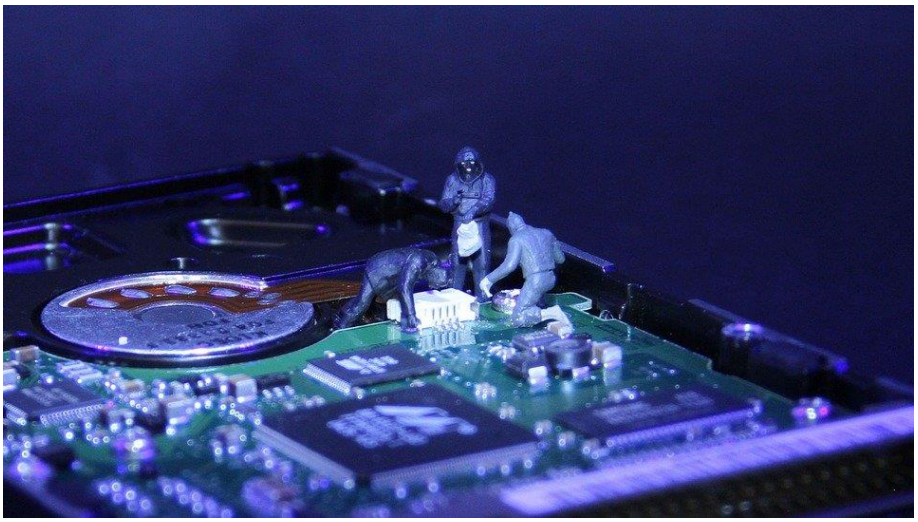
Estándares y *Frameworks*
para la gestión de incidentes de seguridad digital



https://cdn.pixabay.com/photo/2019/01/09/10/24/information-technology-3923009_960_720.jpg

Los estándares y marcos de referencia (*frameworks*) de gestión de incidentes de seguridad son referencias base para adoptar, estructurar, modelar y documentar un proceso adecuado de gestión de incidentes de seguridad digital.

A continuación, se describen los principales estándares y *frameworks* relacionados con la gestión de incidentes de seguridad:

- **ISO/IEC 27035-1,2,3**
  Information technology. Security techniques. Information security incident management

  "ISO / IEC 27035-1: 2016. Tecnología de la información - Técnicas de seguridad - Gestión de incidentes de seguridad de la información - Parte 1: Principios de gestión de incidentes. Es la base de esta Norma Internacional de varias partes. Presenta conceptos y fases básicas de la gestión de incidentes de seguridad de la información y combina estos conceptos con principios en un enfoque estructurado para detectar, informar, evaluar y responder a incidentes y aplicar las lecciones aprendidas."
  Iso.org (2016)

  "ISO / IEC 27035-2: 2016. Tecnología de la información - Técnicas de seguridad - Gestión de incidentes de seguridad de la información - Parte 2: Directrices para planificar y prepararse para la respuesta a incidentes. proporciona las pautas para planificar y prepararse para la respuesta a incidentes. Las directrices se basan en la fase de *Planificación y preparación* y la fase de *Lecciones aprendidas* del modelo de *Fases de gestión de incidentes de seguridad de la información* presentado en ISO / IEC 27035-1."
  Iso.org (2016)

"*ISO / IEC 27035-3: 2020. Tecnología de la información - Gestión de incidentes de seguridad de la información - Parte 3: Directrices para las operaciones de respuesta a incidentes de TIC.* Proporciona pautas para la respuesta a incidentes de seguridad de la información en operaciones de seguridad de las TIC. Este documento (ISO / IEC 27035-3: 2020) lo hace cubriendo en primer lugar los aspectos operativos en las operaciones de seguridad de las TIC desde una perspectiva de personas, procesos y tecnología. Luego se enfoca aún más en la respuesta a incidentes de seguridad de la información en las operaciones de seguridad de las TIC, incluida la detección de incidentes de seguridad de la información, informes, triaje, análisis, respuesta, contención, erradicación, recuperación y conclusión." Tomado y Iso.org (2020)

- **MinTIC MSPI Guía 21 -Gestión de Incidentes**
  Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

  "Lineamientos básicos para poner en marcha un Sistema de Gestión de Incidentes de Seguridad de la información, a través de un modelo propuesto, el cual está concebido para que se puedan integrar los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren".
  MinTIC (2016)

  La guía plantea aspectos generales para realizar la gestión de incidentes, asimismo estructura un modelo de proceso cíclico con etapas de actividades a seguir:
  1. Preparación.
  2. Detección y análisis.
  3. Contención, erradicación y recuperación.
  4. Actividades. Post-Incidente.

  Figura 1
  Ciclo de gestión de incidentes de seguridad

  Nota: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- **NIST Special Publication 800-61 Revision 2**
  Computer Security Incident Handling Guide

  La respuesta a incidentes de seguridad informática se ha convertido en un componente importante de los programas de tecnología de la información (TI). Las amenazas relacionadas con la seguridad se han vuelto no solo más numerosas y diversas, sino también

más dañinas y disruptivas. Una capacidad de respuesta a incidentes es necesaria para detectar incidentes rápidamente, minimizar la pérdida y la destrucción, mitigar las debilidades que fueron explotadas y restaurar los servicios informáticos. Esta publicación (NIST-SP 800-61 Rev.2) ayuda a las organizaciones a establecer capacidades de respuesta a incidentes de seguridad informática y a manejar incidentes de manera eficiente y eficaz. Los temas cubiertos incluyen la organización de una capacidad de respuesta a incidentes de seguridad informática, el manejo de incidentes desde la preparación inicial hasta la fase de lecciones aprendidas posterior al incidente y el manejo de tipos específicos de incidentes. NIST.gov (2012)

Uno de los aspectos interesantes que esta guía o marco de referencia plantea es la comunicación que el equipo de respuesta a incidentes debe mantener con las otras partes del negocio, una ilustración al respecto es la siguiente figura.

Figura 2

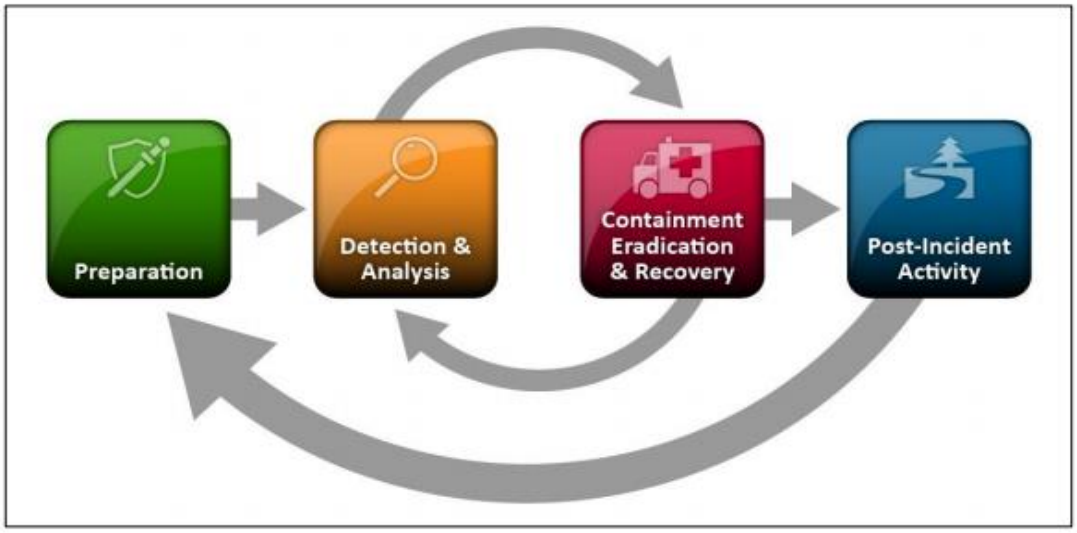
Comunicación equipo de respuesta a incidentes

Nota: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

También estructura un ciclo de vida de respuesta a incidentes el cual se puede apreciar y comprender en la siguiente ilustración.

Figura 3

Incident Response Life Cycle



Nota: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- **NIST *Cybersecurity Framework***
  Marco para la mejora de la seguridad cibernética en infraestructuras críticas

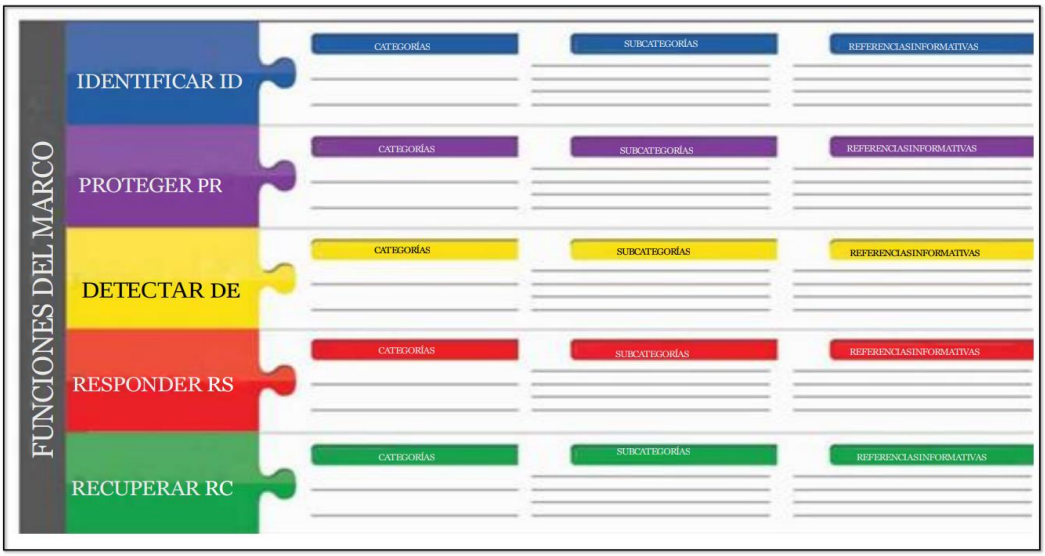
  El Marco se enfoca en el uso de impulsores de negocios para guiar las actividades de seguridad cibernética y en la consideración de los riesgos de seguridad cibernética como parte de los procesos de gestión de riesgos de la organización. El Marco consta de tres partes: el Núcleo del Marco, los Niveles de Implementación y los Perfiles del Marco. El Núcleo del Marco es un conjunto de actividades de seguridad cibernética, resultados y referencias informativas que son comunes en todos los sectores y en la infraestructura crítica. Los elementos del Núcleo proporcionan una guía detallada para desarrollar perfiles individuales en las organizaciones. Mediante el uso de Perfiles, el Marco ayudará a una organización a alinear y priorizar sus actividades de seguridad cibernética con sus requisitos empresariales / de misión, tolerancias de riesgos y recursos. Los Niveles de Implementación proporcionan un mecanismo para que las organizaciones puedan ver y comprender las características de su enfoque para gestionar el riesgo de seguridad cibernética, lo que ayudará a priorizar y alcanzar los objetivos de la seguridad cibernética. NIST.gov (2018)

  Este es un marco más amplio para estructurar acciones para la ciberseguridad, pero que es un excelente referente para la gestión de incidentes y buena gestión de la seguridad digital. En él se establecen un núcleo con una serie de actividades que son de interés para la ciberseguridad en una organización.

  > El Núcleo del Marco proporciona un conjunto de actividades para lograr resultados específicos de seguridad cibernética y hace referencia a ejemplos de orientación en cómo lograr dichos resultados. El Núcleo no es una lista de verificación de las acciones a realizar. Este presenta los resultados clave de seguridad cibernética identificados por las partes interesadas como útiles para gestionar el riesgo de seguridad cibernética. El Núcleo consta de cuatro elementos: Funciones, Categorías, Subcategorías y Referencias Informativas.
  > NIST.gov (2018)

Figura 4

Estructura del Núcleo del Marco



Nota:
https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf