Respuesta y recuperación ante emergencias

Ing. Fredy Bustamante

Introducción

- La regla básica sobre planificación para emergencias es:

  Mantenerlo simple

- Cuanto más complicados sean sus planes de respuesta a emergencias, menos probabilidades habrá de que sean eficaces en una emergencia real.
- Los planes más complejos podrán utilizarse para la recuperación.

Temas

- Descripción general de la gestión de emergencias
- Planes de respuesta a emergencias
- Gestión de crisis
- Recuperación de TI

Descripción general de la gestión de emergencias

Descripción general de la gestión de emergencias

- Independientemente de cómo esté organizada su empresa debe **asignar roles claros**.
- Todos deben saber quién está a cargo o quién toma las decisiones.
  - No puede permitir que en una emergencia varias personas piensen que pueden tomar decisiones pues generará caos.
- A gran escala, cuando ocurre un desastre que afecta a toda una comunidad, es importante conocer las entidades que estarán a cargo de diferentes tareas como rescatar personas, atenderlos, darles comida, etc.
  - No asuma que una entidad llegará a rescatar o apoyar al personal de la empresa, en su planificación incluya **encargados y tareas que permitan cubrir las emergencias sin ayuda externa**.

Planes de respuesta a emergencias

Planes de respuesta a emergencias

- Como personal de TI, solemos participar y tener un rol en específico dependiendo del tipo de emergencia.
- Los planes de emergencia surgen de los riesgos identificados con anterioridad.
- Recordemos que la respuesta a emergencias es la respuesta inmediata al incidente.
  - En un incendio, la respuesta a la emergencia consiste en evacuar el edificio, llamar al departamento de bomberos y, dependiendo el caso, algunos empleados podrán utilizar extintores para intentar controlar el incendio.
- No debe crear un plan para cada tipo de emergencia, por el contrario, tener pocos planes de respuesta generales de los cuales se toma lo que corresponde a la emergencia que ocurre en un momento dado.

Planes de respuesta a emergencias

- Un conjunto básico de tareas de respuesta a emergencias son las siguientes:
  - Proteger al personal
  - Contener el incidente
  - Implementar comando y control (intervención del ERT y del CMT)
  - Respuesta y triaje de emergencias (médicas, evacuación, búsqueda y rescate)
  - Evaluar el impacto y el efecto
  - Notificación
  - Próximos pasos
- Las 3 primeras tareas son las más importantes pues se protege a las personas, se contiene la emergencia y se evalúa la situación.

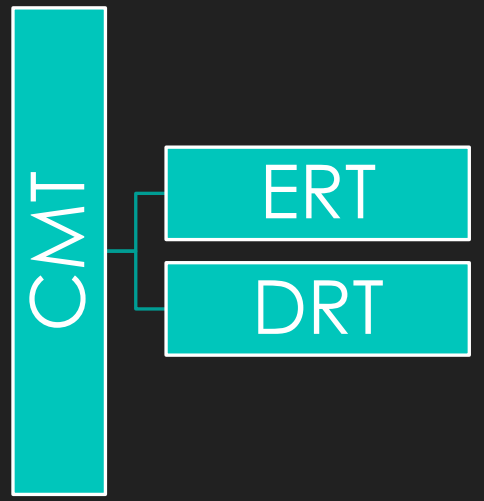
Planes de respuesta a emergencias

- Cada plan debe incluir:
  - Roles y responsabilidades: quién y qué debe hacer cada uno.
  - Herramientas y equipos: extintores, kits de primeros auxilios, cascos, radiocomunicadores, llaves, etc.
    - ERT debe tener un inventario de estos, revisarlos y darles mantenimiento periódicamente.
  - Recursos: recursos humanos como saber quién es experto en qué (relacionado a emergencias), agua, alimentos, otros medicamentos, etc.
  - Acciones y procedimientos: procedimientos de evacuación, qué hacer en caso de derrame químico, inundación, protocolos de comunicación.

Gestión de crisis

ERT: Equipos de respuesta a emergencias

- El ERT debe estar definido con sus roles y responsabilidades, cada persona debe conocer los límites de su autoridad y a quién debe recurrir por ayuda o escalamiento.
- El equipo de gestión de crisis (CMT) puede o no ser el mismo que el ERT.
- CMT
  - Toma decisiones de alto nivel y dirige los recursos de la empresa durante la crisis
  - Coordina entre empleados y partes externas, equipos ERT y DR
  - Único portavoz para empleados y todas las partes externas durante la crisis
  - Implementa el Plan de Continuidad del Negocio (BC) y Recuperación ante Desastres (DR)
  - Mantiene el registro de eventos
- ERT
  - Gestiona, prueba y se prepara solo para la respuesta a emergencias
  - Entrenado para abordar emergencias específicas
- DRT (Equipo de DR)
  - Implementa procedimientos de recuperación de TI y de negocios



Recuperación de TI

CIRT: Computer Incident Response

- Dentro de TI debe existir un equipo que, similar al ERT, pueda dar respuesta ante una emergencia relacionada con o que afecte el hardware y software.
  - Debe cumplir con los mismos requisitos que un ERT pero enfocados en hardware y software.
- Deben tener procedimientos ordenados de cómo restaurar los servicios, las dependencias, los proveedores, passwords, etc.
- Sus principales responsabilidades son:
  - Monitorear
  - Alertar y movilizar
  - Evaluar y estabilizar
  - Resolver
  - Revisar

CIRT: Computer Incident Response

- Más información en https://csrc.nist.gov/pubs/sp/800/61/r2/final

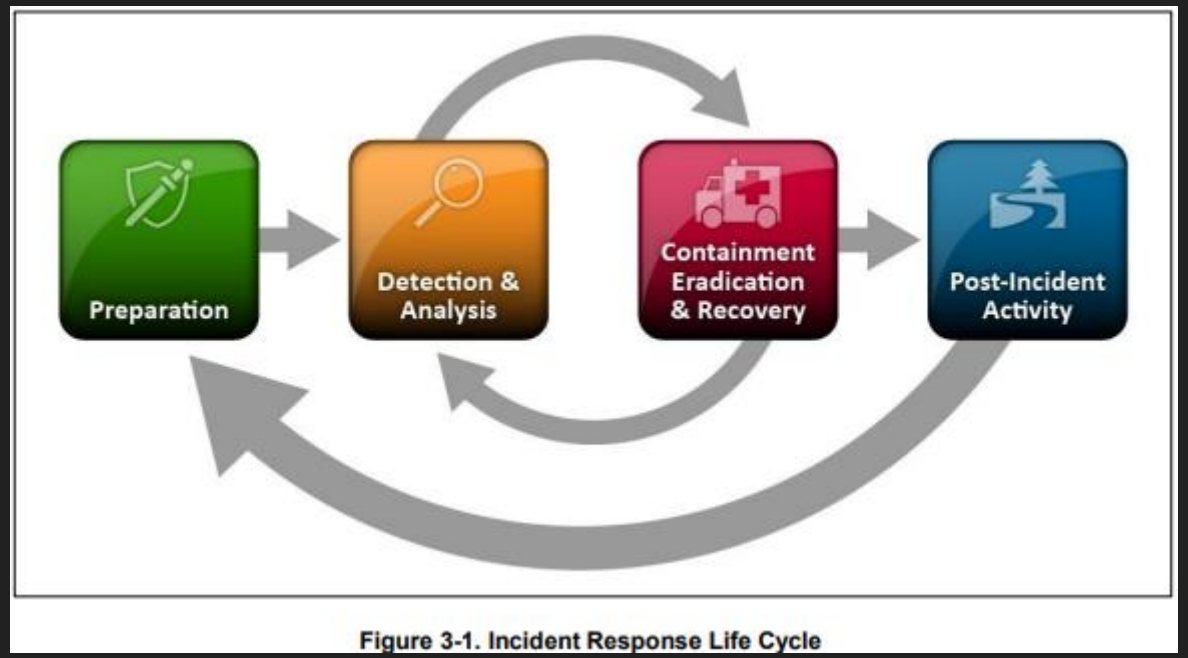


Figure 3-1. Incident Response Life Cycle