



La convergencia de la seguridad



Antonio Villalón
avillalon@s2grupo.es





- Introducción: la convergencia de la seguridad
- La ruptura de las barreras
- ¿Por qué converger?
- Beneficios de la convergencia
- Condiciones para converger
- Obstáculos a la convergencia
- Conclusiones
- Referencias



Introducción: problemática



- Seguridad física.
 - Protección de personas.
 - Protección de bienes inmuebles.
 - ...
- Seguridad lógica.
 - Protección de sistemas.
 - Protección de redes.
 - Protección de información.
 - ...
- Continuidad del negocio.
- Seguridad legal.
- Gestión de riesgos.
- ...



- Seguridad física.
 - Protección de personas.
 - Protección de bienes inmuebles.
 - ...
- Seguridad lógica.
 - Protección de sistemas.
 - Protección de redes.
 - Protección de información.
 - ...
- Continuidad del negocio.
- Seguridad legal.
- Gestión de riesgos.
- ...

PROTECCIÓN DE ACTIVOS
SEGURIDAD DE NEGOCIO
RIESGO



Introducción: convergencia



- **CONVERGENCIA:** Cooperación formal de las diferentes funciones de seguridad en una organización.
 - Principalmente, seguridad física y seguridad lógica, pero también seguridad legal, continuidad del negocio, seguridad de RRHH...
- **OBJETIVO:** Proteger de la mejor forma posible los activos de la organización de cualquier amenaza que les pueda causar un daño, sin importar su origen.
- **IDEA:** Un atacante (o cualquier otra amenaza) nos dañará de la forma más sencilla para él, ya sea física, lógica, legal...
 - “La seguridad es una cadena...”



Introducción: convergencia



- ¿Qué NO es convergencia?
 - Unificar varios departamentos de seguridad del organigrama en uno único, sin ir más allá.
 - Forzar una reunión mensual entre las áreas de seguridad física y seguridad lógica (por ejemplo).
 - Regalar una pistola a los ingenieros de seguridad lógica y un ordenador a los guardias de seguridad: NO buscamos técnicos todoterreno.
 - ...



La ruptura de las barreras



- Existen cinco grandes catalizadores que aceleran y motivan la convergencia de la seguridad en las organizaciones:
 - Convergencia tecnológica.
 - Convergencia de los proveedores.
 - Convergencia de la comunidad de seguridad.
 - Convergencia de las amenazas.
 - Convergencia de la formación.



La ruptura de las barreras: convergencia tecnológica



- NNTT desdibujan las fronteras entre “seguridades”.
- Caso más claro: control de acceso y presencia.
 - Cámaras IP
 - CRAs vía TCP/IP.
 - Detección de intrusos “físicos”.
 - Smart Cards.
 - Legislación.
 - ...
- Otros ejemplos: sistemas SCADA, robos en cajeros automáticos, videovigilancia...



La ruptura de las barreras: convergencia de los proveedores



- Los proveedores de seguridad clásicos se focalizan en un ámbito concreto: coches blindados, cortafuegos, cámaras de seguridad, IDSes...
- La expansión de los negocios hace que se amplie el catálogo de servicios de los proveedores clásicos...
- ... y no sólo dentro de la “miniseguridad” inicial del negocio.
- Algunos ejemplos: Computer Associates, Nortel Networks, Kroll, Unisys...



La ruptura de las barreras: convergencia de la comunidad



- El mundo de la seguridad se basa en buena parte en la confianza y en la colaboración.
- Hasta 2004/2005, las asociaciones que aglutinaban a miembros con diferentes funciones de seguridad no tenían relación entre sí.
- En estos momentos, las colaboraciones son constantes, destacando *The Alliance for Enterprise Security Risk Management*, formada por ISACA, ASIS e ISSA.



La ruptura de las barreras: convergencia de las amenazas



- Como resultado de la convergencia tecnológica, las amenazas contra nuestros activos también convergen.
- Escenario: un ataque que combine elementos físicos y lógicos contra una organización.
- Ejemplo: una bomba en el centro de la ciudad combinada con el bloqueo remoto del control de los semáforos mediante una negación de servicio.
- Recordemos la IDEA que lanzamos al inicio de esta sesión.



La ruptura de las barreras: convergencia de la educación



- Cada vez más habitualmente, los masters en Dirección de Seguridad (física) incluyen referencias a seguridad de la información, como activo crítico que es necesario proteger en cualquier organización.
- Cualquier referencia en seguridad de la información habla también de seguridad física, legal, etc. (por ejemplo, ISO 27002).
- Esto no significa que busquemos personal multidisciplinar a nivel técnico, sino a nivel de gestión: el Director de Seguridad debe ser un gestor del riesgo **global**.



¿Por qué converger?



- Hemos visto catalizadores externos a la organización que pueden beneficiar la convergencia...
- ...pero ¿qué sucede internamente?
- Dentro de la organización, también existen razones importantes que motivan la convergencia de la seguridad:
 - Expansión del “ecosistema” empresarial.
 - Migración de los activos de valor.
 - Factores tecnológicos.
 - Cumplimiento.
 - Factores económicos.



¿Por qué converger?

Expansión del ecosistema empresarial



- Complejidad creciente de las organizaciones.
- Interrelación entre elementos de la organización.
 - Seguridad física, Departamento Legal, Departamento de tecnología, Recursos Humanos...
- Relación entre organizaciones.
 - Proveedores, clientes, partners...
- Pérdida del perímetro de seguridad.
 - Economía global: amenazas globales.



¿Por qué converger?

Migración de los activos de valor



- ¿Qué quiere proteger una organización?
 - 1970: Personas, edificios, productos, maquinaria...
 - 2008: Información, información, información... y todo lo de 1970.
- Información es un activo cada vez más crítico para las organizaciones.
- Dependencia de los activos físicos en activos más intangibles, como la información (y los sistemas que la tratan).
 - ¿Cómo se controla el acceso a nuestras oficinas?



¿Por qué converger? Factores tecnológicos



- Hemos hablado ya de la convergencia tecnológica...
- Esta convergencia hace que diferentes grupos funcionales dentro de la organización deban unificar y compartir sus estrategias.
 - Ejemplo: Control de acceso físico y lógico con las mismas tarjetas inteligentes.
- Busco unificar tecnologías y reducir costes.



¿Por qué converger? Cumplimiento



- Organizaciones cada vez más complejas, sobre las que aparecen nuevas amenazas: nuevas normativas, estándares o leyes a cumplir.
- Cumplimiento complejo que exige la unificación de diferentes puntos de vista de la seguridad.
- Gestión unificada.



¿Por qué converger? Factores económicos



- Reducción del coste en el proceso de gestión del riesgo.
- Un departamento de seguridad único implica menores costes a la organización:
 - Optimización de recursos.
 - Agilización de la seguridad.
 - Riesgos que cambian rápidamente.
 - Transparencia de la función de seguridad.
 - ...
- ¡OJO! No debo reducir la calidad del trabajo en seguridad.



Beneficios de la convergencia



- Hemos comentado factores, tanto externos como internos a la organización, que nos deben hacer plantearnos converger...
 - ... ¿pero qué obtenemos a cambio?
- Los beneficios de la convergencia para nuestra organización son claros:
 - Alineación de la seguridad con el negocio.
 - CSO como referencia única.
 - Intercambio de información.
 - Personal de seguridad versátil.
 - Reducción de costes.



Beneficios de la convergencia: alineación con el negocio



- Actualmente, nadie considera la seguridad como un gasto, sino como una actividad básica para el negocio y la supervivencia de la organización.
- Los objetivos de seguridad deben estar, por tanto, plenamente alineados con los objetivos de negocio.
 - El objetivo de la organización no es (habitualmente) la seguridad.
- Mediante una estrategia de convergencia, se facilita dicha alineación, ya que la gestión de los diferentes puntos de vista de la seguridad está unificada.



Beneficios de la convergencia: CSO como referencia única



- Una persona dentro de la organización es responsable de la SEGURIDAD.
- Visión global de la seguridad en la organización: Plan Director de Seguridad completo, basado en una correcta priorización de los riesgos corporativos.
- Gestión de recursos (humanos, económicos, materiales...) única y alineada con los objetivos de la organización.
- Punto único de contacto (para la Dirección, para los empleados, para el departamento de seguridad, para los clientes...).



Beneficios de la convergencia: intercambio de información



- El intercambio de información se considera en la actualidad como un elemento crítico para la seguridad, tanto para la organización más pequeña como para una nación entera.
 - ISAC (USA), WARP (UK), TISN (AU)...
- La colaboración de las diferentes funciones de seguridad marca objetivos comunes y una estrategia conjunta en la organización...
 - ... a pesar de las diferencias funcionales que pueden existir en diferentes ámbitos de la seguridad.



Beneficios de la convergencia: personal de seguridad versátil



- Un mismo grupo de personas trabaja conjuntamente con el objetivo común de garantizar la seguridad de la organización.
- Se abarcan todos los ámbitos de la seguridad, trabajando de forma efectiva en cada uno de ellos, y coordinados por un gestor global de la seguridad en la organización.
- En ningún momento hablamos de las mismas personas cubriendo todos los ámbitos técnicos de la seguridad.



Beneficios de la convergencia: reducción de costes



- Cualquier organización busca rebajar al mínimo los costes de todos los procesos corporativos sin menoscabar su calidad.
- Una visión convergente de la seguridad facilita dicho ahorro...
 - ... en personal.
 - ... en duplicidad de trabajos.
 - ... en logística.
 - ... en infraestructuras.
 - ... en tecnologías de seguridad.
 - ...



Condiciones para converger



- Hemos analizado los factores que motivan la convergencia de la seguridad y los beneficios que dicha convergencia ofrece a nuestra organización.
- Ahora la pregunta es... ¿qué condiciones debemos garantizar en la organización para poder converger?
- Para que se produzca una convergencia correcta en la seguridad de una organización, deben darse las siguientes condiciones:
 - Apoyo de la alta dirección.
 - Director de Seguridad.
 - Equipo de trabajo.
 - Plan de trabajo.



Condiciones para converger: apoyo de la Dirección



- Como cualquier iniciativa relacionada con la seguridad, la convergencia no será exitosa sin el apoyo de la Dirección.
- Liderazgo y apoyo a la convergencia, considerando la seguridad en su conjunto como un elemento clave para el mantenimiento y desarrollo del negocio.
- Este apoyo es indispensable para garantizar la eficacia y eficiencia de los proyectos de convergencia... y el éxito de los mismos.



Condiciones para converger: El nuevo Director de Seguridad



- Habitualmente, en una misma organización...
 - CSO (*Chief Security Officer*). Responsable de 3G (*Guards, Guns & Gates*).
 - CISO (*Chief Information Security Officer*). Responsable de seguridad de la información (en muchos casos, sólo TIC).
- Convergencia hacia un CSO holístico, multidisciplinar y con una alta capacidad de gestión, reportando a la Dirección y gestionando el riesgo global de la organización.
- **CRÍTICO:** Confianza en el CSO desde todos los ámbitos de la organización.



Condiciones para converger: Equipo de trabajo



- Equipo multidisciplinar.
 - ¡¡RESPECTO!!
- El equipo de trabajo debe comprender y asumir como propio el concepto de convergencia de la seguridad.
- Líder claramente definido para el equipo: CSO.
- Trabajo conjunto para controlar el riesgo de la organización



Condiciones para converger: Plan de trabajo



- Plan de trabajo viable que permita una transición suave desde la situación actual a una situación de convergencia.
 - La convergencia no se logra en un día.
- Evitemos las medidas drásticas.
- Evitemos la confrontación.
- Apoyemos y potenciemos los éxitos como equipo.
- Mantengamos continuamente el apoyo de la Dirección.



Obstáculos a la convergencia



- Parece obvio que una estrategia de convergencia nos puede ayudar a garantizar la seguridad de la organización y, por tanto, su negocio. Pero...
- ...¿qué obstáculos nos podemos encontrar a la hora de converger?
 - Diferencias culturales.
 - Áreas de conocimiento diferentes.
 - Pérdida de control.
 - Factores políticos.



Obstáculos a la convergencia: diferencias culturales



- El respeto (o mejor dicho, su falta) entre el personal dedicado a las diferentes funciones de seguridad puede convertirse en un obstáculo a la convergencia.
 - El personal que trabaja en seguridad lógica ve al que trabaja en seguridad física como “los de pistola en mano”, y estos a los primeros como tecnólogos que se preocupan únicamente de sus “cacharros”.
 - Se consideran grupos de trabajo diferentes.
 - Menosprecio al trabajo del resto.



Obstáculos a la convergencia: diferencias culturales



- ¿Cómo superar este obstáculo?
 - Trabajo conjunto.
 - Formación conjunta (relativa).
 - Concienciación conjunta.
 - Objetivos de seguridad comunes.
- ¿Cómo NO superar este obstáculo?
 - Cambios en el personal.
 - Imposiciones no razonadas.



Obstáculos a la convergencia: áreas de conocimiento diferentes



- Ningún grupo de seguridad (física, lógica, legal, RRHH...) puede asumir de forma independiente la seguridad global.
- ¿Cómo superar este obstáculo?
 - No buscamos que un grupo asuma el trabajo del resto (imposible).
 - Debemos mantener funciones técnicas de seguridad diferentes, pero gestionadas en un mismo punto.
 - Todos trabajamos por un objetivo común: la seguridad.



Obstáculos a la convergencia: pérdida de control



- Sensación de pérdida de control cuando otro grupo de seguridad realiza tareas cercanas a las que realizamos nosotros.
- Sentimientos de desconsideración, de pérdida de presupuesto, miedo a perder el puesto de trabajo...
- ¿Cómo superar este obstáculo?
 - DIFÍCIL: se trata en muchos casos de sensaciones, no de hechos.
 - Trabajo conjunto y confianza.



Obstáculos a la convergencia: factores políticos



- Luchas de poder entre departamentos relacionados con la seguridad de una misma organización.
- Rechazo a la convergencia: intromisión en parcelas de poder, pérdida de peso en la organización, incremento de carga de trabajo...
- ¿Cómo superar este obstáculo?
 - Intervención de la Dirección: se busca mitigar riesgos y reducir costes, no pelear entre nosotros.



Conclusiones



- La convergencia de la seguridad es una tendencia clara en el panorama actual, que a medio plazo puede convertirse en la tónica habitual e incluso en la recomendación/obligación para ciertas organizaciones.
- Un modelo de convergencia puede ser beneficioso, pero un enfoque erróneo puede no sólo no mejorar cualquier situación actual, sino incluso empeorarla.



- *Convergence of Enterprise Security Organization*. Booz, Allen, Hamilton. The Alliance for Enterprise Security Risk Management. Noviembre 2005.
- *Convergence: The Payoff... The Pain*. CSO Magazine, Abril 2005.
- *CSO Fundamentals: ABCs of Physical and IT Security Convergence*. CSO Magazine, Diciembre 2005.
- *Chief Security Officer (CSO) Guideline*. ASIS International, Enero 2004.



Antonio Villalón
Director Técnico de Explotación

S2 Grupo
Vinalopó, 7 bajo
46021 Valencia
Tel.: 963 110 300
Fax: 963 106 086

info@s2grupo.es
www.s2grupo.es

