Universidad Norbert Wiener

FACULTAD DE INGENIERÍA
PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Trabajo de Suficiencia Profesional

Implementación del Marco NIST CSF para mejorar la gestión de ciberseguridad en una consultora de IT, 2026

Para optar el Título Profesional de

Ingeniero de Sistemas e Informática

Presentado por:

Autor: Bueno Reyes, Yhon Vladimir

Código ORCID: https://orcid.org/0000-0001-8021-1876

Asesor: Mg. Chavez Alvarado, Walter Amador

Código ORCID: https://orcid.org/0000-0001-8614-482X

Lima – Perú

2026

Universidad Norbert Wiener	DECLARACIÓN JURADA DE AUTORIA Y DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN		
	CÓDIGO: UPNW-GRA-FOR-033	VERSIÓN: 01 REVISIÓN: 01	FECHA: 08/11/2022

Yo, Yhon Vladimir Bueno Reyes egresado de la Facultad de **Facultad de Ingeniería y Negocios** y Escuela Académica Profesional de **Ingenierías** de la Universidad privada Norbert Wiener declaro que el Informe de Suficiencia Profesional "Implementación del Marco NIST CSF para mejorar la gestión de ciberseguridad en una consultora de IT, 2026" Asesorado por el docente: Walter Amador Chavez Alvarado DNI 09731774 ORCID 0000-0001-8614-482X tiene un índice de similitud de **7 (siete) %** con código oid: oid:14912:609418011 verificable en el reporte de originalidad del software Turnitin.

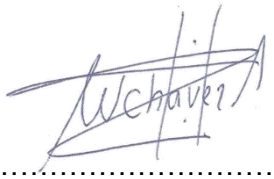
Así mismo:

1. Se ha mencionado todas las fuentes utilizadas, identificando correctamente las citas textuales o paráfrasis provenientes de otras fuentes.
2. No he utilizado ninguna otra fuente distinta de aquella señalada en el trabajo.
3. Se autoriza que el trabajo puede ser revisado en búsqueda de plagios.
4. El porcentaje señalado es el mismo que arrojó al momento de indexar, grabar o hacer el depósito en el turnitin de la universidad y,
5. Asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión en la información aportada, por lo cual nos sometemos a lo dispuesto en las normas del reglamento vigente de la universidad.



……

Firma de autor
Yhon Vladimir Bueno Reyes
DNI: 70165662



……

Firma de Asesor
Walter Amador Chavez Alvarado
DNI: 09731774

Lima, 19 de Mayo del 2026

Índice general

Pag.

Índice tablas ii
Índice figuras iii
Resumen iv
Abstract v
Introducción vi
Capítulo I: Antecedentes y descripción general de la experiencia. 1
1.1 Reseña de la empresa 1
1.2 Ubicación y actividad empresarial 2
1.3 Misión, Visión y Valores 3
1.4 Descripción del puesto desarrollado y su entorno 3
1.5 Problemática y objetivos trazados 5
Capítulo II: Fundamento del Tema elegido 10
2.1 Bases Teóricas 10
2.2 Marco conceptual 11
2.3 Antecedentes (Internacionales, nacionales) 14
2.4 Justificación de la metodología elegida 17
Capítulo III: Aporte y Desarrollo de la Experiencia 18
3.1 Diagnóstico de la situación problemática 18
3.3 Modelo de la propuesta o solución 25
3.4. Resultados 42
Conclusiones 43
Recomendaciones 44
Referencias Bibliográficas 45
Anexos 47

Índice tablas

Pag.

Tabla 1 Presupuesto estimado 28
Tabla 2 Beneficios esperados del proyecto 29
Tabla 3 Estrategia de tratamiento 32
Tabla 4 Relación entre riesgos identificados y controles de seguridad propuestos 33
Tabla 5 Controles implementados 35
Tabla 6 Total de equipos end point protegidos 37

Índice figuras

Pag.

Figura 1 Logo de NSS y IDM Technology 2
Figura 2 Mapa de ubicación de IDM Technology 2
Figura 3 Organigrama de IDM Technology 4
Figura 4 Alternativas de solución frente al problema diagnosticado 20
Figura 5 Línea de tiempo de experiencia profesional 21
Figura 6 Modelo Propuesto – Resumen Ejecutivo 26
Figura 7 Cronograma del proyecto 27
Figura 8 Plan de Migración de Antivirus Corporativo 27
Figura 9 Comparativo de licencia de Microsoft y Costo 29
Figura 10 Ciclo de gestión de riesgos de seguridad de la información 30
Figura 11 Mapa de calor - nivel de riesgo 31
Figura 12 Infraestructura de IT - Alto Nivel 34
Figura 13 Menu de Microsoft Intune 36
Figura 14 Agenda para instalación de agente de SIEM - Wazuh 38
Figura 15 Aprobación de pase a producción de SIM en servidores 39
Figura 16 Evidencia de dashboard de SIEM con los servidores y endpoint 40
Figura 17 Arquitectura de Implementación de SIEM 41

Resumen

El estudio tuvo como objetivo general determinar de qué manera la implementación del marco NIST CSF 2.0 fortalece la gestión de ciberseguridad en la empresa consultora de IT IDM Technology, Lima 2026. Asimismo, a nivel teórico, el estudio plasmo la teoría de la gestión de riesgos de ciberseguridad, orientado a identificar, evaluar y tratar los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información. Por otro lado, en la teoría de marcos de referencia de ciberseguridad, que promueve la estandarización de prácticas y controles; en el mismo sentido, la metodología de desarrollo, se aplicaron de forma adaptativa las funciones de la NIST CSF 2.0 (Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar), alineadas a los procesos de la organización. Así también, los resultados evidenciaron mejoras en la identificación de riesgos, el fortalecimiento de controles preventivos y una detección más temprana de incidentes. Asimismo, se observó un incremento en la madurez organizacional, pasando de un estado inicial a uno intermedio. Se concluye que la adopción del NIST CSF 2.0 permitió reducir la exposición a incidentes críticos, mejorar la confianza de los clientes y consolidar la ciberseguridad como un elemento estratégico. Además, contribuyo a asegurar la continuidad operativa y a fortalecer la resiliencia organizacional frente a amenazas emergentes. Finalmente, se recomienda el hecho de mantener el marco como estándar de institucional, asignar recursos razonables, reforzar mediante auditorias y entrenamientos los controles, y realizar simulaciones de respuesta y recuperación periódicas.

Palabras claves: NIST CSF 2.0, riesgos, controles de seguridad, continuidad operativa, resiliencia organizacional.

Abstract

The overall objective of the study was to determine how the implementation of the NIST CSF 2.0 framework strengthens cybersecurity management at the IT consulting firm IDM Technology, Lima 2026. Furthermore, at the theoretical level, the study addressed the theory of cybersecurity risk management, which is aimed at identifying, assessing, and addressing risks that affect the confidentiality, integrity, and availability of information. Furthermore, in line with the theory of cybersecurity reference frameworks—which promotes the standardization of practices and controls—the NIST CSF 2.0 functions (Govern, Identify, Protect, Detect, Respond, and Recover) were adaptively applied to the organization's processes as part of the development methodology. Furthermore, the results demonstrated improvements in risk identification, the strengthening of preventive controls, and earlier incident detection. Additionally, an increase in organizational maturity was observed, progressing from an initial to an intermediate stage. It is concluded that the adoption of NIST CSF 2.0 helped reduce exposure to critical incidents, improve customer trust, and establish cybersecurity as a strategic element. Furthermore, it helped ensure operational continuity and strengthen organizational resilience in the face of emerging threats. Finally, it is recommended to adopt the framework as an institutional standard, allocate reasonable resources, strengthen controls through audits and training, and conduct periodic response and recovery drills.

Keywords: NIST CSF 2.0, risks, security controls, business continuity, organizational resilience.

7% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

6% Fuentes de Internet
0% Publicaciones
5% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Fuentes principales

6% Fuentes de Internet
0% Publicaciones
5% Trabajos entregados (trabajos del estudiante)

Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1 Internet
repositorio.uwiener.edu.pe 2%

2 Internet
www.coursehero.com 1%

3 Trabajos entregados
Universidad Wiener on 2026-02-10 <1%

4 Internet
repositorioacademico.upc.edu.pe <1%

5 Trabajos entregados
Universidad Wiener on 2026-04-09 <1%

6 Internet
tesis.pucp.edu.pe <1%

7 Trabajos entregados
Universidad Wiener on 2026-03-22 <1%

8 Trabajos entregados
Universidad Nacional Abierta y a Distancia, UNAD,UNAD on 2024-12-08 <1%

9 Trabajos entregados
Universidad Internacional de la Rioja on 2024-11-30 <1%

10 Internet
idmtechnology.com.pe <1%

11 Internet
lecturasmundoempresa.blogspot.com <1%