

# [GSI] Incidentes y su respuesta

Responder ante los incidentes de seguridad es un elemento crítico dentro de los programas de IT

- El proceso de respuesta es altamente complejo.
- Varios frameworks:
  - NIST Special Publication 800-61 → Recurso indispensable
    - Hay varias releases, en este momento hay hasta la release 3.
    - De la Release 2 a la Release 3 hay muchos cambios.
      - La release 2 era bastante abierta y fácil de leer
      - La release 3 no es tan genérica, se acerca más a lo que sería una ISO 27002
  - ISO 27035 → Recurso indispensable
    - Bastante genérica
  - RFC2350: No trata tanto la gestión de incidentes como los equipos de respuesta a incidentes.
  - ENISA: Documento breve sobre la importancia de tener la gestión de incidentes y el CSIRT
  - ISACA: Aproximación a la gestión de incidentes desde el framework de COBIT.

## NIST 800-61

Guía de seguridad para la gestión de incidentes.

### Plan de respuesta a Incidentes

From:  
<http://www.knoppia.net/> - Knoppia



Permanent link:  
[http://www.knoppia.net/doku.php?id=master\\_cs:gsi:respuesta](http://www.knoppia.net/doku.php?id=master_cs:gsi:respuesta)

Last update: **2025/11/24 14:17**