Buenas prácticas en la gestión de **Crisis de Ciberseguridad**

1. Liderazgo, valores y control
Es imprescindible prever quién asumirá el liderazgo en una situación de cibercrisis, en la que toma un rol fundamental la función de Responsable de Seguridad de la Información.
Es importante liderar, tomar y mantener la iniciativa.

2. Planes y protocolos estructurales
Una gestión efectiva viene determinada por la capacidad de anticipación e identificación de los ámbitos más vulnerables (gestión de riesgos).

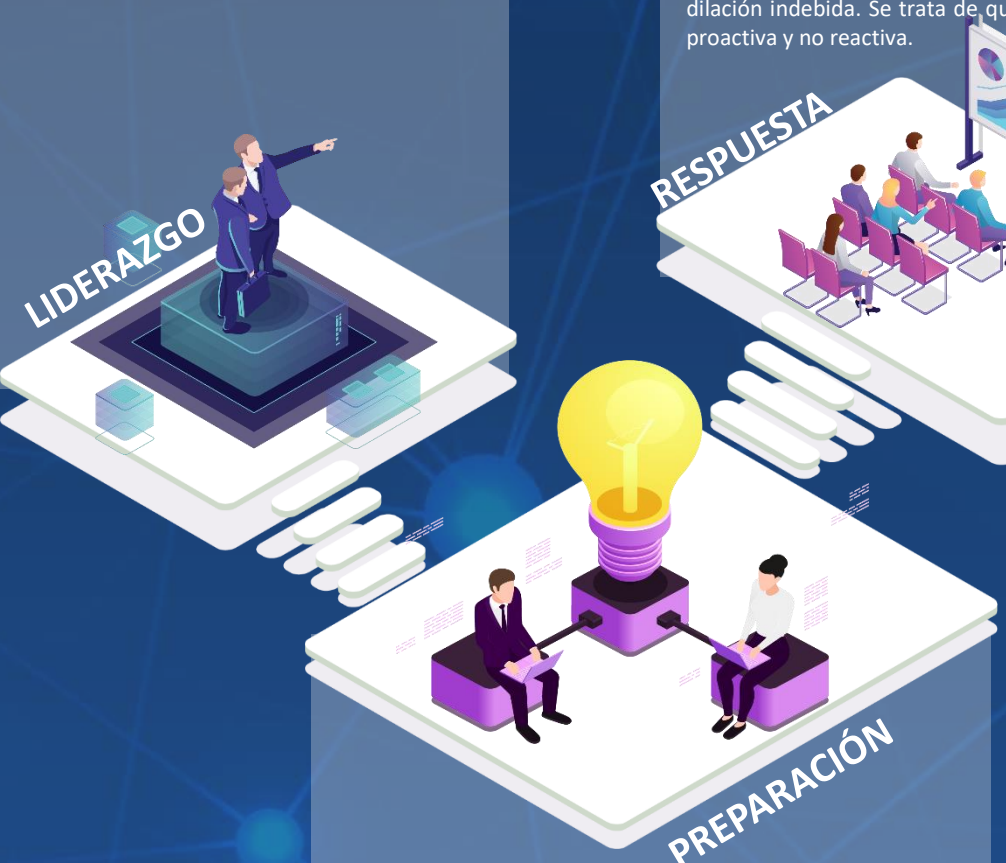
3. Superficie de exposición
Se han de poner constantemente a prueba los planes, procedimientos y configuraciones diseñadas que permitan identificar las vulnerabilidades asociadas a servicios y aplicaciones.

4. Gestión adecuada de grupos de interés
En el caso concreto de los ciberincidentes, toman una importancia fundamental los Grupos de Respuesta ante Emergencias Informáticas (CERT) que proporcionan servicios de soporte y respuesta ante este tipo de eventos.

5. Diagnóstico inicial y escenarios posibles
El primer paso en la gestión de una cibercrisis es llevar a cabo un diagnóstico de lo que está sucediendo. Este ejercicio permite priorizar actuaciones y tomar las primeras decisiones.

6. Coordinación
Disponer de un comité de crisis es uno de los primeros y más importantes pasos a seguir durante una crisis. Dentro de este esquema, aparece como fundamental la figura del Responsable de Seguridad de la Información.

7. Iniciativa y proactividad
La organización debe reaccionar con rapidez y contundencia, haciendo una notificación inicial sin dilación indebida. Se trata de que la organización sea proactiva y no reactiva.



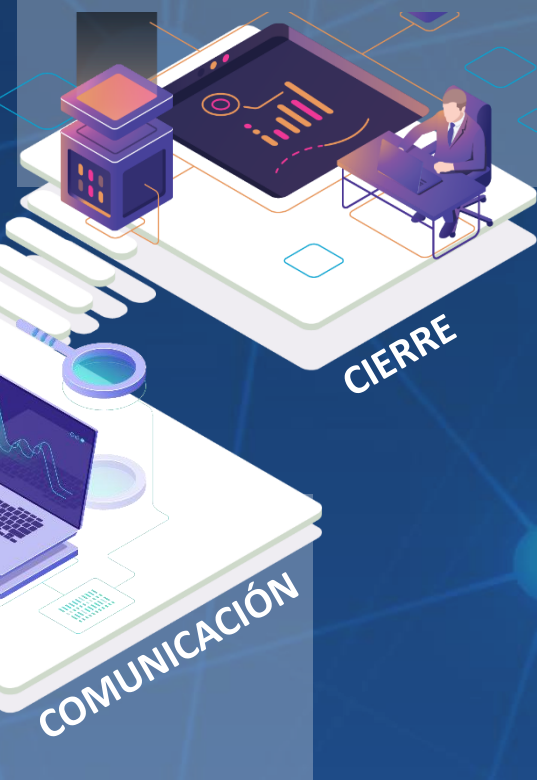
8. Discurso unificado
Es importante diseñar un discurso único y, a la vez, modular el ritmo y la cadencia en su comunicación. El escenario ideal es que la principal fuente de información sea la propia organización.

9. Transparencia, empatía y Asunción de responsabilidades
La adopción de una política abierta y responsable produce una mejora de la credibilidad y reputación de la compañía.

10. Puesta en valor de acciones adoptadas
Una crisis representa una oportunidad para demostrar la capacidad de la organización para solventar una situación compleja.

11. Cierre formal de la crisis
Llevar a cabo los análisis pertinentes, la definición de un plan de acción y el seguimiento de su implantación son pasos indispensables en el cierre de la cibercrisis.

12. Implementación de lecciones aprendidas
Se han de obtener conclusiones de lo sucedido mediante análisis en profundidad y ajustar dichos aprendizajes a los planes de acción e inversión futuros.



Más información en la Guía CCN-CERT BP/20 Buenas Práctica en la gestión de crisis de ciberseguridad

centro criptológico nacional