# Gestión de crisis frente a contingencias, aspectos clave a considerar.


**Javier Cao Avellaneda**
**Lead Advisor en Ciber riesgos en Govertis.**
**Profesor asociado UCAM.**

**@javiercao**


GOVERTIS Advisory Services

Red IRIS

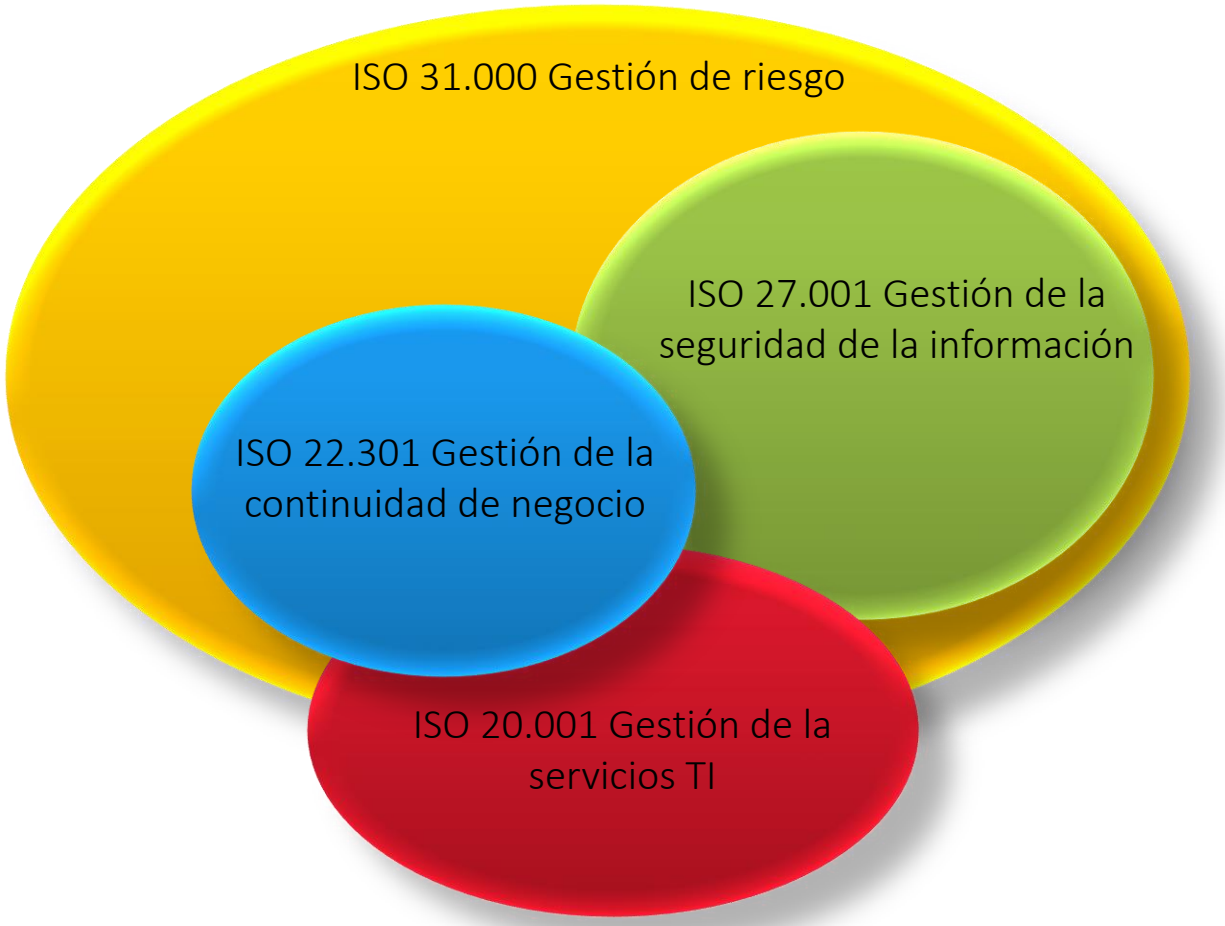
# CONTENIDO.

1. CONTEXTO DE LA GESTIÓN DE CRISIS.
2. GESTIÓN DE INCIDENTES vs GESTIÓN DE CONTINUIDAD.
3. GOBIERNO DE LA CRISIS.
4. GESTIÓN REPUTACIONAL EN SITUACIONES DE CRISIS.

GOVERTIS Advisory Services

Red IRIS

# Entornos donde puede surgir la gestión de crisis.




Una crisis puede suceder por diferentes causas que afectan a aspectos distintos de una Organización.

Es habitual que se vincule a la continuidad del negocio que es parte de la gestión general del riesgo en una Organización y tiene áreas superpuestas con la gestión de la seguridad de la información y la gestión de los servicios TI.

GOVERTIS Advisory Services

Red IRIS

# Gestión del riesgo y gestión de crisis.

- La **gestión de riesgos** implica evaluar las amenazas potenciales y encontrar las mejores formas de evitar esas amenazas. Se trabaja con hipótesis posibles y escenarios de riesgo a mitigar.

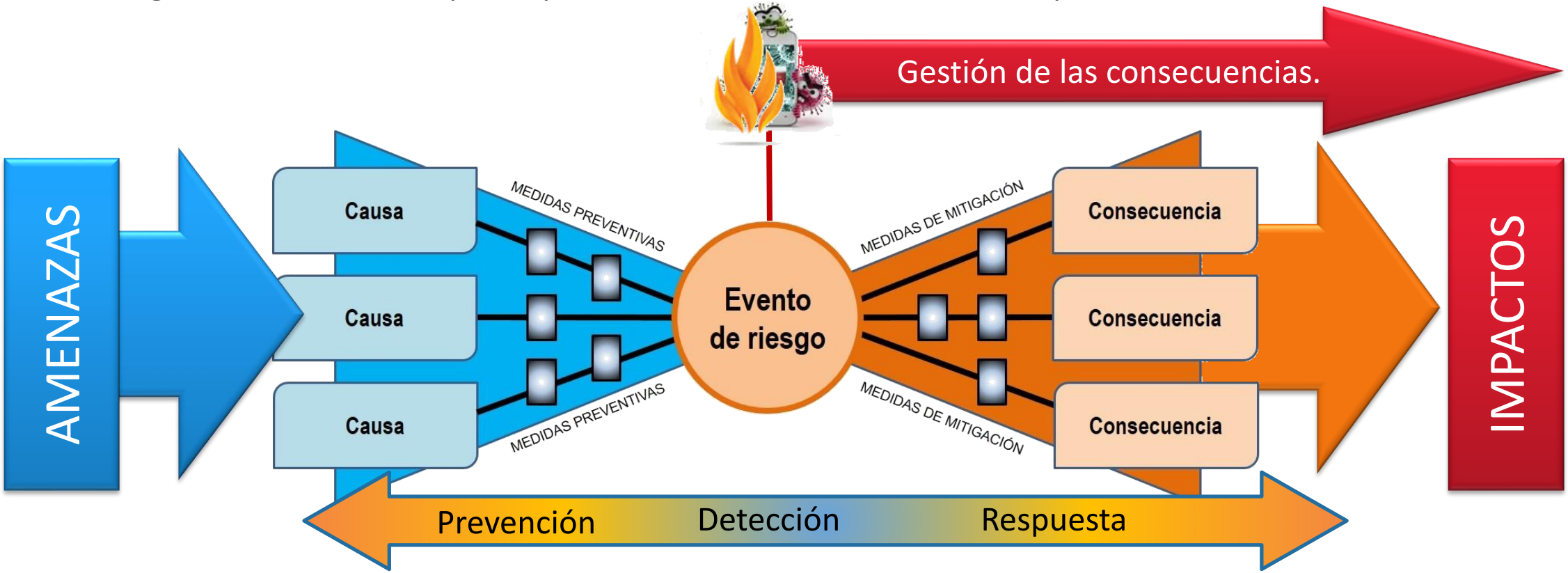
- La **gestión de crisis** implica tratar las amenazas antes, durante y después de que hayan ocurrido. Es una disciplina dentro del contexto más amplio de gestión que consiste en habilidades y técnicas requeridas para identificar, evaluar, comprender y hacer frente a una situación grave, especialmente desde el momento en que ocurre por primera vez hasta el punto en que comienzan los procedimientos de recuperación y se vuelve a la normalidad.

GOVERTIS Advisory Services

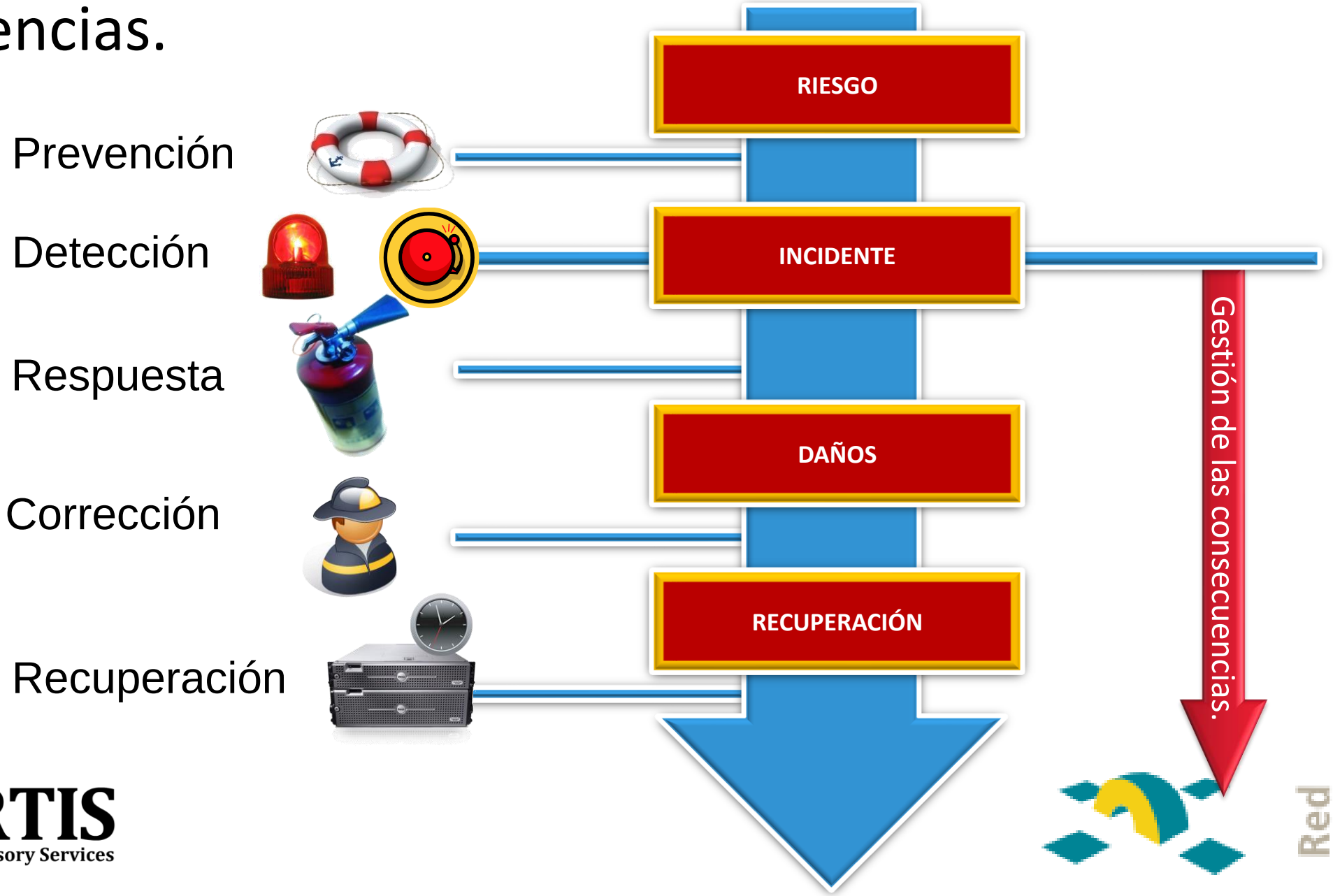
Red IRIS

# Modelo Tie-blow.

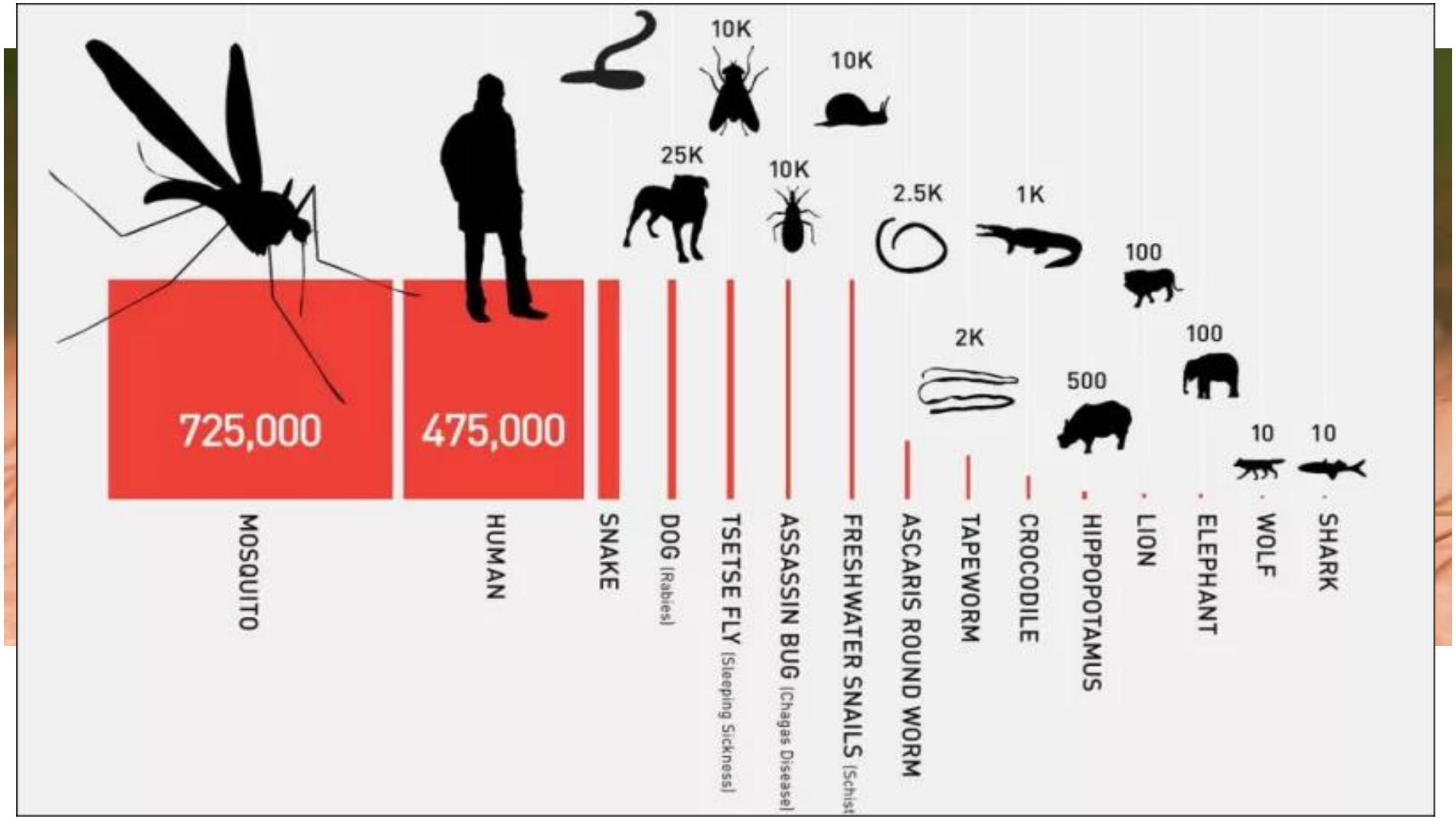
- La gestión del riesgo engloba todas las estrategias (Prevención-detección-respuesta).
- La gestión de crisis supone ya la materialización del suceso y se centra en la reducción de daños.



# Solo pueden aplicarse las estrategias de gestión de consecuencias.



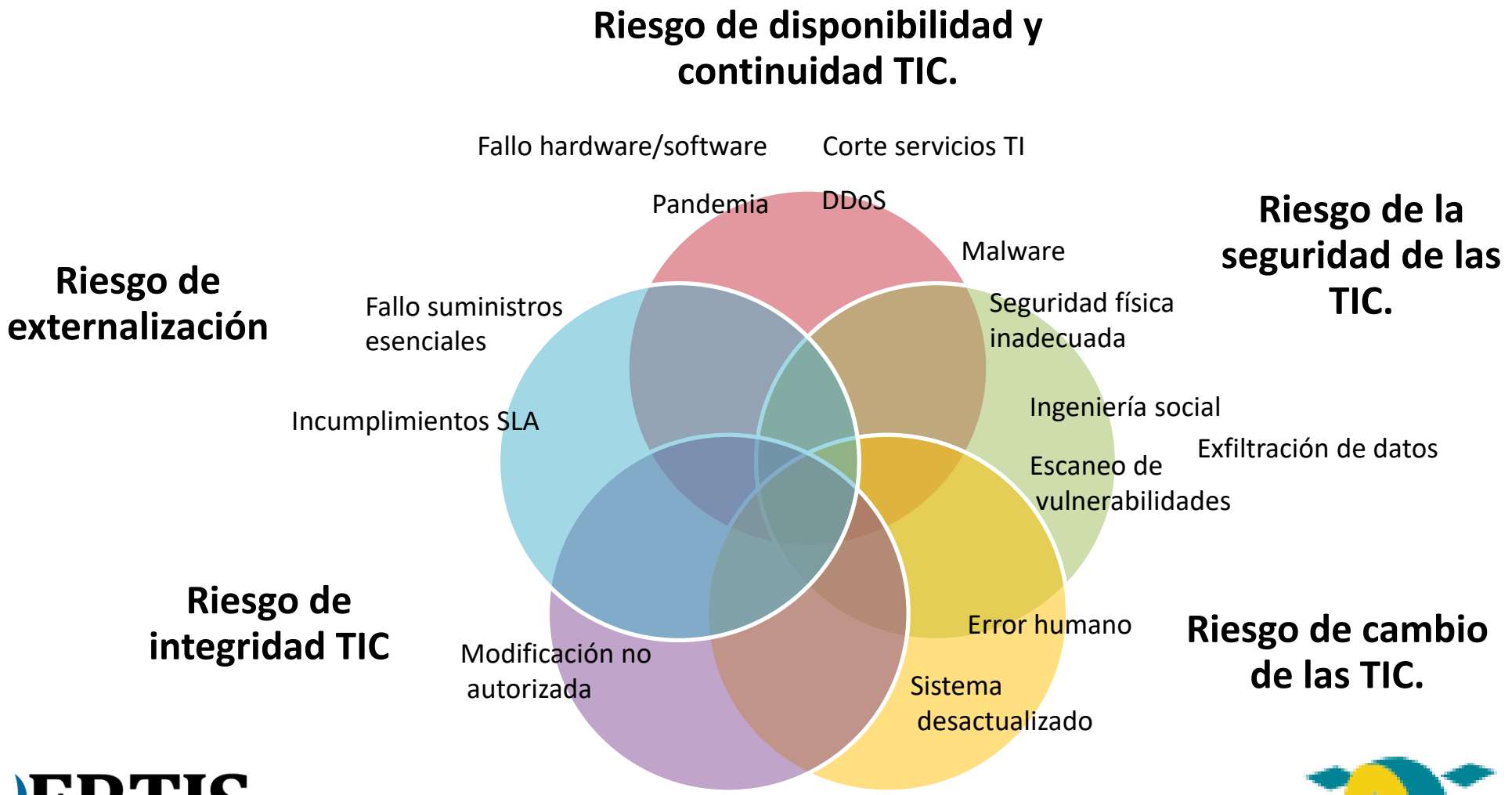
# ¿Animal más mortífero para el ser humano?




GOVERTIS Advisory Services

Red IRIS

# La gestión de riesgos trata de evitar los peores escenarios.



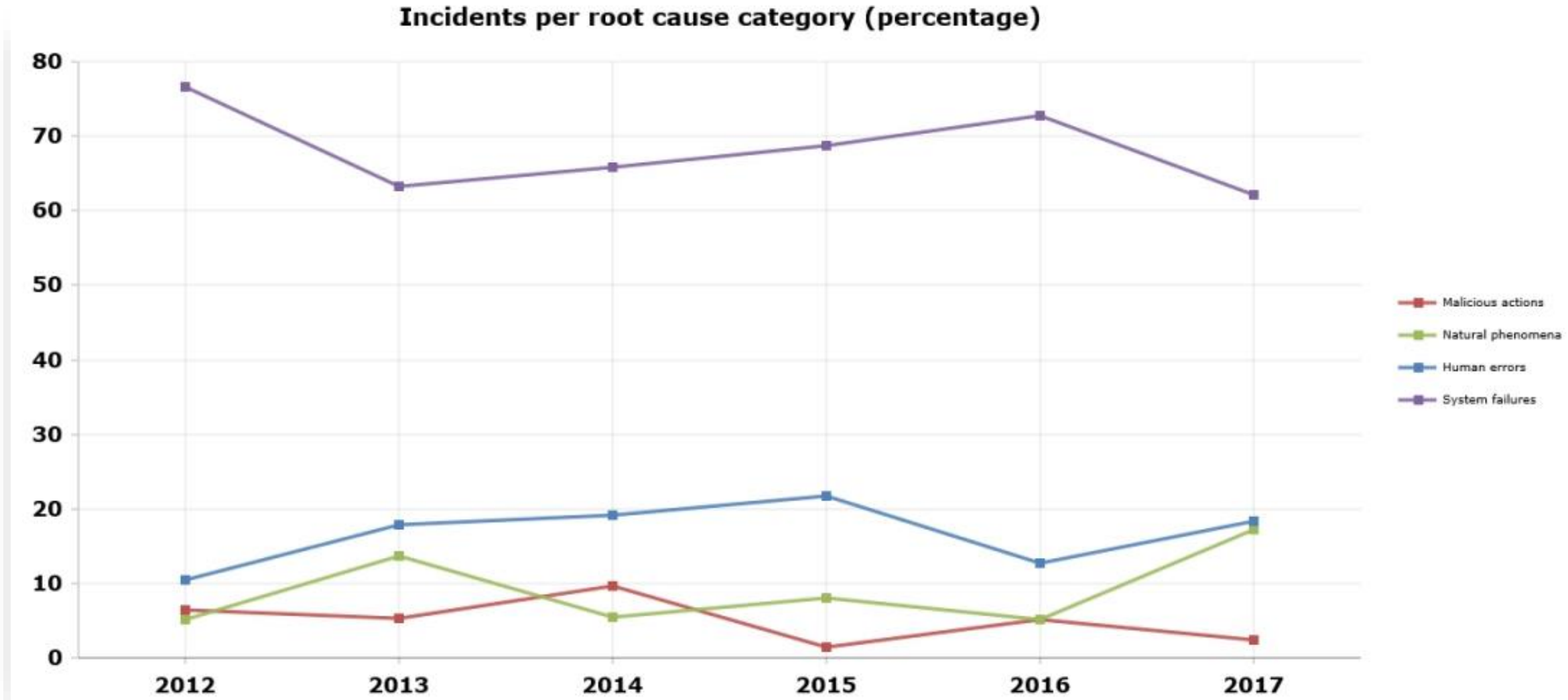
# Existen diferentes tipos de escenarios de riesgo a contemplar.

- **Riesgo de disponibilidad y continuidad TIC:** Asociado al impacto en el rendimiento y disponibilidad de los sistemas y servicios
- **Riesgo de la seguridad de las TIC:** Probabilidad de acceso no autorizado a los sistemas TIC y a los datos
- **Riesgo de cambio de las TIC:** El derivado de la incapacidad de gestionar adecuadamente los cambios en los sistemas TIC
- **Riesgo de integridad TIC:** Relativo al riesgo de que los datos sean incompletos, inexactos, o incoherentes
- **Riesgo de externalización:** Relacionado con la contratación de sistemas o servicios TIC a un tercero.

GOVERTIS Advisory Services

Red IRIS

# Estadísticas “curiosas”

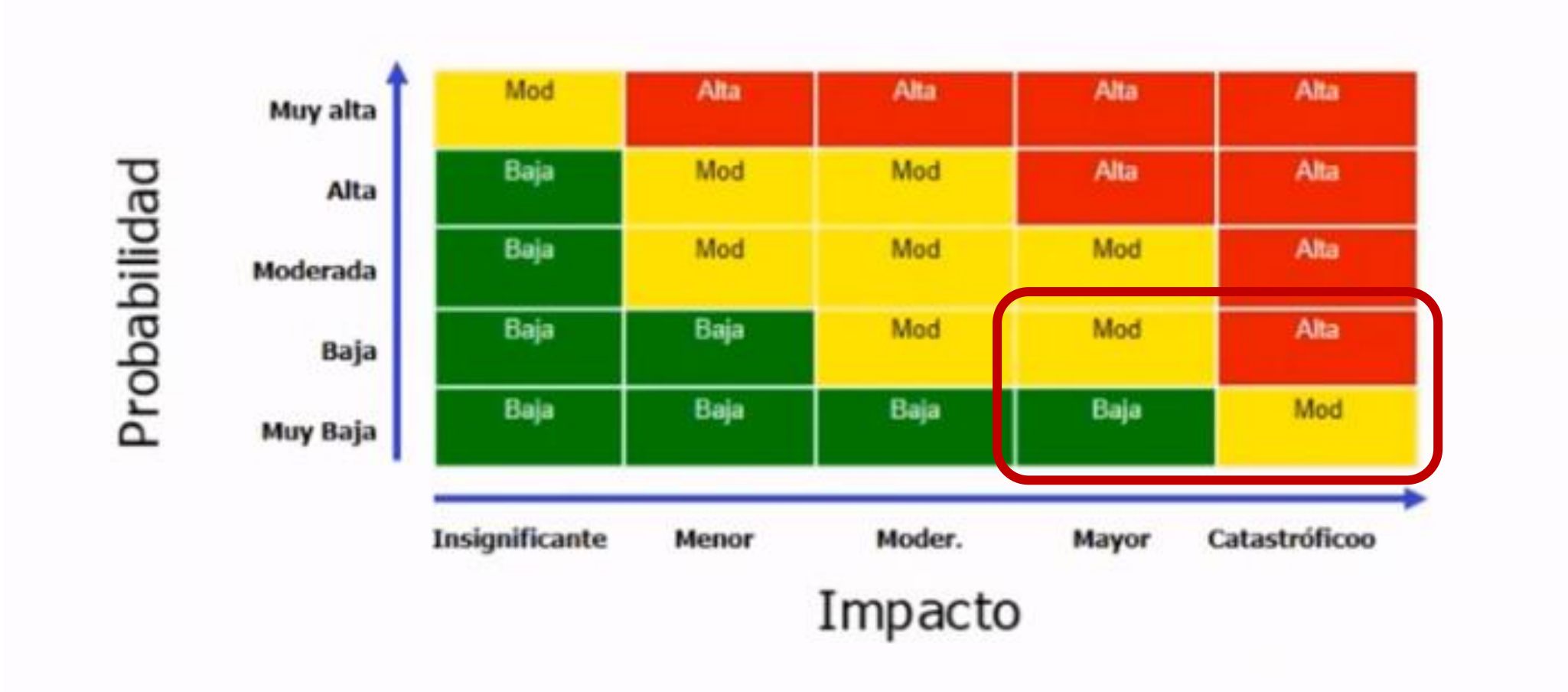



GOVERTIS Advisory Services

RedIRIS

# Las zonas de trabajo deben considerar “cisnes negros”

Alto impacto y muy baja probabilidad pero que provocan situaciones de crisis.

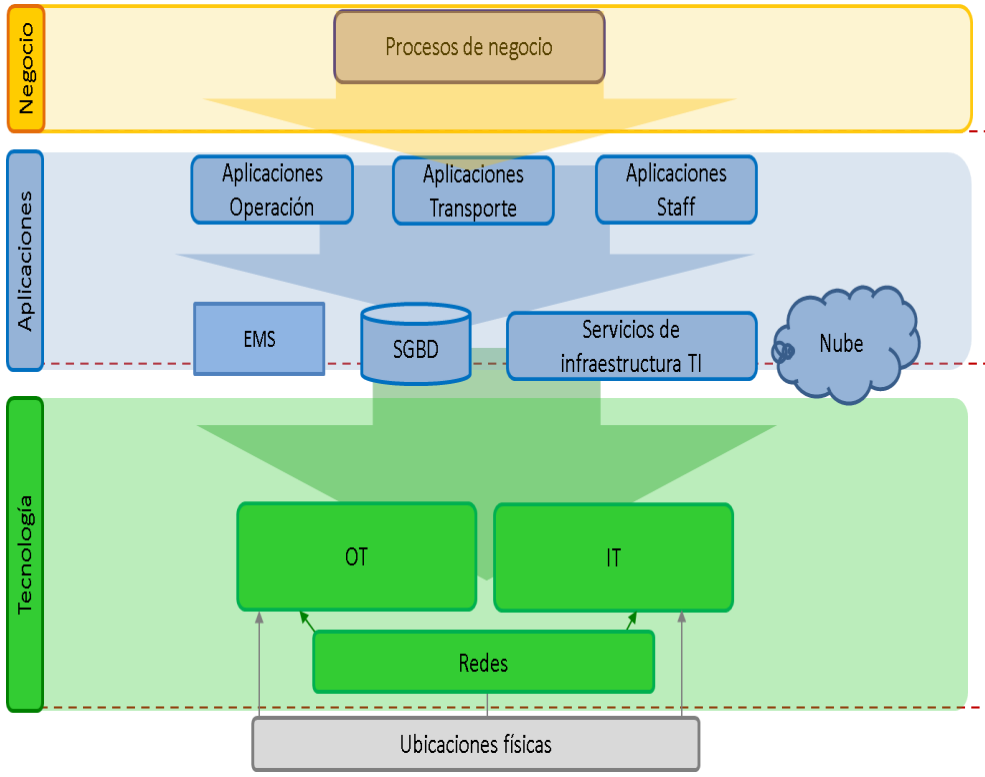


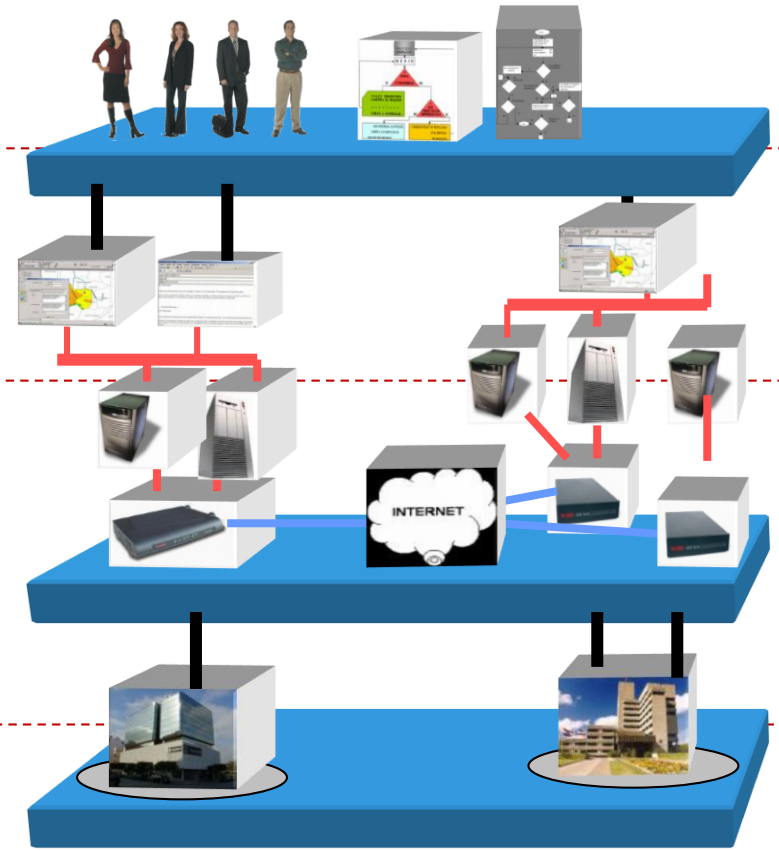

GOVERTIS Advisory Services

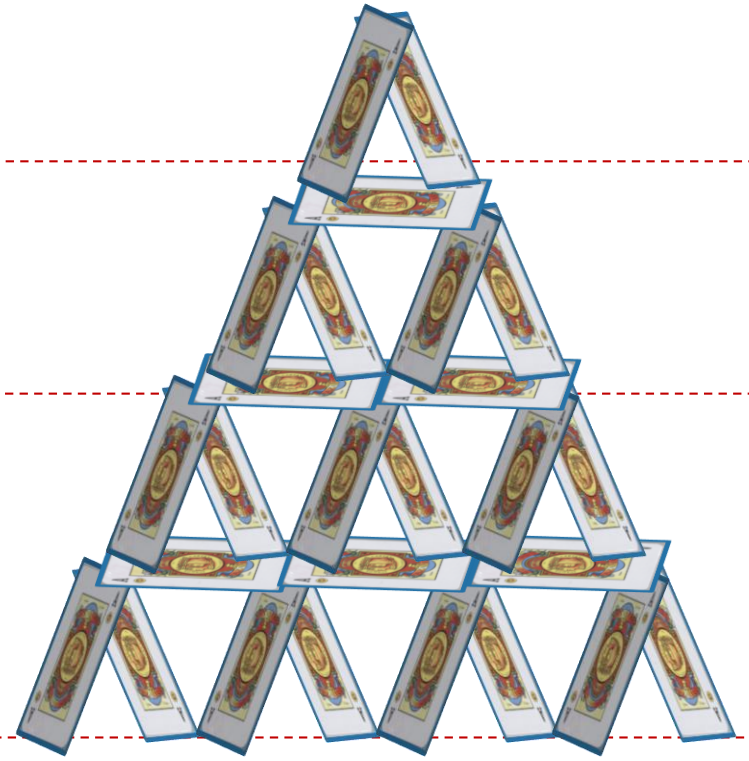
RedIRIS

# Un incidente mal gestionado puede acabar produciendo crisis.

Se pueden producir “efectos avalancha” o “bola de nieve”.



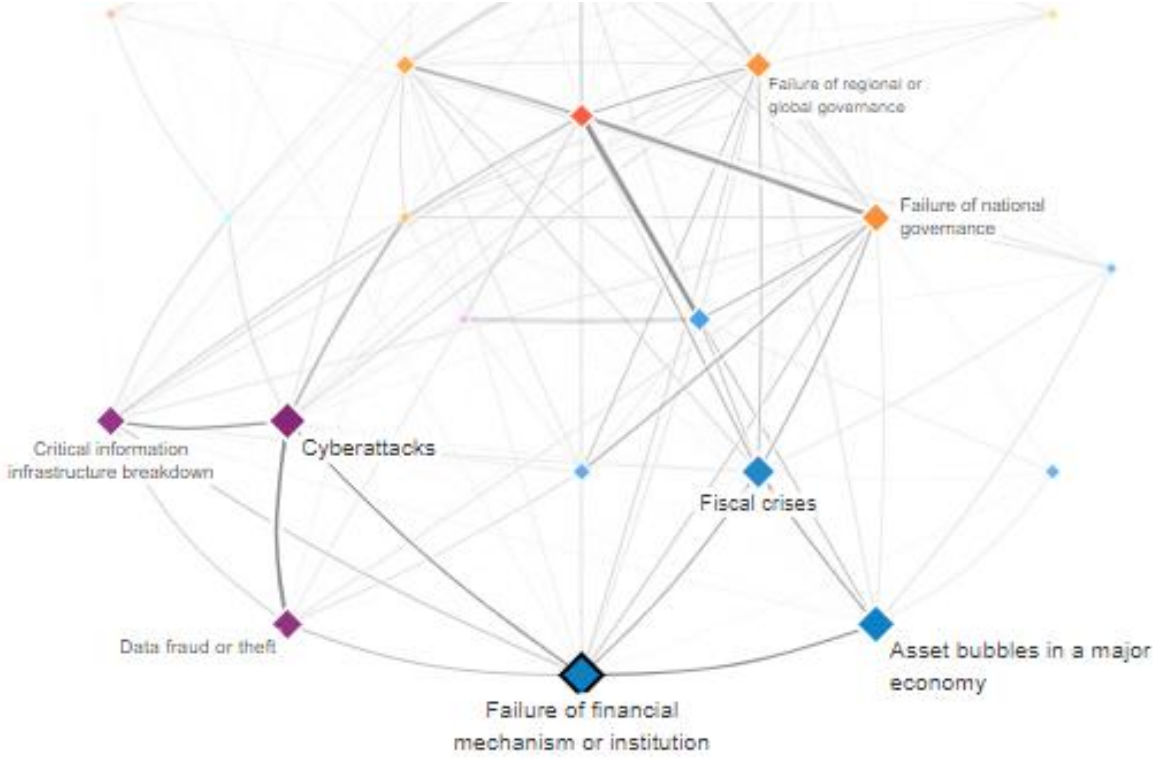



GOVERTIS Advisory Services

GOVERTIS Advisory Services

# Los riesgos además están interrelacionados.




Selected risk

Clear selection

## Failure of financial mechanism or institution

Collapse of a financial institution and/or malfunctioning of a financial system that impacts the global economy

| | |
|---|---|
| Category | Economic Risk |
| Impact | 3.16 |
| Likelihood | 3.17 |

Most connected global risks:

- Asset bubbles in a major economy
- Cyberattacks
- Fiscal crises

WORLD ECONOMIC FORUM

## Top 5 Global Risks in Terms of Likelihood

| | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1st | Asset price collapse | Asset price collapse | Storms and cyclones | Severe income disparity | Severe income disparity | Income disparity | Interstate conflict with regional consequences | Large-scale involuntary migration | Extreme weather events | Extreme weather events | Extreme weather events |
| 2nd | Slowing Chinese economy (<6%) | Slowing Chinese economy (<6%) | Flooding | Chronic fiscal imbalances | Chronic fiscal imbalances | Extreme weather events | Extreme weather events | Extreme weather events | Large-scale involuntary migration | Natural disasters | Failure of climate-change mitigation and adaptation |
| 3rd | Chronic disease | Chronic disease | Corruption | Rising greenhouse gas emissions | Rising greenhouse gas emissions | Unemployment and underemployment | Failure of national governance | Failure of climate-change mitigation and adaptation | Major natural disasters | Cyber-attacks | Natural disasters |
| 4th | Global governance gaps | Fiscal crises | Biodiversity loss | Cyber-attacks | Water supply crises | Climate change | State collapse or crisis | Interstate conflict with regional consequences | Large-scale terrorist attacks | Data fraud or theft | Data fraud or theft |
| 5th | Retrenchment from globalization | Global governance gaps | Climate change | Water supply crises | Mismanagement of population | Cyber-attacks | High structural unemployment or underemployment | Major natural catastrophes | Massive incident of data fraud/theft | Failure of climate-change mitigation and adaptation | Cyber-attacks |

## Top 5 Global Risks in Terms of Impact

| | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1st | Asset price collapse | Asset price collapse | Fiscal crises | Major systemic financial failure | Major systemic financial failure | Fiscal crises | Water crises | Failure of climate-change mitigation and adaptation | Weapons of mass destruction | Weapons of mass destruction | Weapons of mass destruction |
| 2nd | Retrenchment from globalization (developed) | Retrenchment from globalization (developed) | Climate change | Water supply crises | Water supply crises | Climate change | Rapid and massive spread of infectious diseases | Weapons of mass destruction | Extreme weather events | Extreme weather events | Failure of climate-change mitigation and adaptation |
| 3rd | Oil and gas price spike | Oil price spikes | Geopolitical conflict | Food shortage crises | Chronic fiscal imbalances | Water crises | Weapons of mass destruction | Water crises | Water crises | Natural disasters | Extreme weather events |
| 4th | Chronic disease | Chronic disease | Asset price collapse | Chronic fiscal imbalances | Diffusion of weapons of mass destruction | Unemployment and underemployment | Interstate conflict with regional consequences | Large-scale involuntary migration | Major natural disasters | Failure of climate-change mitigation and adaptation | Water crises |
| 5th | Fiscal crises | Fiscal crises | Extreme energy price volatility | Extreme volatility in energy and agriculture prices | Failure of climate-change mitigation and adaptation | Critical information infrastructure breakdown | Failure of climate-change mitigation and adaptation | Severe energy price shock | Failure of climate-change mitigation and adaptation | Water crises | Natural disasters |

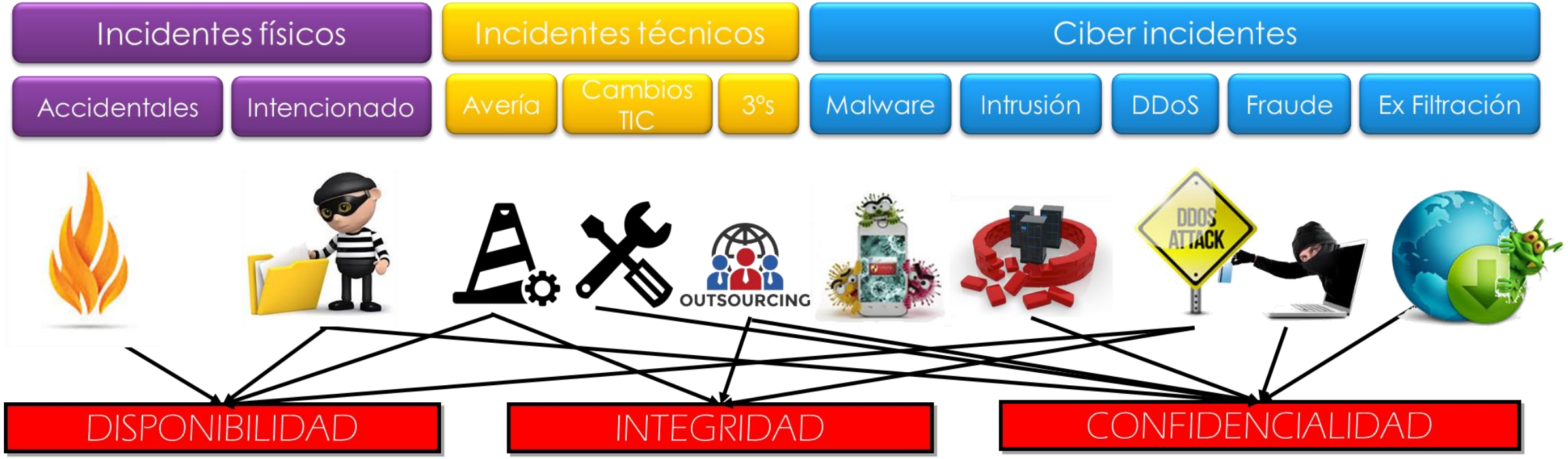
Economic Environmental Geopolitical Societal Technological

GOVERTIS Advisory Services

Red IRIS

# La naturaleza del incidente determina sus consecuencias.

- La naturaleza del evento determina qué tipo de impacto va a producirse (Confidencialidad, Integridad, Disponibilidad o varias a la vez).




GOVERTIS Advisory Services

Red IRIS

# Una crisis es un incidente/accidente con consecuencias serias.


GOVERTIS Advisory Services

RedIRIS

# La palabra "crisis" en japonés significa:

Peligro

危機

Oportunidad

# Definición de Crisis.

- "**Situación compleja y decisiva para la supervivencia de una compañía u organización, producida por sorpresa**, que afecta al público (interno y externo) o/y al producto o/y al proceso o/y a la distribución o/y a la seguridad o/y a los mercados financieros, en la que se acusa una notoria escasez de información y en donde la organización se convierte en centro de atención mediática pudiendo llegar a comprometer su imagen , su credibilidad y su producción, y pudiendo interferir en el desarrollo rutinario de la actividad".

MITROFF y PEARSON (1997).

- "***Situación con un alto nivel de incertidumbre que afecta las actividades básicas y/o la credibilidad de la organización y requiere medidas urgentes***".

ISO/IEC 22301 (Continuidad de negocio).

GOVERTIS Advisory Services

Red IRIS

# Tipologías de crisis.

- A la hora de hacer una clasificación de las tipologías de crisis nos encontramos diferentes criterios, según el concepto en que nos fijemos para identificarlas: **causas**, naturaleza, intensidad, efectos...

| Normal Accidents | | | Abnormal Accidents | | | Natural Accidents |
|---|---|---|---|---|---|---|
| **Economic Crisis** | **Physical Crisis** | **Personnel Crisis** | **Criminal Crisis** | **Information Crisis** | **Reputation Crisis** | **Natural disasters** |
| Recessions | Industrial accidents | Strikes | Product tampering | Theft of proprietary information | Rumour mongering or slander | Earthquakes |
| Stock Market Crashes | Supply breakdowns | Exodus of key personnel | Kidnapping or hostage situations | Tampering with company records | Logo tampering | Floods |
| Hostile Takeovers | Product failures | Workplace violence or vandalism | Acts of terrorism | Cyberattacks | | Fires |

GOVERTIS Advisory Services

Red IRIS

**Técnico/ Económico**

| | |
|---|---|
| Productos o servicios defectuosos<br>Fallos técnicos y accidentes<br>Problemas en los sistemas informáticos<br>Quiebra | Desastres ecológicos y accidentes graves<br>Fallos del sistema a gran escala<br>Desastres naturales<br>OPAS hostiles<br>Crisis gubernamentales<br>Crisis internacionales |
| Incapacidad de adaptarse/ cambiar<br>Ruptura organizativa<br>Mala comunicación<br>Sabotaje<br>Alteración de productos en la fábrica<br>Rumores, difamaciones<br>Actividades ilegales<br>Acoso sexual<br>Enfermedades laborales | Proyección simbólica<br>Sabotaje<br>Terrorismo<br>Secuestro de directivos<br>Alteración de productos fuera de la fábrica<br>Falsificación<br>Rumores, difamaciones<br>Huelgas<br>Boicots |

**Interno** | **Externo**

**Humano/ Social / Organizacional**

# Características de una crisis.

- **1- La sorpresa siempre le es inherente.** No existe ninguna crisis totalmente anticipada puesto que algo que hubiese sigo previsto, jamás conduciría a una crisis.

- **2- Cada crisis es única, raramente dos crisis tienen las mismas causas o efectos.** Siempre hay factores clave que serán únicos en cada caso aunque las muchas crisis pueden tener muchas similitudes en los eventos que causan su origen.

- **3- Toda crisis provoca una situación de urgencia.** Está caracterizada por las complejas dificultades que hay que afrontar y por la afluencia de informaciones negativas a valorar para poder atajar la situación.

GOVERTIS Advisory Services

Red IRIS

# No siempre implican interrupción de servicios.

- Las crisis suelen están generadas por todos aquellos eventos inesperados e/o inevitables de carácter catastrófico que pueden afectar a los activos críticos, la estructura financiera, las personas e incluso la reputación, poniendo en peligro la propia supervivencia de la compañía, y que, siendo verdaderas, no siempre suponen la activación de un plan de continuidad de negocio.
- Las crisis no siempre implican interrupción de la actividad empresarial o amenazas directas a la vida, a la propiedad o a los activos, pero sin embargo, casi siempre suponen un peligro para la reputación de una organización y su marca, incluso si es sólo a través de la necesidad de demostrar una fortaleza y liderazgo efectivo

# La percepción del incidente de seguridad no es proporcional al suceso.

ADSLZONE.net FOROS SOPORTE OFICIAL ACTUALIDAD UTILIDADES

## Un grupo afirma haber hackeado a decenas universidades, ministerios y partidos políticos de España

Un grupo afirma haber hackeado a decenas ...

software

La **administración española** poco a poco va avanzando hacia la **digitalización**, pero hay todavía sistemas anticuados a nivel de software, y cuya seguridad parece no estar al día. Así lo afirma un grupo de **hackeo ético llamado Digital Research Team**, que habría **hackeado** a **universidades, ministerios y hasta a partidos políticos** de España.

## Digital Research Team: el grupo de hackeo ético que está asolando las bases de datos de España

Entre las **universidades** que de momento habrían visto expuestos sus datos encontramos también la Universidad Pablo Olavide de Sevilla, la Universidad de Málaga, la Universidad Rovira i Virgili, la Universidad Politècnica de Catalunya, la Universidad de Huelva, la Universidad de Cádiz, la Universidad de Extremadura, la Universidad de Córdoba, la Universidad Politécnica de Madrid, la Universidad de Ovideo y la Universidad de Zaragoza.

Entre otros afectados también encontramos el **Imserso, el INE**, la Real Federación Española de Atletismo, el Servei de Salut de Baleares, la Sanitat de Catalunya, Comisiones Obreras, y ExtremaduraTrabaja.

Como vemos, la **infosec** de los **organismos públicos** de España deja mucho que desear si este grupo ha conseguido acceder a todas estas instituciones. Algunas instituciones ya se han puesto **en contacto con el hacker para solucionar los fallos al correo digitalresearchteam@secmail.pro**, como es el caso de la Universidad de Huelva.

GOVERTIS Advisory Services

Red IRIS

# Un incidente de seguridad puede generar graves daños reputacionales.

MADRID

## Cifuentes “debe aclarar” la falsificación de sus notas de un máster de la URJC

- PSOE y Podemos reclaman una explicación convincente a la presidenta regional
- Cifuentes habría obtenido un master en una universidad pública con notas falsificadas

REDACCIÓN, MADRID
21/03/2018 10:14

Actualizado a
21/03/2018 13:12

La presidenta regional Cristina Cifuentes en luna reciente edición de los desayunos informativos de Europa Press. (Emilia Gutiérrez)

**Una funcionaria de otro campus entró en el sistema de notas y cambió los dos ‘no presentado’ por sendos ‘notable’, con una nota de 7,5, sin que conste que se hubiera vuelto a matricular en esos créditos**

GOVERTIS Advisory Services

Red IRIS

# Incidente vs Crisis.

Definiciones **ISO 22300:2018.** Security and resilience — Vocabulary.

- **Incidente** – "*situation that might be, or could lead to, a disruption, loss, emergency or crisis*".
- **Crisis** – "*unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property or the environment*".

- **Los incidentes dan origen a una crisis,** principalmente aquellos que no son gestionados de manera adecuada y oportuna.
- La crisis es un tipo de incidente que tiene la capacidad de impactar significativamente a la organización

GOVERTIS Advisory Services

Red IRIS

# Incidente vs Crisis.

- Un **incidente** es un evento o situación negativa que no detiene el negocio como de costumbre y / o no amenaza el impacto negativo a largo plazo sobre las personas, el entorno, los procesos de negocio, la reputación o los objetivos de la organización. Sin embargo, esto no quiere decir que los incidentes no sean importantes y deban ser detectados y gestionados rápidamente. **Los incidentes mal administrados pueden convertirse en crisis y lo hacen.**

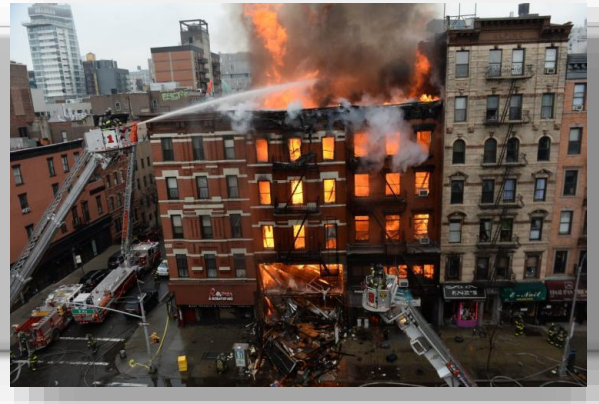
- Una **crisis** es un evento o situación negativa que impacta, o amenaza con afectar, a las personas (partes interesadas), el medio ambiente, las operaciones comerciales, la reputación de la organización y / o el resultado final de la organización, a largo plazo. Una crisis es un evento negativo que detendrá los negocios como de costumbre hasta cierto punto, ya que requerirá atención inmediata y orientación del liderazgo.

Melissa Agnes, Crisis Ready (2019).

GOVERTIS Advisory Services

Red IRIS

# Contingencias, incidentes y gestión de crisis.



- Incidentes que generan interrupción de servicios.


- Incidentes que comprometen infraestructuras o información.


GOVERTIS Advisory Services

RedIRIS

# CONTENIDO.

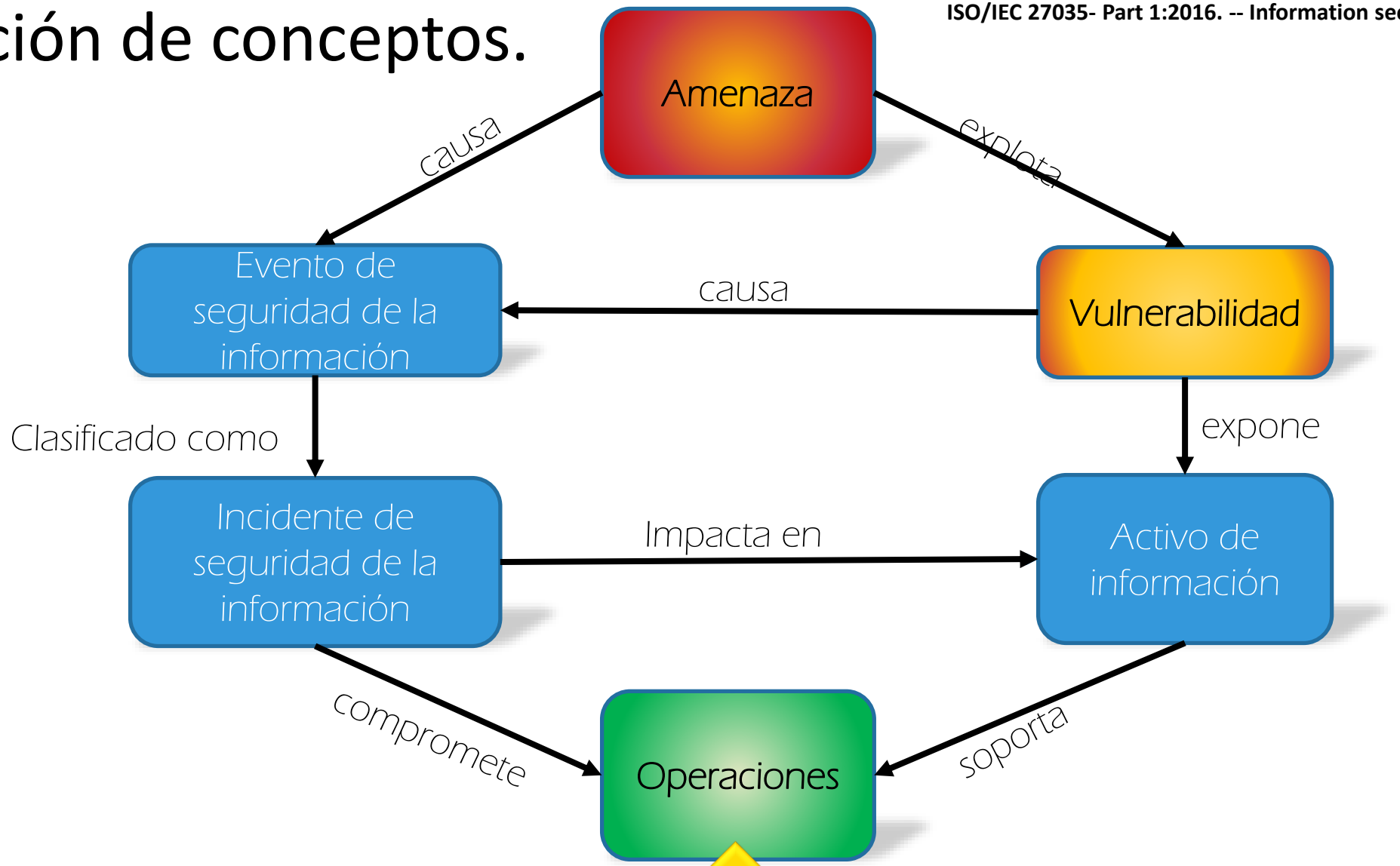
1. CONTEXTO DE LA GESTIÓN DE CRISIS.
2. GESTIÓN DE INCIDENTES vs GESTIÓN DE CONTINUIDAD.
3. GOBIERNO DE LA CRISIS.
4. GESTIÓN REPUTACIONAL EN SITUACIONES DE CRISIS.

GOVERTIS Advisory Services

Red IRIS

# Relación de conceptos.

ISO/IEC 27035- Part 1:2016. -- Information security incident management.




Incidentes
Interrupciones.
Crisis.

GOVERTIS Advisory Services

Red IRIS

# Terminología según estándares ISO 27035 e ISO 22301.

- **Evento de seguridad:** ocurrencia en un sistema, servicio o equipo de red que indica que una posible brecha de seguridad, incumplimiento o fallo de un control o una situación desconocida que pueda ser relevante en seguridad. **ISO/IEC 27035:2016. -- Information security incident management.**

- **Incidente de seguridad:** uno o varios eventos que seguridad que tengan una probabilidad considerable de comprometer los servicios de negocio o amenazar a la seguridad de la información. **ISO/IEC 27035:2016. -- Information security incident management.**

- **Incidente:** evento que puede ser o podría conducir a una interrupción, pérdida, emergencia o crisis. **ISO/IEC 22301:2019. – Business continuity management systems-Requirements.**

- **Interrupción:** Incidente, ya sea anticipado o no, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo con los objetivos de una organización. **ISO/IEC 22301:2019. – Business continuity management systems-Requirements.**

GOVERTIS Advisory Services

AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

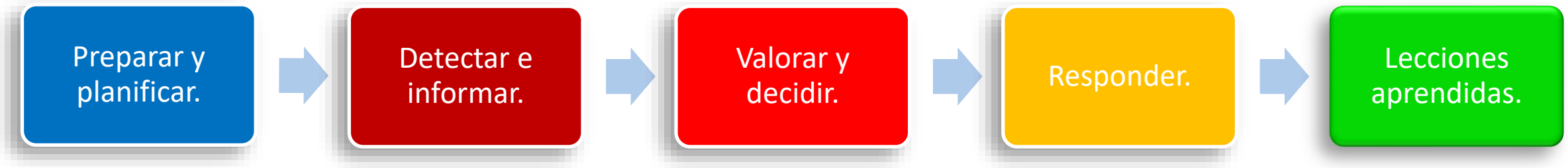
# Incidentes: terminología según el estándar ISO 27035.

- **Gestión de incidentes de seguridad de la información:** ejercicio de un enfoque coherente y efectivo para el manejo y respuesta de incidentes de seguridad de la información.
- **Manejo de incidentes:** acciones de detectar, informar, evaluar, responder, tratar y aprender de la información incidentes de seguridad
- **Respuesta al incidente**: acciones tomadas para mitigar o resolver un incidente de seguridad de la información, incluidas aquellas tomadas para proteger y restaurar las condiciones operativas normales de un sistema de información y la información almacenado en él
- **Punto de contacto (PoC):** función o rol organizacional definido que sirve como coordinador o punto focal de información sobre actividades de gestión de incidentes.
- **Equipo de respuesta a incidentes (IRT):** equipo de miembros de la organización debidamente capacitados y confiables que manejan incidentes durante su ciclo de vida. Es habitual denominar este tipo de equipos como CERT (Equipo de respuesta a emergencias informáticas) o CSIRT (Respuesta a incidentes de seguridad informática)

GOVERTIS Advisory Services

Red IRIS

# Proceso de gestión de incidentes según ISO 27.035.

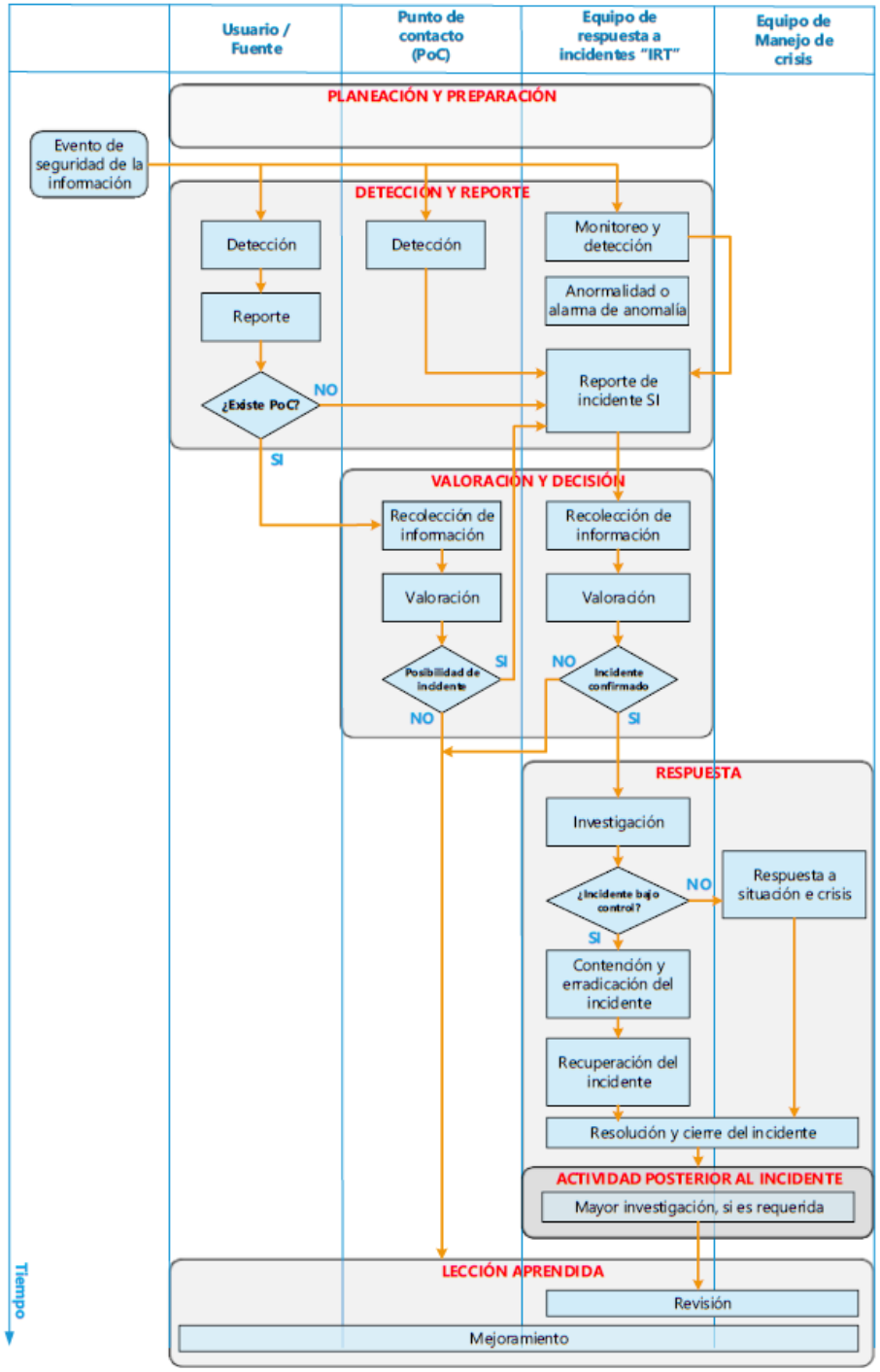



GOVERTIS Advisory Services

RedIRIS

# ISO 27035- Proceso de gestión de incidentes de seguridad.

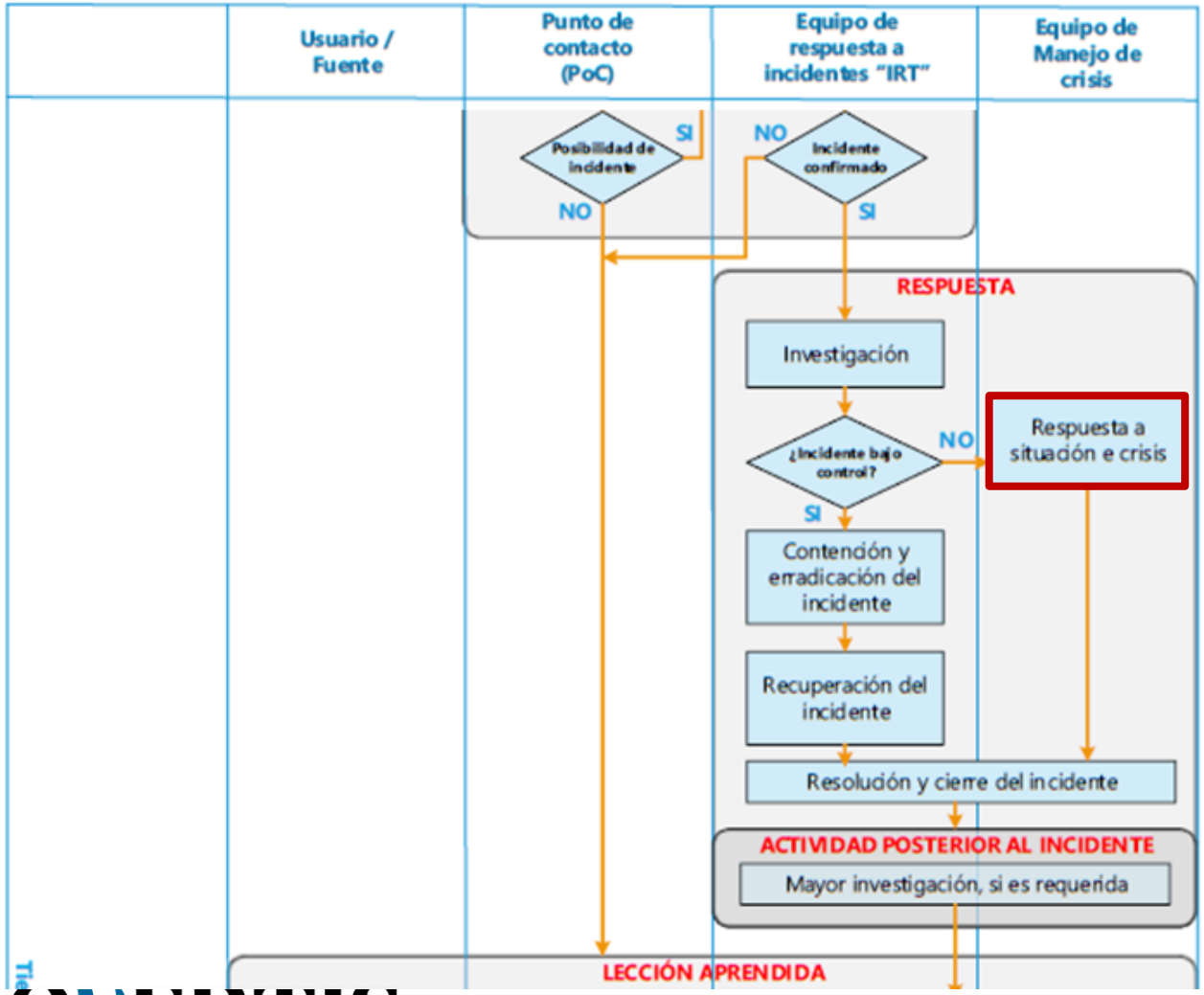
- El estándar define un diagrama de flujo con las actividades esenciales del proceso de gestión de incidentes.




GOVERTIS Advisory Services

Red IRIS

# Gestión de incidentes y respuesta frente a crisis.




- Cuando el incidente no puede ser controlado o el tiempo de respuesta va a tener consecuencias relevantes, se invoca a la respuesta a situación de crisis.

GOVERTIS Advisory Services

Red IRIS

# Continuidad: terminología según el estándar ISO 22301.

- **Continuidad de negocio:** capacidad de una organización para asegurar la entrega de productos o servicios dentro de plazos aceptables a una capacidad predefinida durante una interrupción.

- **Plan de continuidad de negocio:** información documentada que guía a una organización a responder frente a una interrupción y define las actividades de recuperación y restauración de los procesos de entrega de productos o servicios de forma consistente con los objetivos de continuidad.

- **Maximun tolerable period of disruption (MTPD):** Máxima ventana de tiempo durante la que se produce impacto por no reanudar las actividades que sería tolerable por la organización.

GOVERTIS Advisory Services

Red IRIS

# ¿Qué es la gestión de la continuidad de negocio?

RIESGO = Función (Probabilidad x Impacto)

Prevenir Riesgo

**Objetivo:**
- Disminuir las probabilidades de ocurrencia de incidentes (vulnerabilidad).
- Reducir el potencial impacto de cada una de las amenazas.

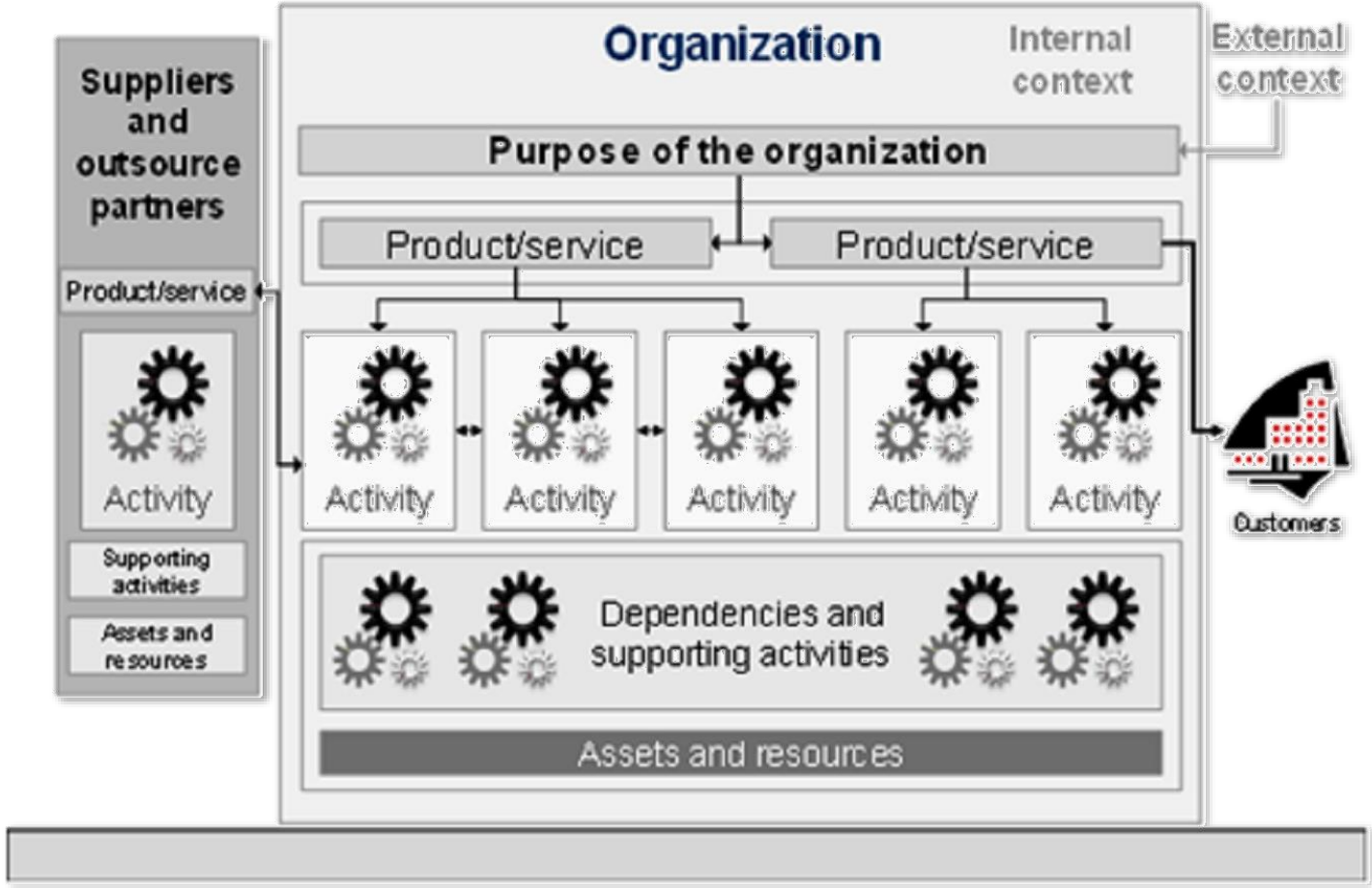
Reaccionar incidentes

**Objetivo:**
- Reaccionar de manera rápida y coordinada en caso de incidente.
- Minimizar los daños una vez producido el incidente.

GOVERTIS Advisory Services

Red IRIS

# En continuidad se identifican todas las piezas necesarias para asegurar los objetivos de la organización.



# ¿Qué es un plan de continuidad de negocio?

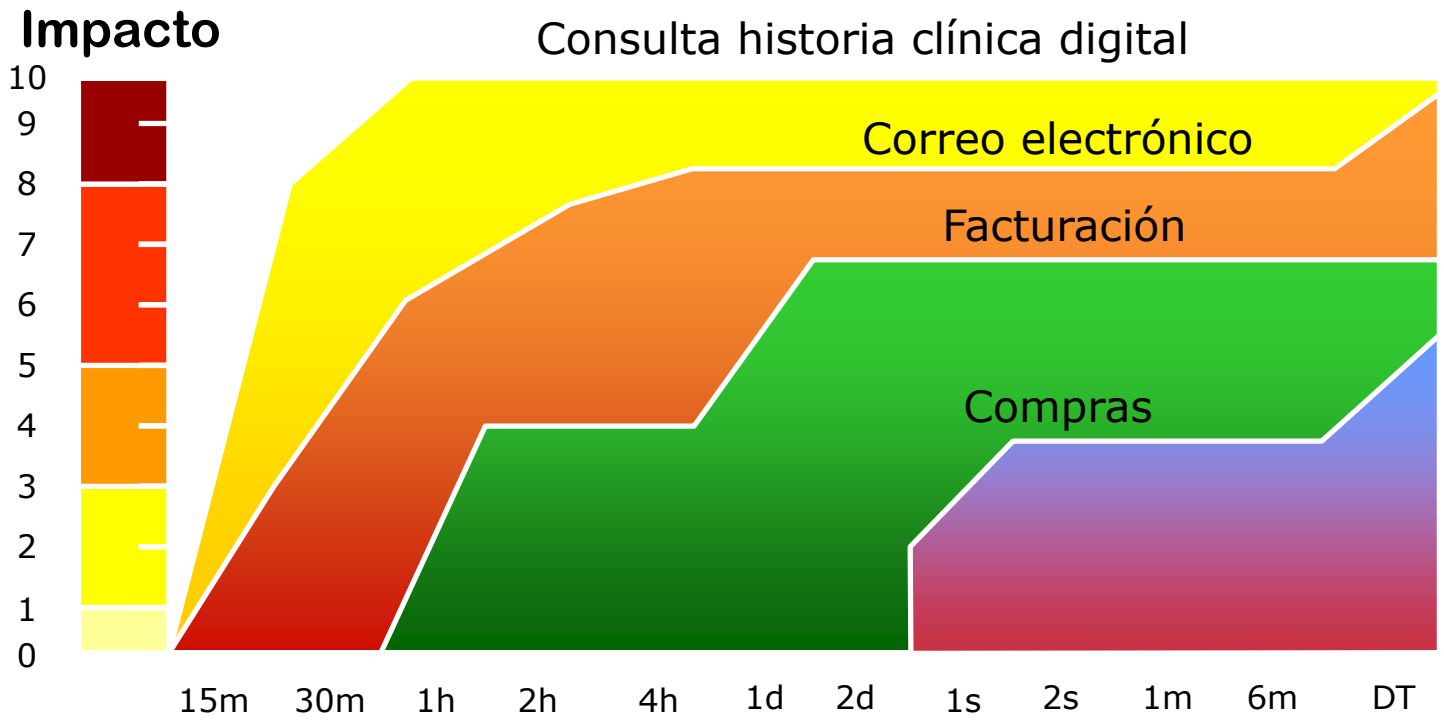
- Es el conjunto de **procedimientos y estrategias** que hay que llevar a cabo para **asegurar** la **supervivencia** de la **compañía** en el caso de que sufra una **interrupción grave** sobre su negocio, generando un impacto mínimo o nulo tanto económico como a la imagen de la compañía.

- El objetivo principal de un **"Plan de Continuidad de Negocio“ (PCN)** es **proporcionar** a la Organización **una solución práctica y fiable para recuperar las actividades y procesos críticos** del negocio en caso de ocurrir una contingencia o siniestro tanto parcial como total.

GOVERTIS Advisory Services

Red IRIS

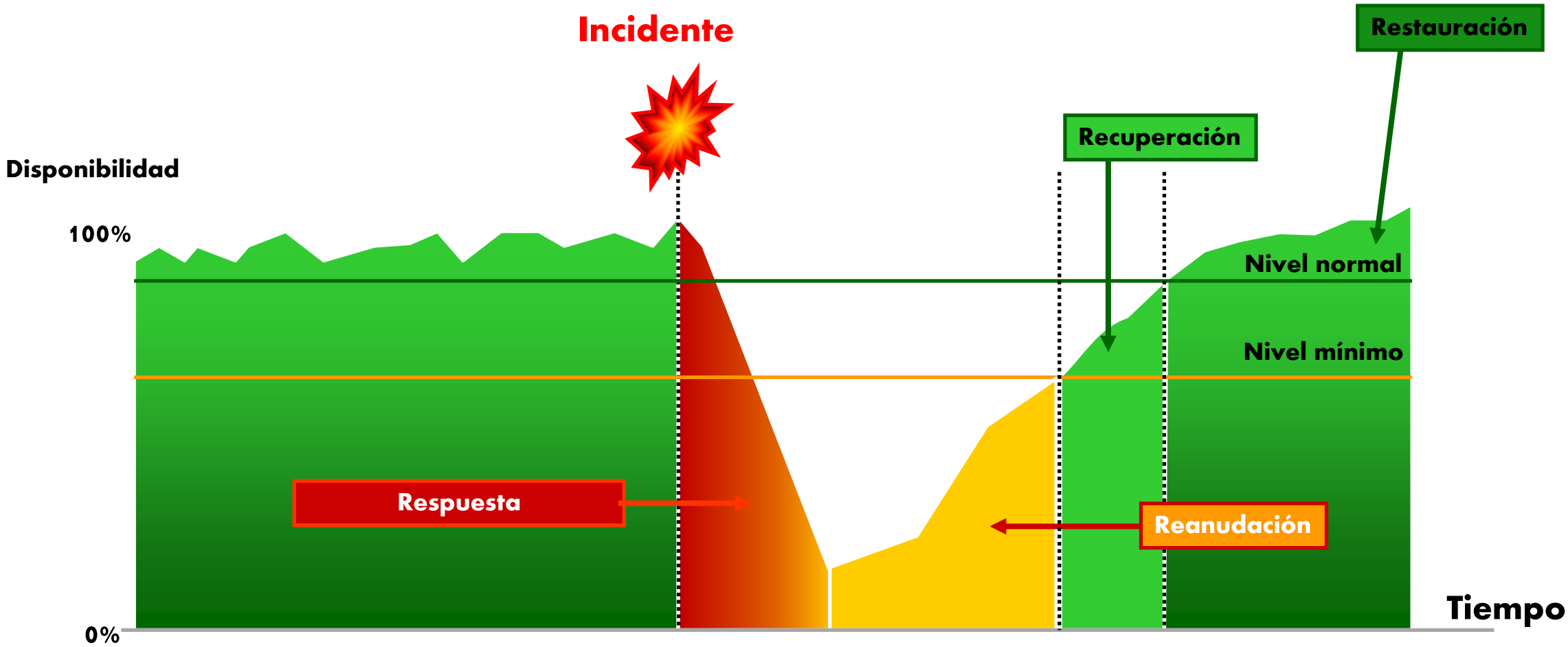
# Una crisis en continuidad se produce si se superan ventanas máximas de interrupción y daño.




GOVERTIS Advisory Services

RedIRIS

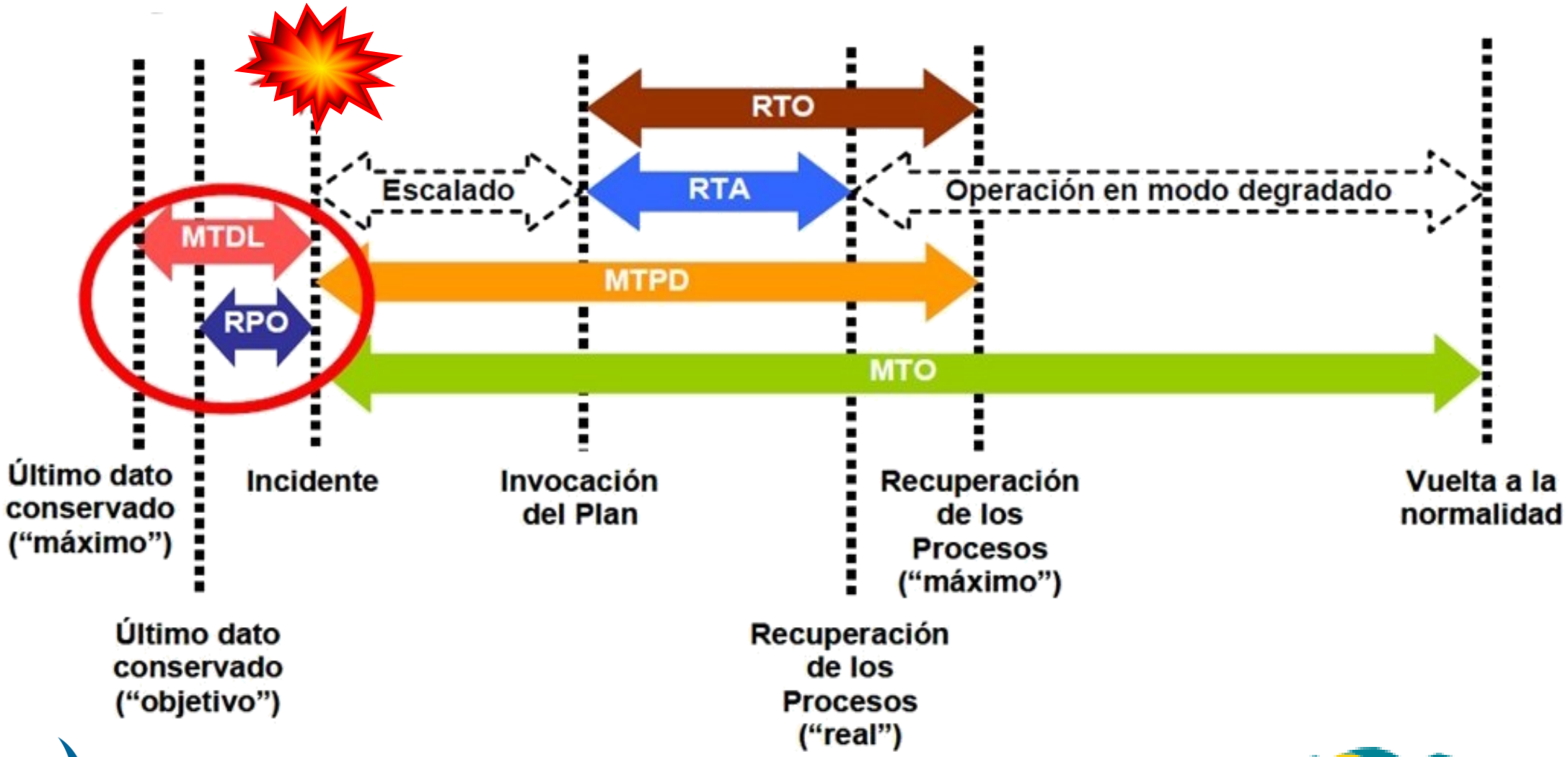
# Fases de gestión de una interrupción.




GOVERTIS Advisory Services

RedIRIS

# MTPD, RTO: Ventanas de tiempo de recuperación.



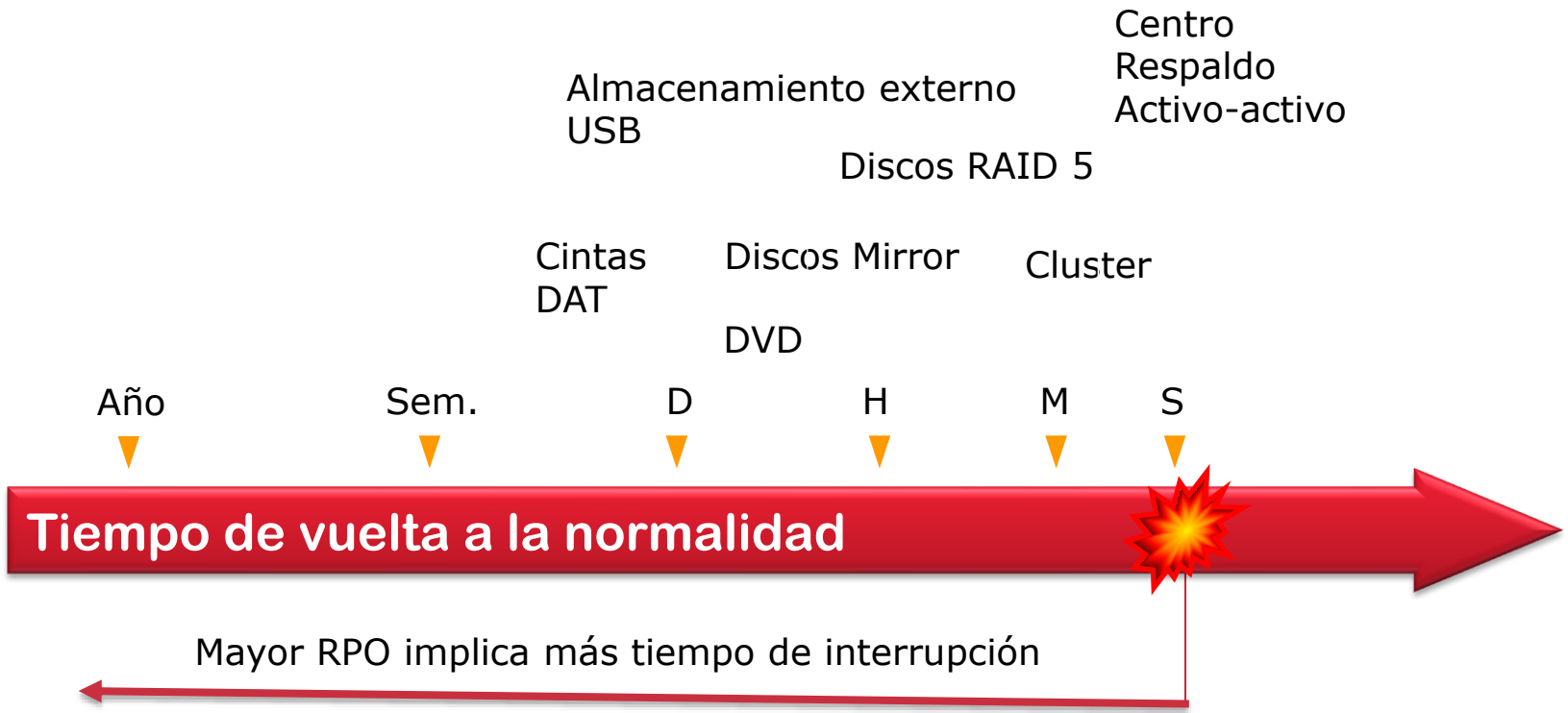

GOVERTIS Advisory Services

Red IRIS

# Las estrategias de continuidad condicionan los tiempos de recuperación.

- Return Point Objetive (RPO): Momento de restauración o instante hasta el que recuperar datos.
- Return Time Objetive (RTO): Cuánto tiempo se tardará en volver a levantar dispositivo.

**¿Hasta donde debo recuperar?**

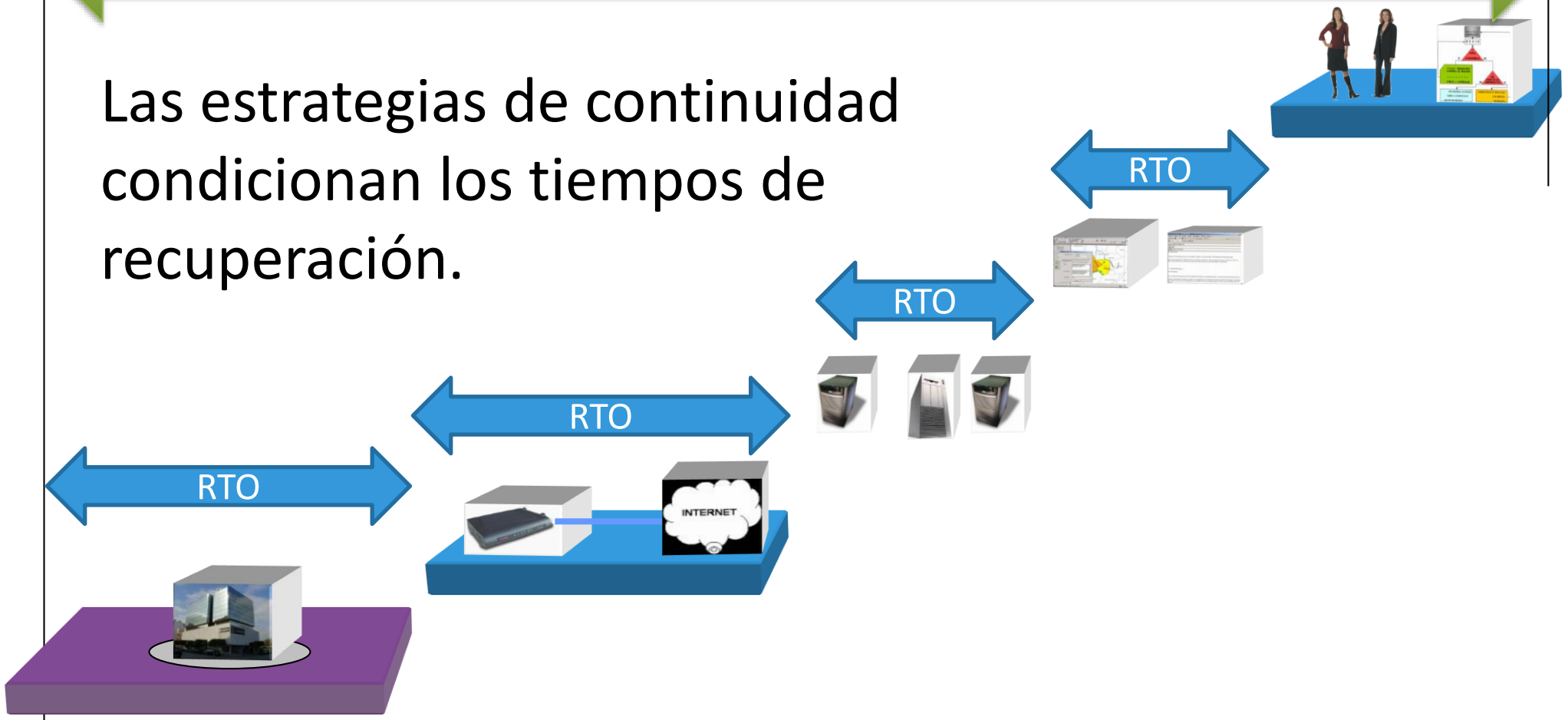



GOVERTIS Advisory Services

RedIRIS

MTPD (Maximum Tolerable Period of Disruption)

Las estrategias de continuidad condicionan los tiempos de recuperación.




Procesos

Aplicaciones y datos

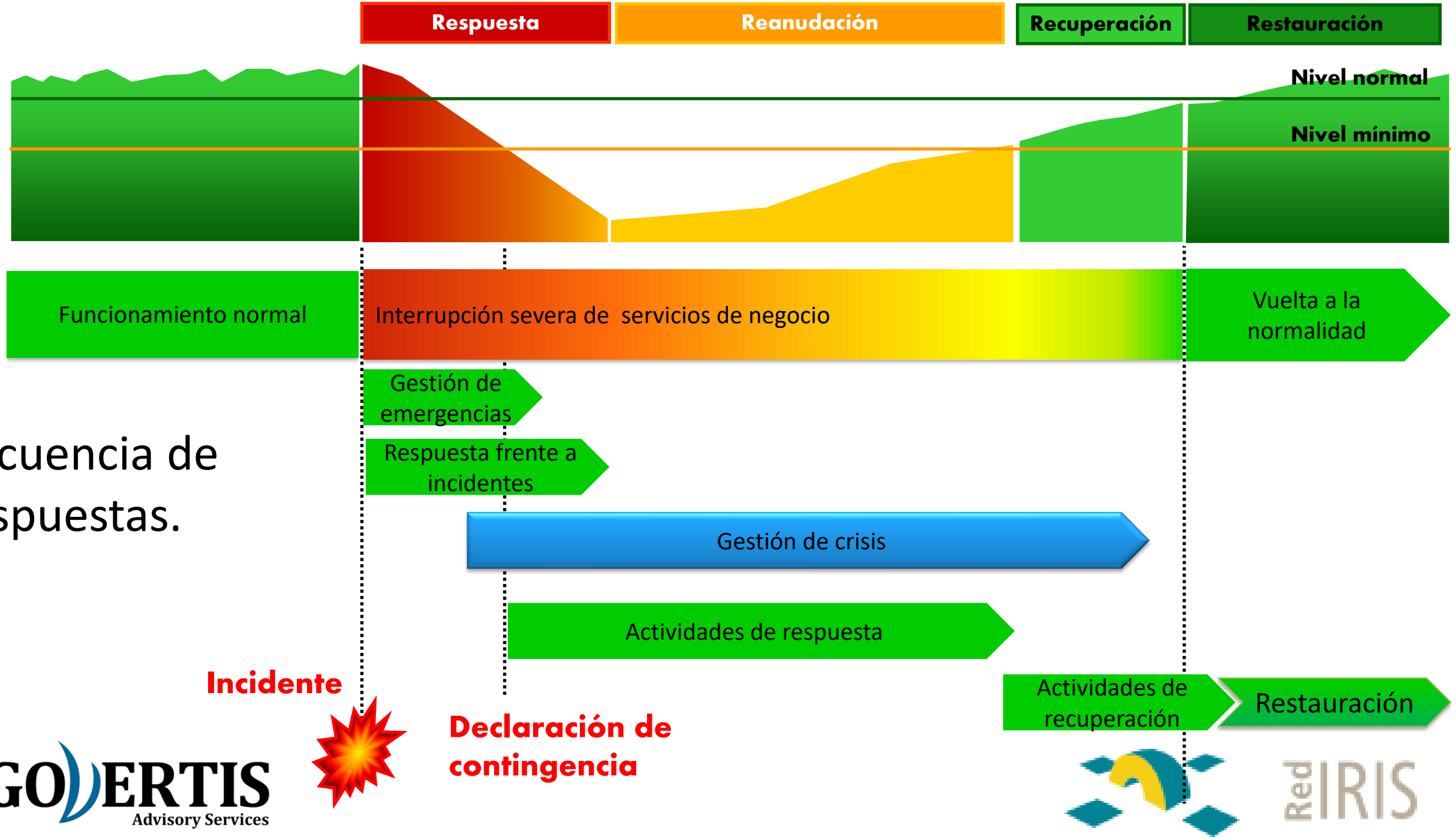
Sistemas

Comunicaciones

Instalaciones

GOVERTIS Advisory Services

RedIRIS




# Secuencia de respuestas.

GOVERTIS Advisory Services

Red IRIS

# Fases del proceso de continuidad de negocio.

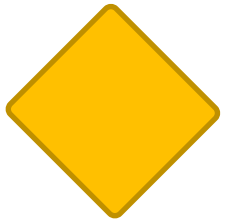

F1. Respuesta.
F2. Reanudación.
F3. Recuperación.
F4. Restauración.

GOVERTIS Advisory Services

Red IRIS

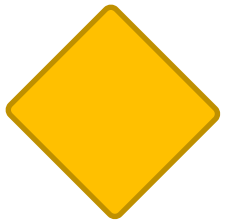
# ¿Cuándo se toman las decisiones?

¿Activa Comité de crisis?



- El incidente se complica y el tiempo de vuelta a la normalidad puede producir impacto en la organización.

¿Activa Plan de continuidad?



- Se requiere poner en marcha las actuaciones de reanudación, recuperación para asegurar la restauración de los entornos afectados.

GOVERTIS Advisory Services

Red IRIS

# ¿Cuándo estamos en crisis?


GOVERTIS Advisory Services

Red IRIS

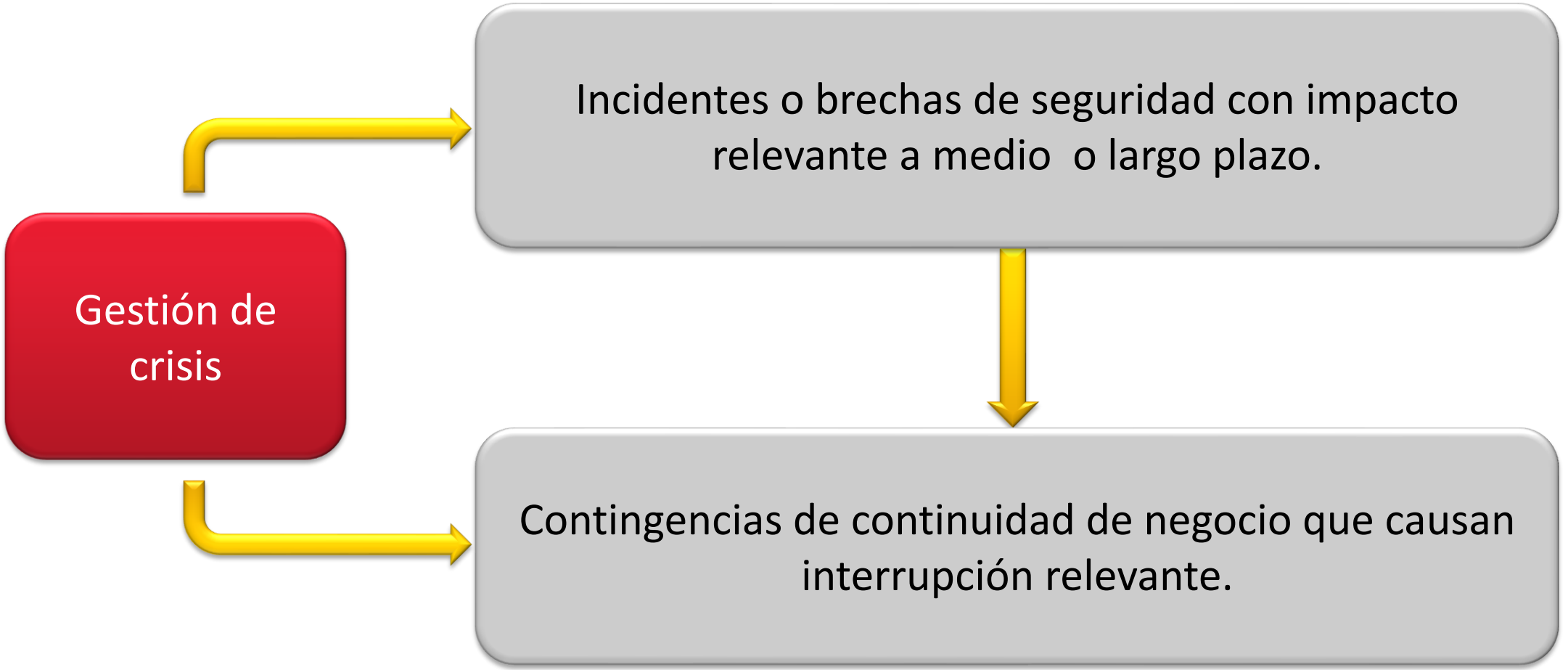
# ¿Cuándo estamos en crisis?

- No siempre deben cumplirse todos los criterios definidos, para algunas organizaciones puede ser suficiente uno de ellos para declarar una crisis.

- La definición de estos criterios debe realizarse teniendo en cuenta los escenarios.

- Los escenarios deben identificar situaciones que afecten gravemente a la organización y contemplar grandes grupos de situaciones que se gestionarían de forma similar.
  - Escenario de contingencia en comunicaciones.
  - Escenario de contingencia por indisponibilidad de CPD.
  - Escenario de contingencia por malware.

# Situaciones que provocan una gestión de crisis




GOVERTIS Advisory Services

RedIRIS

# Los planes de respuesta se agrupan por escenarios.

- La gestión de contingencias debe atender a agrupar en “escenarios” las situaciones posibles para disponer de planes de respuesta adecuados según la naturaleza de las amenazas.


GOVERTIS Advisory Services

Red IRIS

# Grandes escenarios con casuísticas similares: Ejemplos

Avería en dispositivos críticos

Incidente en proveedor crítico


Crisis reputacional

Ataque o Intrusión


Error humano

Daños físicos

GOVERTIS Advisory Services

Red IRIS

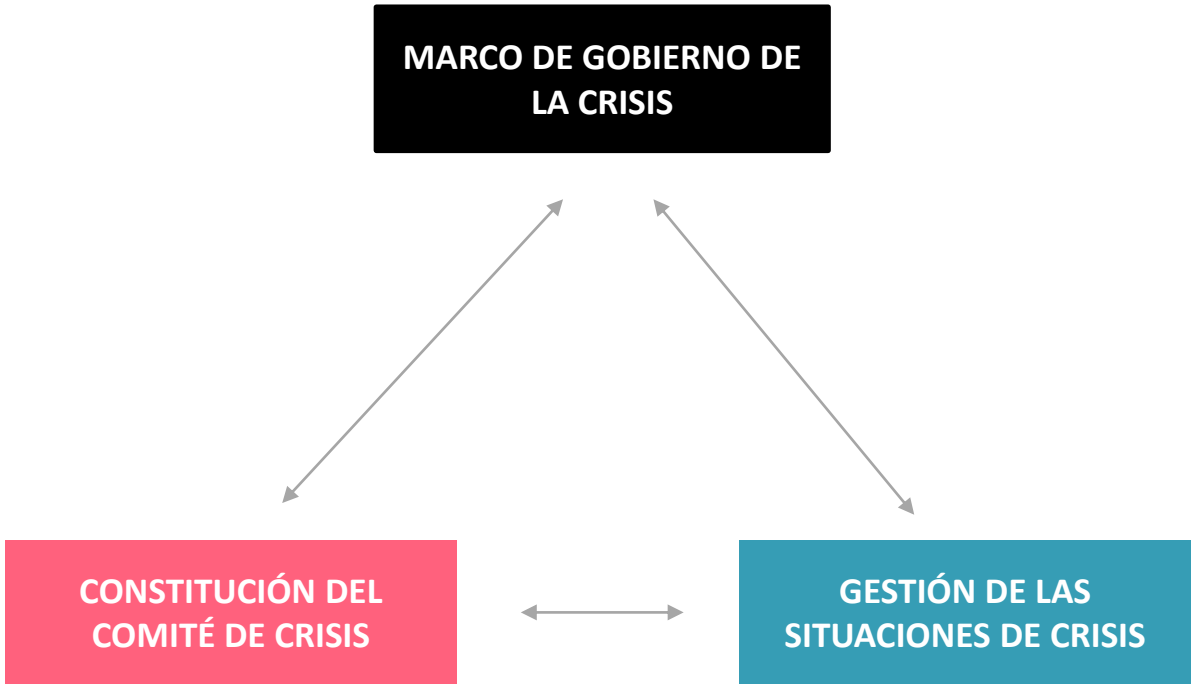
# CONTENIDO.

1. CONTEXTO DE LA GESTIÓN DE CRISIS.
2. GESTIÓN DE INCIDENTES vs GESTIÓN DE CONTINUIDAD.
3. GOBIERNO DE LA CRISIS.
4. GESTIÓN REPUTACIONAL EN SITUACIONES DE CRISIS.

GOVERTIS Advisory Services

Red IRIS

# Gobierno de situaciones de crisis.




GOVERTIS Advisory Services

Red IRIS

# Elementos del marco de gobierno de una crisis.

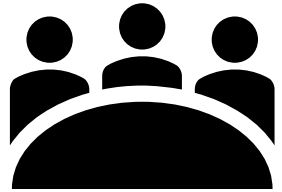

Comité de crisis.

Plan de gestión de crisis.

GOVERTIS Advisory Services

Red IRIS

# Comité de crisis.



- Es el órgano gestor de las situaciones de contingencia y responsable del Plan de Gestión de Crisis y el Plan de Continuidad de Negocio en su globalidad.

- Se deben definir las **comunicaciones necesarias** para la correcta gestión de las actividades que se deben realizar durante el transcurso de la crisis. Es necesario asegurar que el Comité de Crisis **disponga de toda la información relevante** de una manera precisa y en un corto período de tiempo, para poder tomas las decisiones y medidas de actuación necesarias de cara a paliar la duración e intensidad de la situación de crisis.

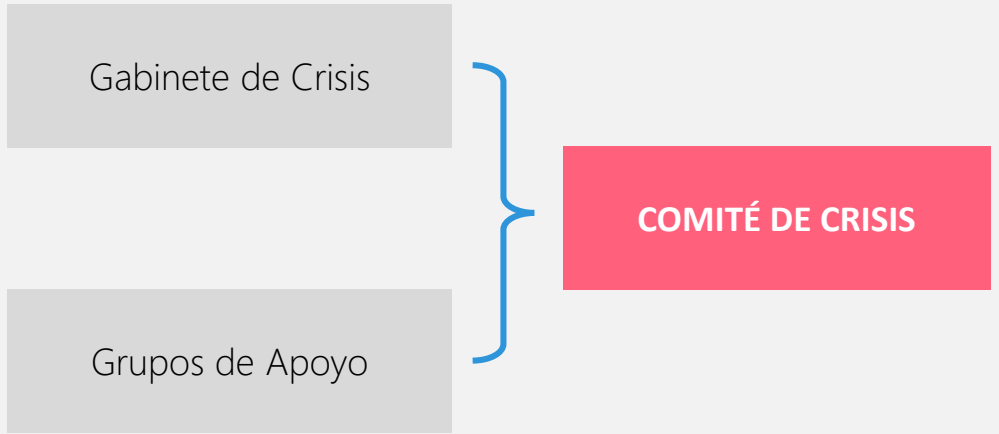
GOVERTIS Advisory Services

Red IRIS

## Constitución del Comité de Crisis

| | |
|---|---|
| 1 | Funciones globales |
| 2 | Composición y miembros |
| 3 | Funciones particulares |
| 4 | Salas de Gestión de Crisis |
| 5 | Ubicación de los Grupos de Apoyo |

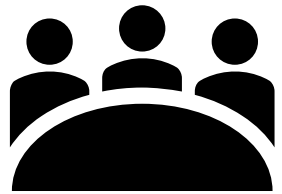
## Composición del Comité de Crisis




GOVERTIS Advisory Services

Red IRIS

# Funciones del Comité de crisis.



- **Como gestor de las situaciones de contingencia.**
    1. Dirigir y coordinar las actuaciones en situaciones de contingencia.
    2. Canalizar la comunicación interna y todas las actuaciones relacionadas con los empleados en caso de contingencia
    3. Canalizar la comunicación con organismos externos.
    4. Dirigir y supervisar la elaboración del informe o informes de recuperación ante la contingencia (seguimiento y control).
    5. Articular los procedimientos de vuelta a la normalidad y dirigir las etapas para su cumplimentación efectiva en el tiempo más corto posible.
- **Como responsable de la asegurar la adecuada gestión frente a contingencias.**
    1. Diseñar, ejecutar y valorar las pruebas y el mantenimiento del Plan de Gestión de Crisis en particular y del Plan de Continuidad de Negocio global en general.
    2. Promover la difusión de la cultura de continuidad entre los empleados de la Organización.

GOVERTIS Advisory Services

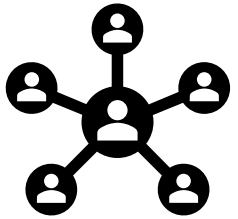
Red IRIS


- El Gabinete de Crisis es el órgano **responsable directo** de la gestión de la situación de contingencia y de la dirección de la continuidad en general.
- Para el completo desarrollo de sus funciones **este Gabinete se podrá apoyar**, cuando lo considere necesario, **en los Grupos de Apoyo.**
- **Todos los cargos del Gabinete de Crisis tendrán un miembro titular** y, al menos, **un miembro alternativo** definido y comunicado.

- La misión de los miembros de estos grupos es la de **colaborar, a petición del Gabinete de Crisis,** y dentro de su ámbito de actuación, en la evaluación de la gravedad y consecuencias de la contingencia, la articulación de las medidas tendentes a solventar o paliar la crisis, y la gestión de las comunicaciones pertinentes.
- Asimismo, son los **responsables** últimos de la **recuperación de sus actividades y servicios críticos**.

GOVERTIS
Advisory Services

# Grupos de apoyo.

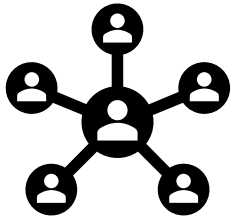


- La misión de los miembros de estos grupos es la de **colaborar, a petición del Gabinete de Crisis,** y dentro de su ámbito de actuación, en la evaluación de la gravedad y consecuencias de la contingencia, la articulación de las medidas tendentes a solventar o paliar la crisis, y la gestión de las comunicaciones pertinentes.
- Asimismo, son los **responsables** últimos de la **recuperación de sus actividades y servicios críticos**.
- Los **Grupos de Apoyo** a la Crisis estarán **compuestos por los equipos operativos** encargados de recuperar las actividades de la Organización, junto con sus responsables (que pertenecen al Gabinete de Crisis y actuarán como interlocutores entre ambos Comités).
- En función de la contingencia acaecida, el Gabinete de Crisis podrá convocar a uno o más equipos operativos para que formen parte de los Grupos de Apoyo a la Crisis.
- En los **Grupos de Apoyo**, al igual que en el Gabinete, existirá para cada integrante **un miembro titular** y, al menos, **un miembro alternativo.**

GOVERTIS Advisory Services

Red IRIS

# Grupos de apoyo.

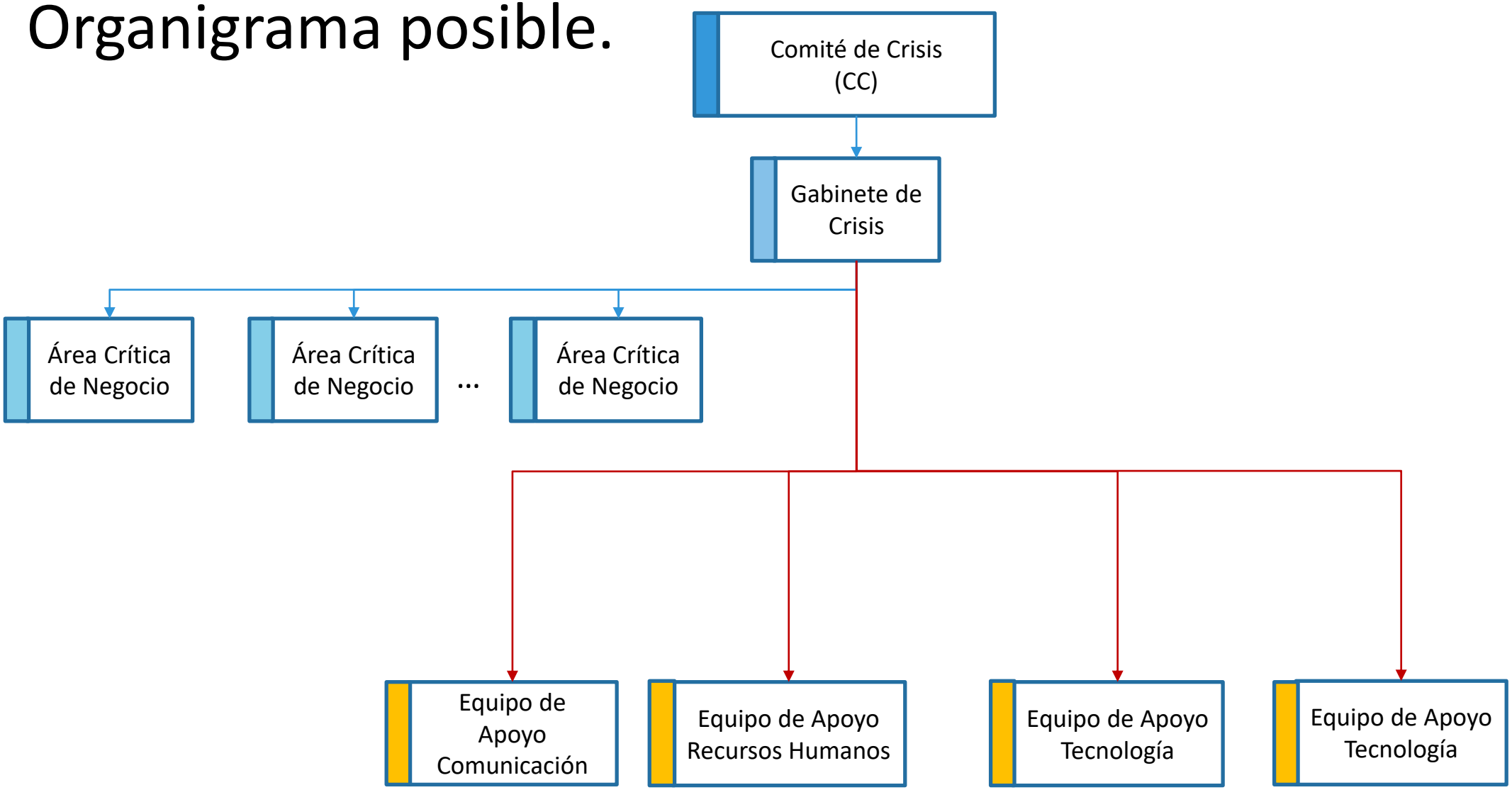


- El responsable del grupo de apoyo estará presente en el Gabinete de crisis.
- El diseño de los distintos grupos de apoyo dependerá del conjunto de escenarios contemplados.
- Estos grupos de apoyo se ajustan a las actividades de recuperación de las que serán responsables.
- Ejemplos de grupos de apoyo pueden ser:
  - Grupo de apoyo a la emergencia.
  - Grupo de apoyo de contingencia de seguridad física.
  - Grupo de apoyo de contingencias de RR.HH.
  - Grupo de apoyo de comunicación.
  - Grupo de apoyo de contingencia tecnológica.

GOVERTIS Advisory Services

Red IRIS

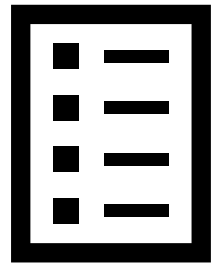
# Organigrama posible.




GOVERTIS Advisory Services

RedIRIS

# Plan de gestión de crisis.



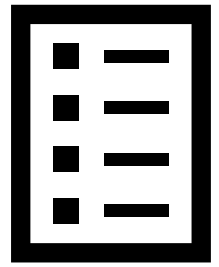
- El Plan de Gestión de Crisis pretende posibilitar una **respuesta uniforme y coordinada**, **en el plazo** previsto, a **cualquier contingencia** que pueda afectar de una u otra forma a la prestación de los servicios de la Organización, a fin de conseguir el restablecimiento de las actividades que soportan dichos servicios, protegiendo tanto al personal como a la propia organización, y velando por el desarrollo del negocio de la Organización de modo que se incurra en el **mínimo impacto** sobre los usuarios y actividades de la organización.

- Es preciso **establecer la estructura organizativa** soporte de cualquier situación de crisis que afecte a la continuidad del negocio en la Organización, y los **procedimientos de actuación** en caso de que se materialicen los escenarios de contingencia previstos o cualquier otro que no esté previsto.

GOVERTIS Advisory Services

Red IRIS

# Contenidos de un Plan de gestión de crisis.



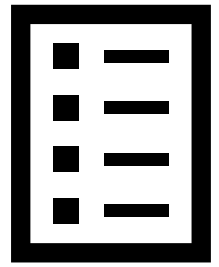
- El índice de un Plan de gestión de crisis debe contemplar los siguientes puntos:

1. Constitución del Comité de Crisis.
   - Composición.
   - Sala de gestión de crisis (Ubicaciones de trabajo).
   - Ubicación de los equipos de apoyo.
2. Gestión de las situaciones de crisis.
   - Procedimiento de alerta.
   - Procedimiento de evaluación.
   - Procedimiento de declaración de desastre.
   - Primeras comunicaciones tras la declaración de desastre.

GOVERTIS Advisory Services

Red IRIS

# Contenidos de un Plan de gestión de crisis.

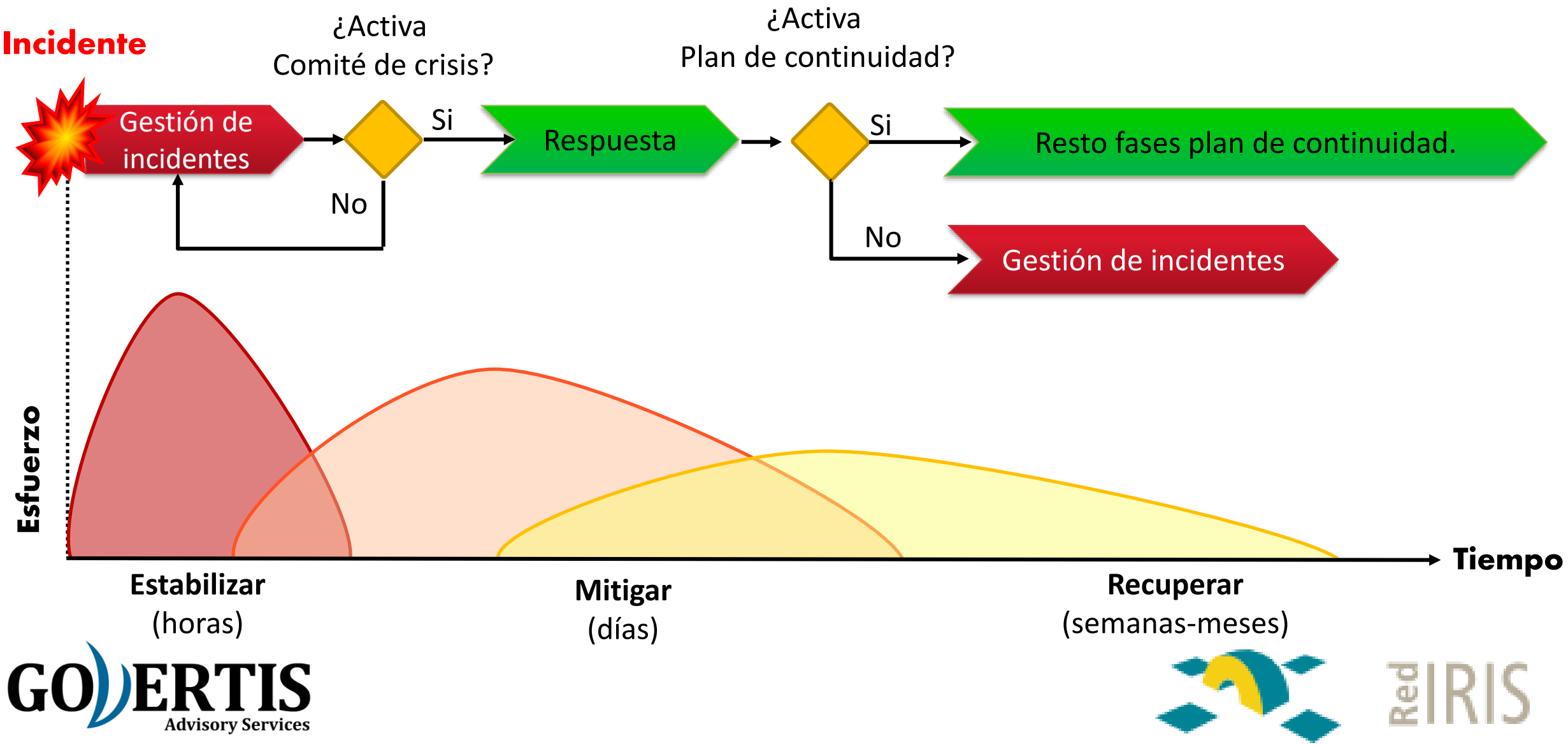


3. Flujos de comunicación durante la crisis.
   - Comunicación del gabinete de crisis hacia los grupos de apoyo.
   - Comunicaciones de los grupos de apoyo al gabinete de crisis y dentro del gabinete de crisis.
   - Flujo de comunicaciones y tareas en gabinete de crisis y grupos de apoyo.
4. Plan de mantenimiento y actualización.
5. Plan de formación.
6. Plan de pruebas.
7. Anexos.
   - Guía de valoración y triaje.
   - Ubicaciones de las salas de crisis.
   - Comunicados tipo.

GOVERTIS Advisory Services

Red IRIS

# Proceso de gestión de crisis.




GOVERTIS Advisory Services

Red IRIS

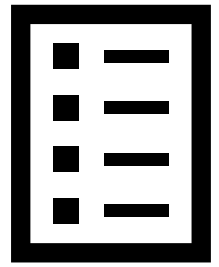
# Fases del proceso de continuidad de negocio.


F1. Respuesta.
F2. Reanudación.
F3. Recuperación.
F4. Restauración.

GOVERTIS Advisory Services

Red IRIS

# Planes de respuesta.



- El Planes de respuesta atenderán a escenarios de contingencia. Deben contemplar lo necesario para coordinar las fases del proceso de respuesta, rreanudación, recuperación para asegurar la restauración del entorno.
- El índice de un Plan de respuesta para un escenario debe contemplar los siguientes puntos:
  - Objetivos.
  - Escenario de contingencia cubierto.
  - Centros de trabajo involucrados durante la ejecución.
  - Roles y responsabilidades.
  - Activación del equipo vinculado al plan (Gabinete de crisis y equipos de apoyo).
  - Descripción de las fases.

GOVERTIS Advisory Services

Red IRIS

# Planes de respuesta.

F1

F1. Respuesta.

F2

F2. Reanudación.

F3

F3. Recuperación.

F4

F4. Restauración.

Toma de cualquier acción inmediata para contener el incidente y evaluar peores escenarios.

Aprovisionar recursos necesarios para reanudar las operaciones

Proporcionar unos servicios mínimos que permitan las continuidad de servicios.

Volver a la normalidad

GOVERTIS Advisory Services

RedIRIS

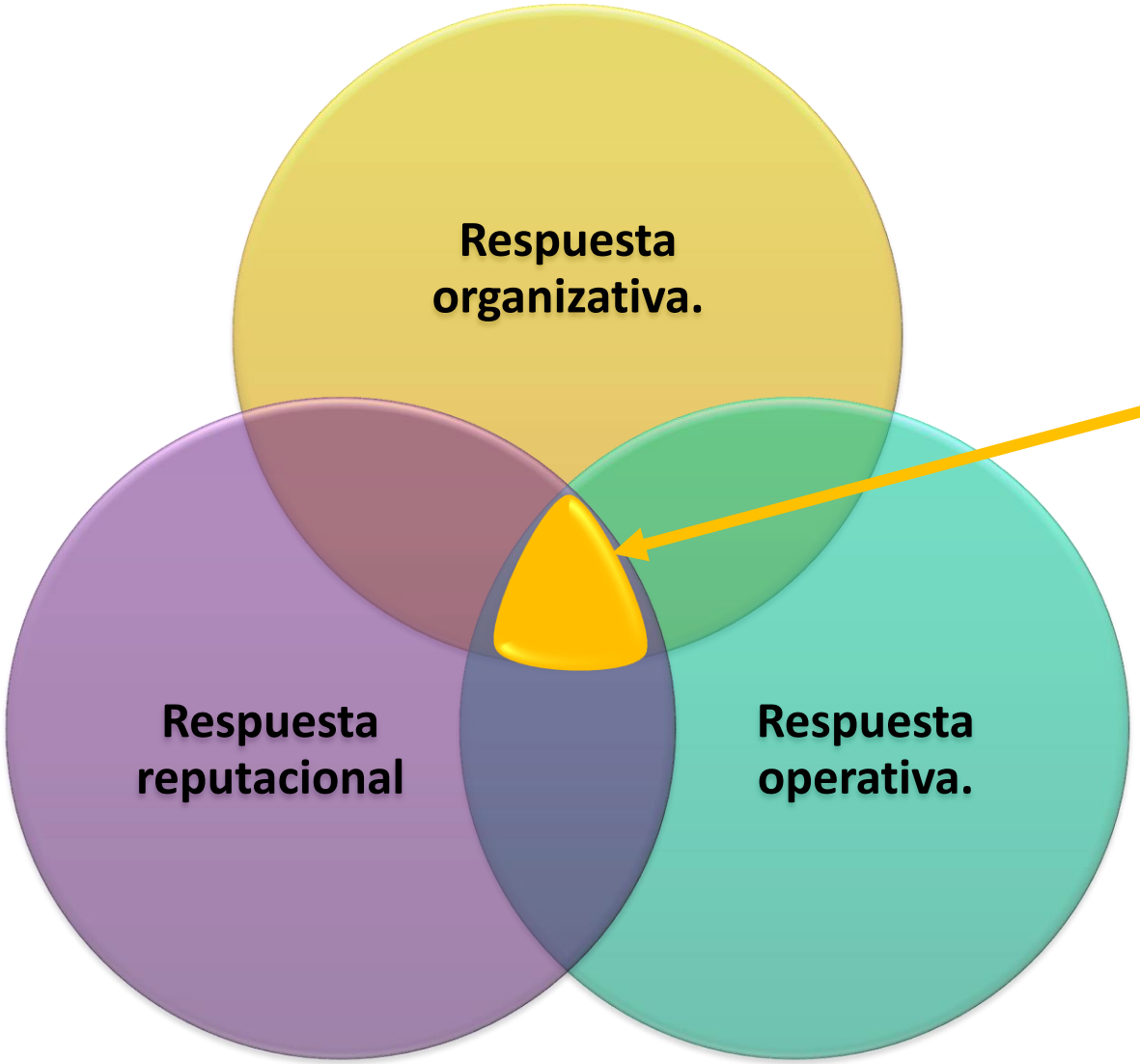
# CONTENIDO.

1. CONTEXTO DE LA GESTIÓN DE CRISIS.
2. GESTIÓN DE INCIDENTES vs GESTIÓN DE CONTINUIDAD.
3. GOBIERNO DE LA CRISIS.
4. GESTIÓN REPUTACIONAL EN SITUACIONES DE CRISIS.

GOVERTIS Advisory Services

Red IRIS

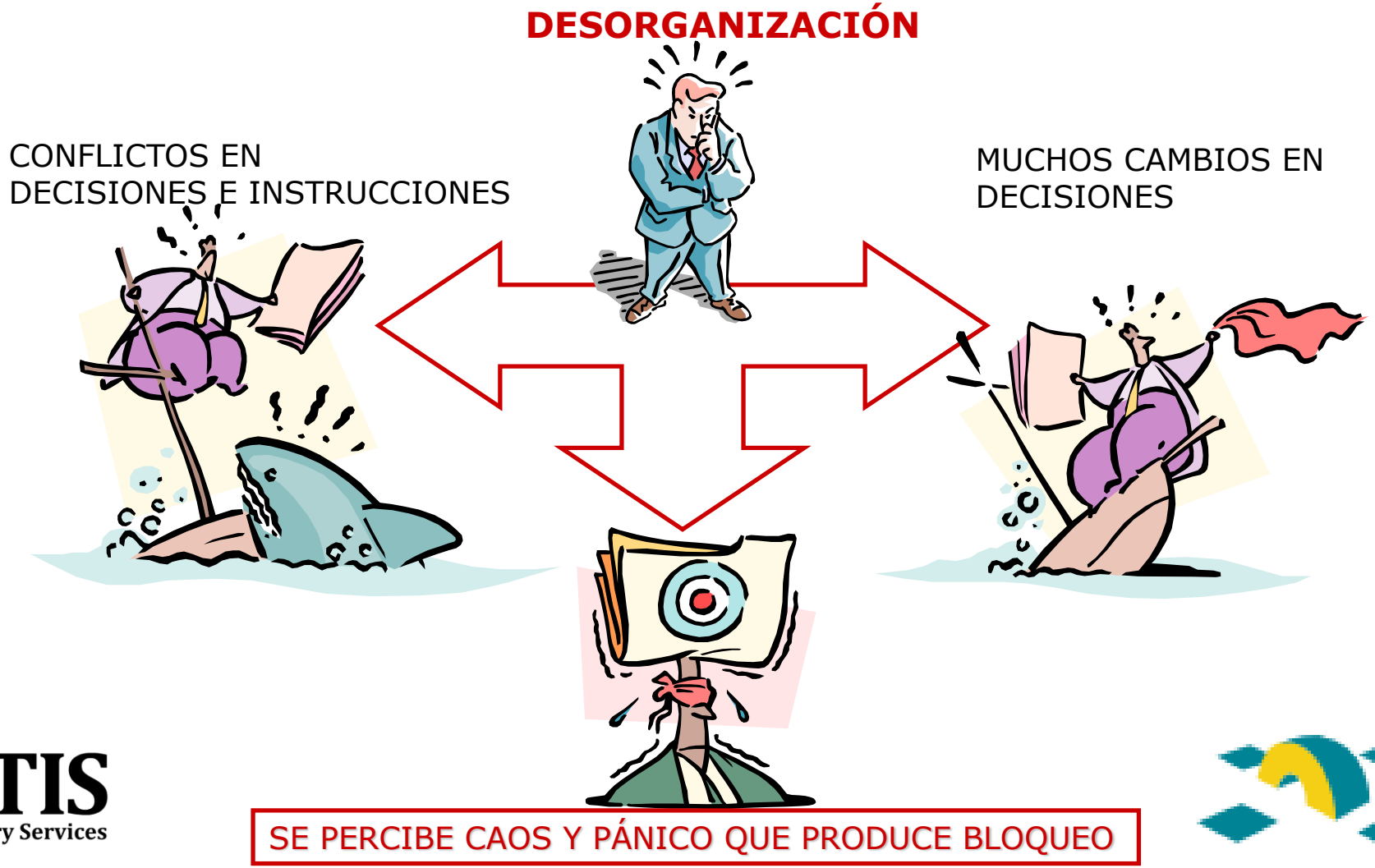
# Aspectos a considerar en la gestión de crisis.




Una gestión de crisis efectiva está condicionada por la buena coordinación de estos aspectos

# Sin plan para la gestión de crisis.

**Respuesta reputacional**




GOVERTIS Advisory Services

Red IRIS

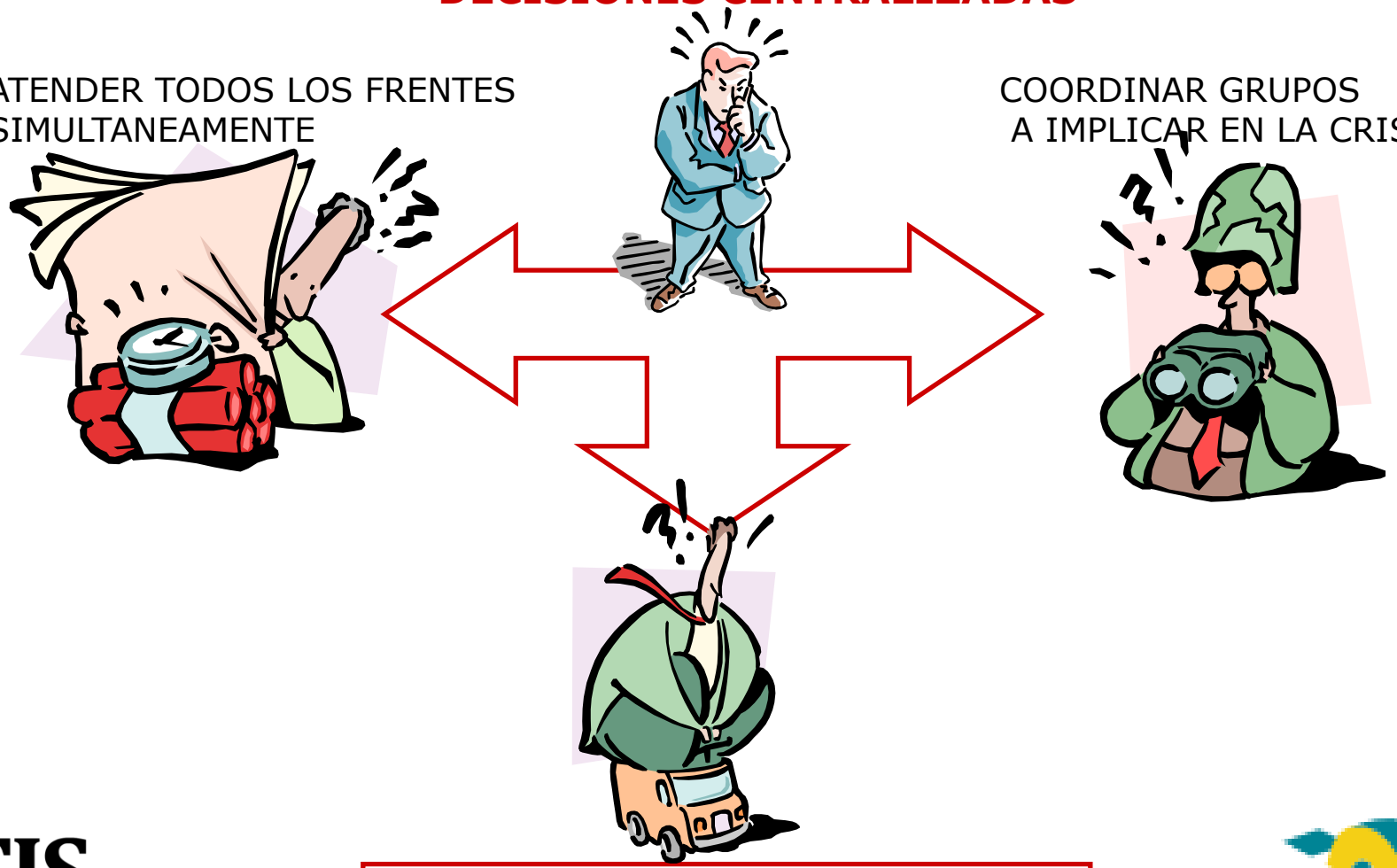
# Con plan para la gestión de crisis.

**Respuesta reputacional**

**DECISIONES CENTRALIZADAS**

ATENDER TODOS LOS FRENTES SIMULTANEAMENTE

COORDINAR GRUPOS A IMPLICAR EN LA CRISIS



SE PERCIBE CONTROL DE LA SITUACIÓN

GOVERTIS Advisory Services

Red IRIS

# Elementos clave en la respuesta reputacional

**Respuesta reputacional**

1. Debe controlarse la ventana temporal en la que debe informarse. Dependerá del tipo de incidente, requerirá información más continua o más espaciada en el tiempo.
2. Debe contemplarse quienes son nuestras partes interesadas y sus expectativas.
3. Debe identificarse el PEOR ESCENARIO y estar preparado.
4. Debe adecuarse el contenido de la comunicación a la información disponible de la que se tiene absoluta certeza.
5. DOS REGLAS DE ORO:
    1. “NO MENTIR”.
    2. “LA REPUTACIÓN ES SOLO LA CONSECUENCIA DE SU COMPORTAMIENTO”.

GOVERTIS Advisory Services

Red IRIS

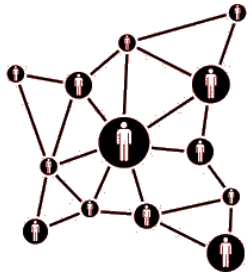
# Comunicación y notificación de incidentes o crisis.

**Respuesta reputacional**

- Los objetivos del plan de comunicación son:
  - Homogeneización y coordinación de la información que es notificada hacia el exterior.
  - Definición de los diferentes responsables o portavoces.
  - Crear un UNICO PUNTO de contacto y atención mediática.
  - Control de la distribución de información crítica, en ocasiones sensible respecto  lo sucedido.
- Es necesario ahora considerar los requisitos de notificación existentes (ENS y RGPD).

GOVERTIS Advisory Services

Red IRIS



# Inventario de partes interesadas.

**Respuesta reputacional**

- Es necesario conocer a nuestras partes interesadas y las expectativas que tienen en este tema respecto a nuestra organización.
  - Si son internas o externas.
  - El tipo de trato: transparencia y honestidad.
  - El ámbito al que pertenecen y el tipo de información que requieren en la comunicación y/o notificación.
  - Los tiempos máximos tolerados en la comunicación.
  - El tipo de informe que deben recibir.

GOVERTIS Advisory Services

Red IRIS

# Definir protocolos de comunicación.

**Respuesta reputacional**

- La Organización puede establecer protocolos de comunicación que atiendan a diferentes necesidades. Estos protocolos pueden contemplar como criterios:
  - Tipos de partes interesadas a las que se dirigen y contenidos o información necesaria a comunicar.
  - Tipo de incidentes y requisitos informativos mínimos que se establecen por la regulación.
- Cada uno de estos protocolos, puede diseñar notas de comunicación "Tipo" que permitan disponer de plantillas que sean fáciles de completar y agilicen el proceso de notificación o comunicación de incidentes. Cada plantilla se ajustará, según el protocolo, para adecuarse en cuanto a redacción y contenido a la finalidad por la que ese protocolo se establece. Pueden ser protocolos los siguientes tipos:
  - PROTOCOLO DE COMUNICACIÓN DE EMERGENCIAS.
  - PROTOCOLO DE NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD DE DATOS PERSONALES.
  - PROTOCOLO DE NOTIFICACIÓN INCIDENTES DE DISPONIBILIDAD.
  - PROTOCOLO DE DENUNCIA DE DELITOS.
  - PROTOCOLO DE COMUNICACIÓN MEDIOS DE COMUNICACIÓN Y PRENSA.

# Definir “plantillas de notas de comunicación”.

**Respuesta reputacional**

*Estimado cliente:*

*El pasado día X, la Organización ACME ha sufrido un incidente* **(<Especificar si se considera necesario el tipo de incidente, las causas que lo han producido si se saben en un primer momento>)** *y ha ocasionado una brecha de seguridad en los tratamientos de datos de carácter personal que la Entidad gestiona en la prestación de servicios bajo la figura de encargado de tratamiento.*

*Nos ponemos en contacto con usted porque como responsable del tratamiento, podría verse afectado por el incidente debido a* **(<Descripción de los motivos por los que se considera afectado, en relación con los tratamientos de datos que se vean involucrados en el incidente. Según el caso, se indicará si el daño se ha materializado o existe un riesgo potencial de que ocurra>)**.

*Queremos comunicarle que los tratamientos y la información que pueden estar afectados incluye:*

**(<Descripción de los tipos de datos que se han visto afectados>).**

*La protección y el manejo seguro de la información personal de nuestros clientes es extremadamente importante para nosotros. La Organización ha realizado las actividades de contención y recuperación necesarias para solventar el suceso. Si usted tiene cualquier duda o cuestión relacionada con el incidente, le recordamos que puede ponerse en contacto con nuestro Delegado de Protección de Datos mediante las siguientes vías:*

- *Email*
- *Dirección postal.*

*De igual forma le indicamos quién es la persona que ostenta la figura de Responsable de Seguridad por si usted tiene cualquier duda o cuestión relacionada con el incidente o las medidas de seguridad aplicadas. Le recordamos que puede ponerse en contacto con nuestro Responsable de Seguridad de la Información mediante las siguientes vías:*

- *Email*
- *Dirección postal.*

*Agradecemos su comprensión mientras estamos trabajando en solucionar el incidente. Estamos concentrados en resolver lo antes posible lo sucedido para seguir manteniendo su confianza en nuestra Entidad.*

*Atentamente,*

*Firmado: (Cargo o portavoz del Comité de Brechas de Seguridad).”*

GOVERTIS Advisory Services

Red IRIS

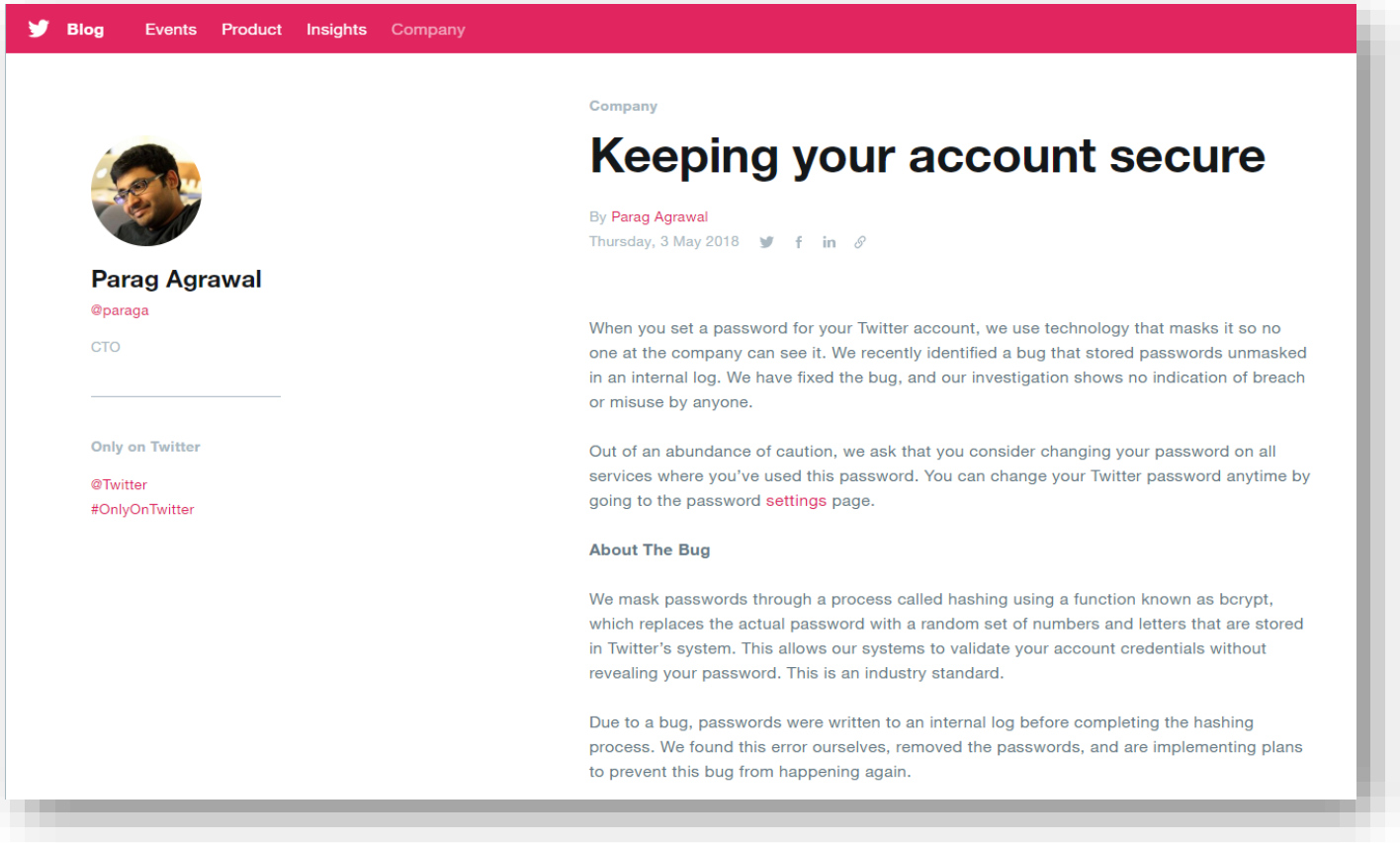
# ¿Comunicar o no al interesado?.

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

GOVERTIS
Advisory Services

Red IRIS

# Cuando comunicar se convierte en algo positivo.



Blog Events Product Insights Company



Parag Agrawal

@paraga

CTO

Only on Twitter

@Twitter
#OnlyOnTwitter

Company

## Keeping your account secure

By Parag Agrawal
Thursday, 3 May 2018

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.

GOVERTIS Advisory Services

Red IRIS

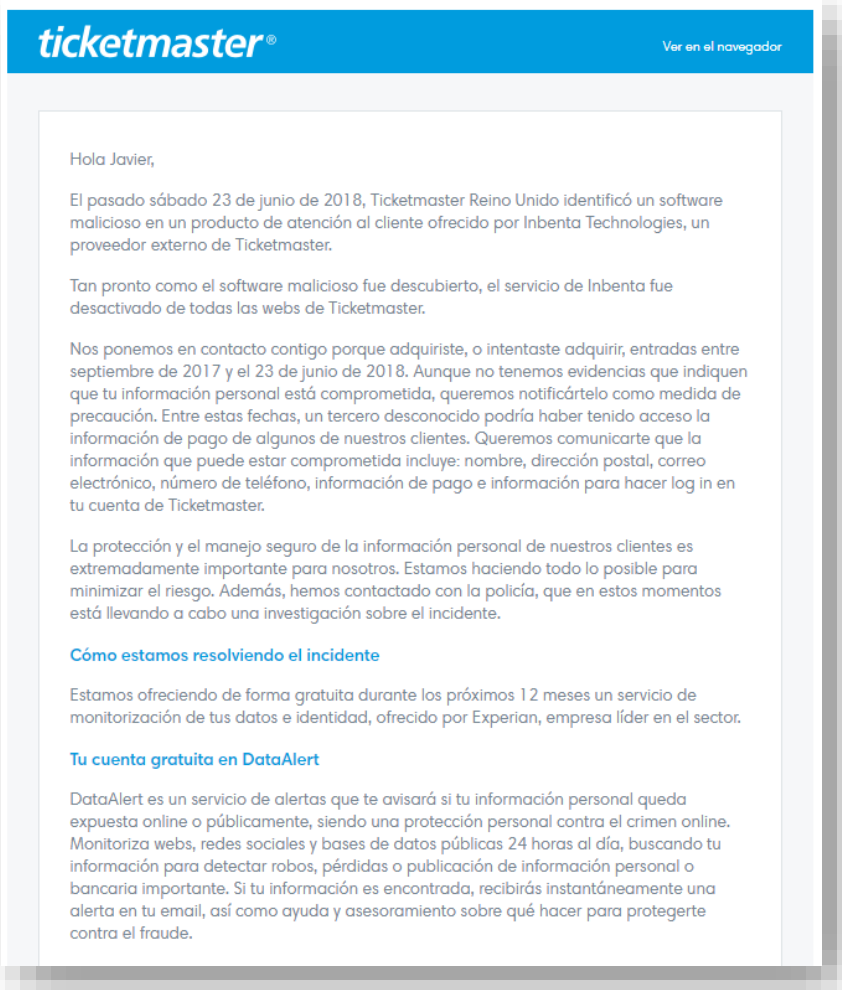
# Cuidar el mensaje al interesado.

- **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 de un incidente y por tanto, tener una actitud empática hacia él.**
- **Debemos coordinar el texto con el área de comunicación corporativa.**

GOVERTIS Advisory Services

Red IRIS

# Cuidar el contenido del mensaje según destinatario.



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.**

GOVERTIS Advisory Services

Red IRIS


"Las improvisaciones son mejores cuando se las prepara".

**William Shakespeare.**

**Muchas gracias por la atención prestada.**