Organiza:

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Partner:

GOVERTIS Advisory Services

Colabora:

Telefónica

Insight exclusivo DPD-DPO sobre RGPD

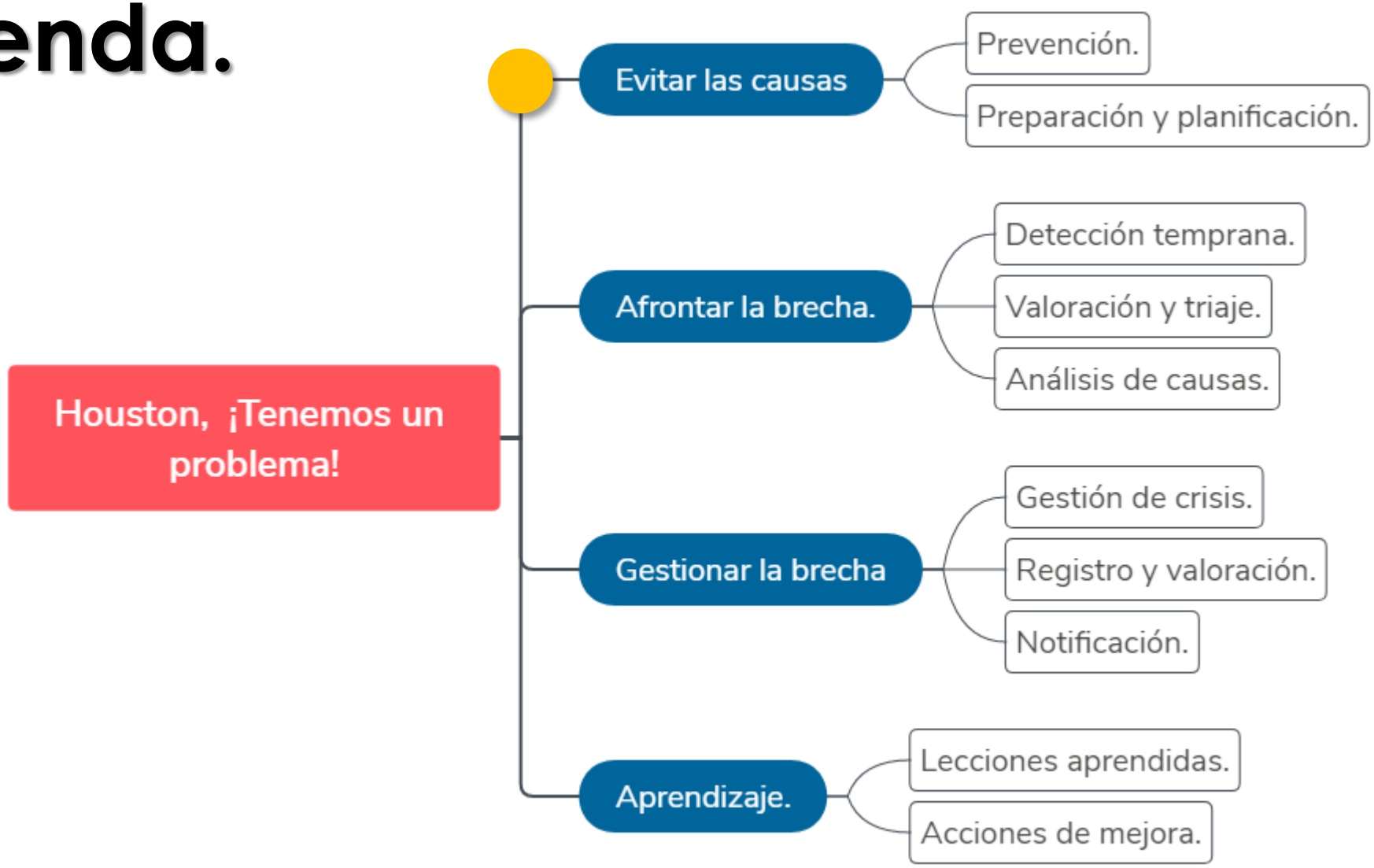
¡Houston, tenemos un problema!

Javier Cao Avellaneda.

Lead Advisor en Ciber Riesgo, Govertis.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Agenda.


Houston, ¡Tenemos un problema!
Evitar las causas
Prevención.
Preparación y planificación.
Afrontar la brecha.
Detección temprana.
Valoración y triaje.
Análisis de causas.
Gestionar la brecha
Gestión de crisis.
Registro y valoración.
Notificación.
Aprendizaje.
Lecciones aprendidas.
Acciones de mejora.

"La mejor victoria es vencer sin combatir".

Sun Tzu. El arte de la guerra.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

"El mejor procedimiento de gestión de brechas de seguridad es el que nunca ha tenido que ejecutarse".

Seguridad de los datos personales del RGPD.

Construir seguridad:

- Orientación a riesgo. (Art. 32)
- Ingeniería de la privacidad. (Arts. 25, 35 y 36)

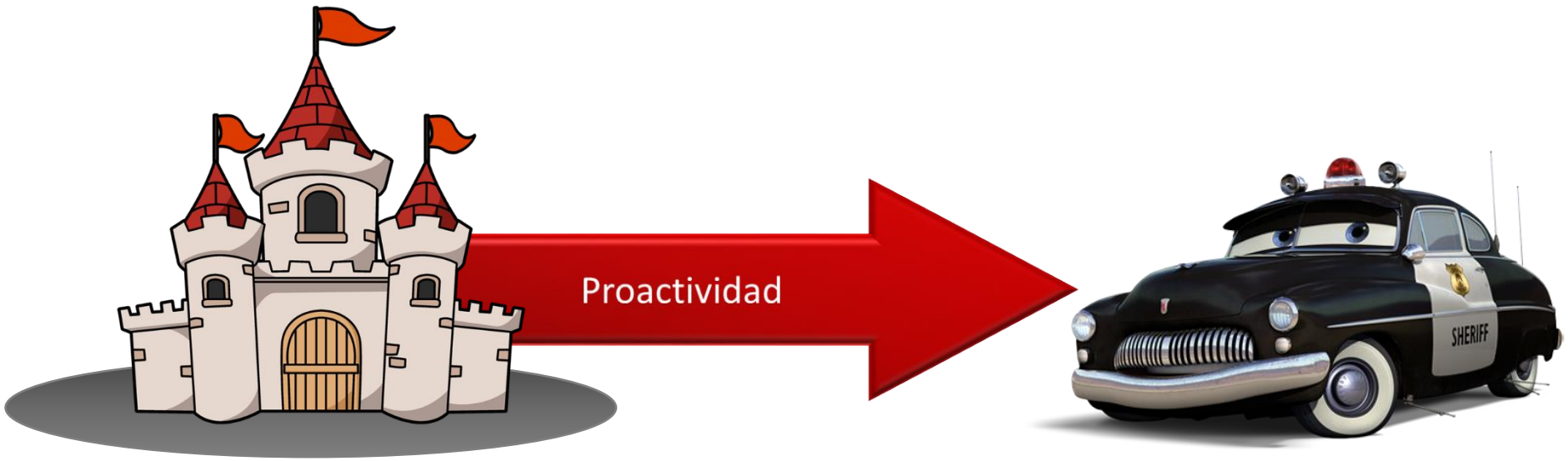
Asumir consecuencias por falta de protección:

- Presión reputacional. (Art. 33)
- Transparencia con el interesado. (Art. 34)

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Protección desde la responsabilidad activa.

- El RGPD supone un giro de 180º en materia de seguridad de la información.
- Pasamos de un modelo "prescriptivo" a un modelo "orientado a riesgo".



Evitar las causas
- Prevención.
- Preparación y planificación.

MEDIDAS PREVENTIVAS

MEDIDAS DE RECUPERACIÓN

AMENAZAS

Causa

Causa

Causa

MEDIDAS PREVENTIVAS

MEDIDAS PREVENTIVAS

RIESGO

MEDIDAS DE MITIGACIÓN

MEDIDAS DE MITIGACIÓN

Consecuencia

Consecuencia

Consecuencia

IMPACTOS

Estrategias de gestión del riesgo

Prevención Detección Respuesta

Brechas de seguridad.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Las causas no suelen ser inmediatas y cuestionarán la responsabilidad activa.

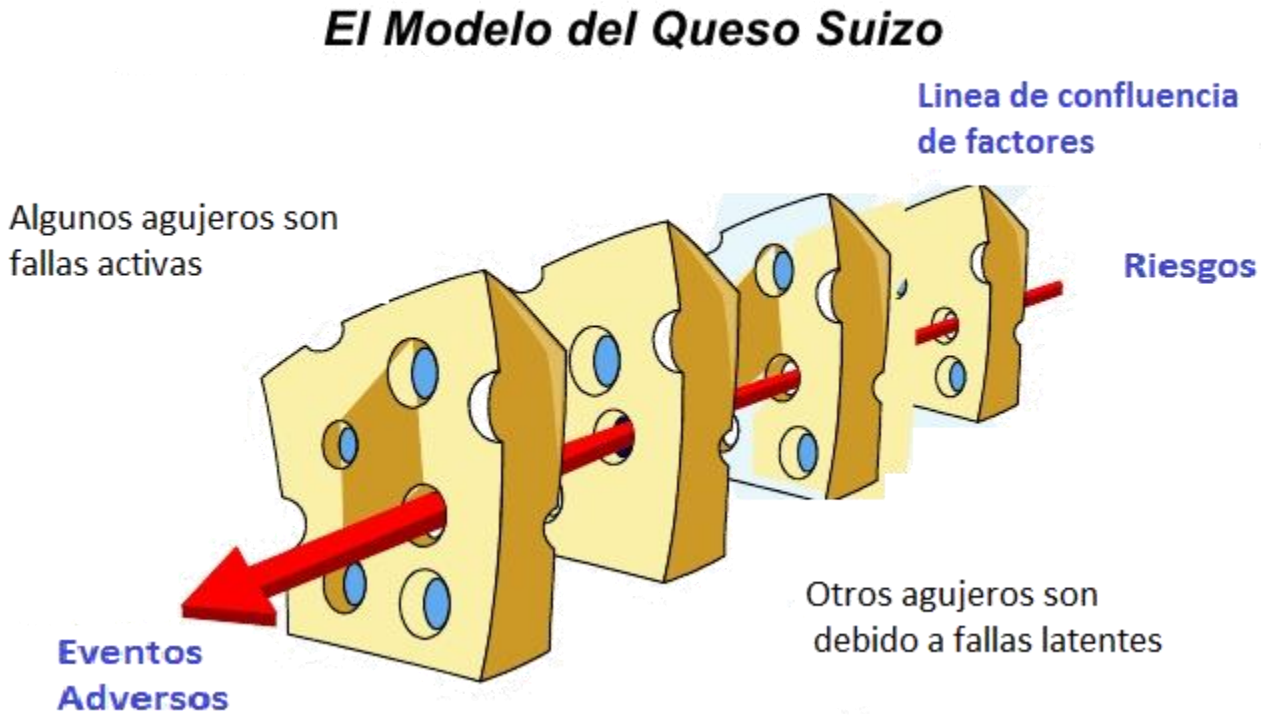
Intensificar la lucha contra el error humano.

Modelo del Queso Suizo -James Reason (1995).

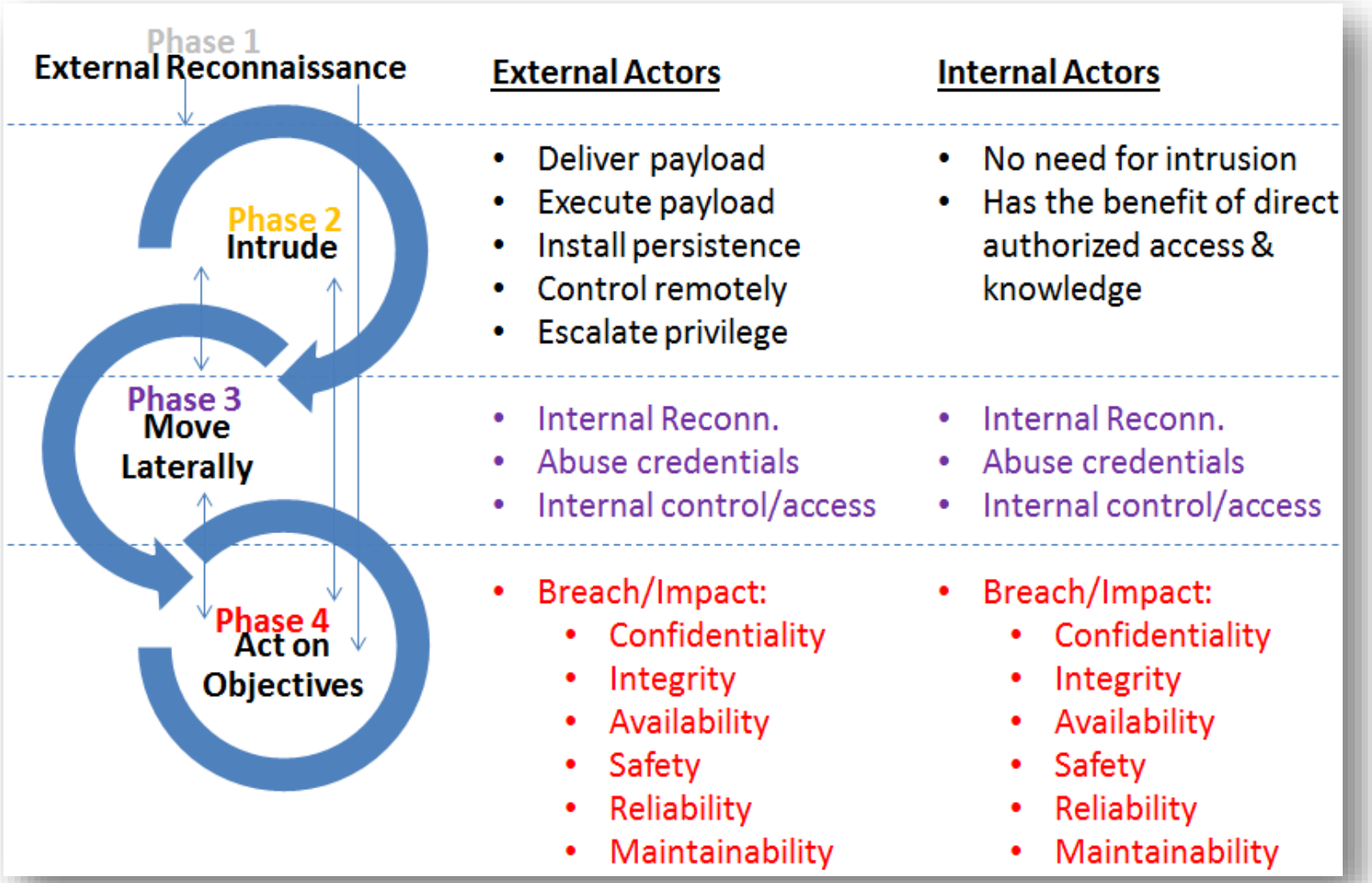
Barreras para impedir amenazas cómo láminas de queso.

Contempla dos tipos de errores:

- **Activos:** Son acciones u omisiones, incluyendo errores e incumplimientos, que tienen consecuencias adversas inmediatas.
- **Latentes:** Creadas por diseño deficiente, objetivos incompatibles, defectos de organización o malas decisiones de la Dirección.



AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

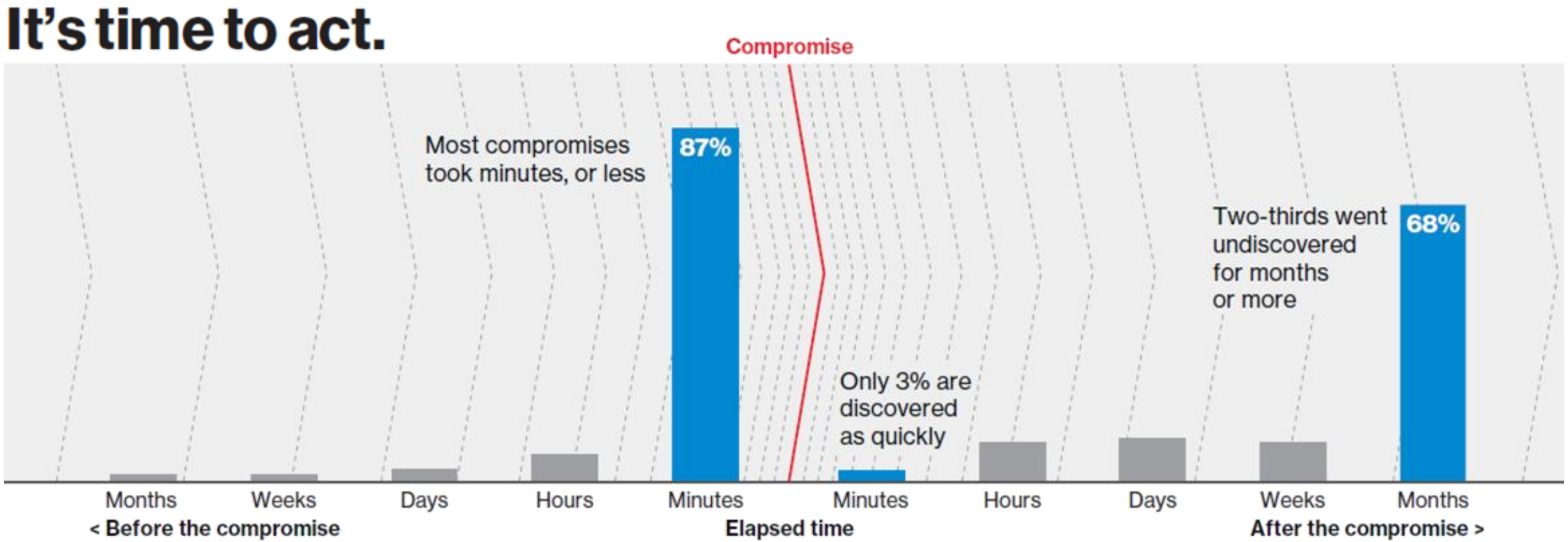


Los actores van paso a paso.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Evitar las causas
- Prevención.
- Preparación y planificación.

El tiempo de detección sigue siendo alto.



Fuente: Verizon- 2018 Data Breach Investigations Report.
https://www.verizonenterprise.com/verizon-insights-lab/dbir/

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

- Evitar las causas
  - Prevención.
  - Preparación y planificación.

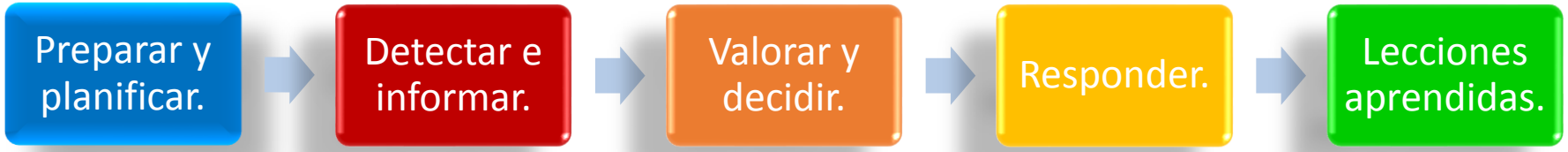
Una brecha es un fracaso en prevención y protección.

Según las causas, podrá poner en cuestión el cumplimiento de nuestra responsabilidad activa.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Referencias para la gestión de incidentes.

ISO 27035: 2016 - Proceso de gestión de incidentes de seguridad de la información.



Guía para la gestión y notificación de brechas de seguridad de la AEPD.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Procedimiento de gestión de brechas de seguridad.

Cuestiones clave a considerar en el diseño:

- Roles y responsabilidades a involucrar.
- Metodología de valoración y triaje de incidentes.
- Protocolos de comunicación interna y toma de decisiones.
- Coordinación con partes interesadas para realizar las comunicaciones/notificaciones oportunas.
- Seguimiento y reevaluación continua.
- Aprendizaje y mejora.

Evitar las causas
- Prevención.
- Preparación y planificación.

Procedimiento de gestión de brechas de seguridad.

¡ALARMA!
Ocurre el suceso y se detecta.

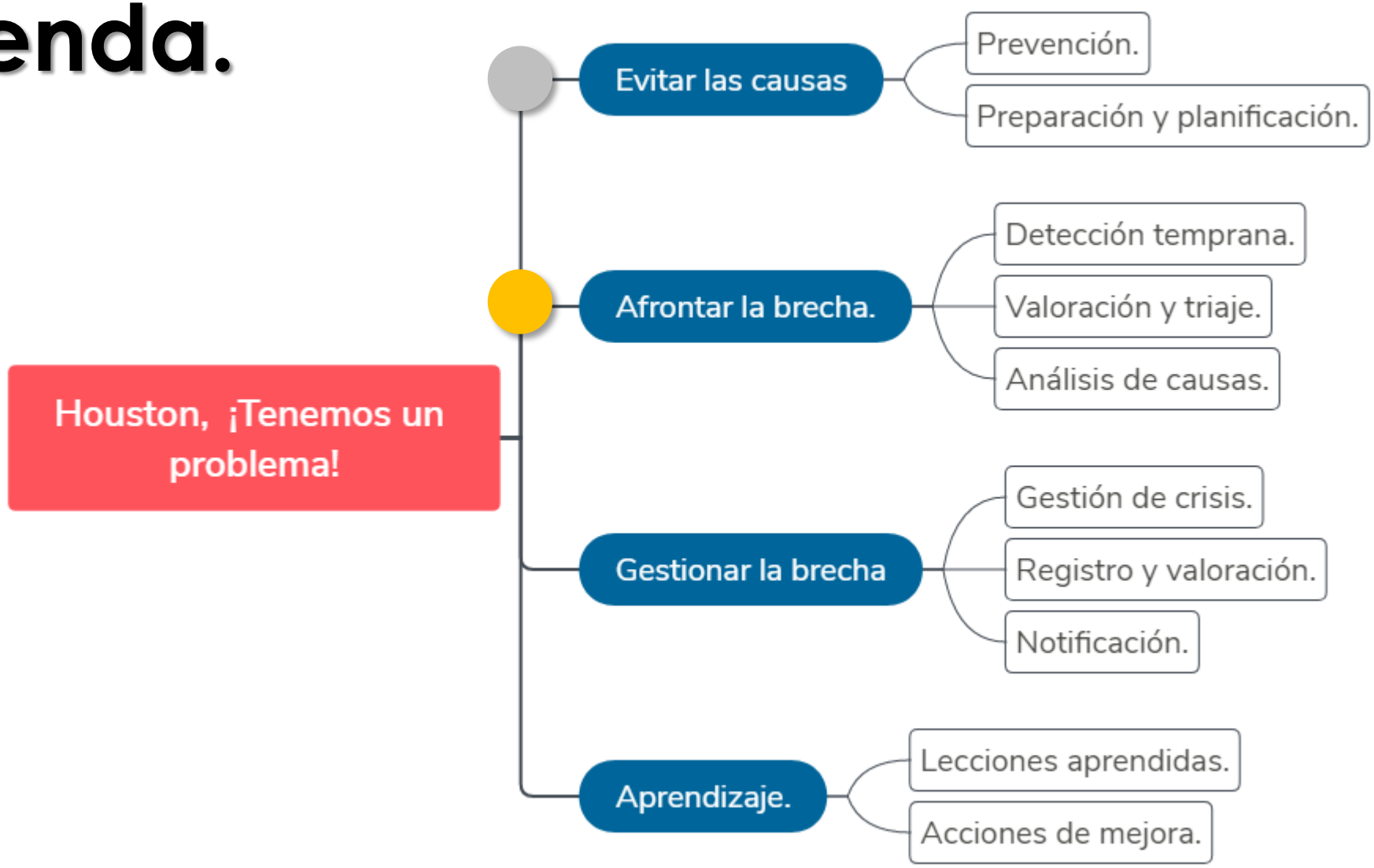
TRIAJE
Se valora para decidir la respuesta.

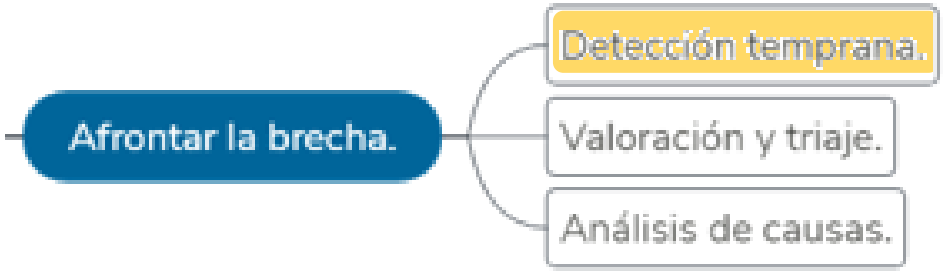
RESPUESTA
Acciones de contención y respuesta del evento.
Se inician las comunicaciones y/o notificaciones.

MEJORA.
Se verifica el cierre del suceso y se obtienen lecciones aprendidas.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Agenda.


Houston, ¡Tenemos un problema!
Evitar las causas
Prevención.
Preparación y planificación.
Afrontar la brecha.
Detección temprana.
Valoración y triaje.
Análisis de causas.
Gestionar la brecha
Gestión de crisis.
Registro y valoración.
Notificación.
Aprendizaje.
Lecciones aprendidas.
Acciones de mejora.



Detección y recogida de información.

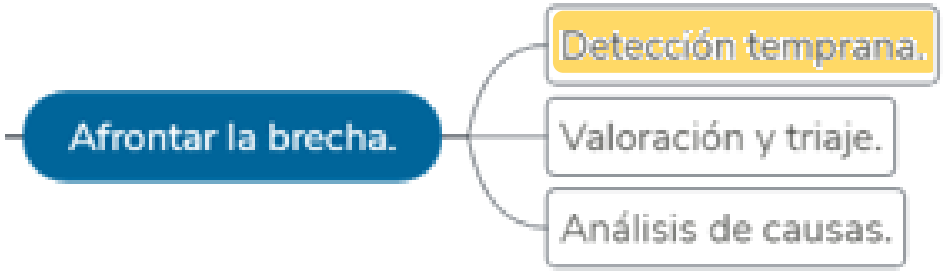
Obtener datos relevantes para el triaje inicial.

Factores de probabilidad:

- Naturaleza del evento.
- Peligrosidad y gravedad.
- Tiempo de impacto y complejidad de resolución.

Factores de impacto:

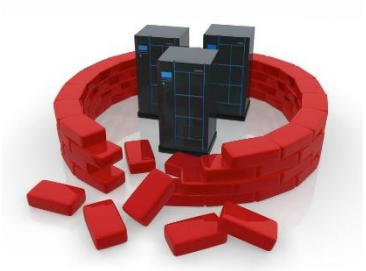
- Alcance y áreas afectadas.
- Visibilidad reputacional.
- Volumetría de interesados.
- Tipo de tratamientos y riesgos asociados.
- Indemnizaciones o incumplimientos.



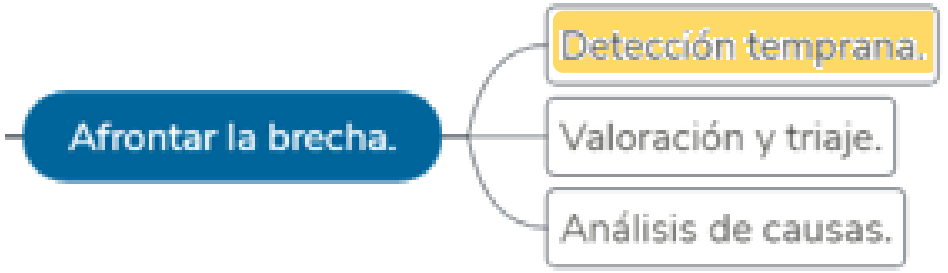
Análisis del suceso.

La naturaleza del evento condiciona las acciones de contención y respuesta.

Daños físicos		Ciberincidentes				
Accidentales	Intencionado	Malware	Intrusión	DDoS	Fraude	Ex Filtración



ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD



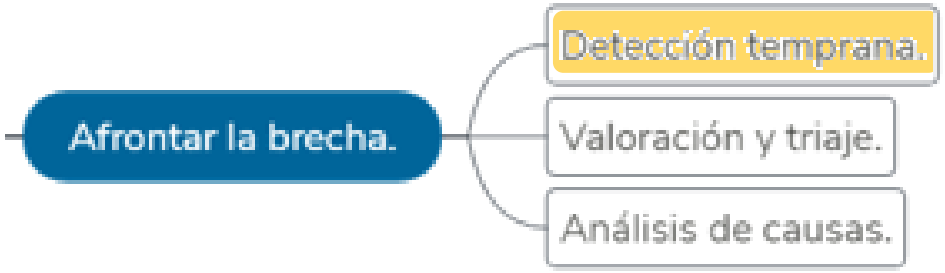
Control sobre la información del suceso.

El impacto reputacional depende de cómo se da a conocer el suceso.

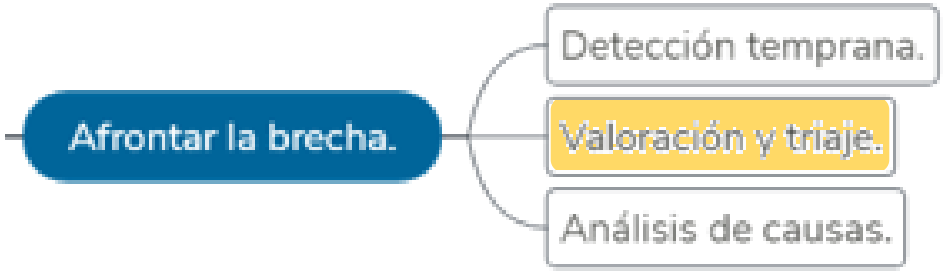
- **CONTROLADO:** Es la organización la que informa de lo que ocurre.

- **NO CONTROLADO:** Son los sucesos se publican en Internet y pillan por sorpresa.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD



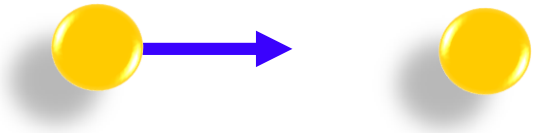
Control sobre la información del suceso.



Consecuencias del suceso para el interesado.

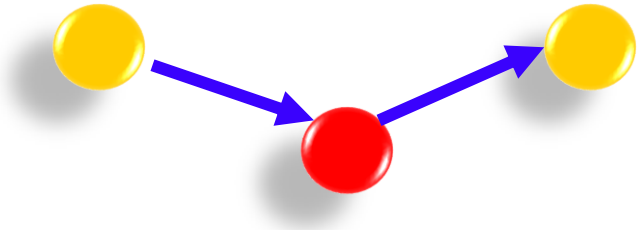
La naturaleza del evento determina qué tipo de impacto va a producirse.

Destrucción o pérdida



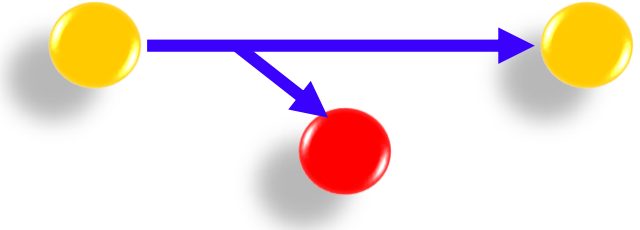
DISPONIBILIDAD

Alteración accidental o ilícita



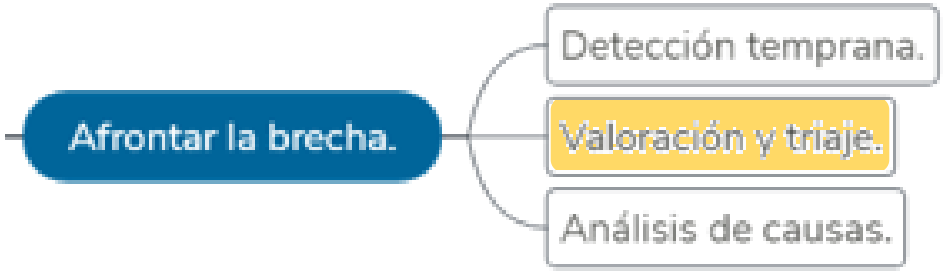
INTEGRIDAD

Comunicación o acceso no autorizado



CONFIDENCIALIDAD

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD



Valoración desde la perspectiva RGPD.

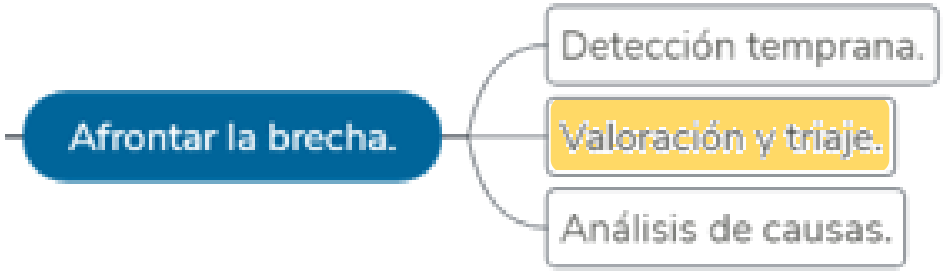
Aprovechar los criterios de impacto utilizados para las EIPD.

TIPO

- Daño material
- Daño moral
- Daño físico

SEVERIDAD

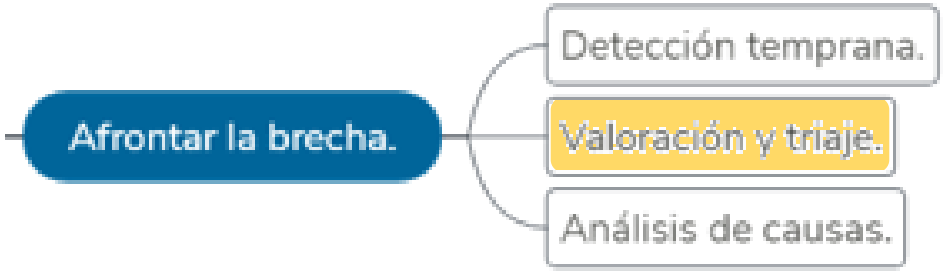
	Ejemplos de posibles daños físico, material o moral
Despreciable: *Los interesados no se verán prácticamente afectados o encontrarán alguna pequeña inconveniencia*	▪ Molestias o irritación. ▪ Se incumplen obligaciones materiales sin perjuicios relevantes. ▪ No se priva de los derechos y libertades.
Limitado: *Los interesados podrán encontrar inconveniencias no significativas*	▪ Estrés o padecimientos físico menores. ▪ Costes extra, denegación de acceso a algunos servicios o incumplimiento de obligaciones materiales con perjuicios económicos. ▪ Se priva de los derechos y libertades de los interesados, por ejemplo, por difamación de un interesado por divulgación de datos personales.
Significativo: *Los interesados encontrarán consecuencias significativas, que deberían poder superar sin dificultades serias.*	▪ Empeoramiento del estado de salud o agresiones físicas. ▪ Apropiación indebida de fondos, pérdida del empleo o incumplimiento de obligaciones materiales con perjuicios económicos relevantes. ▪ Se agrede contra los derechos y libertades de los interesados, por ejemplo, una citación judicial, entrar en una lista de morosidad o divulgación de datos personales con impacto significativo en la reputación del interesado.
Máximo: *Los interesados encontrarán consecuencias significativas o incluso irreversibles, que podrán no llegar a superarse.*	▪ Agresiones físicas con consecuencias irreparables. ▪ Asunción de una deuda inafrontable, imposibilidad de volver a trabajar o incumplimiento de obligaciones materiales con perjuicios económicos irreparables. ▪ Se agrede significativamente contra los derechos y libertades de los interesados, por ejemplo, padecimiento psicológico con consecuencias a largo plazo o irreparables por la divulgación de datos sensibles.



Valoración del riesgo para el interesado.

Otros factores a considerar:

- Causa que da pie al incidente.
- Volumen de datos afectados.
- Facilidad de identificación del interesado.
- El contexto que supone quién es el responsable del tratamiento.
- Qué tipo de población demográfica es la afectada.

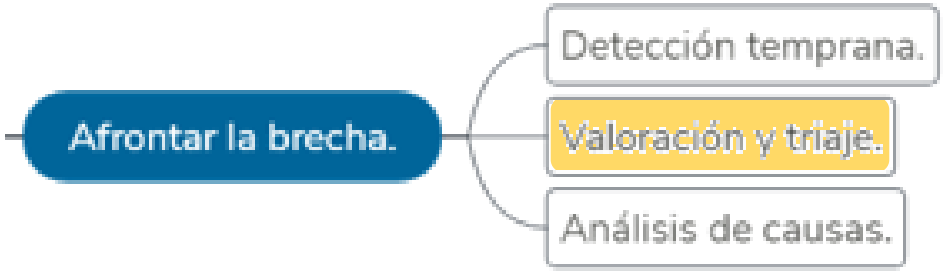


Valoración del riesgo para el interesado.

Decidir si supondrá un riesgo para el interesado tras valorar de forma objetiva y metodológica estos factores.

RIESGO

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

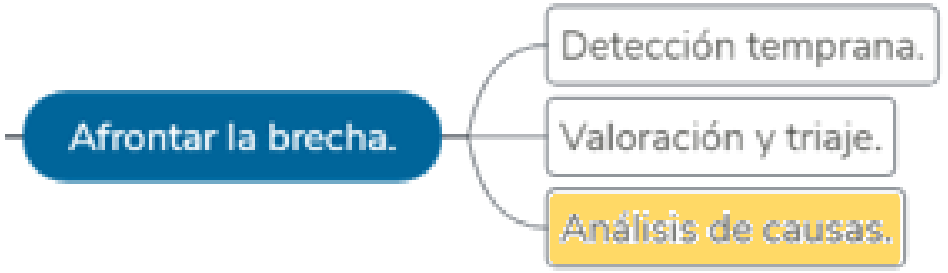


Triaje sobre el incidente: qué, cuándo y cómo.

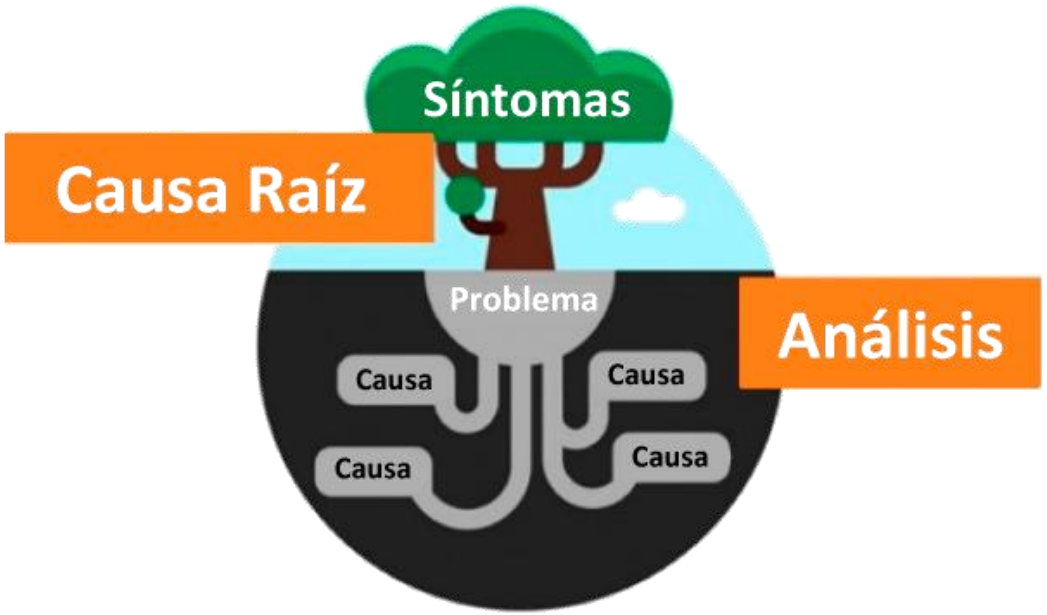
Punto de contacto: alguien debe valorar inicialmente lo ocurrido y hacer el triaje inicial.

Modelo Manchester de triaje médico.

Nivel	Color	Categoría	Tiempo de Atención
I	ROJO	INMEDIATO	INMEDIATO
II	NARANJA	EMERGENCIA	10 MINUTOS
III	AMARILLO	URGENCIA	60 MINUTOS
IV	VERDE	MENOS URGENTE	120 MINUTOS
V	AZUL	NO URGENTE	DISPENSARIO



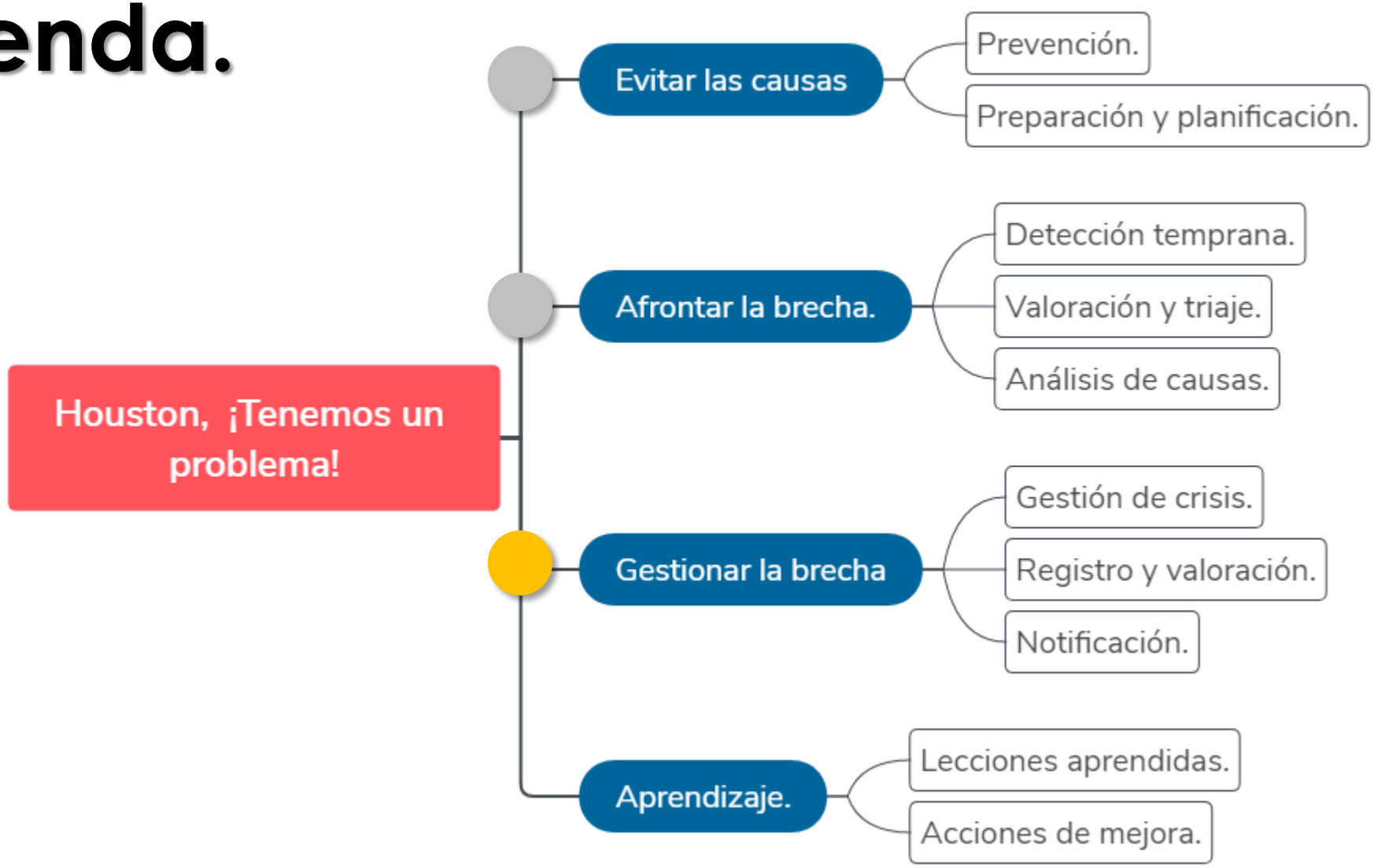
Análisis de las causas responsables de la violación de seguridad.

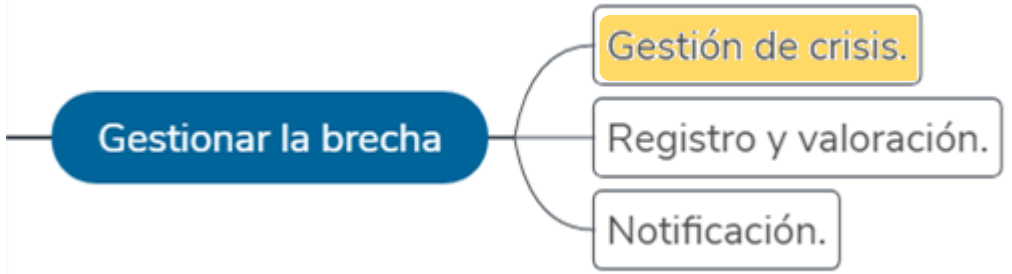


El por qué del incidente puede ponernos en evidencia y modificará la estrategia de comunicación.

- Error humano.
- Fallo de las medidas existentes.
- Desactualización de los sistemas.

Agenda.


Houston, ¡Tenemos un problema!
Evitar las causas
Prevención.
Preparación y planificación.
Afrontar la brecha.
Detección temprana.
Valoración y triaje.
Análisis de causas.
Gestionar la brecha
Gestión de crisis.
Registro y valoración.
Notificación.
Aprendizaje.
Lecciones aprendidas.
Acciones de mejora.



Roles y responsabilidades de coordinación.

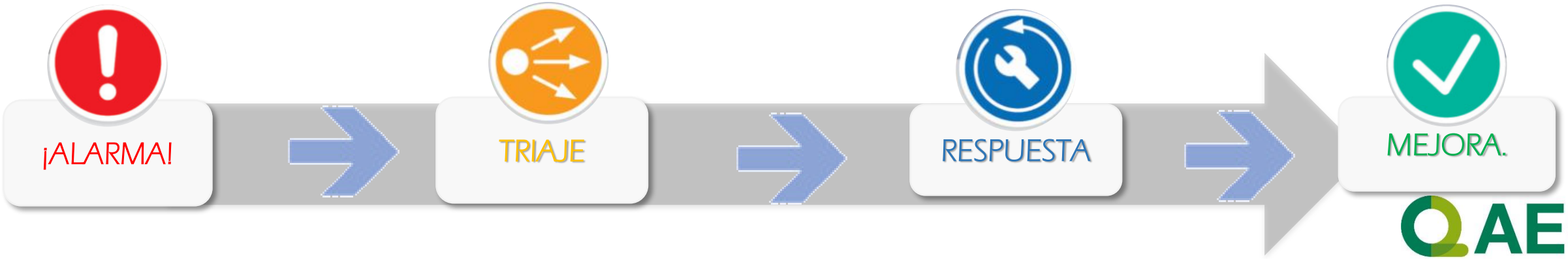
PoC

Equipo de valoración

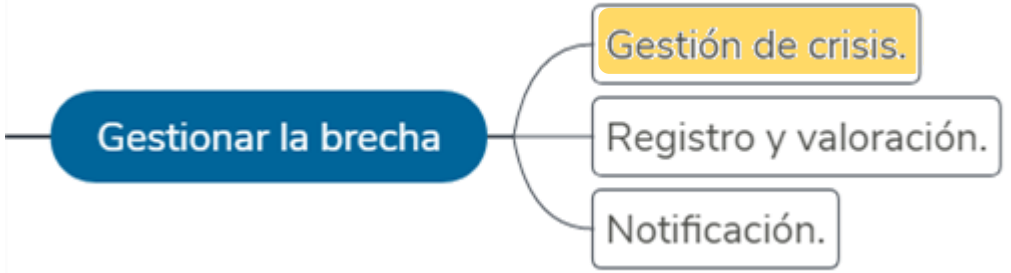
- CISO
- DPO
- Área del Tratamiento afectado

Equipo de gestión de crisis

- CISO
- DPO
- Comunicación.
- RRHH
- Todas las partes interesadas



AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

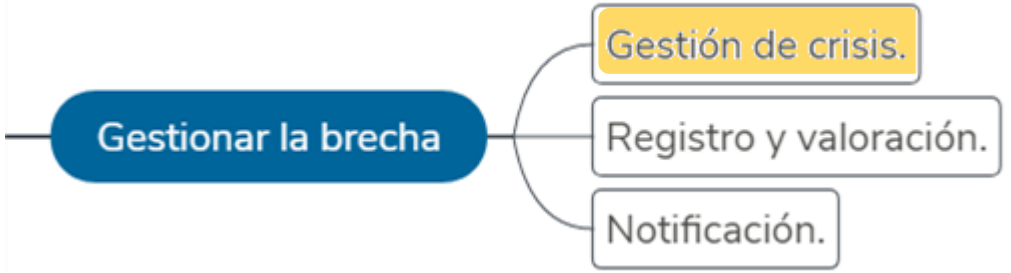


Comunicación interna inicial.

Equipo de valoración

El **protocolo interno inicial** de gestión de brechas debe:

- Establecer criterio de a quién informar el PoC cuando algo suceda.
- Definir a partir de qué nivel de triaje se reúne el equipo de valoración.
- Valoración inicial ágil y rápida.
- Según resultados, escalado y coordinación del incidente al equipo de crisis.

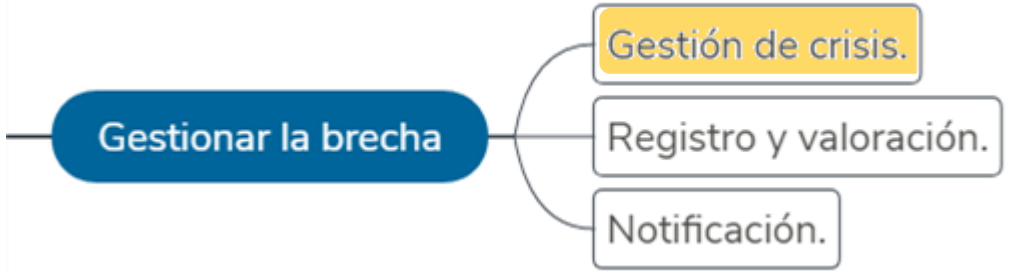


Comunicación interna en brechas de riesgo.

Equipo de gestión de crisis

Cuando la brecha supone riesgo y escala:

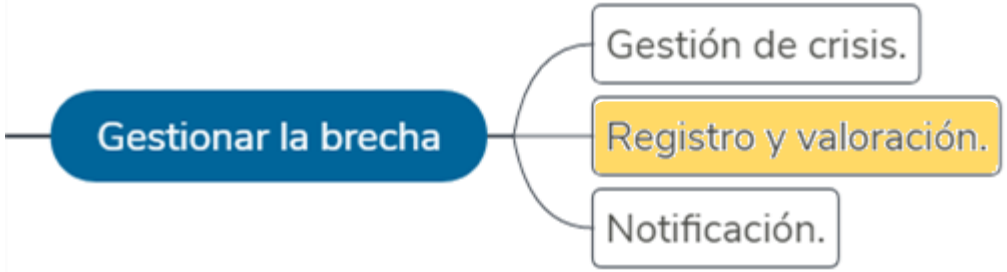
- Debe involucrar a todos los actores internos que deben valorar impacto y consecuencias.
- Debe establecer las pautas de comunicación y notificación.
- Debe formalizar el registro del incidente.
- Debe supervisar la evolución y cierre.
- Debe aprobar acciones de mejora.



Entrenar la coordinación y ejecución del procedimiento.

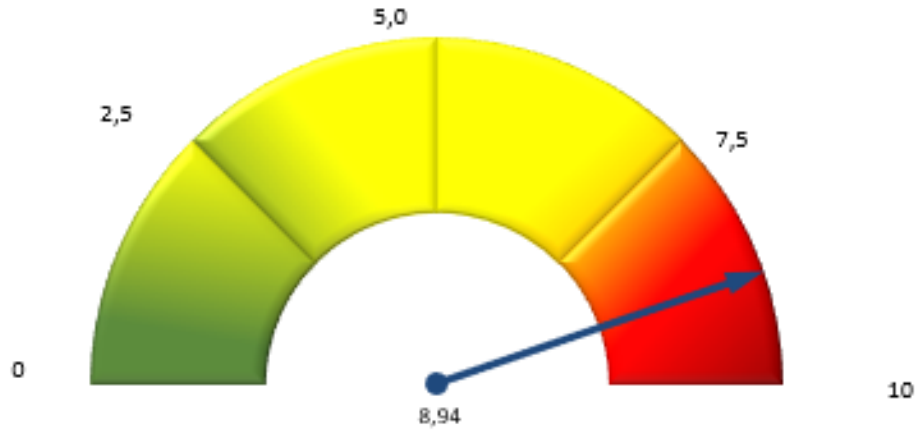
Es necesario garantizar la correcta ejecución cuando se produzca la brecha:

- Entrenar las tareas de valoración y triaje.
- Engrasar las labores de coordinación y comunicación y/o notificación de brechas.



Valoración final del riesgo.

Tipo de incidente	**Exfiltración de información**
DIMENSIONES AFECTADAS:	**CONFIDENCIALIDAD**
NIVEL DE RIESGO:	

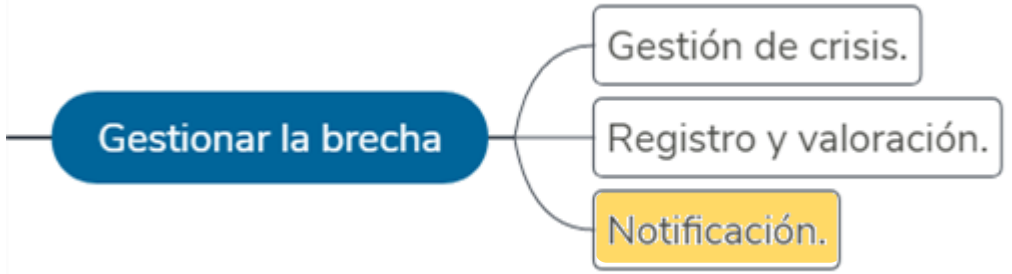


Reunida toda la información es necesario estimar el nivel de riesgo con el que se registrará el incidente.

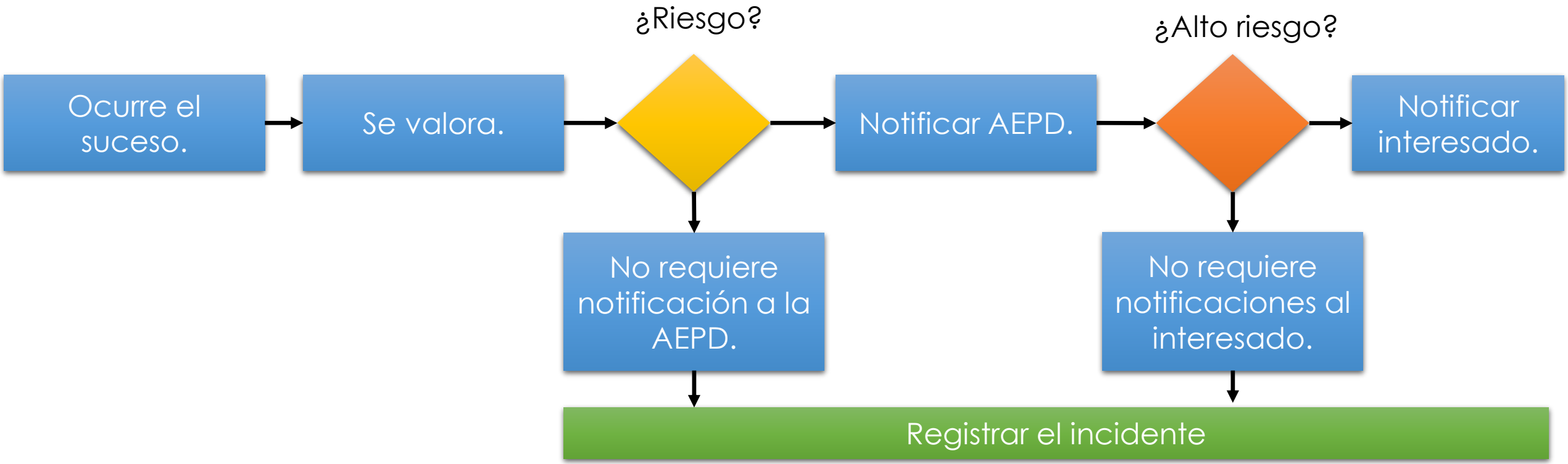
Es necesario considerar los resultados de las medidas de seguridad aplicadas.

Independientemente de si se notifica o no, el incidente debe quedar registrado.

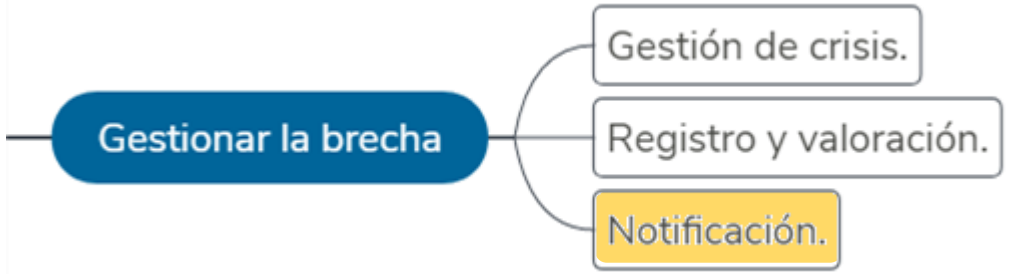
AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD



Decisiones respecto a la notificación.



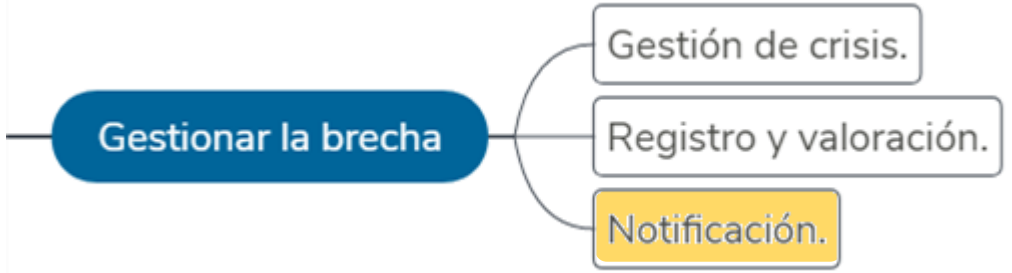
Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679.
GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29



Responsable del tratamiento: Los plazos de la notificación a la AEPD.

"En caso de violación de la seguridad de los datos personales, **el responsable del tratamiento la notificará a la autoridad de control competente** de conformidad con el artículo 55 **sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella**, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas".

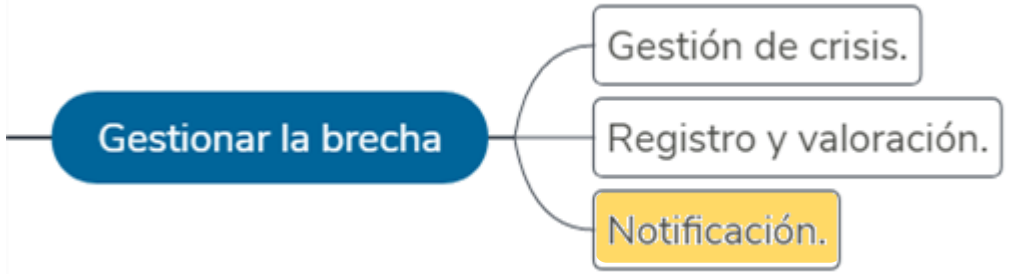
AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD



"Ser consciente" de la violación de seguridad.

El GT29 piensa que debe considerarse que un responsable del tratamiento «tiene constancia» cuando tenga **un grado razonable de certeza** de **que se ha producido un suceso que compromete datos personales.**

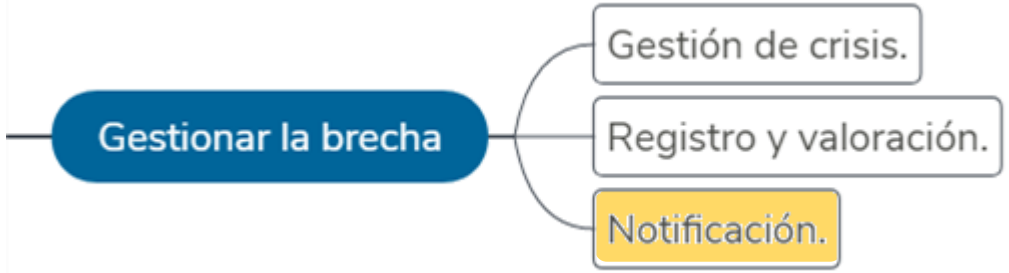
Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679.
GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29



Encargado de tratamiento: Los plazos de la notificación al responsable del tratamiento.

"El encargado del tratamiento notificará **sin dilación indebida** al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento."

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

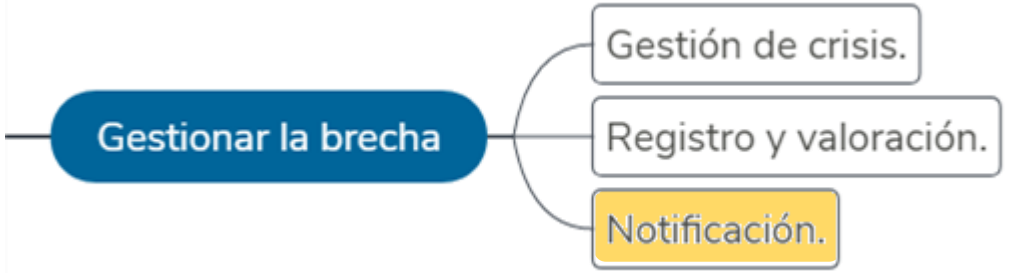


¿Comunicar o no al interesado?.

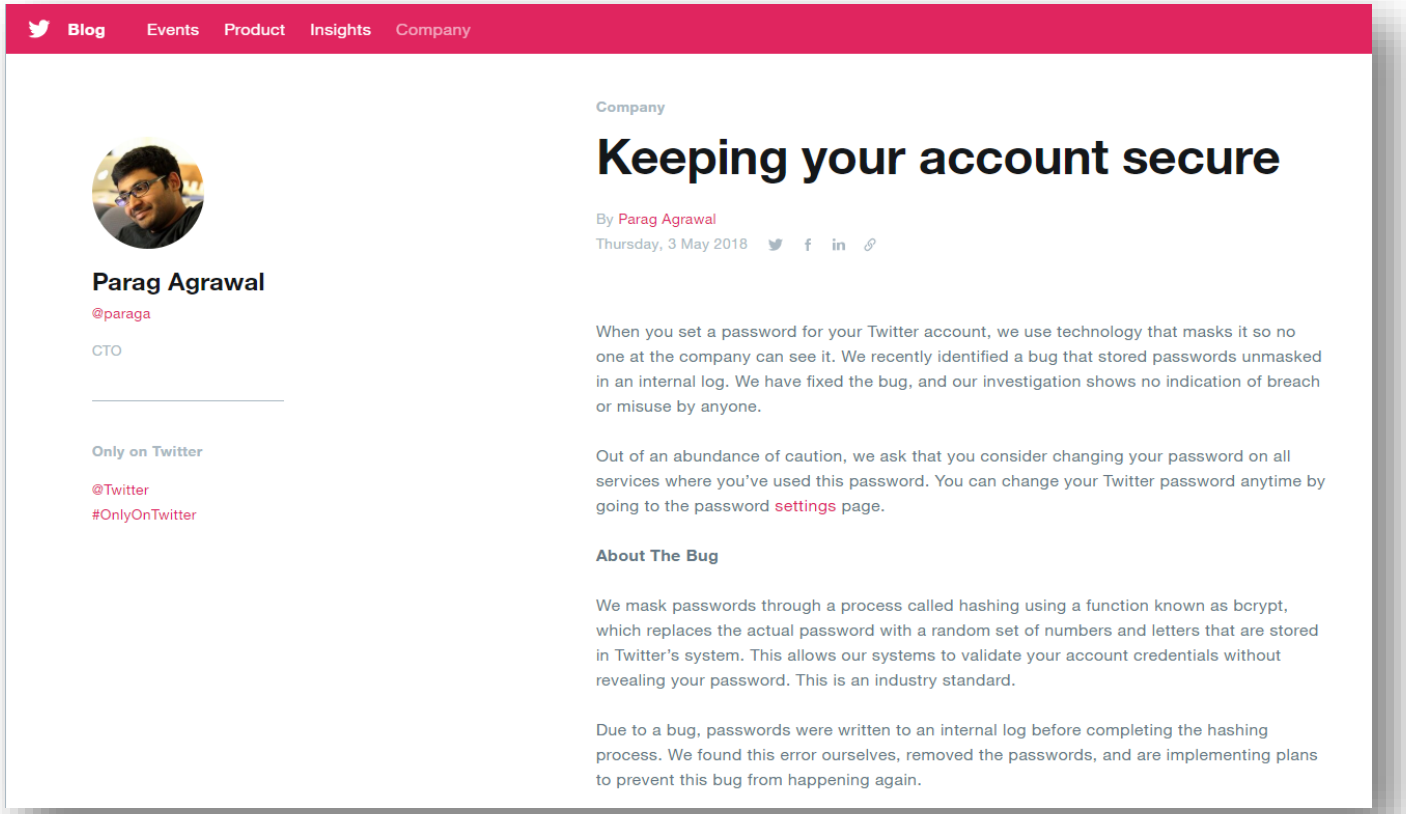
En caso de duda, el responsable del tratamiento debe pecar por exceso de precaución y notificar.

Los criterios de comunicación e imagen corporativa pueden pesar más que la obligación establecida por el RGPD.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD



¿Notificar o comunicar?



Blog Events Product Insights Company

Company

Keeping your account secure

By Parag Agrawal
Thursday, 3 May 2018

Parag Agrawal
@paraga
CTO

Only on Twitter
@Twitter
#OnlyOnTwitter

When you set a password for your Twitter account, we use technology that masks it so no one at the company can see it. We recently identified a bug that stored passwords unmasked in an internal log. We have fixed the bug, and our investigation shows no indication of breach or misuse by anyone.

Out of an abundance of caution, we ask that you consider changing your password on all services where you've used this password. You can change your Twitter password anytime by going to the password settings page.

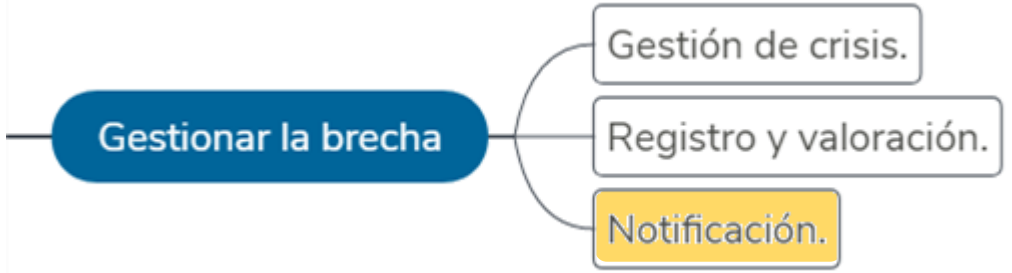
About The Bug

We mask passwords through a process called hashing using a function known as bcrypt, which replaces the actual password with a random set of numbers and letters that are stored in Twitter's system. This allows our systems to validate your account credentials without revealing your password. This is an industry standard.

Due to a bug, passwords were written to an internal log before completing the hashing process. We found this error ourselves, removed the passwords, and are implementing plans to prevent this bug from happening again.

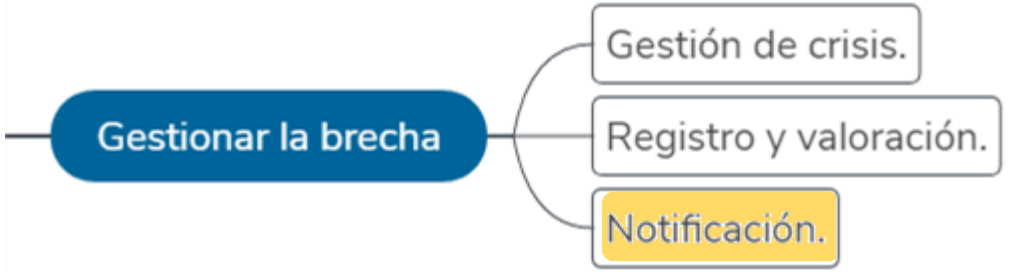
- Twitter detecta error de programación.
- No hay brecha sino sólo potencialidad improbable pero preventivamente decide solicitar cambios de contraseña.
- Evidencia responsabilidad proactiva pese al impacto reputacional.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

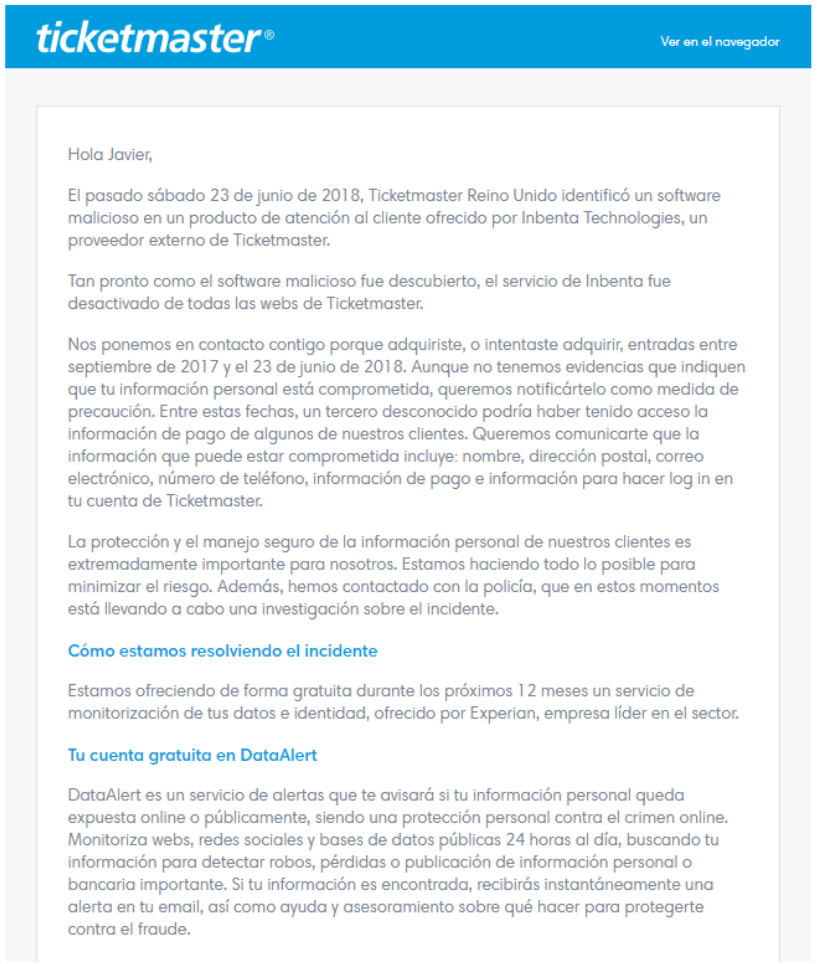


Cuidar el mensaje al interesado.

- **El contenido debe ser claro, informativo sobre lo sucedido y las posibles consecuencias para el interesado.**
- **Debe explicar también las acciones de resolución realizadas.**
- **El interesado es víctima y por tanto, tener una actitud empática hacia él.**
- **Debemos coordinar el texto con el área de comunicación corporativa.**



Cuidar el mensaje.



ticketmaster® Ver en el navegador

Hola Javier,

El pasado sábado 23 de junio de 2018, Ticketmaster Reino Unido identificó un software malicioso en un producto de atención al cliente ofrecido por Inbenta Technologies, un proveedor externo de Ticketmaster.

Tan pronto como el software malicioso fue descubierto, el servicio de Inbenta fue desactivado de todas las webs de Ticketmaster.

Nos ponemos en contacto contigo porque adquiriste, o intentaste adquirir, entradas entre septiembre de 2017 y el 23 de junio de 2018. Aunque no tenemos evidencias que indiquen que tu información personal está comprometida, queremos notificártelo como medida de precaución. Entre estas fechas, un tercero desconocido podría haber tenido acceso la información de pago de algunos de nuestros clientes. Queremos comunicarte que la información que puede estar comprometida incluye: nombre, dirección postal, correo electrónico, número de teléfono, información de pago e información para hacer log in en tu cuenta de Ticketmaster.

La protección y el manejo seguro de la información personal de nuestros clientes es extremadamente importante para nosotros. Estamos haciendo todo lo posible para minimizar el riesgo. Además, hemos contactado con la policía, que en estos momentos está llevando a cabo una investigación sobre el incidente.

Cómo estamos resolviendo el incidente

Estamos ofreciendo de forma gratuita durante los próximos 12 meses un servicio de monitorización de tus datos e identidad, ofrecido por Experian, empresa líder en el sector.

Tu cuenta gratuita en DataAlert

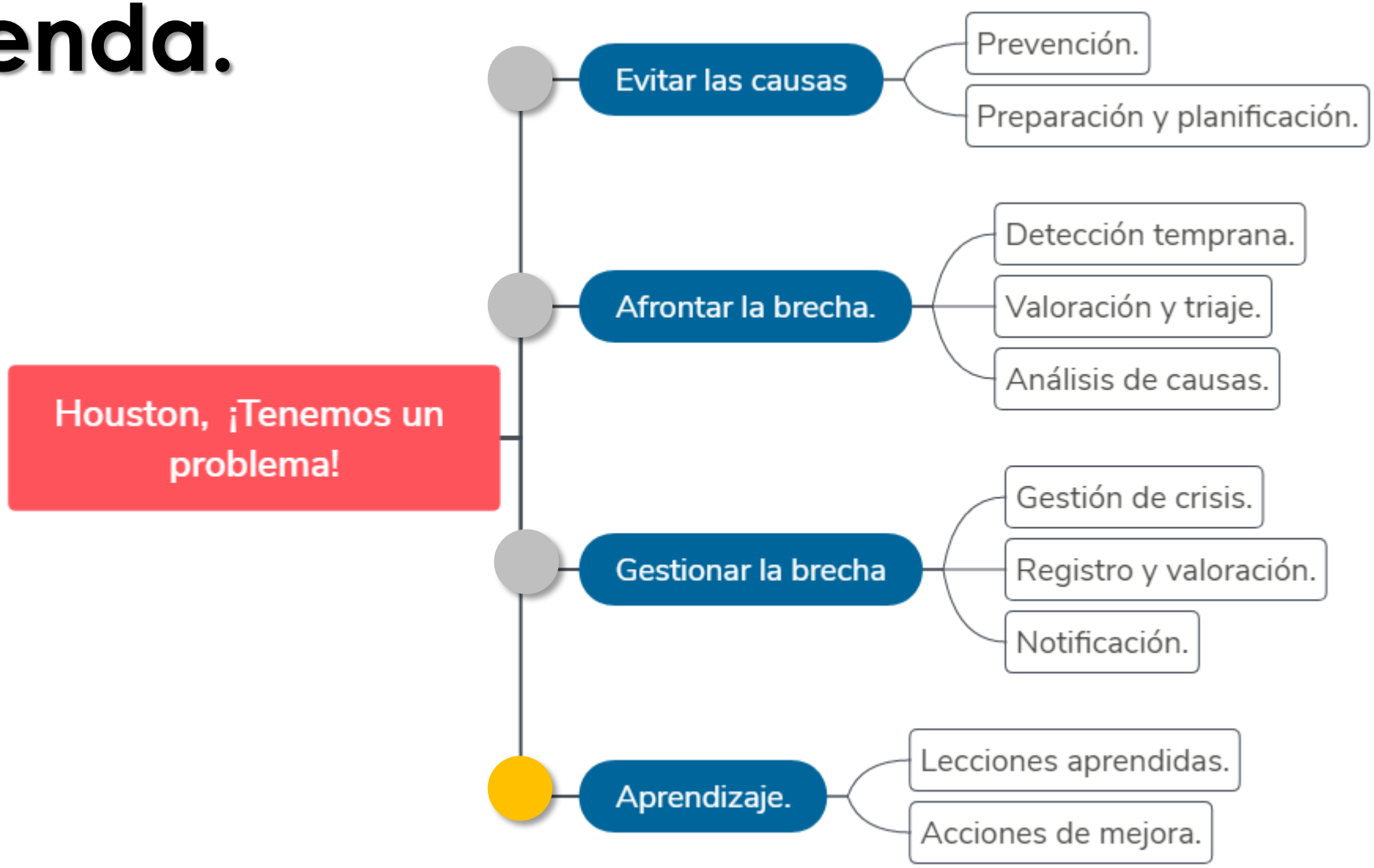
DataAlert es un servicio de alertas que te avisará si tu información personal queda expuesta online o públicamente, siendo una protección personal contra el crimen online. Monitoriza webs, redes sociales y bases de datos públicas 24 horas al día, buscando tu información para detectar robos, pérdidas o publicación de información personal o bancaria importante. Si tu información es encontrada, recibirás instantáneamente una alerta en tu email, así como ayuda y asesoramiento sobre qué hacer para protegerte contra el fraude.

Caso Ticketmaster:

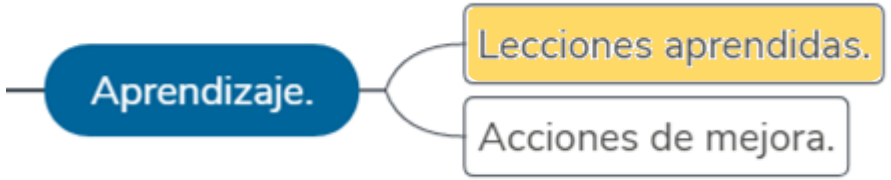
- **Informa de los hechos al interesado.**
- **Pide comprensión por el suceso.**
- **Compensa el posible daño proporcionando de forma gratuita el acceso a un servicio de alertas que avisa si la información personal queda expuesta online.**

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Agenda.



AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

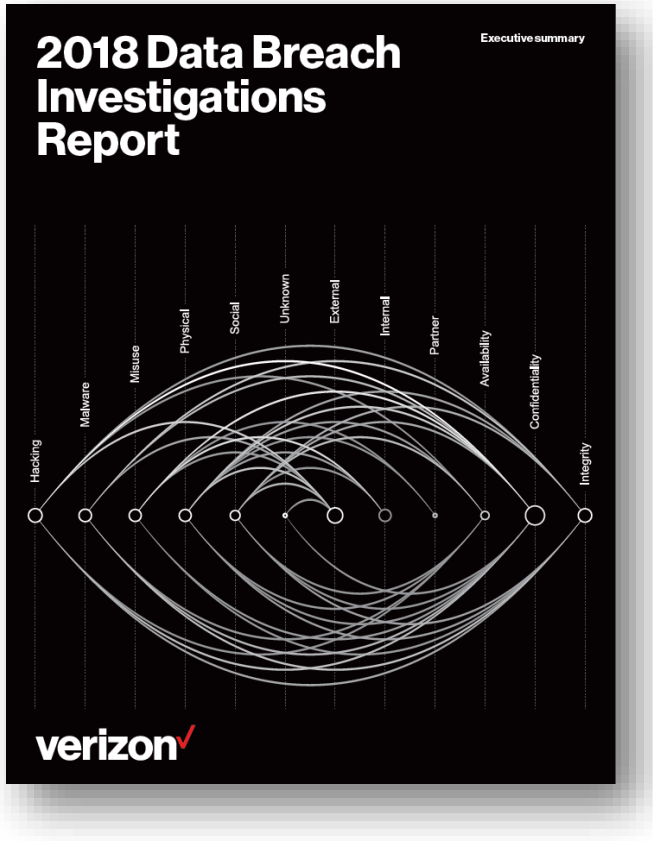


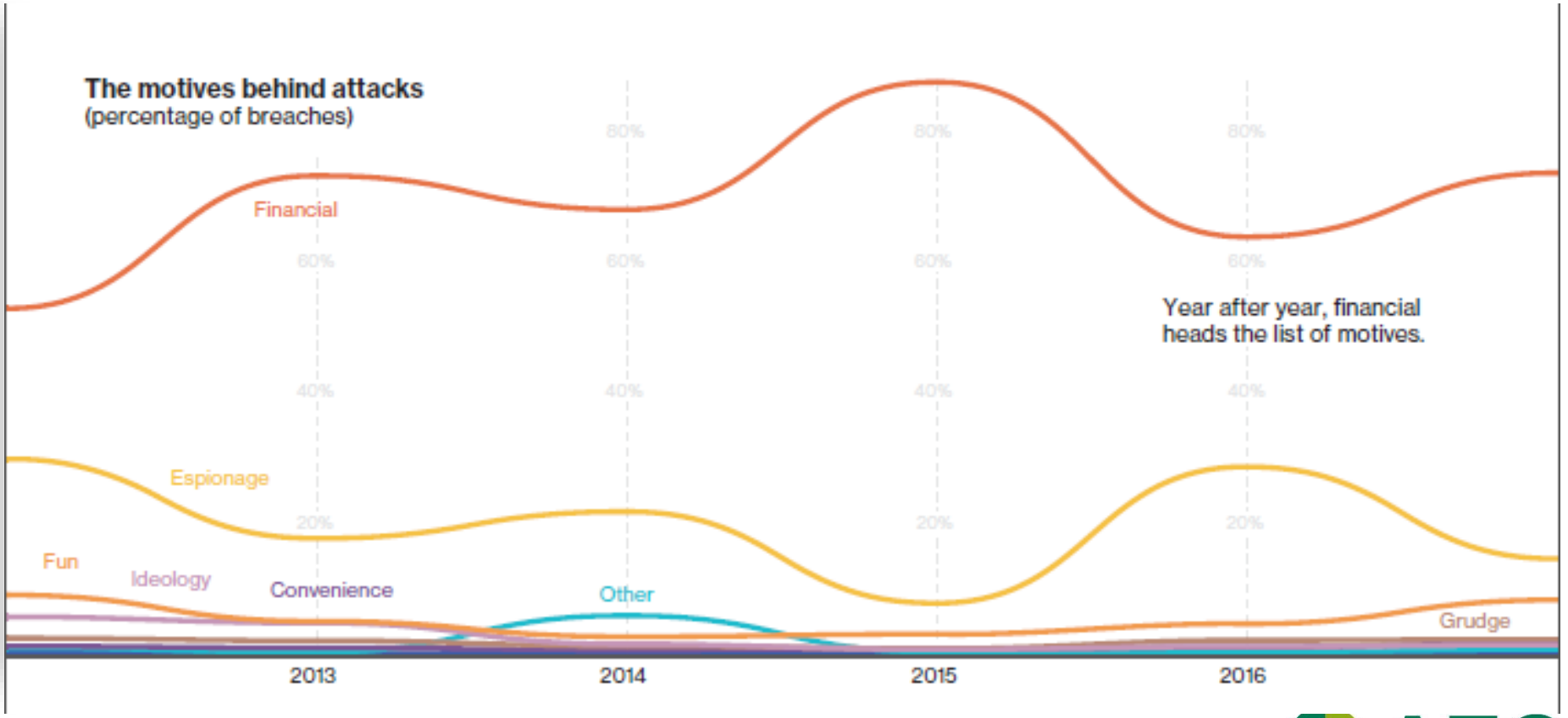
Aprender el fracaso.

- Identificar errores o actualizar información que se haya evidenciado obsoleta.
- Analizar la información forense que todavía esté pendiente de procesar y que pueda aportar mejoras.
- Comunicar los resultados del proceso y realizar una valoración final del incidente.

Aprendizaje.
- Lecciones aprendidas.
- Acciones de mejora.

Las estadísticas indican tendencias por sectores.



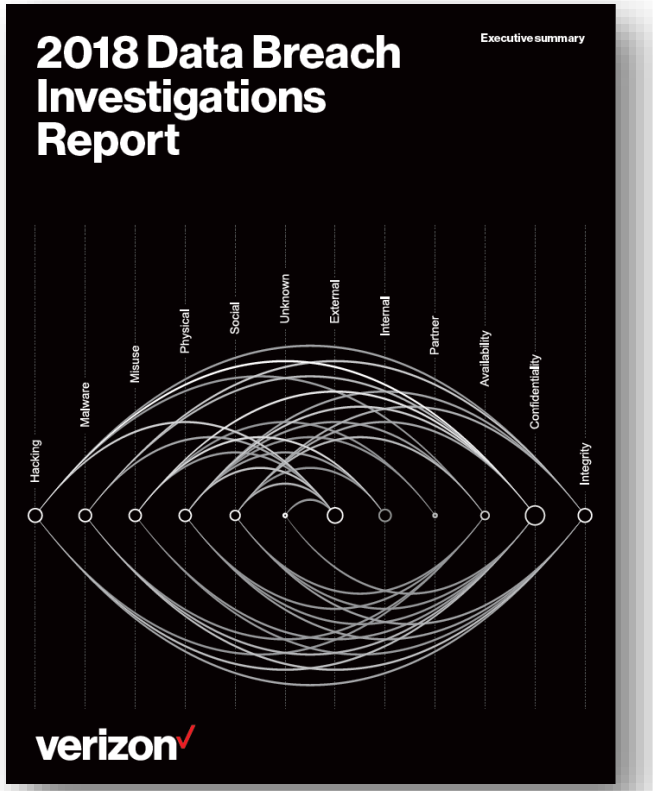


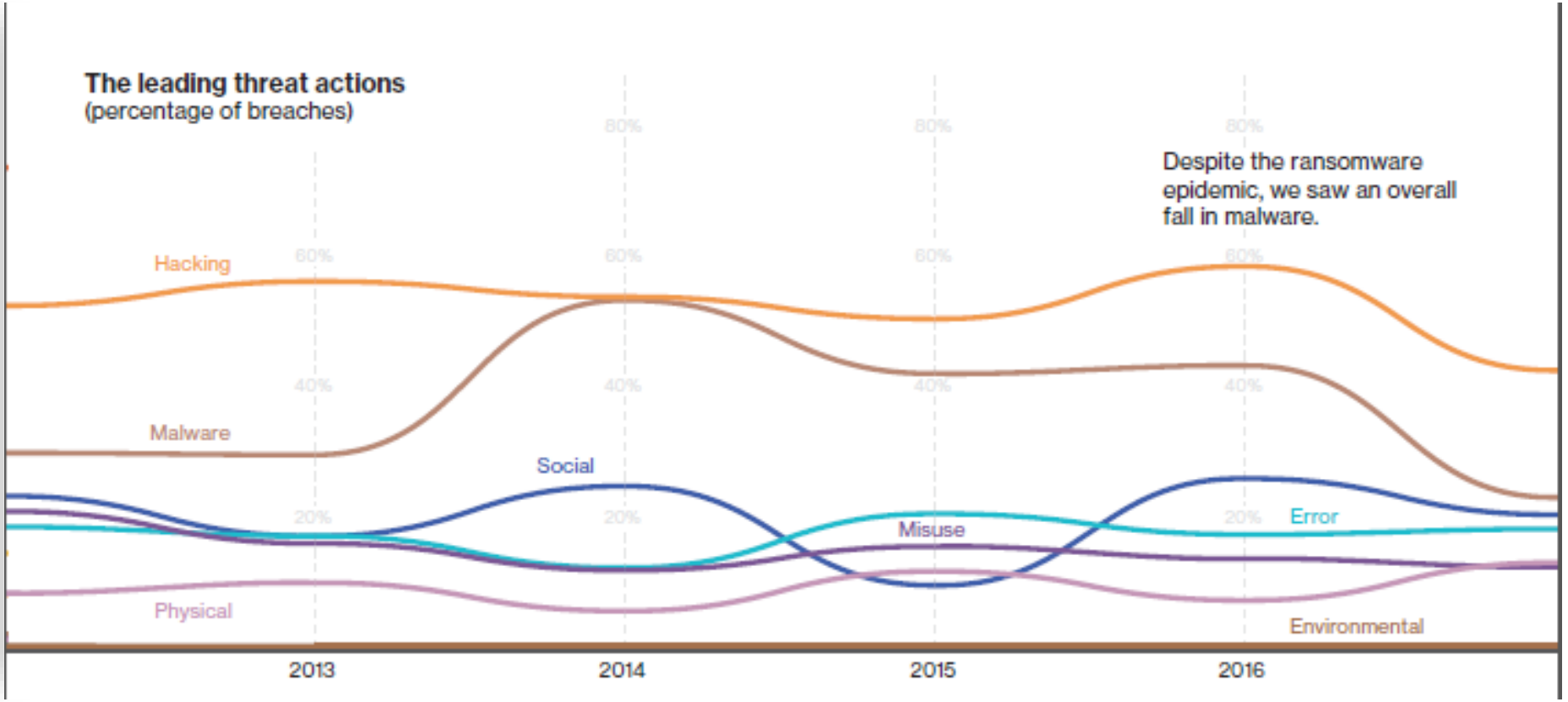
Fuente: Verizon- 2018 Data Breach Investigations Report.
https://www.verizonenterprise.com/verizon-insights-lab/dbir/

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Aprendizaje.
- Lecciones aprendidas.
- Acciones de mejora.

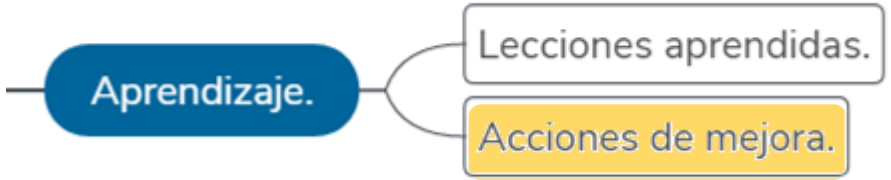
Las estadísticas muestran las amenazas más habituales.





Fuente: Verizon- 2018 Data Breach Investigations Report.
https://www.verizonenterprise.com/verizon-insights-lab/dbir/

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD



Si una brecha es mala, dos es peor.

- Del análisis de causas y errores deben iniciarse acciones de mejora.
- Identificar errores activos y latentes que hayan propiciado el factor humano.
- Mejorar los mecanismos de protección o contemplar la incorporación de nuevos.

El daño probablemente esté hecho, sólo la gestión del incidente podrá atenuar daños.

Gracias por la atención prestada.

Javier Cao Avellaneda.

Lead Advisor en Ciber Riesgo, Govertis.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD