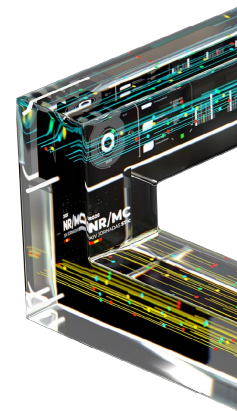
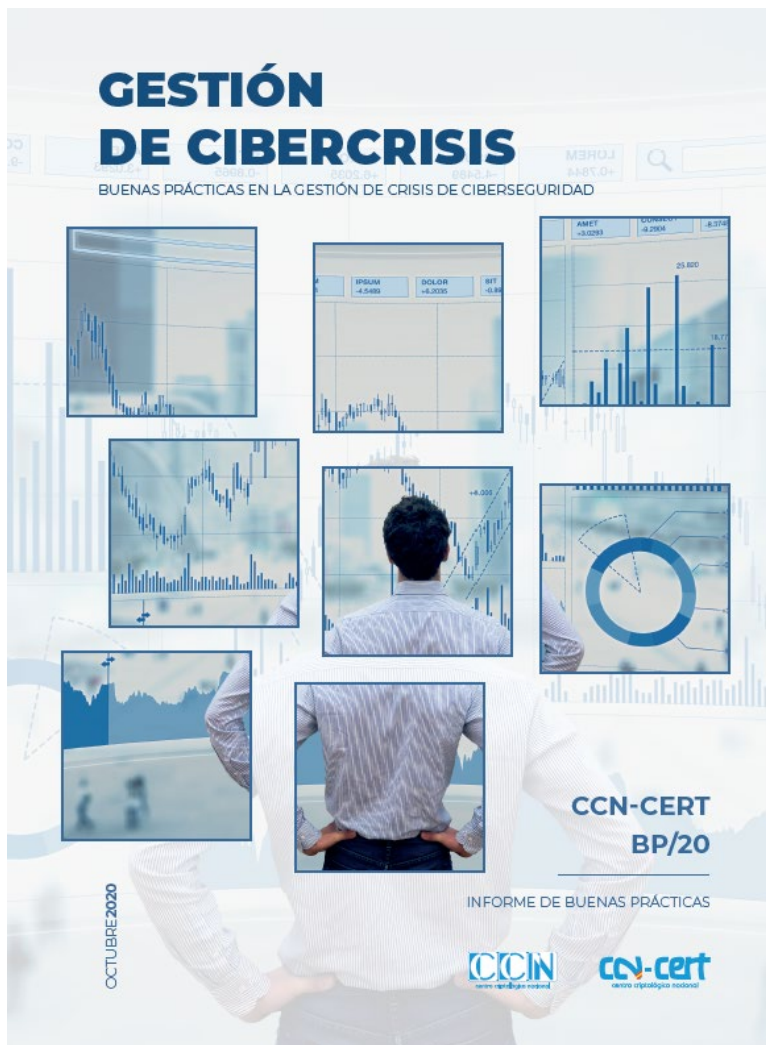


#XIVJORNADASCCNCERT

**Gestión de cibercrisis.
Buenas prácticas en la gestión
de crisis de ciberseguridad**





*Elisabet Viladomiu
Albert Girbal*

Institut Cerdà

Elisabet.viladomiu@icerda.org

Edita:



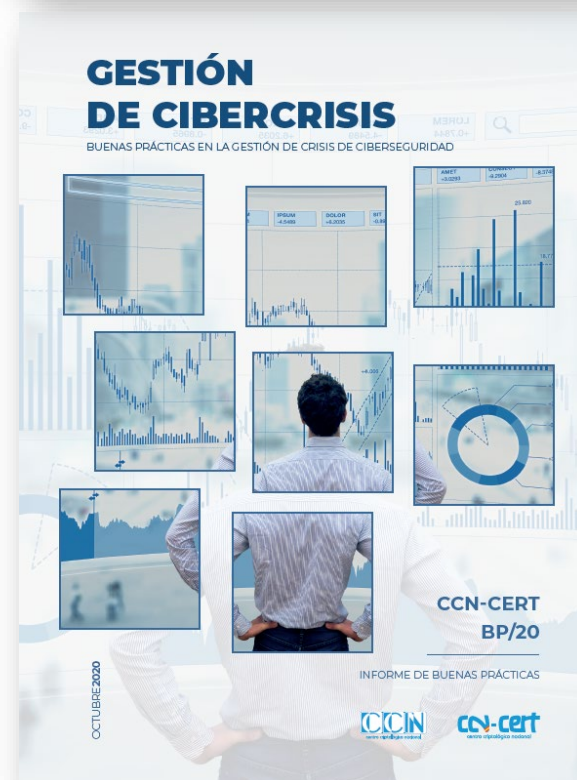
Centro Criptológico Nacional, 2020



2.5.4.13-Qualified Certificate: AAPP-
SEP-M-SW-KPSC, ou=sello electrónico,
serialNumber=528001551, o=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2020.11.05 18:42:46 +01'00'

Institut  Cerdà

El informe:



Índice

	página
1. Sobre CCN-CERT, CERT Gubernamental Nacional	4
2. Introducción	5
3. Casos de estudio	9
4. Buenas prácticas en la gestión de crisis por ciberincidentes	10
BP.1 Liderazgo, valores y control	10
BP.2 Planes y protocolos estructurales	11
BP.3 Comité de Crisis. Configuración	12
BP.4 Control permanente de la superficie de exposición	15
BP.5 Gestión adecuada de grupos de interés. Stakeholders	16
BP.6 Diagnóstico inicial y escenarios posibles	18
BP.7 Coordinación	19
BP.8 Iniciativa y proactividad	20
BP.9 Discurso unificado y fuente oficial de información	21
BP.10 Transparencia, empatía y asunción de responsabilidades	23
BP.11 Puesta en valor de las acciones adoptadas	24
BP.12 Cierre formal de la crisis	25
BP.13 Implementación de lecciones aprendidas	26
5. Conclusiones y recomendaciones	27
Anexo 1. Caso de estudio Ciberespionaje	29
Anexo 2. Caso de estudio Ransomware	34
Anexo 3. Caso de estudio Intento de Sustracción de fondos	40
Anexo 4. Orientación sobre niveles y criterios de evaluación y clasificación de cibercrisis	46

Casos de estudio

Forma práctica de mostrar las principales acciones que se han de llevar a cabo en 3 casos



1

Ciberspionaje:

en este anexo se explican las cuestiones necesarias a tener en cuenta en la gestión de ciber crisis ante un caso de ciberspionaje.



2

Ransomware:

en este anexo se explican las cuestiones necesarias a tener en cuenta en la gestión de ciber crisis provocada por un ataque dirigido a través de malware del tipo ransomware.



3

Extorsión y sustracción de fondos:

en este anexo se explican las cuestiones necesarias a tener en cuenta en una gestión de ciber crisis ante posibles ataques que tienen por objeto la extorsión y sustracción de fondos de la víctima.



4

Resumen de las conclusiones principales:

en este anexo se resumen las conclusiones principales de los casos de estudio anteriormente expuestos.



¿Cibercrisis?

Una crisis es una situación de **baja probabilidad** que cuando sucede genera un **gran impacto** y cuyos efectos perduran en el **tiempo** sobre



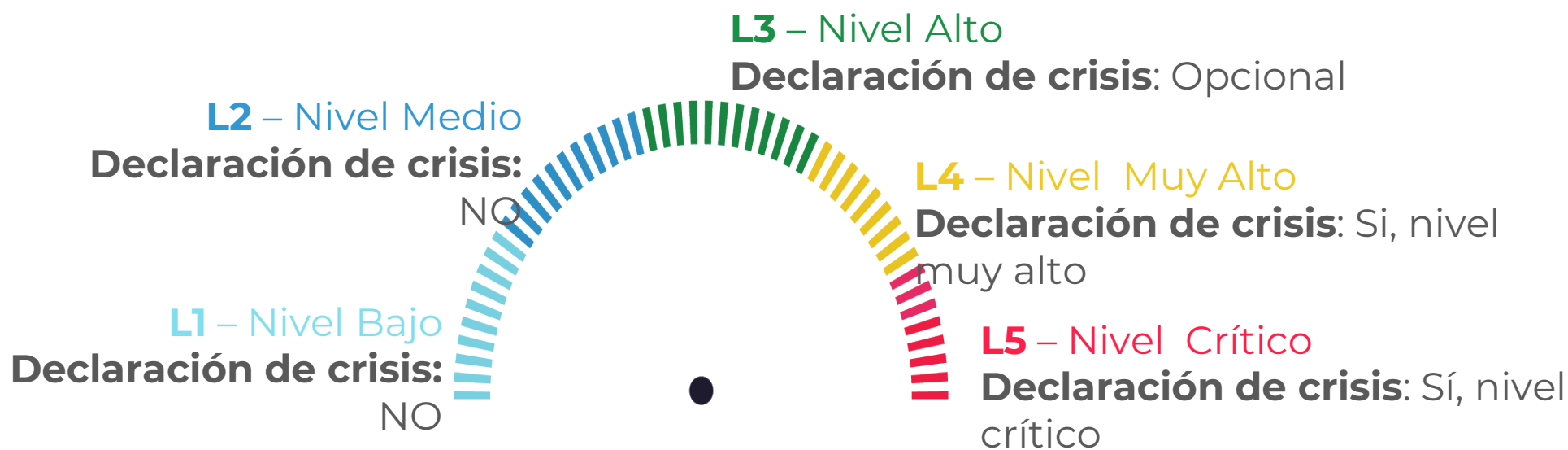
El bien o servicio



Su reputación e imagen



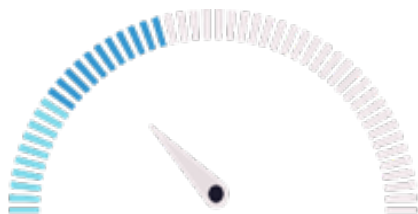
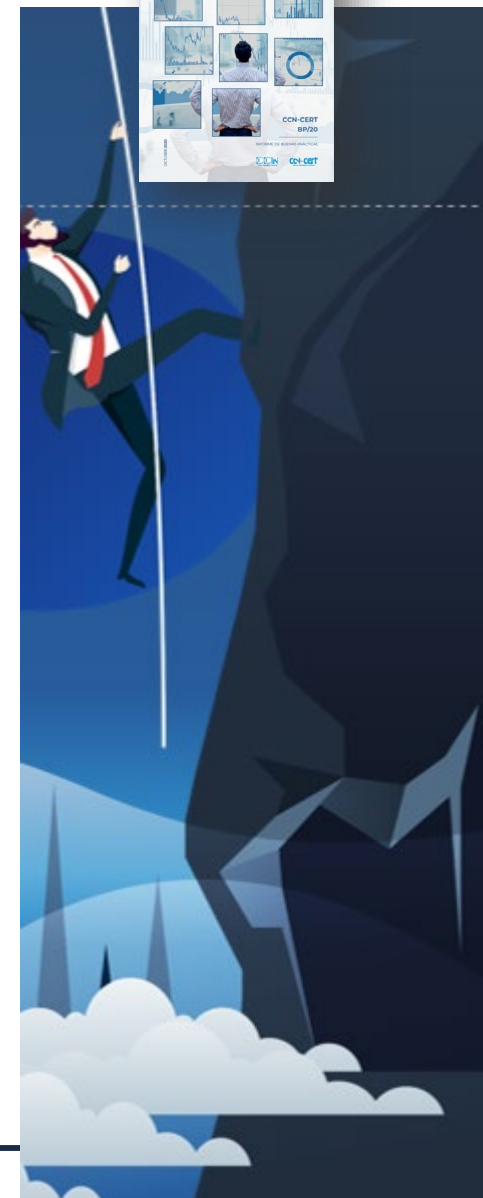
La sociedad en general



Nivel de peligrosidad del incidente atendiendo a la taxonomía de la Guía CCN-STIC 817 – Gestión de incidentes

Activación de comité

de crisis por ciberincidente



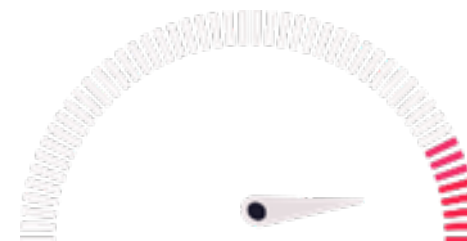
L1 – Nivel Bajo

L2 – Nivel Medio



L3 - Nivel Alto

L4 – Nivel Muy Alto



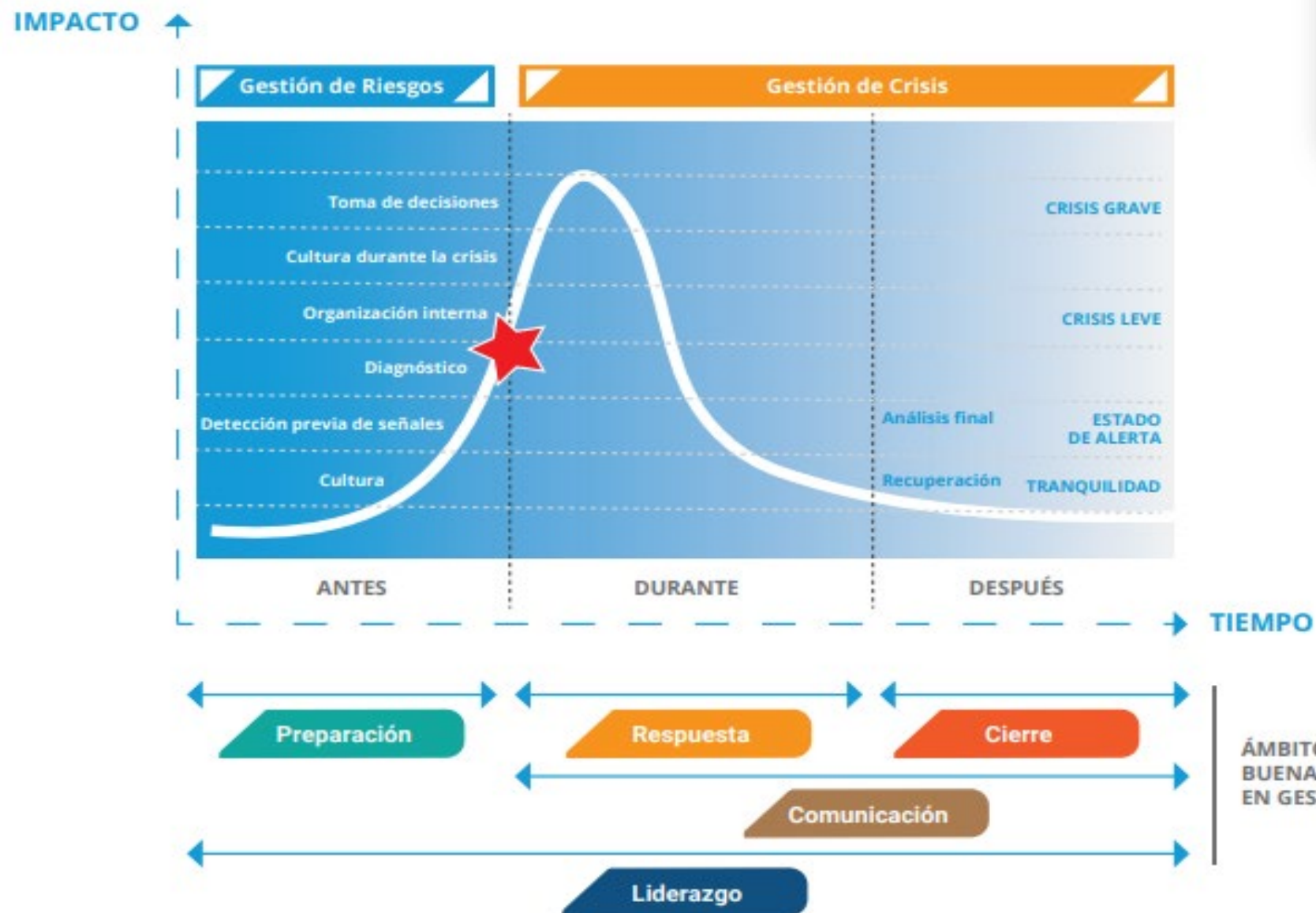
L5 – Nivel Crítico

Equipos de nivel operativo
(bronce)

Comité de Crisis
(silver)
+
equipo(s) bronce

Comité de Crisis Alto nivel
Estratégico (gold)
+
aportaciones comité silver y bronce

Fases de una crisis



Buenas prácticas

Liderazgo

BP.1 Liderazgo, valores y control

Preparación

BP.2 Planes y protocolos estructurales

BP.3 Comité de Crisis. Configuración

BP.4 Control permanente de la superficie de exposición

BP.5 Gestión adecuada de grupos de interés. Stakeholders

Respuesta

BP.6 Diagnóstico inicial y escenarios posibles

BP.7 Coordinación

BP.8 Iniciativa y proactividad

Comunicación

BP.9 Discurso unificado y fuente oficial de información

BP.10 Transparencia, empatía y asunción de responsabilidades

BP.11 Puesta en valor de las acciones adoptadas

Cierre

BP.12 Cierre formal de la crisis

BP.13 Implementación de lecciones aprendidas

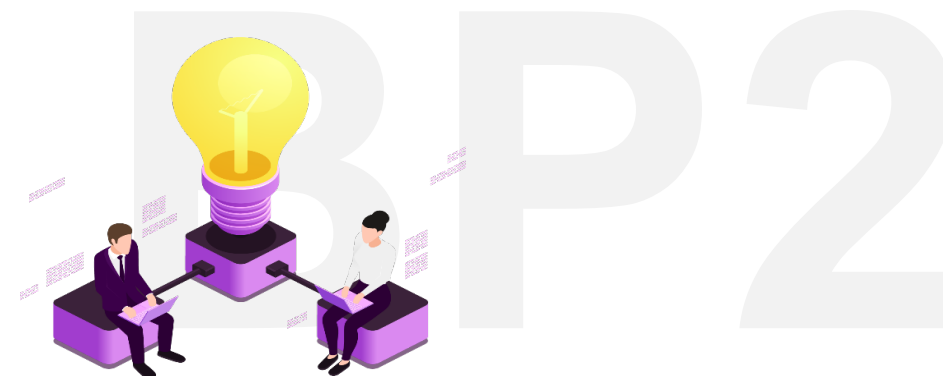


Buenas prácticas



BP.1 Liderazgo, valores y control

- Iniciativa
- Confianza / Reputación previa: basada en valores
- **Función de Responsable de Seguridad de la Información: 1º en categorizar el evento y la idoneidad o no de convocar el Comité de Crisis.**



BP.2 Planes y protocolos estructurales

- Se preparan en tiempos de normalidad.
- Vulnerabilidad / ciberamenazas > constante ejercicio de **prospectiva**.
- Difundidos y probados

Buenas prácticas

BP3

BP.3 Comité de Crisis. Configuración

- Gestión > decisiones
- Previamente definido > nivel peligrosidad e impacto
- Roles no cargos



Establecido / Origen	Atributo	Nivel 1 BAJO	Nivel 2 MEDIO	Nivel 3 ALTO	Nivel 4 MUY ALTO	Nivel 5 CRÍTICO
Otros atributos de Gestión de Crisis	Declaración de Crisis	No	No	Opcional	Sí, Nivel Muy Alto	Sí, Nivel Crítico
	Ámbito de gestión / Gobierno de la crisis	No requiere Comité de Crisis / RSI / Equipo Respuesta Incidente	Sí requiere Comité de Crisis / BRONZE TEAM	Sí requiere Comité de Crisis / SILVER TEAM	Sí requiere Comité de Crisis / SILVER TEAM	Sí requiere Comité de Crisis Alta Dirección / GOLD TEAM

Buenas prácticas

BP4

BP.4 Control permanente de la superficie de exposición

- Probar (planes, procedimientos, configuraciones diseñadas...) > **identificar vulnerabilidades** >
- **Medir para gestionar**
- Entrenamiento equipos > **simulacros**



#XIVJORNADASCNCERT

BP.5 Gestión adecuada de grupos de interés

- Mapa de stakeholders
- Ciber >

Grupos de Respuesta a Incidentes de Seguridad CERT (casos A, MA y C notificación obligatoria)

Autoridad competente

Cadena de proveedores

BP5



Buenas prácticas

BP.6 Diagnóstico inicial y escenarios posibles

- Información ? Improvisación ?

//

- ... Priorizar actuaciones (notificaciones)
- Criterios de clasificación (gravedad e impacto) escalado de incidentes* (Anexo 4)



			Nivel 1 BAJO	Nivel 2 MEDIO	Nivel 3 ALTO*	Nivel 4 MUY ALTO*	Nivel 5 CRÍTICO*
CCN-STIC 817	Establecido / Origen	Tipología de Impacto					
		Externo	Afectación a la seguridad nacional	---	---	Afecta apreciablemente a actividades oficiales o misiones en el extranjero	Afecta apreciablemente a la seguridad nacional
		Externo	Afectación a la seguridad ciudadana	---	---	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales	Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas
		Interno	Afectación a infraestructuras críticas/servicio esencial	---	---	Afecta a un servicio esencial	Afecta a una infraestructura crítica
		Interno	Afectación a sistemas	Afecta a los sistemas de la organización	Afecta a más del 20 % de los sistemas de la organización	Afecta a sistemas clasificados RESERVADO	Afecta a sistemas clasificados SECRETO
		Interno	Interrupción del servicio	Interrupción en la prestación del servicio superior al 5 % de usuarios	Interrupción en la prestación del servicio superior a 1 hora y superior al 10 % de usuarios	Interrupción en la prestación del servicio superior a 8 horas y superior al 35 % de los usuarios	Interrupción en la prestación del servicio superior a 8 horas y superior al 50 % de los usuarios
		Interno	Recursos en jornadas personas	El ciberincidente precisa para resolverse entre 1 y 5 jornadas-persona	El ciberincidente precisa para resolverse entre 5 y 50 jornadas-persona	El ciberincidente precisa para resolverse entre 50 y 100 jornadas-persona	El ciberincidente precisa para resolverse más de 100 jornadas-persona
		Interno	Impacto económico	Entre 0,0001 % y 0,002 % del PIB actual	Entre el 0,001 y 0,05 % del PIB actual	Entre el 0,05 % y el 0,07 % del PIB actual	Entre el 0,07 % y el 0,1 % del PIB actual
		Externo	Afectación geográfica	Superior a 1 CCAA	Superior a 2 CCAA	Superior a 3 CCAA	Superior a 4 CCAA
		Externo	Impacto reputacional	Puntual, sin eco mediático	Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación)	Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) afectando a la imagen del país (marca España) y cobertura continua en medios de comunicación nacionales	Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales
OTROS ATRIBUTOS DE GESTIÓN DE CRISIS	Interno / actividad / operaciones	Afectación a los procesos críticos	Sin afectación en procesos críticos	Con afectación a procesos críticos y recuperación de la actividad interrumpida dentro de su RTO (%)	Recuperación de una actividad interrumpida ligeramente por encima de su RTO (%)	Recuperación de una actividad interrumpida por encima de su RTO (%)	Recuperación de una actividad interrumpida o desconocida o muy por encima de su RTO (%)
	Social	Afectación a las relaciones con los grupos de interés	Las expectativas y la confianza de los grupos de interés no se ven afectadas	Las expectativas y la confianza de los grupos de interés se ven mínimamente afectadas	Las expectativas y la confianza de los grupos de interés se ven afectadas	Las expectativas y la confianza de los grupos de interés se ven fuertemente afectadas	Las expectativas y la confianza de los grupos de interés se ven fuertemente afectadas durante un largo periodo de tiempo
	Social	Alarma social	Sin alarma	Sin alarma	Principio de alarma en población con/sin causa justificada	Alarma en población con/sin causa justificada	Pánico en población con/sin causa justificada
	Económico	Daños a terceros / entorno	Sin daños a terceros / entorno	Daños materiales leves (valoración €7)	Daños moderados (valoración €7)	Daños graves (valoración €7)	Daños muy graves (valoración €7)
	Económico	Pérdidas económicas (estimación)	Sin pérdidas o pérdidas insignificantes. Coste dentro de parámetros presupuestarios aceptables	Pérdidas por valor hasta coste de reposición	Pérdidas por valor hasta coste de reposición	Pérdidas por valor hasta coste de reposición	Pérdidas por valor hasta coste de reposición
	Legal	Implicaciones legales	Sin implicaciones	Sin implicaciones	Sin implicaciones	Reclamaciones aisladas de terceros y/o indicios de delito	Reclamaciones masivas de terceros y/o materialización de delito
	De gestión	Declaración de crisis	No	No	Opcional	SI, de nivel MUY ALTO	SI, de nivel CRÍTICO

* Nivel de peligrosidad y del Nivel de impacto potencial de la Guía de Seguridad de las TIC CCN-STIC 817 y de la Guía Nacional de Notificación y Gestión de Ciberincidentes

Buenas prácticas

BP.7 Coordinación

- La improvisación y la falta de coordinación ... fracaso.

//

- Toma de decisiones y su ejecución
- **Responsable de Seguridad de la información (RSI) > coordinación**

> Equipo operativos // Comité de crisis //
CERT // Responsable del Tratamiento de
Datos

Aspectos

- Valores
- Entrenamiento
- Relación

#XIVJORNADASCNCCERT

BP.8 Iniciativa y proactividad

- Lentitud, reticencia, falta diagnóstico, ... pérdida de tiempo (y del CERT)

//

- Reaccionar con rapidez y contundencia (1º avisos)
 - notificación inicial sin dilación indebida y
 - tomar la iniciativa (internamente o con empresa especializada)

... rápida actuación con CERT_{REF}

Buenas prácticas



BP.9 Discurso unificado y fuente oficial de la información

- Múltiples fuentes ? Mensajes contradictorios ? A remolque..

//

- Lo mejor que puede pasar en una crisis, es que la principal fuente de información sea la propia organización.
- Ciber > equilibrio entre comunicar externamente y “alertar” de que se está actuando...
- Proactividad y discurso único, ritmo y cadencia.

BP9

Buenas prácticas

BP.10 Transparencia, empatía y asunción de responsabilidades

- La mentira, la narración sesgada, el mutismo o la pasividad...peores opciones

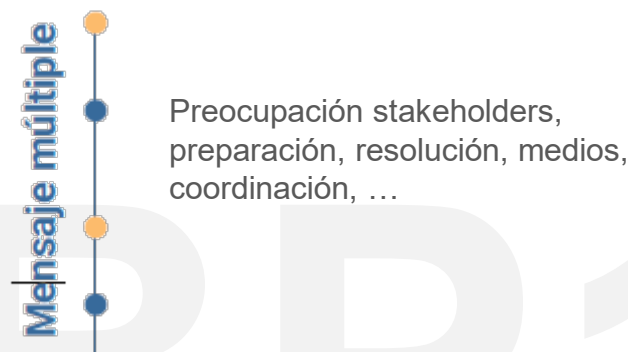
//

- Política abierta y responsable > a la vez que se necesita tiempo.
- Ciber > Evitar mencionar las causas del incidente, su responsable, datos que la investigación pueda revelar o las posibles consecuencias para la organización o para otro grupo de interés.

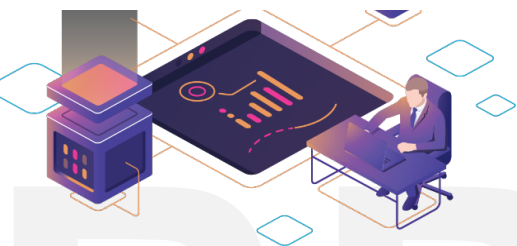
#XIVJORNADASCNCERT

BP.11 Puesta en valor de las acciones adoptadas

- Crisis > Oportunidad demostrar la capacidad
- Medidas preventivas y correctivas



Buenas prácticas



BP.12 Cierre formal de la crisis

- Tiempo para el análisis, evaluación,
- Conclusiones y lecciones aprendidas ...plan de acción
- Comunicar ... > externa e internamente (agradecimientos)

BP.13 Implementación de lecciones aprendidas

- Acciones concretas
- Seguimiento implantación
- Objetivos medibles.

The New York Times

TECNOLOGÍA

El 'mea culpa' de Samsung por la crisis del Note 7 revela sus fallas gerenciales

Por Paul Mozur

23 de enero de 2017

23 ene,



En resumen

Buenas prácticas en la gestión de Crisis de Ciberseguridad



BP.1 LIDERAZGO, VALORES Y CONTROL

LIDERAZGO

BP.2 PLANES Y PROTOCOLOS ESTRUCTURALES

BP.3 COMITÉ DE CRISIS. CONFIGURACIÓN

BP.4 CONTROL PERMANENTE DE LA SUPERFICIE DE EXPOSICIÓN

BP.5 GESTIÓN ADECUADA DE GRUPOS DE INTERÉS. STAKEHOLDERS

BP.6 DIAGNÓSTICO INICIAL Y ESCENARIOS POSIBLES

BP.7 COORDINACIÓN

BP.8 INICIATIVA Y PROACTIVIDAD

RESPUESTA

PREPARACIÓN

CIERRE

COMUNICACIÓN

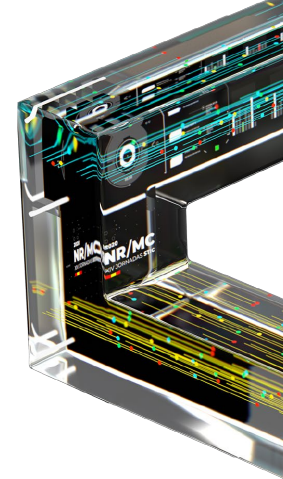
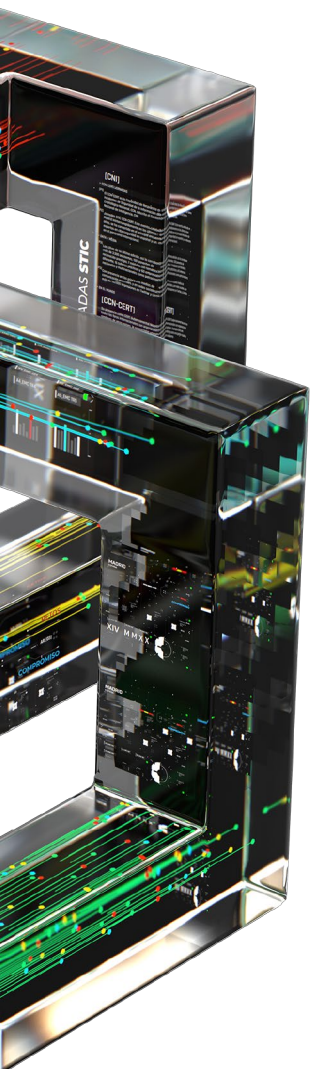
BP.12 CIERRE FORMAL DE LA CRISIS

BP.13 IMPLEMENTACIÓN DE LECCIONES APRENDIDAS

BP.9 DISCURSO UNIFICADO Y FUENTE OFICIAL DE INFORMACIÓN

BP.10 TRANSPARENCIA, EMPATÍA Y ASUNCIÓN DE RESPONSABILIDADES

BP.11 PUESTA EN VALOR DE LAS ACCIONES ADOPTADAS



MUCHAS GRACIAS

#XIVJORNADASCCNCERT

Institut  Cerdà