC en España

El rol del Director de Seguridad (aparte de lo dispuesto en la normativa…)

- Líder de la seguridad corporativa en las IICC.
  - Protección del negocio.
  - Responsabilidad sobre la **seguridad**, sin apellidos.
- Gestión global del riesgo (lógico, físico, humano…).
  - Debemos tomar consciencia del riesgo…
  - …y hacer que el resto de la organización la tome.
- ¿Qué **NO** hacer con la seguridad lógica/tecnológica/de la información…?
  - Pensar que no es un problema.
  - Pasar a otros la responsabilidad.

PIC en España

El rol del Director de Seguridad (aparte de lo dispuesto en la normativa…)

- ¿Qué hacer con la seguridad lógica/tecnológica/de la información…?

QUITARLE EL APELLIDO

- Elemento clave para…
  - …la seguridad particular de nuestras organizaciones.
  - …la seguridad de nuestras IICC.
  - …la seguridad de nuestro país.
- Hagamos lo mismo que hacemos con otros ámbitos de protección.
  - Planificar → Hacer → Comprobar → Actuar → Planificar…
- Es SEGURIDAD. Punto.

Conclusiones

- Ciberataques, ciberguerra… son conceptos que han dejado la ciencia ficción para convertirse en realidad.
  - Mismos problemas que hace siglos… a través de nuevos medios.
  - Quitemos la etiqueta “ciber”.
- Los elementos tecnológicos pueden ser un punto débil de nuestra seguridad corporativa.
  - No sólo seguridad lógica.
- Debemos protegernos desde el punto de vista tecnológico al igual que lo hacemos desde cualquier otro punto de vista.
  - Si no evaluamos estos aspectos de nuestra seguridad, otros lo harán por nosotros.
- Seamos conscientes del riesgo.

Y NO CONECTEMOS CUALQUIER COSA A UNA RED.

Referencias

- *"An inside look at Stuxnet"*. Jon Larimer, IBM X-Force. Noviembre, 2010.http://blogs.iss.net/archive/papers/ibm-xforce-an-inside-look-at-stuxnet.pdf
- *"Duqu: A Stuxnet-like malware found in the wild, technical report"*. Laboratory of Cryptography of Systems Security (CrySyS), Budapest University of Technology and Economics. Octubre, 2011. http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf
- *"Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East".* Symantec Security Response. Mayo, 2012. http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east

AENOR Empresa Registrada UNE-EN ISO 9001 ER-0343/2008

AENOR Seguridad Información UNE-ISO/IEC 27001 SI-0002/2006

AENOR Gestión Servicios TI UNE-ISO/IEC 20000-1 STI-0001/2011

AENOR Gestión I+D+i UNE 166002 IDI-0066/2010

GRACIAS

S2 GRUPO

Ramiro de Maeztu, 7
46022 Valencia
Tel. (+34) 963 110 300
Fax (+34) 963 106 086

Orense, 85. Ed.Lexington
28020 Madrid
T. (+34) 915 678 488
F. (+34) 915 714 244

info@s2grupo.es
www.s2grupo.es
www.securityartwork.es