Gestión de **Crisis de Ciberseguridad**

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

El bien o servicio de la organización que lo sufre

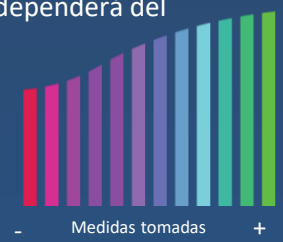
Su reputación e imagen

La sociedad en general

Necesidad de implementar ciberseguridad.

En el ámbito de la ciberseguridad, las cibercrisis requieren tomar decisiones rápidas con información limitada. La probabilidad de que este acontecimiento tenga lugar dependerá del grado de preparación previa de la organización.

La probabilidad será muy pequeña si se han tomado un gran número de medidas preventivas y progresivamente mayor cuanto menor sea el trabajo de prevención llevado a cabo con anterioridad.



¿Cuándo se considera que existe una cibercrisis?

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

El Comité de Crisis es el órgano encargado de gestionar, tomar decisiones y coordinar las acciones necesarias para hacer frente o resolver la emergencia que haya sido calificada como crisis. A modo orientativo y aunque depende del tamaño y de las capacidades de la organización, un esquema de gestión es el siguiente:

Equipos de nivel operativo (Bronze) - Equipos de nivel operativo muy especializados y concretos

Comité de Crisis (Silver) - Representantes de direcciones funcionales y con probablemente más de un equipo bronze trabajando en aspectos operativos, muy especializados y concretos

Comité de Crisis Estratégico (gold) - En un ciberataque de categoría crítica la cúpula de la organización (Consejero/a Delegado/a, Dirección General y miembros previamente designados) será quien tome las decisiones finales dentro del Comité gold, según las aportaciones tanto del comité silver como del bronze

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

centro criptológico nacional