

Gestión del riesgo de ciberseguridad organizacional

Síntesis: Análisis forense y profesionalización en ciberseguridad.



Este componente aborda principalmente el análisis forense digital, mostrando su importancia y procedimiento dentro de la ciberseguridad. El proceso forense sigue varias etapas clave enfocadas en la evidencia y manejo de la información.

Además, se ejemplifican prácticas comunes en análisis forense y paralelamente, se incluyen comparativas entre el NIST Risk Management Framework (RMF) y la norma ISO/IEC 27005, destacando sus diferencias en origen, aplicación, estructura y enfoque metodológico para la gestión de riesgos en seguridad de la información.

También se presentan certificaciones claves en ciberseguridad, detallando certificaciones básicas, avanzadas, ofensivas, de gestión y especializadas en *cloud* o forense.

Por último, se resalta la importancia de complementos como cursos cortos, microcertificaciones y formación en línea, que facilitan la actualización continua e igualmente, se relaciona la importancia de la sensibilización del usuario en todos los procesos de ciberseguridad.

En suma, el contenido enfatiza en la importancia del análisis forense digital como pilar en la investigación y defensa en ciberseguridad, la gestión de riesgos a través de marcos reconocidos y la necesidad de formación constante y certificaciones especializadas para abordar los retos contemporáneos de la seguridad informática.

