S2 Grupo
Gestión de incidentes de Seguridad

Antonio Villalón

Contenidos

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[1].

Es **imposible** planificar un incidente.

Es **muy posible** que el impacto asociado a un incidente sea alto.

1. Definición basada en ISO/IEC TR 18044:2004. *Information technology - Security techniques - Information security incident management.*

Detección y notificación

¿Quién puede detectar un incidente?

Detección automática o manual.

¿Cómo notificarlo?

Medios ágiles de notificación.

Publicitación de los canales de notificación.

Prueba periódica de funcionamiento.

Incidente vs. debilidad.

La detección y notificación tempranas son críticas.

Procedimientos de respuesta ante incidentes

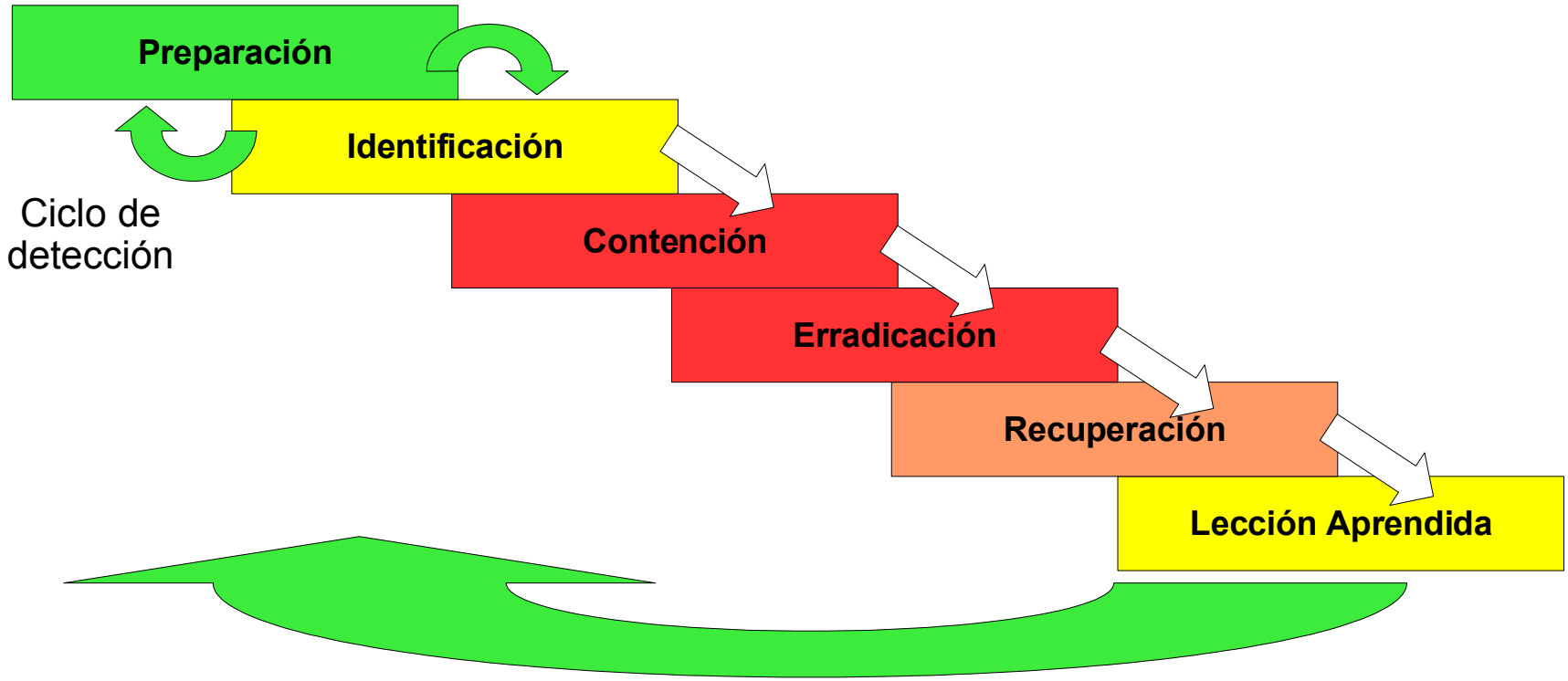
- Identificación del origen y las causas
- Comunicación a los afectados o implicados
- Contención
- Acciones correctivas

Responsabilidades

- ¿Quién hace qué ante un incidente?

Pruebas de los procedimientos

- Cuando el incidente se produce, es el peor momento para probar.


Preparación
Identificación
Ciclo de detección
Contención
Erradicación
Recuperación
Lección Aprendida

IDEA: No puedo garantizar que no se produzcan incidentes; por tanto, de aquellos que sucedan, aprendamos todo lo posible.

¿Qué ha fallado para que se produzca el incidente?

Mejoras en los procedimientos de defensa

Mejoras en los controles técnicos

Mejoras en la comunicación y notificación

¿Qué ha fallado en la respuesta ante el incidente?

Mejoras en la respuesta organizativa: tiempos de respuesta, responsabilidades...

Mejoras en la respuesta técnica.

¿Qué haríamos si mañana nos volviera a ocurrir lo mismo?

Análisis forense. Adquisición, obtención, preservación y presentación de evidencias electrónicas procesadas y conservadas en un medio computacional determinado.

Nos permite...

Evaluar por qué se ha producido el incidente

Determinar cuál ha sido su alcance real

Estimar el impacto asociado al incidente

Recopilar evidencias

Presentación de pruebas ante posibles denuncias, peritajes, procesos internos... o simplemente para confirmar hipótesis.

La denuncia ante FFCCSE es **necesaria** siempre que se haya producido un delito (Art. 259 LEC).

Cualquier denuncia tiene asociado un **impacto** para la organización que hay que valorar antes de efectuarla.

En España, es posible realizar cualquier denuncia ante:

Cuerpo Nacional de Policía

http://www.policia.es/

Guardia Civil

http://www.guardiacivil.es/

Ante un incidente de seguridad puede ser necesario un **informe pericial** por diferentes motivos: juicios, seguros, responsabilidad interna...

Un informe por parte de un **perito cualificado** garantiza una visión independiente de los hechos ocurridos y de los impactos asociados al incidente.

¿Quién puede realizar un peritaje?

Empresas especializadas en **servicios de seguridad**.

¿Quién nos ha ayudado con el incidente? ¿Lo hemos gestionado de forma interna?

En el ámbito autonómico, el **Colegio Oficial de Ingenieros en Informática de la Comunidad Valenciana** dispone de un Turno de Actuaciones Profesionales.

http://www.coiicv.org/

Ante un incidente de seguridad...

...debemos disponer de mecanismos de detección y notificación tempranas.

...debemos reaccionar de forma adecuada, identificando el origen, las causas y el alcance del incidente, y estimando de forma inicial el impacto asociado.

Respuesta **organizativa** y **técnica**.

Error habitual: fase de erradicación en primer lugar.

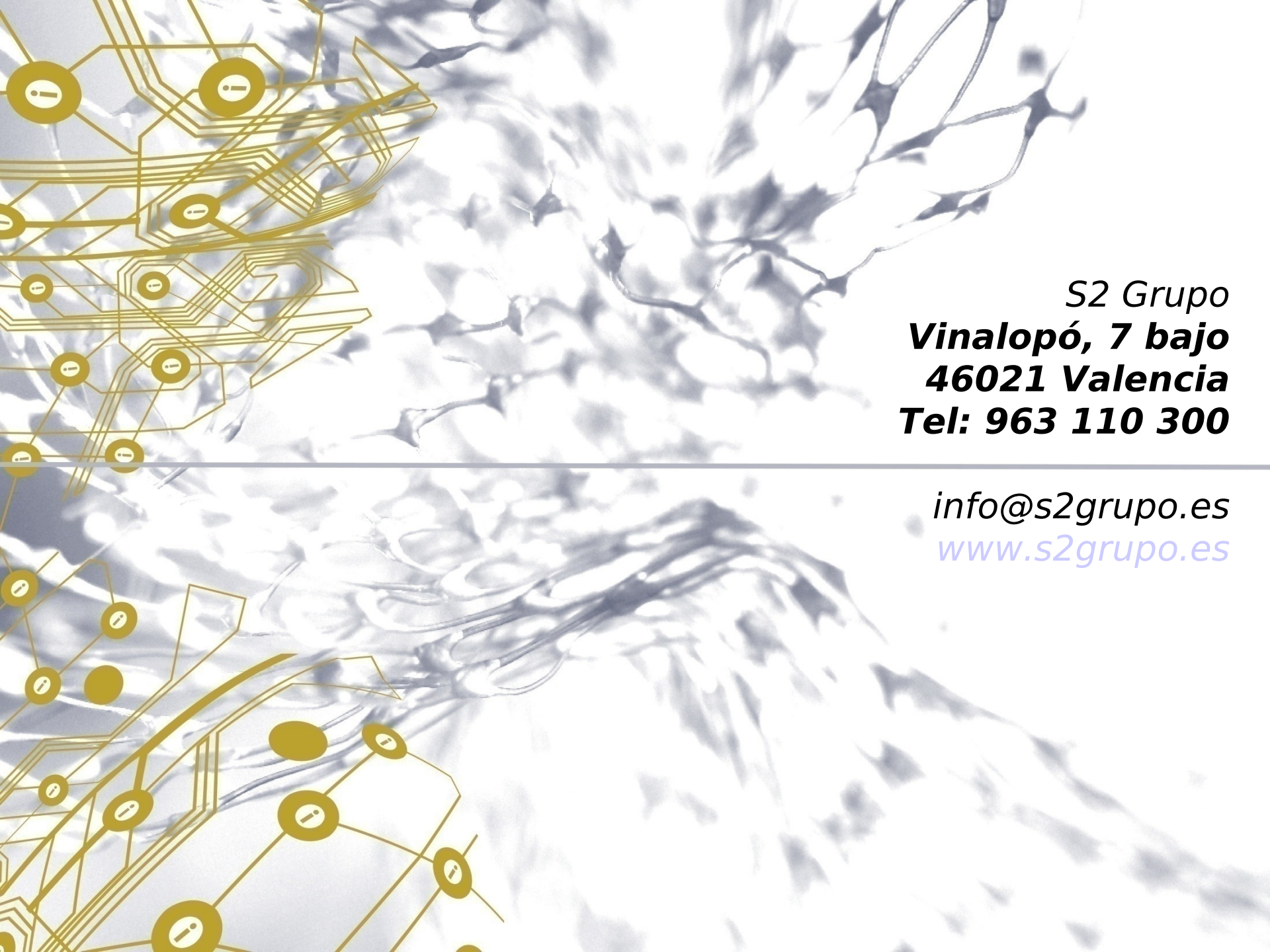
...debemos **aprender** de lo sucedido.

...existen multitud de **medios especializados** a nuestra disposición: CSIRT-CV, FFCCSE, empresas de seguridad, COIICV...

¡Dejemos que nos ayuden!

Muchas gracias a todos

¿Preguntas?



S2 Grupo
Vinalopó, 7 bajo
46021 Valencia
Tel: 963 110 300

info@s2grupo.es
www.s2grupo.es