Security A(r)t Work

www.securityartwork.es
www.s2grupo.es

S2 GRUPO

Seguridad dentro y fuera de la nube

Antonio Villalón
Director de Seguridad
avillalon@s2grupo.es

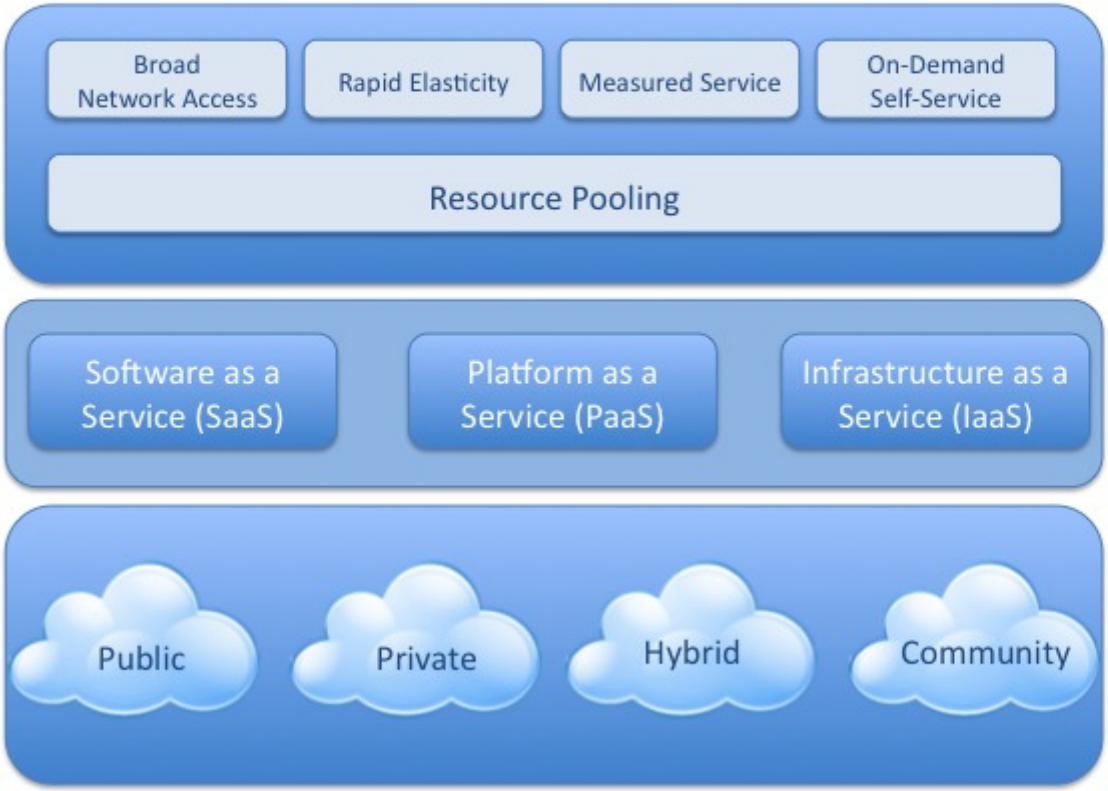
AENOR ER Empresa Registrada UNE-EN ISO 9001 ER-0343/2008
AENOR ER Seguridad Información UNE-ISO/IEC 27001 SI-0002/2006
AENOR ER Gestión Servicios TI UNE-ISO/IEC 20000-1 STI-0001/2011
AENOR ER Gestión I+D+i UNE 166002 IDI-0066/2010

Introducción

- Nuestro trabajo es **proteger el negocio** desde todos sus puntos de vista: personas, procesos, infraestructuras físicas… e **información**.
- Un día el CEO nos comunica que tenemos que migrar a la nube…
  - ¿Quién se lo ha dicho?
- …y nos pregunta cómo hacerlo de forma segura.
- Como esto nos pilla mayores, empezamos a ver qué es eso de la nube (en el NIST, que de seguridad saben un rato).
- Al principio nos recuerda algo y no sabemos el qué…
  - sed s/cloud/mainframe/g
- …pero nos topamos con cuatro modelos de despliegue (público, privado, híbrido y comunidad) y tres modelos de servicio (SPI) que nos proporciona un *Cloud Provider* (CP).
  - Doce combinaciones, sin contar mutaciones. ¡Toma ya!

Introducción

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



Introducción

- Primera impresión: de una u otra forma confío mi información a un tercero que la pasará por servidores de medio mundo.
  - ¿Confío o me fío?
  - Dos preocupaciones principales: **confidencialidad** y **control**.
- Seguridad implica confianza. Siempre acabo confiando en alguien…
  - …¡pero el CP me pide unos niveles de confianza hasta ahora reservados a mi mujer… o más!
- ¿Qué hago yo para proteger a la organización, y en especial a su información?
  - Dicen que gestionar (y si soy optimista, mejorar).
- ¿Debo seguir haciendo lo mismo en la nube?
  - Yo creo que sí… al menos de momento.
- ¿Cómo empiezo?
  - La gran pregunta. ¿ISO 2700X?

Análisis de riesgos

- He hecho un análisis de riesgos que tengo siempre en mi pantalla… y además lo actualizo en tiempo real, lo reviso periódicamente y mil cosas más…
  - ¿Habrá hecho lo mismo el CP? Seguro que sí.
  - ¿Se preocupará tanto como yo de MIS riesgos? Esto…
- Si me voy a la nube, ¿qué hago con mi análisis?
  - Modificaciones sustanciales de los niveles de probabilidad e impacto de las amenazas habituales.
  - Nuevas amenazas.
- ¿Debo rehacer mi AR por completo?
  - Seguramente sí.
  - ¿Me dará el CP los datos que necesito? ¿Cuándo?
  - Base para las decisiones que se tomarán después.

Política de Seguridad

- Tengo un papel colgado en mi despacho que dice lo buenos y seguros que vamos a ser.
  - ¿Debo cambiarlo? Creo que no…
  - ¿Lo tiene el CP? Espero que sí…
- Ese papel se refina en normativas, procedimientos, especificaciones de requisitos, etc.
  - Aquí ya toca cambiar cosas.
- Tendré que ampliar y modificar mis documentos para adaptarme al nuevo paradigma…
  - …sin descuidar lo anterior: no todo es la nube.
- ¿Podrán cubrir esos papeles los mínimos que necesito?

Aspectos organizativos

- La organización interna de mi seguridad está controlada: acuerdos de confidencialidad, definición de responsabilidades, contacto con terceros…
  - Pues que siga tan controlada. Enhorabuena.
  - Cambios menores en la nube… al menos por la parte que me toca.
- La relación con terceros (proveedores, *partners*…) también creo tenerla controlada.
  - Ahora deberé potenciarla al máximo.
  - Mi seguridad pasa a depender en buena parte de la seguridad del CP.
- Posiblemente deba confiar tanto en el CP (un proveedor, a fin de cuentas) como en la gente de IT (internos, compañeros).

Gestión de activos

- Mis activos están inventariados, tienen responsable asignado y una política de uso aceptable.
  - Los del CP seguro que también… desde su punto de vista.
  - ¿Y desde el mío?
- Mi información se clasifica, marca y trata según procedimientos internos, incluyendo caducidad, destrucción, etc.
  - ¿Qué me garantiza el CP? ¿Qué pasa con SaaS?
- ¿Dónde están mis activos? ¿Dónde están mis datos?
  - ¡En la nube!

Seguridad ligada a RRHH

- Hasta ahora realizo un estupendo *CV screening* del personal…
  - … ¿lo hace también el CP?
- Hasta ahora, mantengo una política de formación e información en seguridad para el personal…
  - …¿y él?
- Reviso que la seguridad de RRHH es conforme a mi normativa.
  - ¿Cuál es la suya?
- Cuando alguien deja la organización me encargo de cerrar las puertas correspondientes…
  - …espero que el CP también.
- …
- Independientemente de todo, ¿son sus objetivos o requisitos equivalentes a los míos?

Seguridad física y del entorno

- Quiero creer que las instalaciones –en especial, los CPD, archivos… donde se ubica información clasificada- del CP son al menos tan seguras como las mías :)
  - Control y registro de acceso físico a zonas de la organización.
  - Monitorización ambiental en CPD.
  - Suministros básicos garantizados.
  - …
- Por tanto, desde este punto de vista sin duda mejoro mi seguridad… ¿verdad?
  - No hay duda que el CP me proporcionará un listado de las personas que han accedido físicamente a mi infraestructura en cuanto yo se lo pida, o un histórico de monitorización de parámetros ambientales del mes pasado… ¡por supuesto!

Gestión de Comunicaciones y Operaciones

- ¿Tendrá el CP todo su operación documentada? ¿Podré auditarla?
- ¿Qué controles técnicos implanta él y cuáles implanto yo?¿Qué garantías me ofrece? De IaaS a SaaS.
  - Antivirus, firewall, IDS/IPS, parches…
  - ¿Tengo acceso a los registros?
  - ¿Podría saber cuántas veces me han atacado durante el último mes?
- El CP hará copias de seguridad de mis recursos.
  - Y yo también si puedo, por si acaso.
- ¿Me permitirá el CP quitarme de encima el problema de los dispositivos extraíbles?
  - No, obviamente.
- El CP monitoriza sus recursos y por tanto los míos. No hay duda.
  - ¿Me proporcionará los *logs*? ¿Me avisará cuando algo vaya mal?

Control de acceso

- ¿Cómo accederé a mis recursos en la nube? ¿Con un password?
  - ¿Puedo disponer de autenticación robusta? Pagándola, por supuesto…
- ¿Cómo se garantiza el *need to know*?
- ¿Es capaz el CP de detectar anomalías en el acceso?
  - Y lo más importante…¿qué hace si las detecta?
- ¿Qué sucede si me roban credenciales? ¿Qué hace el CP?
  - ¿Y en cuánto tiempo?
- Y si estoy en una nube pública, ¿se controla el acceso a las interfaces de administración? ¿cómo?
- Si la movilidad me había roto el perímetro casi por completo, la nube me lo destroza…

Adquisición, desarrollo y mantenimiento de sistemas

- Seguro que el CP tiene implantado un buen procedimiento de control de cambios.
  - Yo también.
  - ¿Seremos compatibles siempre?
- ¿Debo definir nuevos casos de uso para mis aplicaciones?
  - Y por tanto, también de **abuso**.
- ¿Puedo analizar las vulnerabilidades de mis recursos en la nube?
  - ¿Servirá para algo?
- ¿Y si almaceno código fuente propio en la nube?
  - Mismos problemas y ventajas que con el resto de información.
- ¿Y qué hay de las claves criptográficas?
  - ¿Generación en la nube? ¿Entropía?
  - ¿A quién se las doy?

Gestión de incidentes

- Tengo un procedimiento de gestión de incidentes que cubre desde la notificación al aprendizaje, pasando por el simulacro periódico.
  - ¿Lo tendrá el CP? Al menos para SUS incidentes, seguro.
- Si algo sucede, ¿en qué me ayudará el CP? ¿cómo lo hará?
  - ¿Cómo podré notificarle?
  - ¿Podré disponer de una imagen de mis recursos para hacer un forense?
  - ¿Me dará los *logs* que le solicite?
  - ¿Aprenderá conmigo?
- ¿Y qué hay de la validez de la prueba y la recolección y preservación de evidencias?
  - Este tema mejor dejarlo, incluso sin nubes de por medio…

Gestión de continuidad de negocio

- Con mis datos distribuidos por la nube, aquí sí que voy a mejorar…
- ¿Dónde puedo firmar los RPO y RTO?
  - Los podré negociar con el CP, ¿no?
- ¿Quién me notificará de una degradación considerable del servicio?
  - ¿Me llamará el CP?
- ¿Ante un problema en el servicio seré igual de importante que mi vecino, más importante que él… o menos importante?
- Y tendré que hacer pruebas periódicas de mis planes de continuidad…
  - …junto al CP, por supuesto.

Compliance

- Esto de tener información confidencial (tanto datos de carácter personal como información clasificada) en la nube no parece muy bueno, ¿no?
- ¿Dónde se ubica físicamente la información? ¿Externaliza servicios el CP? ¿Qué jurisdicción aplicamos?
- Esto se nos escapa…¿llamamos a un abogado?
- ¿Y qué hay del cumplimiento técnico?
  - ¿Derecho de auditoría? ¿Hasta dónde?
- ¿Quién se ajusta a los estándares del otro?
  - ¿Se dignarán organizaciones como Google, Amazon o Microsoft a modificar *algo* porque yo se lo diga?

Entonces…¿migro a la nube?

- Análisis de riesgos *First Cut*.
- Beneficios:
  - Escalabilidad.
  - Costes.
  - Flexibilidad.
  - …
- Riesgos relevantes:
  - Pérdida de control.
  - Confidencialidad.
  - *Compliance*.
  - Riesgos derivados de infraestructuras compartidas (aislamiento, borrado de datos….).
  - Dependencia del CP.
  - …

Entonces…¿migro a la nube?

- Alternativas: nubes privadas, VPC…
- ¿Quién opera la nube? ¿En quién confío (o de quién me fío)?
- ¿Resuelven todos mis problemas?
  - Ni mucho menos :(
- ¿Qué hago?
  - Como hemos dicho antes, siempre tengo que confiar en algo o en alguien (en la nube o fuera de ella).
  - Pero…¿hasta dónde confiar?
- Análisis de riesgos particularizado en cada caso.
  - El análisis no es matemático, solo un apoyo en la toma de decisiones.
- Algunos consejos de gente que sabe…

Entonces…¿migro a la nube?

- Nueve palabras clave para MI seguridad en la nube (Robert Gellman):
  - *Terms of Service.*
  - *Location, location, location.*
  - *Provider, provider, provider*.
- *Risk Appetite*:
  - Los acuerdos de servicio deben ser aceptables.
  - La ubicación de la información no debe introducir restricciones legales que no podamos asumir.
  - El CP debe ser confiable (recordemos que vamos a proporcionarle nuestra información).
- Algunos ejemplos…

Ya, pero…¿migro a la nube?

- Si la seguridad de mis datos no me ha preocupado hasta ahora ni me preocupará en un futuro…
  - …migra a la nube en la modalidad que quieras. Tendrás problemas equivalentes a los actuales, pero más baratos.
  - Replantea tu posición, aunque sea por las sanciones :)
- Si la seguridad de mis datos me preocupa hasta cierto punto…
  - …me puedo plantear una nube pública.
  - En función del modelo de entrega, mayor o menor seguridad (IaaS > PaaS > SaaS). En términos generales, por supuesto.
- Si la seguridad de mis datos me preocupa algo más…
  - …nube privada, IaaS.
- Si vivo de la seguridad de mis datos…
  - …nube privada gestionada por la organización. ¿Vale la pena?
- También puedo, en cualquier caso, intentar no migrar a la nube…

Vale, me lo pensaré…

- Sea como sea, no debemos descuidar los aspectos de seguridad ni dentro ni fuera de la nube.
  - Los *pendrives* no se cifran en ninguna nube.
  - La movilidad sigue siendo un problema.
  - El papel también hay que protegerlo.
  - Sigue habiendo información clasificada en equipos finales.
  - Los usuarios… siguen siendo usuarios.
  - Es obligatorio cumplir las leyes.
  - Siguen existiendo cortafuegos, controles de acceso, antivirus, permisos en Unix :)
  - …
- *All it is, is a computer attached to a network.* Larry Ellison, Oracle CEO.

Conclusiones

- No todo lo que hay en la nube es malo… ni bueno.
- La migración a la nube es un hecho que en ocasiones no depende de nosotros. No siempre podremos pararlo, aunque a veces queramos.
- Debemos adaptarnos y buscar una solución aceptable para la organización.
- Diferentes modelos, diferentes costes… y diferente seguridad.
  - Del todo a la nada.
- No hay una solución única para todos: analicemos los riesgos en cada caso y tomemos decisiones justificadas.
  - O demos la información adecuada para que se tomen.
- Migremos o no, nuestra seguridad no sólo estará en la nube…
  - …siempre habrá una parte fuera de ella.

Referencias

- Cloud Computing. Benefits, risks and recommendations for information security. *ENISA*. Noviembre, 2009.
- Security Guidance for Critical Areas of Focus in Cloud Computing v2.1. *Cloud Security Alliance*. Diciembre, 2009.
- Guidelines on Security and Privacy in Public Cloud Computing. *NIST. Draft SP 800-144*. Enero, 2011.
- Privacy in the clouds: Risks to privacy and confidentiality from Cloud Computing. *Robert Gellman. World Privacy Forum*. Febrero, 2009.
- Schneier on Security: Cloud Computing. *Bruce Schneier*. Junio, 2009.

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