Security A(r)t Work

www.securityartwork.es
www.s2grupo.es

S2 GRUPO

Gestión de Incidentes

Diez errores habituales

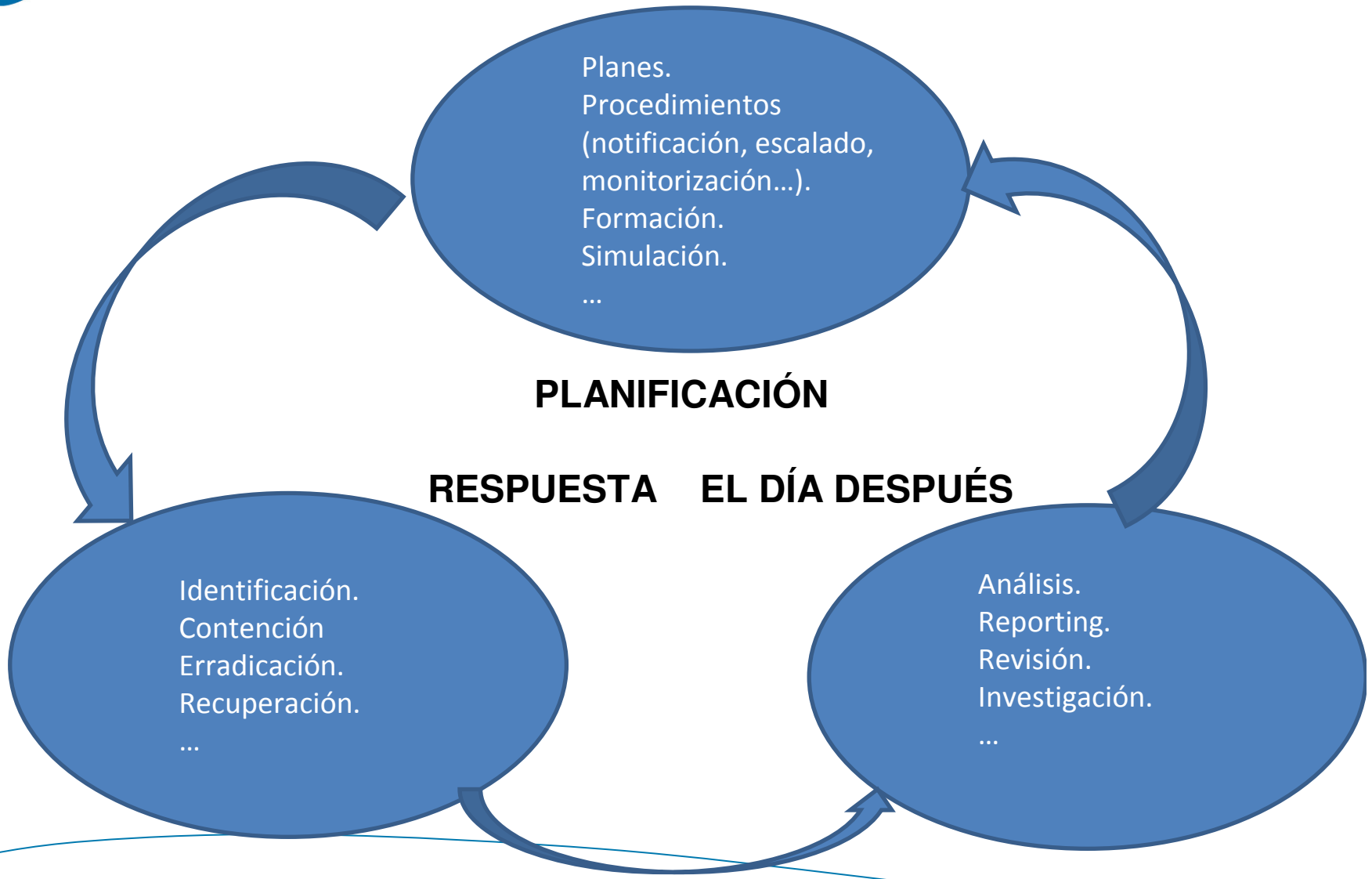
Antonio Villalón
Director de Seguridad
avillalon@s2grupo.es

Introducción

- Incidente de seguridad: Conjunto de uno o más eventos de seguridad **no planificados** y con una **probabilidad significativa** de comprometer las operaciones del negocio y amenazar a la seguridad corporativa (ISO/IEC TR 18044:2004… próxima ISO 27035).

- La gestión de incidentes de seguridad es un **proceso continuo** que debe controlar las actividades **antes**, **durante** y **después** de que un incidente ocurra.

Gestión de incidentes



Error #1: PLANIFICACIÓN

FALTA DE MONITORIZACIÓN

- Nos enteramos tarde y mal… frecuentemente por terceros.
- *No news, good news?*
- Soy puramente **reactivo**: lo peor que puedo hacer en seguridad.

SOLUCIONES

- Monitorizar (obvio, ¿no?).
- ¿El qué? Todo lo que pueda causar un incidente
  - Desde la infraestructura TI a los empleados, pasando por parámetros medioambientales.
- Procesar la información generada por los monitores.
- ¡Que el exceso de información no se convierta en un problema!
  - Si queremos pasar de la nada al todo, tendremos un problema.ç
  - Correlación.

Error #2: PLANIFICACIÓN

FALTA DE PROCEDIMIENTOS Y PLANIFICACIÓN

- Incluso aunque monitoricemos… llega el día D y la hora H y no sabemos qué hacer.
- ¿A quién llamamos? ¿Cuáles son las prioridades de la organización?¿Quién es responsable de…? ¿Debemos comunicarlo?
- El momento en que un incidente se materializa es el peor para pensar.
  - Las situaciones de tensión nos transforman… en todos los ámbitos de la vida…
  - …y si no, preguntadle a un guardaespaldas.

SOLUCIONES

- Todo lo relevante debe estar escrito y ser accesible por los implicados.
- A la hora de planificar, pensemos en las prioridades del negocio.
- CRÍTICO: Agilidad de la notificación, y por tanto de la respuesta.
- OJO: Recordemos que el papel es muy sufrido (ver error siguiente).

Error #3: PLANIFICACIÓN

FALTA DE SIMULACROS

- Ya tenemos todo analizado y escrito, pero probamos que funciona correctamente justo cuando se produce un incidente.
- Recordemos: en una situación de tensión nos transformamos…
  - ¡incluso nos volvemos “tontos”!
- Como decimos, el papel es muy sufrido… la realidad no.

SOLUCIONES

- De nuevo, miremos a nuestros vecinos de seguridad física…
  - ¿Alguien trabaja en protección contra incendios? ¿En prevención de emergencias?
- Simulacros periódicos.
  - Incluso por temas de continuidad de negocio.

Error #4: RESPUESTA

IDENTIFICACIÓN ERRÓNEA

- Si identificamos mal un incidente, trabajaremos en la línea equivocada.
  - Esto siempre es malo, pero a la hora de gestionar un incidente es fatal.
- Nos focalizamos en los efectos, no en las causas.

SOLUCIONES

- Dediquemos N minutos a pensar fríamente.
- Analicemos todas las posibles causas… y su probabilidad.
- Dos cabezas piensan más que una, y tres más que dos.
  - Y si son de áreas diferentes, mejor todavía.
  - Y si participa alguien de negocio, ya brindamos.

Error #5: RESPUESTA

LO PRIMERO, RECUPERAR

- Queremos recuperar y poco más, sin pensar en otra cosa.
  - Queremos quitarnos el problema de encima y nos focalizamos en la recuperación.
- Erradicamos antes que contenemos, recuperamos antes que erradicamos…
- Mejor ejemplo: contaminación vírica… mientras erradique y no contenga, poco haré.

- **SOLUCIONES**
- La recuperación es el paso final de la respuesta –justo antes del día después-, no el primero.
- Identificamos, contenemos, erradicamos y recuperamos.
  - EN ESTE ORDEN.

Error #6: AFTERMATH

DESCONOCIMIENTO LEGAL

- Somos ingenieros, no abogados.
  - Nos complicamos con análisis forenses estupendos… que luego no sirven para nada.
  - Incautamos un disco duro durante días y queremos usarlo como prueba en un juicio.
  - …
- Sabemos qué hay que hacer técnicamente y cómo hacerlo, pero no tenemos ni idea de sus formas o de su (i)legalidad.

SOLUCIONES

- Las actividades relativas a seguridad deben tener un respaldo legal muy fuerte, gestión de incidentes incluida.
  - Especialmente si vamos a denunciar… o si alguien puede denunciarnos.
- El jefe de un GIR debe tener conocimientos –o apoyos- no sólo técnicos. Y el resto de personal, también.

Error #7: AFTERMATH

SECRETISMO

- ¡Qué no se entere nadie!
- No dejamos que nos ayuden
  - A veces, ni siquiera quienes hemos contratado para hacerlo.
- No compartimos información… con nadie.

SOLUCIONES

- Transparencia.
- Ayudemos a que nos ayuden.
  - SOC, CSIRT… equipos públicos y privados.
- *Information sharing.*
  - Con quien corresponde.
  - Con las debidas precauciones.

Error #8: AFTERMATH

DENUNCIAS (et al.)

- El problema de las FFCCSE.
  - Necesaria siempre que se haya producido un delito (art. 259 LECri).
  - ¿Medios ágiles?
  - El problema de la comisaría (puesto, cuartel, etc.).
- El problema judicial
  - ¿Peritos informáticos? ¿Quién puede peritar?
  - Desconocimiento de NNTT por parte del ámbito judicial.

SOLUCIONES

- Formación, formación, formación…
- Grupos especializados en FFCCSE y Juzgados.
- Agilidad.
- Formación… ¿lo había comentado?

Error #9: AFTERMATH

LECCIÓN NO APRENDIDA

- Volvemos rápido a nuestra rutina.
- Priorizamos funcionalidad ante seguridad (de forma incorrecta).
- Nos es más cómodo seguir trabajando como siempre frente a cambiar, aunque el “como siempre” pueda motivar incidentes.
- Cambiamos el “eso no pasa nunca” por el “eso nunca volverá a pasar”

SOLUCIONES

- El hombre es el único animal que tropieza dos veces con la misma piedra… recordémoslo.
- Aprendamos de nuestros errores y de los errores de otros.
- Realimentemos nuestros procedimientos y planificaciones.
  - ¡No hemos escrito la Biblia!

Error #10: P/R/A

NOS ENCANTA COMPLICARNOS

- Buscamos la perfección…
  - …y cuanto más complejo sea lo que hacemos, mejor… ¿no?
- Procedimientos farragosos que a la hora de poner en práctica molestan más que ayudan.
- Soluciones tecnológicas complejas a problemas triviales.
- Hipótesis de trabajo que harían las delicias de guionistas de cine.
- Conclusiones y propuestas de mejora imposibles de cumplir.
- ¿Sigo?

SOLUCIÓN:

- Las cosas sencillas suelen ser muy efectivas.
- KISS

Conclusiones

- La gestión de incidentes es un **proceso**, y son tan importantes las fases de planificación (ANTES) y post-incidente (DESPUÉS) como la respuesta propiamente dicha (DURANTE).
- La teoría es muy sencilla…
  - …y la práctica debe serlo.
- Los errores son simples…
  - …pero seguimos cometiéndolos.
- El momento de respuesta ante un incidente es el menos indicado para tratar de pensar, organizar, decidir…
  - Hagámoslo antes.
- Recuerden: es **imposible** impedir que ocurra un incidente.
- Ya que antes o después ocurrirá, estemos preparados… y aprendamos de nuestros errores.

GRACIAS

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