Cuestionario

**Tema:** ISO/IEC 27001 vs. NIST Cybersecurity Framework (CSF)

# Instrucciones:

* Responda cada pregunta en 3–5 oraciones.
* Cite al menos una fuente confiable (norma, documento oficial, guía del NIST, Ministerio TIC, Superintendencia Financiera de Colombia, etc.).
* Sea claro y use ejemplos prácticos cuando corresponda.

# Preguntas

1. **Definición y propósito**

Explique qué es ISO/IEC 27001 y cuál es su objetivo principal. Mencione además si se trata de una norma certificable o no.

ISO/IEC 27001 es una norma internacional que establece los requisitos para implementar un **Sistema de Gestión de Seguridad de la Información (SGSI)**. Su objetivo principal es proteger la confidencialidad, integridad y disponibilidad de la información mediante controles de seguridad y procesos documentados. Es una **norma certificable**, lo que permite a las organizaciones demostrar, a través de auditorías, que cumplen con estándares internacionales.

**Fuente:** ISO/IEC 27001:2022 – International Organization for Standardization.

# Funciones del NIST CSF

¿Cuáles son las funciones principales del NIST Cybersecurity Framework (versión 1.1) y qué nueva función se incorpora en la versión 2.0 (2024)?

El **NIST Cybersecurity Framework (CSF)** versión 1.1 se basa en cinco funciones principales: **Identify, Protect, Detect, Respond, y Recover**. Estas funciones ayudan a las organizaciones a gestionar riesgos de ciberseguridad de forma estructurada. En la **versión 2.0 (2024)** se incorpora la nueva función **Govern (Gobernar)**, que refuerza el liderazgo, la toma de decisiones y la alineación de la ciberseguridad con los objetivos estratégicos de la organización.

**Fuente:** NIST CSF 1.1 (2018) y NIST CSF 2.0 (2024).

# Comparación de enfoques

¿Cuál es la diferencia entre el enfoque de ISO/IEC 27001 (basado en un SGSI) y el enfoque de NIST CSF (flexibilidad y madurez)?

ISO/IEC 27001 se enfoca en la **gestión continua** de la seguridad mediante un SGSI, basado en el ciclo **Plan-Do-Check-Act (PDCA)**, orientado a procesos y certificación. En cambio, el NIST CSF se centra en la **flexibilidad y madurez**, proporcionando guías adaptables a organizaciones de cualquier tamaño, sin exigir certificación. Esta diferencia hace que ISO/IEC 27001 sea más formal y estructurado, mientras que NIST CSF es más dinámico y práctico.

**Fuente:** ISO/IEC 27001:2022; NIST CSF 1.1.

# Similitudes clave

Mencione al menos dos aspectos en los que ISO/IEC 27001 y NIST CSF son similares y explique por qué esas coincidencias son relevantes para una organización.

Tanto ISO/IEC 27001 como NIST CSF:

1. **Gestionan el riesgo de ciberseguridad**, ayudando a priorizar amenazas críticas.
2. **Promueven la mejora continua**, ya que ambos marcos requieren revisiones y ajustes periódicos.

Estas similitudes son relevantes porque las organizaciones pueden integrarlos para fortalecer sus defensas y alinear la seguridad con los objetivos del negocio.

**Fuente:** NIST CSF 1.1; ISO/IEC 27001:2022.

# Ventajas y desventajas

Identifique una ventaja y una desventaja de implementar ISO/IEC 27001, y una ventaja y una desventaja de aplicar NIST CSF.

* **SO/IEC 27001:**
  + Ventaja: otorga **certificación reconocida internacionalmente**, mejorando la reputación y cumplimiento regulatorio.
  + Desventaja: requiere **altos costos y recursos**, lo cual puede ser difícil para PyMEs.
* **NIST CSF:**
  + Ventaja: es **gratuito y flexible**, ideal para iniciar programas de ciberseguridad.
  + Desventaja: al no ser certificable, puede no demostrar formalmente el cumplimiento a clientes o reguladores.

# Fuente: ISO.org; NIST.gov

# Complementariedad práctica

Describa cómo una organización podría utilizar ambos marcos en conjunto para mejorar su postura de ciberseguridad.

Una organización puede usar **ISO/IEC 27001** para estructurar un **SGSI** con políticas, procedimientos y controles documentados; al mismo tiempo, puede aplicar el **NIST CSF** como una **guía operativa** para priorizar amenazas y evaluar la madurez de sus procesos. Por ejemplo, una empresa financiera podría mantener la certificación ISO para cumplir requisitos legales y usar NIST CSF para medir el progreso en detección y respuesta a incidentes. Esta combinación mejora la postura de ciberseguridad y la hace más dinámica ante nuevos riesgos.

**Fuente:** ISO/IEC 27001:2022; NIST CSF 2.0.

# Aplicación en Colombia

Relacione la Ley 1581 de 2012 (protección de datos personales) con ISO/IEC 27001 y NIST CSF. ¿Cómo ayudan estos marcos al cumplimiento de esta normativa?

La **Ley 1581 de 2012** protege los datos personales de los ciudadanos colombianos. ISO/IEC 27001 ayuda a cumplir esta ley al establecer controles para proteger la **confidencialidad e integridad de los datos**, mientras que NIST CSF ofrece buenas prácticas para detectar y responder a incidentes que comprometan esa información. Juntos, ambos marcos fortalecen la gobernanza de los datos personales y ayudan a evitar sanciones por incumplimiento.

**Fuente:** Ley 1581 de 2012; Superintendencia de Industria y Comercio (SIC).

# Normativa sectorial

La Circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia establece lineamientos de ciberseguridad. Explique cómo ISO/IEC 27001 y NIST CSF podrían apoyar a una entidad financiera en cumplir con esta regulación.

**La Circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia exige a las entidades del sector financiero implementar controles para la gestión de riesgos de ciberseguridad. ISO/IEC 27001 facilita el cumplimiento al ofrecer un SGSI formal y auditable, mientras que NIST CSF permite evaluar la madurez de las funciones críticas (como detectar y responder a ciberataques). Esto permite a los bancos y aseguradoras cumplir con la normativa y demostrar resiliencia ante incidentes.**

**Fuente:** Superintendencia Financiera de Colombia, Circular Externa 007 de 2018.

# Caso práctico de PyME

Imagine que una pequeña empresa colombiana quiere mejorar su seguridad digital pero no tiene presupuesto para certificarse en ISO/IEC 27001. ¿Qué marco recomendaría implementar primero y por qué?

Si una **PyME colombiana** carece de presupuesto para certificarse en ISO/IEC 27001, se recomienda iniciar con **NIST CSF**, ya que es **gratuito, flexible y escalable**. Esto le permite implementar prácticas básicas como identificar activos críticos, proteger la red y planificar respuestas a incidentes. Una vez que la empresa madure sus controles y tenga más recursos, puede avanzar hacia la certificación ISO para cumplir con requisitos formales de socios comerciales o contratos.

**Fuente:** NIST CSF 1.1; MinTIC Colombia.

# Reflexión crítica

En su opinión, ¿es más valioso para una organización contar con una certificación ISO/IEC 27001 o aplicar buenas prácticas basadas en NIST CSF sin certificación? Justifique su respuesta con ejemplos o casos reales.

Contar con una **certificación ISO/IEC 27001** puede ser más valioso para empresas que operan en sectores regulados (como bancos o salud) porque demuestra oficialmente el cumplimiento de estándares internacionales. Sin embargo, para organizaciones pequeñas o en crecimiento, **aplicar buenas prácticas de NIST CSF** puede generar beneficios inmediatos en reducción de riesgos sin los costos de certificación. Por ejemplo, una PyME tecnológica puede fortalecer su postura de seguridad con NIST CSF y más adelante buscar la certificación ISO para obtener ventaja competitiva.

**Fuente:** ISO/IEC 27001:2022; NIST CSF 2.0.

Cree una nota en [**Obsidian**](https://obsidian.md/)utilizando **Markdown** en la que organice de manera clara lo aprendido sobre **ISO/IEC 27001 y NIST CSF**.

Su nota debe incluir:

* + Un **título principal** (nivel 1 #).
  + Subtítulos (nivel 2 ##) para: *Definiciones, Similitudes, Diferencias, Normativa Colombiana, Ejemplo de Aplicación*.
  + Una **lista con viñetas** que resuma al menos 3 similitudes y 3 diferencias entre ISO/IEC 27001 y NIST CSF.
  + Un **enlace interno** (propio de Obsidian, con [[ ]]) hacia otra nota suya (por ejemplo, [[Glosario de Términos de Seguridad]]).
  + Una **tabla** en Markdown que compare brevemente ISO/IEC 27001 vs NIST CSF (mínimo 2 filas, 2 columnas).