TESIS

UNIVERSIDAD CIENTÍFICA DEL SUR

UNIVERSIDAD CIENTÍFICA DEL SUR

FACULTAD DE INGENIERÍA

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS EMPRESARIALES

"APLICACIÓN DE LA METODOLOGÍA NIST EN LA MEJORA DE CIBERSEGURIDAD DE LA EMPRESA TPX, 2023"

Tesis para optar el título profesional de:

INGENIERO DE SISTEMAS EMPRESARIALES

Presentado por:

Marlon Enrique Nuñez Cosinga (0000-0001-8640-8602)

Asesor:

Carlos Enrique Lopez Sovero (0000-0002-1316-2848)

Lima – Perú

2025

Tesis publicada con autorización del autor
No olvide citar esta tesis

ACTA DE SUSTENTACIÓN DE TESIS

Lima, 31 de octubre del 2025

Los integrantes del Jurado de tesis:

Presidente	Luis Alberto Torres Cabanillas
Miembro 1	José Alfredo Diaz León
Miembro 2	Manuel Antonio Pereyra Acosta

Se reúnen para evaluar la tesis titulada:
"Aplicación de la metodología NIST en la mejora de ciberseguridad de la empresa TPX, 2023"

Presentado por el bachiller:
Marlon Enrique Nuñez Cosinga

Para optar al título profesional de
Ingeniero de Sistemas Empresariales

Asesorados por:
Carlos Enrique López Sovero

Luego de haber evaluado el informe final de tesis y evaluado el desempeño del estudiante de la Carrera de **Ingeniería de Sistemas Empresariales** en la sustentación, concluyen de manera unánime ( ) por mayoría simple ( ) calificar a:

Tesista:	**Marlon Enrique Nuñez Cosinga**		
Nota (en letras):	**Quince**		
Aprobado (X)	Aprobado - Muy buena ()	Aprobado - Sobresaliente ( )	Desaprobado ( )

Los miembros del jurado firman en señal de conformidad.

Luis Alberto Torres Cabanillas	Carlos Enrique López Sovero
Presidente del Jurado	*Asesor*
José Alfredo Diaz León	Manuel Antonio Pereyra Acosta
Miembro 1	*Miembro 2*

ANEXO: FORMATO DE DECLARACIÓN DE ORIGINALIDAD DE CONTENIDO DE INFORME FINAL DE TESIS O TRABAJO DE INVESTIGACIÓN

UNIVERSIDAD CIENTÍFICA DEL SUR

DECLARACIÓN DE ORIGINALIDAD DE CONTENIDO DE INFORME FINAL DE TESIS / TRABAJO DE INVESTIGACIÓN[1]

Lima,07 de Febrero del 2026____

Señor,
Dr. Percy Mayta Tristan

Vicerrectorado de Investigación

Universidad Científica del Sur
Presente. –

De nuestra consideración,

1. Yo: **Marlon Enrique Nuñez Cosinga**, egresado de la carrera de (nombre de la carrera) de la Universidad Científica del Sur, en conjunto con el asesor: **Carlos Enrique López Sovero**, declaramos que este informe final de tesis titulado: **"APLICACIÓN DE LA METODOLOGIA NIST EN LA MEJORA DE CIBERSEGURIDAD DE LA EMPRESA TPX, 2023**", sustentado para obtener el título: Ingeniero de Sistemas Empresariales, es original.

   Es decir, no contiene plagio parcial ni total, cuando se utilizó información de fuentes externas se reconoció la autoría mediante la adecuada citación y los resultados obtenidos son producto entero de mi (nuestra) investigación y no han sido falseados ni fabricados. Todo esto en cumplimiento del Código de ética en la investigación, Reglamento del Comité de Integridad Científica, Reglamento de Propiedad Intelectual, Normas y procedimientos de los trabajos de investigación para la obtención de títulos profesionales y grados académicos [2], que afirmamos conocer en su totalidad.

   Por ello, en caso de identificarse alguna situación de plagio, falsificación o fabricación de resultados, nos allanamos al proceso de investigación que establezca la Universidad y las posibles sanciones que pudieran surgir.

Firmamos en conformidad con lo declarado,

Firma tesista
DNI: 10868433

Firma del asesor de tesis
DNI:06255052

[1] En conformidad con la Resolución del Consejo Directivo N° 084-2022-SUNEDU/CD
[2] Los documentos están en: https://investigacion.cientifica.edu.pe/reglamentos/

INFORME DE REVISIÓN DE ORIGINALIDAD

Título del documento evaluado. Aplicación de la metodología NIST en la mejora de ciberseguridad de la empresa TPX, 2023

Autores. Marlon Enrique Nuñez Cosinga

Mecanismo de revisión de originalidad. Evaluación con Turnitin (ID 2887455654)

Código de registro. PRE-12-2024-00559

Resultado de la evaluación. 9%

Revisado por. Magaly Kelly Guerrero Huaracallo.

Comentarios sobre la revisión. Filtros usados: excluir fuentes de menos de 15 palabras; excluir citas.



v.2.0. Aplicación de la metodología

INFORME DE ORIGINALIDAD

9%	8%	2%	5%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.uisrael.edu.ec Fuente de Internet	1%
2	Submitted to Instituto Tecnológico y de Estudios Superiores de Occidente Trabajo del estudiante	1%
3	www.gub.uy Fuente de Internet	1%
4	www.coursehero.com Fuente de Internet	<1%
5	repositorio.ucenfotec.ac.cr Fuente de Internet	<1%
6	up-rid.up.ac.pa Fuente de Internet	<1%
7	Submitted to Integración Blackboard Trabajo del estudiante	<1%

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

ÍNDICE

1 Resumen 3
2 Abstract 4
3 Introducción 5
4 Materiales y Métodos 44
4.1 Tipo de la Investigación: 44
4.2 Diseño y Corte de la Investigación 45
4.3 Enfoque de la Investigación 45
4.4 Nivel de Investigación 45
4.5 Población y Muestra 45
4.6 Instrumentos 47
5 Procedimientos (pasos y aportes tecnológicos) 49
5.1 Estrategia de análisis de datos 71
6 Aspectos Éticos 82
7 Limitaciones del Estudio 83
8 Resultados 85
9 Discusión 90
10 Conclusión 92
11 Referencias Bibliográficas 96
12 Anexos 100

ÍNDICE DE ILUSTRACIONES

Ilustración 1: Intentos de Ataque en America Latina 2020 / 2021 11
Ilustración 2: Cuadro Informativo de la empresa TPX 16
Ilustración 3: Componentes de Ciberseguridad del NIST (2018) 34
Ilustración 4: Componentes de Ciberseguridad NIST (2023) 35
Ilustración 5: Estructura organizativa de la empresa TPX 38
Ilustración 6: Calculadora de Muestra 47
Ilustración 7: Evaluación de Madurez en Ciberseguridad de la Empresa TPX 55
Ilustración 8: Nivel de Madurez vs Perfil Objetivo en las Funciones NIST 67
Ilustración 9: Inversión Requerida vs Beneficio Esperado por el Área de Mejora 67
Ilustración 10: Impacto a las Brechas de Seguridad en los Objetivos del Negocio 67
Ilustración 11: Gestión de análisis de S.I.- NIST y su respectivo Roadmap 69
Ilustración 12:Proceso Completo de la Investigación 85
Ilustración 13: Proceso de Evaluación de Resultados 86

Tesis publicada con autorización del autor
No olvide citar esta tesis

Ilustración 14: Gráfico de Correlación de Spearman 89
Ilustración 15: DESPUÉS - Nivel de Madurez..... 91
Ilustración 16: ANTES - Nivel de Madurez..... 91
Ilustración 17: Diagráma General del Proceso 114
Ilustración 18: Metodología en la mejora de la Ciberseguridad de TPX 116
Ilustración 19: Herramienta creada basada en NIST CSF 120

ÍNDICE DE TABLAS

Tabla 1: FODA de la empresa TPX 24
Tabla 2: Matriz de Información crítica de la empresa TPX..... 41
Tabla 3: Matriz de Calor 42
Tabla 4: Principios básicos de la Información 42
Tabla 5: Análisis de fiabilidad para D1, D2, D3, D4, D5 48
Tabla 6: Evaluación de Cuestionario 49
Tabla 7: Escala Likert 49
Tabla 8: Matriz AS IS situación actual de Ciberseguridad en la empresa TPX..... 50
Tabla 9: Matriz de madurez de Ciberseguridad de la empresa TPX 56
Tabla 10: Baremo de las 5 dimensiones..... 57
Tabla 11: Nivel y Rango Variable General 58
Tabla 12:Alineación de los KPI's con las Funciones del NIST de la Empresa TPX 59
Tabla 13: Evaluación de acuerdo con la Metodología NIST - Empresa TPX 61
Tabla 14: Niveles de Madurez Actual vs. Perfil Objetivo en las Funciones NIST..... 67
Tabla 15: Respectivos Valores Rango y Amplitud 71
Tabla 16: Coeficiente de Confiabilidad Alfa de Cronbach 73
Tabla 19: Prueba de rangos con signo de Wilcoxon..... 76
Tabla 20: Histograma de frecuencia - variable..... 77
Tabla 21: Tabla de frecuencias..... 77
Tabla 22: Tabla de Prueba de Normalidad 1 77
Tabla 23: Tabla de Prueba de normalidad 2 78
Tabla 26: Prueba de rangos con signo de Wilcoxon..... 79
Tabla 27: Tabla de Varianza Postest..... 81
Tabla 28: Resumen Estadístico..... 82
Tabla 30: Tabla de Resumen de los Procesos de Evaluación de Resultados..... 86

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

APLICACIÓN DE LA METODOLOGIA NIST EN LA MEJORA DE CIBERSEGURIDAD DE LA EMPRESA TPX, 2023

1 Resumen

La investigación tiene como propósito aplicar un modelo de ciberseguridad, con el fin de optimizar la seguridad de la información en la compañía TPX, usando NIST. Cabe mencionar que el diseño del estudio es cuasi experimental y aplicado; también es cuantitativo según su enfoque y explicativo según su naturaleza. Asimismo, se utilizaron herramientas para llevar a cabo el estudio de campo, como un cuestionario, fichas de observación, y entrevistas; todo, mediante un muestreo no probabilístico por conveniencia. El coeficiente Rho Spearman de 0.621 que se obtuvo como resultado de la prueba de hipótesis general, señala una correlación positiva entre las dos variables. Esto demuestra que adoptar un modelo de ciberseguridad incrementa la seguridad de la información en la compañía TPX. Así, a través de directrices, estrategias y supervisiones, el modelo contribuye a administrar y reducir los riesgos que enfrentan igualmente las pequeñas y medianas empresas.

Palabras Clave: Metodología NIST, Ciberseguridad, seguridad empresarial

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

2 Abstract

The purpose of this research is to apply a cybersecurity model to optimize information security at TPX, using NIST standards. The study design is quasi-experimental and applied; it is also quantitative in its approach and explanatory in its nature. Tools used for the field study included a questionnaire, observation sheets, and interviews, all conducted using non-probability convenience sampling. The Spearman's rho coefficient of 0.621, obtained from the general hypothesis test, indicates a positive correlation between the two variables. This demonstrates that adopting a cybersecurity model increases information security at TPX. Thus, through guidelines, strategies, and oversight, the model helps manage and reduce the risks faced by small and medium-sized enterprises (SMEs).

Keywords: NIST Methodology, Cybersecurity, Enterprise Security

Tesis publicada con autorización del autor
No olvide citar esta tesis

3 Introducción

En el siglo XXI, las tecnologías disruptivas han transformado profundamente la forma en que las empresas funcionan y los datos pueden ser interceptados o dañados. Además, dispositivos como ordenadores portátiles, teléfonos móviles y dispositivos portátiles pueden convertirse en portales a las redes de hogares, empresas y centros sanitarios. La mayoría de los productos de consumo tienen poca ciberseguridad. (Raynor, 2022)

Muchas empresas de este siglo son "tecno dependientes", y esta tendencia está creciendo a medida que más empresarios confían en la automatización, la interconexión computacional y los procesos en línea para su negocio. Pero, debido a la presencia de vulnerabilidades, el uso de la tecnología en los procesos comerciales puede poner en peligro la información digital. (Chinchilla & Allende, 2017).

La ciberseguridad se ha vuelto un asunto estratégico esencial para las compañías de todo el mundo, especialmente en la gestión empresarial en esta era digital. (Balasinorwala & Bhagwani, 2023)

Las amenazas cibernéticas, desde ataques de ransomware, transacciones multimillonarias por ataques de APT, hasta robo de datos confidenciales, son omnipresentes y pueden tener un impacto devastador en la continuidad del negocio y la reputación de una empresa. En este contexto, la gestión efectiva de la ciberseguridad ha adquirido una importancia crucial para garantizar la supervivencia y el crecimiento sostenible de las organizaciones.

Tesis publicada con autorización del autor
No olvide citar esta tesis

De acuerdo a (Delgado, Methodology Based on the NIST Cybersecurity Framework as a proposal for Cybersecurity Management in Government Organizations, 2021) señala que: Muchas organizaciones no tienen un proceso claro para gestionar la ciberseguridad, lo que resulta en una gestión deficiente y sin indicadores. Sobre si están implementando la metodología que se basan en el marco de ciberseguridad de NIST.

Como nos dice el autor, la ciberseguridad es ya una prioridad en todo el mundo a medida que las amenazas y ataques cibernéticos siempre continúan evolucionando. Se debe proteger los activos críticos y sobre todo los datos sensibles, que es esencial en la era digital. (Schneier, 2016), en nuestro caso la investigación se orientó a proteger información categorizada como critica en la empresa TPX.

(Kamalanathan, Srinivas, & Krishnashree, 2021) Se han producido numerosos ciberataques dirigidos, vulnerando tanto a datos personales de pacientes (información) de empresas privadas como a datos científicos sobre determinados tratamientos, lo que ha expuesto a los sistemas a una muy amplia gama de riesgos relacionados con el robo, la explotación, la indisponibilidad o la destrucción de estos datos sensibles información.

Schneier, (2015) En el ámbito internacional el autor advierte los activos de información críticos, como bases de datos de clientes, sistemas financieros y plataformas de comunicación, son objetivos prioritarios para los cibercriminales. Él argumenta que la globalización de la tecnología ha expuesto a las

Tesis publicada con autorización del autor
No olvide citar esta tesis

organizaciones a riesgos transnacionales, donde las amenazas ya no se limitan a fronteras geográficas, sino que impactan a empresas de todo el mundo.

Bowen (2018) Hace mención sobre la Información Security Handbook que la publicación tiene como objetivo informar a los miembros del equipo de administración de seguridad de la información (jefes de agencia; directores de datos; funcionarios superiores de seguridad de la información de la agencia (SAISO), también llamados directores de seguridad de la información (CISO) y administradores de seguridad de la información) respecto a los distintos elementos de la seguridad de la información que se anticipa que acometerán esa seguridad. El manual ofrece directrices para una aproximación más consistente a los programas de seguridad.

(Ghernaouti 2013) En el sector regional argumenta que la protección de los activos críticos de información en América Latina es fundamental para mitigar el impacto de las amenazas cibernéticas, señalando que la falta de regulaciones específicas y la baja inversión en ciberseguridad colocan a las empresas en una posición vulnerable. Ghernaouti subraya la importancia de una estrategia integral que incluya tanto al sector público como al privado para mejorar las capacidades defensivas frente a los ataques cibernéticos y proteger infraestructuras clave como sistemas financieros y de telecomunicaciones.

La seguridad la información debería gestionarse dentro de la ciberseguridad, centrándose en salvaguardar los activos de información para prevenir amenazas

Tesis publicada con autorización del autor
No olvide citar esta tesis

a los datos que se procesan, almacenan y transmiten por medio de los sistemas de información en línea. (ISACA, 2017)

Se menciona además que la variedad confusa de directrices, estándares y requisitos reglamentarios en materia de ciberseguridad, presenta problemas para las empresas y también para los servicios públicos hoy en día. (Dolezilek & Hussey, 2011)

En este contexto, la aplicación efectiva del Framework NIST (National Institute of Standards and Technology) se presenta como un enfoque fundamental para mejorar la ciberseguridad empresarial. Este marco de trabajo proporciona una sólida estructura que abarca las dimensiones de identificación, prevención, detección, respuesta y recuperación, brindando directrices claras y mejores prácticas para abordar los desafíos cibernéticos según lo plantea el NIST.

En la región latinoamericana presenta serias deficiencias en la creación de políticas nacionales de seguridad cibernética y en el desarrollo de habilidades para enfrentar los riesgos y amenazas del ciberespacio en dimensiones que tienen un impacto en la seguridad nacional y la política exterior. Por otro lado (NIST, El Marco de Ciberseguridad del NIST, 2021) nos indica que “Hay que ser consciente de que la ciberseguridad es algo de lo que hay que preocuparse y saber qué pasos seguir.

(Rizzo & Pagola, 2019) La alineación de las funciones, categorías y subcategorías con los requisitos comerciales, la tolerancia al riesgo y los

Tesis publicada con autorización del autor
No olvide citar esta tesis

recursos de la organización es lo que determina el perfil del marco de trabajo de NIST.

Yañez (2022) Señala que el "NIST Cybersecurity Framework" puede proporcionar un proceso metodológico para que las organizaciones aseguren su plataforma tecnológica, describiendo su postura actual de seguridad cibernética, estableciendo y evaluando el progreso hacia el objetivo deseado.

León (2021) Nos menciona que en Perú se cuenta con un documento que se denomina: La Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales y que se aprobó mediante Resolución Directoral N° 019-2013-JUS/DGPDP. Es reconocido internacionalmente y lo importante es que lo siguen usando, y aplicando en otros lugares, aquí en Perú se debería estar aplicando en todas las empresas.

Entre tanto en Perú se analiza cómo la guerra en el ciberespacio afecta tanto a países desarrollados como en desarrollo, y cómo los ataques cibernéticos pueden causar daños económicos importantes a nivel global. Además, destaca el papel que juegan organizaciones como las Naciones Unidas y la OEA en la defensa cooperativa frente a estas amenazas, aunque menciona que, en la región de América Latina, aún falta mucho por hacer en materia de ciberseguridad. (Benavides, 2018)

Fisch & White, (1999) Definen los activos críticos de información como aquellos componentes, sistemas o datos fundamentales cuya interrupción o pérdida

Tesis publicada con autorización del autor
No olvide citar esta tesis

afectaría gravemente la capacidad de una organización para operar. Además, subraya que la ciberseguridad es el conjunto de medidas tecnológicas y administrativas destinadas a proteger esos activos de amenazas externas e internas.

Realidad Problemática

La ciberseguridad es un reto mundial a causa del incremento de los ataques cibernéticos, la digitalización de servicios y la dependencia de tecnologías emergentes. Según Bruce Schneier, experto en seguridad informática, "la seguridad cibernética es un problema complejo que requiere soluciones técnicas, políticas y sociales" (Schneier, 2018). Además, el informe de McAfee y el Centro de Estudios Estratégicos e Internacionales (CSIS) estima que los costos globales del cibercrimen superan los $1 billón de dólares anuales (McAfee & CSIS, 2020).

El Informe de Riesgos Globales del Foro Económico Mundial (2023) destaca que los ciberataques son una de las principales amenazas para la economía mundial, especialmente con el aumento de ataques de ransomware y la explotación de vulnerabilidades en sistemas críticos (Forum, 2023)

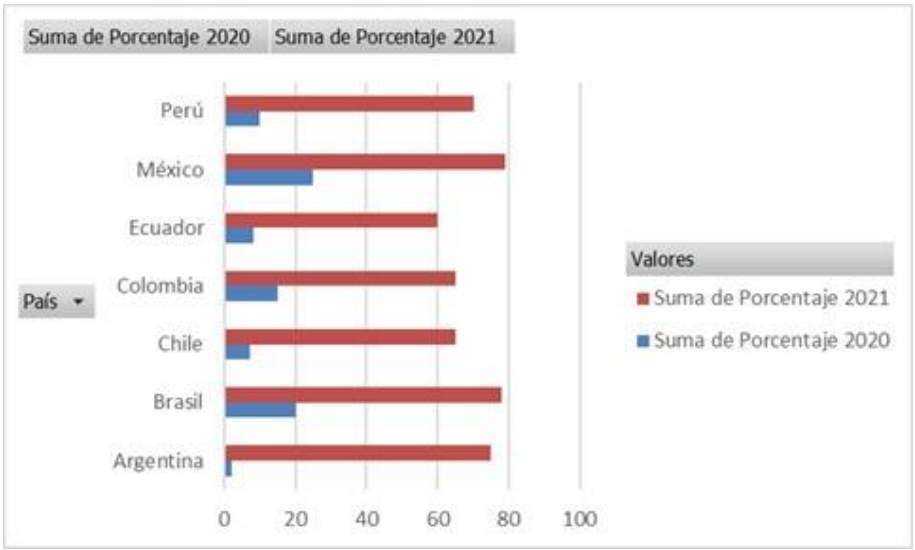
En Sudamérica, la ciberseguridad enfrenta desafíos como la falta de inversión en infraestructura y la ausencia de marcos legales robustos. Según la Organización de los Estados Americanos (OEA), "la región necesita fortalecer sus capacidades de ciberseguridad para proteger infraestructuras críticas y datos personales" (OEA, 2020). Además, un informe de ESET revela que países como Brasil, Argentina y México son los más afectados por ciberataques en la

Tesis publicada con autorización del autor
No olvide citar esta tesis

región, con un aumento del 40% en incidentes de ransomware en 2022 (ESET, 2022)

Mendoza & Vega (2019) Comenta que es justo preocuparse por la seguridad de los sistemas de cómputo en la red. Entre los ataques exitosos que se están volviendo más comunes, se encuentran el robo de claves de acceso a cuentas de usuarios, las filtraciones masivas de información documental de clientes corporativos, los ciberataques distribuidos que niegan el servicio en páginas web y la vigilancia digital orientada hacia documentos clasificados cada vez están siendo más frecuentes. En Sudamérica se registró un aproximado de 1 000M de intentos de ataques sacando un promedio de 50 000 atentados por día,

Ilustración 1: Intentos de Ataque en America Latina 2020 / 2021



Fuente: Elaboración Propia

como países perjudicados tenemos a Brasil 46.69%, México 22.57%, Colombia 8.07%, Perú 5.56%, Ecuador 3.86%, Chile 2.29% y Argentina 1.93%. (Pontiroli, 2020)

Tesis publicada con autorización del autor
No olvide citar esta tesis

Ferreira & Mamede (2022) Nos dice que definir un modelo adecuado de respuesta a determinados incidentes de ciberseguridad es un desafío sumamente crítico al que se enfrentan todas las empresas diariamente. Sin embargo, a pesar de ello, no siempre hay una acción adecuada a estos incidentes. Esto se debe a la falta de modelos predictivos basados en datos (evidencia). Existe una importante inversión en investigación para identificar los principales factores que pueden provocar este tipo de incidentes, intentando siempre tener la respuesta más adecuada y, en consecuencia, potenciando la capacidad de respuesta y el éxito.

La ciberseguridad se considera entonces una estrategia para proteger los sistemas informáticos del robo de información e intenta ayudar a reaccionar ante problemas de seguridad. (Corletti, 2017)

Dedeker explica que, ante el aumento de las filtraciones de datos empresariales, el NIST introdujo el Marco de Ciberseguridad (CSF) de 2014 para asistir a las organizaciones en la disminución de los riesgos cibernéticos que ponen en peligro sus activos esenciales. Dedeke, (2017) describe los elementos fundamentales del CSF, junto con sugerencias para organizaciones en distintos niveles de adopción.

El NIST Cybersecurity Framework (CSF) es uno de los estándares más reconocidos internacionalmente para la administración de riesgos de ciberseguridad. Según el propio NIST, "el CSF proporciona un enfoque flexible y repetible para gestionar los riesgos de ciberseguridad, basado en estándares y

Tesis publicada con autorización del autor
No olvide citar esta tesis

mejores prácticas" (National Institute of Standards and Technology [NIST], 2018). Este marco es ampliamente utilizado por organizaciones tanto del sector público como privado.

Dempsey & Nolan, (2014), en su trabajo NIST Special Publication (SP) 800-161, discuten cómo las empresas pueden utilizar el marco NIST para gestionar riesgos de ciberseguridad en sus cadenas de suministro. Ellos destacan que "el NIST CSF proporciona un enfoque estructurado para que las empresas identifiquen y mitiguen riesgos en sus operaciones y relaciones comerciales" (Dempsey & Nolan, 2014)

Ross & McEvilley (2018), en su guía NIST Special Publication (SP) 800-160, discuten cómo las empresas pueden aplicar el marco NIST para desarrollar sistemas seguros desde su diseño. Ellos argumentan que "el NIST CSF permite a las empresas pueden integrar la seguridad en cada fase del ciclo de vida de sus sistemas, reduciendo vulnerabilidades y costos a largo plazo" (Ross & McEvilley, 2018)

En Perú, la ciberseguridad es un tema emergente. Según el Banco Interamericano de Desarrollo (BID), "Perú ha avanzado en la implementación de políticas de ciberseguridad, pero aún enfrenta desafíos en la protección de infraestructuras críticas y la capacitación de profesionales" (BID, 2021). El Instituto Nacional de Estadística e Informática (INEI) reportó que, en 2021, el 54% de las empresas peruanas experimentaron al menos un incidente de seguridad cibernética (INEI, 2021).

Tesis publicada con autorización del autor
No olvide citar esta tesis

En Lima, la ciberseguridad es un desafío creciente debido a la alta concentración de empresas e instituciones del gobierno. Según un estudio de la Cámara de Comercio de Lima (CCL), "el 60% de las PYMEs en Lima no cuentan con un plan de ciberseguridad, lo que las hace vulnerables a ataques" (CCL, 2022). Además, el Ministerio de Transportes y Comunicaciones (MTC) ha implementado iniciativas para promover la conciencia en ciberseguridad, pero aún se necesita mayor capacitación y recursos (MTC, 2023).

La empresa TPX es una empresa desarrolladora de marketing digital que incluye diseño de Ux & Ai establecida desde el 2020 y una de las muy pocas que existe en el rubro de desarrollo puramente digital, el trabajo digital es totalmente su core de negocio y con un nicho de empresas medianas que están en expansión, donde se ha establecido en las redes sociales y es su principal canal de comunicación con los clientes.

TPX se enfrenta a una situación problemática en ciberseguridad que ha generado dificultades para administrar sus recursos de información digital. A pesar de su juventud, la empresa ya ha enfrentado problemas de seguridad, como ataques de ransomware que han resultado en la pérdida de múltiples activos de información, donde se secuestró información delicada y todo esto pueden seguir afectando su operatividad, reputación y posiblemente sus finanzas. Además, Se encontró que ellos han tenido amenazas como ransomware, phishing y ataques por malware; también posiblemente por la falta de un plan de acción contra estas amenazas; Y según Ross et al. (2018), "la ausencia de un marco de gestión de riesgos, como el NIST Cybersecurity

Tesis publicada con autorización del autor
No olvide citar esta tesis

Framework (CSF), aumenta la probabilidad de incidentes y dificulta la respuesta efectiva ante ataques" (Ross et al., 2018).

Al ser una empresa joven (como la mayoría de las empresas en el Perú), es probable que TPX haya priorizado el crecimiento y la innovación sobre la seguridad, dejando brechas en el control de su infraestructura tecnológica que a su vez controlan los activos de información de la empresa. Como lo señala Kshetri “las empresas emergentes, en su afán por crecer rápidamente, a menudo descuidan la implementación de controles de seguridad básicos, como firewalls, cifrado de datos y autenticación multifactor, lo que las hace vulnerables a ciberataques" (Kshetri, 2020)

La empresa cuenta con los departamentos de Tecnología, Marketing y diseño Ux & Ai, Legal, Operaciones, etc. como se muestra en su organigrama (ilustración 7).

Los incidentes de ciberseguridad que van en contra de los activos de información que contiene la empresa ya han afectado a TPX, lo que podría generar pérdidas financieras enormes, daños a la reputación y la posible interrupción de servicios críticos. Gartner (2023) advierte que " Las organizaciones que carecen de un plan de respuesta a incidentes bien definido experimentan tiempos de recuperación más prolongados y mayores costos financieros después de un ciberataque" (Gartner, 2023).

Tesis publicada con autorización del autor
No olvide citar esta tesis

Con la evolución continua de las comunicaciones, así como el nuevo trabajo remoto, esta empresa es un perfecto ejemplo de las nuevas empresas que están emergiendo y que necesitan tener un marco de trabajo para seguir y saber si están preparados para posibles ataques de ciberseguridad y sobre todo los riesgos que corren sus activos de información. Y aquí también la importancia ya que este es un ejemplo de una empresa formal en expansión y que se va haciendo grande pero también puede perderlo todo (activos de información) incluso en poco tiempo del despegue. Y esto refleja la realidad empresarial peruana, donde las empresas operan en un entorno nacional que no prioriza la ciberseguridad, dejándolas expuestas a riesgos digitales. Los activos de información, que son muchas veces el core del negocio, pueden ser vulnerados, robados o destruidos, lo que puede llevar al fracaso de las empresas y a la pérdida del capital que impulsa el desarrollo económico. Las empresas son el motor que mueve a los países, y su vulnerabilidad ante las ciberamenazas no solo las afecta a ellas, sino también al progreso nacional".

Ilustración 2: Cuadro Informativo de la empresa TPX

EMPRESA:	TPX SAC
RUBRO:	Marketing Digital
MISIÓN:	Organización enfocada en brindar servicios de marketing digital de las empresas para lograr el éxito esperado, utilizando creatividad además de la innovación y tecnología.
VISIÓN:	Llegar a ser líder nacional en la provisión de soluciones innovadoras de marketing digital.

Fuente: Elaboración Propia

Tesis publicada con autorización del autor
No olvide citar esta tesis

Al no tener ningún tipo de conocimiento previo de la empresa TPX con respecto a su estado de ciberseguridad y el manejo de sus activos, se realiza las dos fases de un modelo de gestión como son el AS IS que mostrará de cómo se encuentra la empresa y luego el TO BE donde nos da la versión optimizada y además se define soluciones a los problemas y se evalúa las posibles mejoras.

Situación Actual (AS IS)

La empresa TPX presenta un nivel de madurez bajo en la gestión de ciberseguridad desde que se hizo un análisis de activos de información. Se denotó la falta de una gestión estructurada de los activos críticos, junto con deficiencias en detección, respuesta y recuperación ante incidentes, que genera un alto riesgo de exposición a ataques cibernéticos. Sin un enfoque proactivo basado en la metodología NIST, la seguridad de la empresa sigue siendo reactiva e insuficiente para proteger sus datos y operaciones.

La empresa no tiene un inventario formal y actualizado de sus activos de información, lo que dificulta la gestión efectiva de los riesgos.

Problemática Detectada:

- Falta de un catálogo (CMDB según ITIL) de activos críticos (bases de datos, servidores, dispositivos de red).
- No se han clasificado los activos según su nivel de criticidad y confidencialidad.
- No existe una matriz clara de riesgos asociados a cada activo.
- Falta de asignación de propietarios responsables de cada activo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

La empresa cuenta con medidas básicas de seguridad, pero estas son insuficientes para proteger eficazmente los activos digitales.

Problemática Detectada:

- Falta de cifrado de datos en reposo y en tránsito.
- Uso de contraseñas débiles sin una política estricta de autenticación.
- Controles de acceso inadecuados (accesos concedidos sin justificación ni revisión periódica).
- Ausencia de un sistema centralizado de gestión de identidad y accesos (IAM).

La detección de incidentes se realiza de forma manual y reactiva, con herramientas insuficientes para la identificación temprana de amenazas.

Problemática Detectada:

- No se cuenta con un sistema de monitoreo en tiempo real para detectar accesos no autorizados.
- Falta de correlación de eventos de seguridad (SIEM).
- No existen mecanismos para la identificación proactiva de vulnerabilidades en la infraestructura.
- Respuesta tardía ante incidentes debido a la falta de visibilidad de los activos expuestos.

La empresa no tiene procedimientos y fundamentos de respuesta a incidentes, aunque carecen de normalización y de sincronización con un conjunto de mejores prácticas

.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Cuestión Identificada:

- Falta un plan oficial de respuesta a incidentes basado en NIST.
- La administración de incidentes se basa en la experiencia del personal y no en protocolos definidos.
- Falta de roles y responsabilidades definidas en caso de un ciberataque.
- No se realizan simulacros ni entrenamientos en respuesta a incidentes.

La empresa tiene serias deficiencias en sus estrategias de recuperación de activos y continuidad operativa tras un incidente de seguridad.

Problemática Detectada:

- No se han implementado planes de recuperación ante desastres (DRP).
- Falta de respaldo regular de los datos críticos y ausencia de pruebas de restauración.
- No existen estrategias de redundancia para minimizar el impacto de un ciberataque.
- La empresa no tiene acuerdos de recuperación con proveedores externos.

Situación Recomendada (TO BE)

El TO BE que se realizó es la representación del estado objetivo que la empresa TPX alcanzará tras la implementación de la metodología NIST, mejorando significativamente su postura de ciberseguridad con respecto a sus activos de

Tesis publicada con autorización del autor
No olvide citar esta tesis

información. Esta transformación permitirá que la organización pase de un enfoque reactivo a un enfoque preventivo y resiliente.

1.- Identificación

Implementar un sistema estructurado para la identificación y clasificación de activos de información, alineado con NIST.

Mejoras Clave:

- Creación de un inventario digital actualizado de activos críticos (servidores, bases de datos, sistemas).
- Clasificación de los activos según su criticidad y nivel de confidencialidad.
- Asignación de propietarios responsables para cada activo, con roles y permisos bien definidos.
- Implementación de una matriz de riesgos específica para cada activo.

2.- Protección

Asegurar la integridad, disponibilidad y confidencialidad de los activos mediante controles avanzados.

Mejoras Clave:

- Establecimiento de una política de gestión para el cifrado de datos, que contemple estándares como AES-256 para datos en reposo y TLS 1.3 para datos en tránsito.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Diseño e incorporación progresiva de una estrategia de autenticación robusta, priorizando la adopción de mecanismos como la autenticación multifactor (MFA) en sistemas críticos.
- Desarrollo de un modelo de gobernanza de identidades y accesos (IAM) que incluya lineamientos para la asignación, revisión y revocación periódica de privilegios.
- Formulación de un plan de arquitectura de seguridad perimetral, que integre la segmentación de redes y la evaluación de tecnologías como firewalls de próxima generación.

- Implementación progresiva de una metodología basada en el enfoque Zero Trust, orientada a minimizar accesos no autorizados a través de controles dinámicos y verificación continua.

3.- Detección

Implementar un sistema robusto de monitoreo y detección de vulnerabilidades en tiempo real.

Mejoras Clave:

- Definición de una estrategia para la gestión centralizada de eventos de seguridad, considerando la futura adopción de un sistema SIEM (gestión de eventos e información de seguridad) para correlacionar y analizar incidentes.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Desarrollo de una política de evaluación continua de vulnerabilidades, que contemple el uso de herramientas automatizadas como Nessus u OpenVAS como parte del proceso de gestión del riesgo.

- Elaboración de un marco de referencia para la protección de endpoints, que incluya la evaluación de soluciones EDR (Endpoint Detection and Response) dentro de un enfoque integral de defensa.

- Planificación del establecimiento de un Centro de Operaciones de Seguridad (SOC) con criterios de operación continua (24/7), alineado a las necesidades y recursos organizacionales.

- Formulación de una metodología de gestión de inteligencia de amenazas, que permita integrar fuentes confiables de Threat Intelligence para una prevención anticipada de ataques.

4.- Respuesta

Desarrollar una estrategia de respuesta a incidentes conforme a NIST, con procedimientos establecidos y capacitados.

Mejoras Clave:

- Elaboración de una estrategia metodológica para la formulación de un Plan de Respuesta ante Incidentes (IRP), de acuerdo con las pautas del marco NIST.
- Creación de un modelo organizativo con funciones y responsabilidades bien definidas para la correcta administración de incidentes de seguridad.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Diseño de un programa continuo de formación y concienciación, orientado al desarrollo de capacidades del equipo TI y del personal general en gestión de incidentes.
- Planificación e incorporación de simulacros periódicos de ciberataques, incluyendo escenarios como ransomware y phishing, como parte de una cultura de preparación institucional.
- Evaluación e inclusión de una estrategia para la administración de herramientas SOAR (Orquestación, Automatización y Respuesta de Seguridad), con el objetivo de optimizar la eficacia operativa en la gestión de incidentes.

5.- Recuperación

Garantizar la recuperación eficiente de los activos de información y la continuidad operativa ante incidentes.

Mejoras Clave:

- Diseño y estructuración de un Plan de Recuperación ante Desastres (DRP) como política organizacional, incluyendo directrices para respaldos periódicos.
- Definición de un cronograma metodológico para pruebas regulares de recuperación de datos, asegurando su integridad y disponibilidad.
- Planificación de una estrategia de redundancia geográfica, orientada a reducir riesgos operativos ante contingencias.
- Evaluación y formalización de acuerdos contractuales con proveedores externos para servicios de recuperación y continuidad.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Desarrollo de una política institucional para la adopción de soluciones de backup en la nube, incluyendo requisitos de cifrado de extremo a extremo y cumplimiento normativo.

Se empleó la herramienta desarrollada por Albert S. Humphrey (2005), que posibilita establecer la estrategia y el beneficio comparativo de una compañía a través de una matriz FODA (fortalezas, oportunidades, amenazas y debilidades). Fuentes externas e internas de comprensión del mercado y la empresa se usaron para llevar a cabo el análisis FODA. A continuación, se presenta la estrategia cruzada FODA y se tiene lo siguiente:

Tabla 1: FODA de la empresa TPX

FACTORES	FORTALEZAS (F)	DEBILIDADES (D)
INTERNOS	- Infraestructura tecnológica básica establecida.	- Falta de un Plan Formal de Ciberseguridad alineado con NIST.
	- Personal técnico con conocimientos en TI.	- Baja madurez en la identificación de activos de información.
	- Compromiso de la alta dirección para mejorar la seguridad	- Ausencia de un Centro de Operaciones de Seguridad (SOC) propio.
	- Uso de herramientas básicas de monitoreo de seguridad.	- Escaso entrenamiento al personal sobre ciberseguridad.
	- Implementación parcial de antivirus y firewalls.	- Políticas de seguridad no documentadas ni actualizadas.
FACTORES	**OPORTUNIDADES (O)**	**AMENAZAS (A)**
EXTERNOS	- Aumento de la adopción de estándares de ciberseguridad como NIST en el sector empresarial.	- Incremento de ataques cibernéticos como ransomware, phishing y APTs (Amenazas Persistentes Avanzadas).

Tesis publicada con autorización del autor
No olvide citar esta tesis

	- Disponibilidad de herramientas de ciberseguridad basadas en inteligencia artificial y machine learning.	- Evolución constante de nuevas amenazas digitales.
	- Acceso a programas de capacitación gratuita sobre ciberseguridad.	- Cumplimiento parcial de las regulaciones nacionales e internacionales (Ley de Protección de Datos Personales).
	- Posibles alianzas estratégicas con proveedores de soluciones de seguridad.	- Falta de cultura organizacional sobre la importancia de la ciberseguridad.
	- Regulaciones emergentes que exigen a las empresas implementar marcos de seguridad como NIST.	- Creciente dependencia de los servicios en la nube sin medidas de protección adecuadas.

Fuente: Elaboración propia

Luego de este análisis, se detalló el objetivo, de implementar un modelo de ciberseguridad para mejorar la seguridad de la información, basada en NIST en la empresa TPX. Se busca analizar y evaluar cómo el uso de este marco contribuye a fortalecer las estrategias de identificación, prevención, detección, respuesta y recuperación frente a amenazas y vulnerabilidades cibernéticas, impactando positivamente en la seguridad y continuidad de las operaciones de la empresa.

La metodología que se empleó en el diseño de estudio es cuasiexperimental, de tipo aplicado, tiene un enfoque cuantitativo, según la naturaleza es de nivel explicativo, de igual forma, se aplicó instrumentos para realizar el estudio de campo como cuestionario, fichas de observación, y entrevistas; todo, mediante un muestreo no probabilístico por conveniencia. El resultado de la contrastación

Tesis publicada con autorización del autor
No olvide citar esta tesis

de hipótesis general muestra que el coeficiente Rho Spearman es de 0.621, lo que prueba que hay una correlación positiva entre las dos variables.

Los hallazgos de este estudio indican que el uso de la metodología NIST en la empresa TPX mejora significativamente su capacidad de respuesta ante incidentes de ciberseguridad y puede reducir la probabilidad de vulnerabilidades no detectadas. A través de la implementación del marco NIST, la empresa logra mejorar sus procesos en las cinco dimensiones evaluadas (identificación, prevención, detección, respuesta y recuperación), lo que resulta en una mayor protección de sus activos críticos de información y una respuesta más eficiente ante ataques cibernéticos.

Cabe señalar que se debe reconocer, analizar y gestionar el riesgo de seguridad cibernética, la metodología debe aplicarse fundamentalmente como un proceso ordenado. Una compañía puede aplicar sus procesos vigentes y superponerlos a este marco para reconocer y analizar el riesgo de seguridad cibernética y de esta forma poder obtener una hoja de ruta siempre para mejora; pero se debe tener en cuenta que el Framework no fue ni está diseñado para reemplazar ningún proceso existente. La organización debe y puede desde un principio determinar las actividades que son punto clave en el negocio y así prestar atención a los servicios críticos y de esta manera priorizar los recursos financieros para optimizar el efecto de la inversión a través del uso del marco (Framework), como para lo que fue creada, es decir una herramienta de gestión de riesgos de seguridad cibernética. (NIST, 2018)

Tesis publicada con autorización del autor
No olvide citar esta tesis

Antecedentes

Dentro de los antecedentes nacionales, se encuentran investigaciones vinculadas con la gestión del NIST, como Calderón que propone un plan de seguridad de la información con NIST basado en la norma ISO 27001 para mejorar la protección de datos en una empresa peruana de TI. Evalúa los riesgos y establece políticas de seguridad alineadas con estándares internacionales para mitigar amenaza. Su investigación es de tipo aplicativa, con un énfasis en la elaboración de una propuesta para optimizar la seguridad de la información; su diseño es no experimental y descriptivo, dado que se sugiere un plan fundamentado en la norma ISO 27001 sin alterar variables. Él finaliza en un esquema de seguridad de la información sugerido que facilita a la empresa mejorar sus políticas de seguridad, minimizando riesgos para que cumplan con estándares internacionales. (Calderón, 2018). también podemos mencionar a Apaza Tineo donde su investigación analiza cómo la adopción de medidas de ciberseguridad en compañías medianas del ámbito financiero puede disminuir la exposición a ciber incidentes, subrayando la relevancia de la capacitación y sensibilización del equipo; El enfoque de su investigación es descriptivo, centrado en examinar la adopción de medidas de ciberseguridad en empresas del sector financiero; tiene un diseño no experimental, de campo, pues recoge información de empresas medianas sin intervención directa; y en esa investigación concluye que las políticas de ciberseguridad son efectivas en la reducción de riesgos, pero la falta de formación adecuada en los empleados sigue siendo un desafío clave. (Apaza, 2020).

Tesis publicada con autorización del autor
No olvide citar esta tesis

También es importante mencionar la investigación de Pérez que evalúa la protección de la información en compañías peruanas empleando el marco NIST, reconociendo las vulnerabilidades más significativas y sugiriendo mejoras, su investigación es de carácter cuantitativa, con el propósito de Cuantificar la seguridad de la información en compañías peruanas, su diseño es no experimental, transversal, utilizando el marco NIST para la valoración de vulnerabilidades y termina concluyendo que las empresas evaluadas presentan deficiencias en la función de detección del NIST, lo que expone a las organizaciones a ataques no detectados a tiempo. (Peréz, 2019)

Marco Teórico

Es en este contexto se plantea esta investigación. El problema central que abordamos es el siguiente:

¿En qué medida un modelo de ciberseguridad permite mejorar la seguridad de la información, basada en NIST en la empresa TPX, 2023?

Para responder a esta pregunta, se analizó toda la empresa en detalle y en cada una de las dimensiones, explorando estrategias y mejores prácticas que permitan a las organizaciones fortalecer su resiliencia cibernética en un entorno empresarial dinámico y desafiante. La investigación busca proporcionar un marco estratégico y soluciones prácticas que ayuden a las empresas a superar impases de ataques informáticos y así mejorar la protección de sus activos

Tesis publicada con autorización del autor
No olvide citar esta tesis

críticos de manera efectiva. Y para ello nos hacemos preguntas específicas como:

¿En qué medida la implementación de un modelo de ciberseguridad basado en NIST mejora la identificación de riesgos y activos críticos en la seguridad de la información en la empresa TPX, 2023?

Y es aquí donde se considera que es una parte crucial e importante poder saber identificar las amenazas, y tener claro los riesgos y los activos críticos en la empresa es de suma importancia. Esta tesis logra demostrar que la implementación del modelo de ciberseguridad NIST mejora notablemente la identificación de riesgos y activos críticos en organizaciones como TPX (2023), al facilitar la priorización de acciones de protección. Este enfoque es respaldado por Peréz (2019), quien destaca su utilidad en detectar deficiencias en los procesos de identificación, y por Schneier (2009), quien enfatiza la importancia de identificar amenazas y activos como base de una gestión de seguridad efectiva.

Pero una vez identificadas cual sería la siguiente acción inmediata para continuar, entonces nos hacemos la siguiente pregunta:

¿En qué medida la adopción de controles de ciberseguridad basados en NIST fortalece la protección de la información sensible en la empresa TPX, 2023?

Las medidas preventivas a través de los ya conocidos ataques es importante saber tomarlas y para ello debemos de conocer cómo se presentan los diferentes ataques.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Bruce Schneier señala que: “EL auténtico problema de la seguridad en las comunicaciones no es la criptografía sino el resto del proceso” Schneier, (2009). Se refiere entonces a que no es la herramienta que podamos usar para protegernos sino el resto de los procesos, y es cuando hacemos la siguiente pregunta:

¿En qué medida la implementación de un modelo de ciberseguridad basado en NIST optimiza la detección temprana de incidentes de seguridad en la empresa TPX, 2023? La tesis sostiene que se debe hacer mejoras en la detección temprana de actividades sospechosas para evitar la sustracción de los activos críticos.

De esta forma nace nuestra siguiente duda:

¿En qué medida la aplicación de estrategias de respuesta basadas en NIST mejora la eficiencia en la gestión de incidentes de seguridad en la empresa TPX, 2023?. Si tenemos que preocuparnos en el proceso debemos preocuparnos también en las mejores prácticas y enfoques para desarrollar planes de respuesta eficaces en las empresas como TPX.

Bhagwani & Balasinorwala (2023) resalta la importancia de mantenerse alerta y proactivo frente a las crecientes amenazas cibernéticas. Es importante para una empresa continuar y más aún saber cómo recuperarse de un terrible ataque hay casos de empresas que fueron atacadas y perdieron información valiosa como lo fue en el 2020 la empresa eléctrica EDP de España; extorsionándola con millones de euros y amenazándola con publicar la información de miles de sus clientes. Es por ello que se realizó la siguiente pregunta: ¿En qué medida la aplicación de mecanismos de recuperación basados en NIST mejora la

Tesis publicada con autorización del autor
No olvide citar esta tesis

continuidad operativa de la empresa TPX, 2023? La respuesta a como planificar y ejecutar una estrategia de recuperación es una pregunta que nos llevará a meternos a evaluar y entender aspectos señalados por el NIST y que lo desarrollé a lo largo de la tesis, como veremos a continuación.

Hay que señalar que a nivel mundial según el Instituto AV-TEST, se detectan más de 390,000 programas de malware al día en el mundo. De esta forma hay abundantes cantidades de programas maliciosos para elegir objetivos. Esto sólo por la cantidad ya es un peligro inminente.

Zimroz (2022), en su Investigación llamada “Marco de Ciberseguridad del NIST y criterios de ciberseguridad MITRE” nos aclara que toma dos marcos de ciberseguridad, uno es el NIST y el otro el MITRE ambos marcos tienen como objetivo desarrollar enfoques y controles de resiliencia cibernética para mitigar los ataques cibernéticos maliciosos. Proporcionando a las organizaciones las herramientas y el conocimiento para poder proteger datos, información y activos críticos valiosos, de las amenazas cibernéticas, garantizando de alguna manera siempre la confidencialidad, integridad y disponibilidad de la información. (NIST Cybersecurity Framework and MITRE Cybersecurity Criteria, n.d.)

Cymerman (2010) señala que Irán sufrió el 27 de septiembre del 2010, fue el primer ataque cibernético más increíble de la historia del planeta. Cuando Irán sufrió un ataque informático contra sus instalaciones nucleares. Algo que hasta ese momento nunca se había visto en la historia.

Tesis publicada con autorización del autor
No olvide citar esta tesis

El ataque global de ransomware, WannaCry, se extendió por múltiples continentes y organizaciones el viernes 12 de mayo de 2017. Aunque no fue un objetivo directo, una de las mayores víctimas de este ataque fue el Servicio Nacional de Salud (NHS) de Inglaterra. NAO(2017).

A pesar de contar con profesionales de la seguridad TI, como el Dr. Chema Alonso entre sus filas, TELEFÓNICA también fue una de sus víctimas.

Goncalves & Serrao (2021) presentan una base para desarrollar un modelo genérico y flexible para manipular los factores clave dentro de las organizaciones: proceso, recursos humanos, tecnología, etc. También presentan una fórmula para extrapolar el porcentaje de cumplimiento del marco de ciberseguridad del NIST y medir la ciberseguridad actual. El riesgo y asignación de inversiones financieras son objetivos de cumplimiento específicos, así como reducción de la superposición de recursos actuales. (Security and Privacy Controls for Information Systems and Organizations, n.d.)

Boden (2017) nos dice que los superordenadores no bastan, pero la explosión combinatoria para la que se requiere más cálculos de los que se pueden realizar es inminente y es por ello que en la investigación que se hizo hasta el momento del presente (2023) ya hay algunos pininos donde podemos ver que IBM ha desarrollado algunas librerías para que se pueda trabajar con computadoras cuánticas y la I.A. (Inteligencia Artificial) juntas estableciendo una especie de puente que sería como la siguiente evolución para las próximas defensas frente a ataques muy complejos, así que también la ciberseguridad tendrá que trabajar

Tesis publicada con autorización del autor
No olvide citar esta tesis

en ese aspecto y es una tarea aún más compleja, y por ello se debe de comenzar antes que sea demasiado tarde.

Möller, (2023). según el trabajo de Dietmar Moller señala que el objetivo de NIST y MITRE es desarrollar enfoques y controles de resiliencia cibernética para mitigar los ataques cibernéticos maliciosos. La resiliencia cibernética permite anticipar, resistir, recuperarse y adaptarse a condiciones adversas, tensiones, ataques cibernéticos o compromisos en sistemas de información, redes, recursos de infraestructura y otros.

Es importante destacar que mientras el espacio cibernético siga creciendo a nivel comercial, los ciberdelincuentes se verán más interesados en buscar nuevas estrategias para llevar a cabo sus estafas. (Álvarez, 2018).

Un ataque a una empresa pequeña podría tener un costo de 100 mil dólares, pero si es a una institución, organización social o al mismo Estado, el daño sería irreparable, lo que implicaría no solo la pérdida de activos, sino también la confianza de los inversionistas. (Ormachea, 2020).

Vivanco, Bolaños & Angulo (2020) comentan, que un porcentaje de las víctimas de ataques por Ransonware, lamentablemente, han pagado el rescate, como en 2012, cuando Symantec pudo desmantelar una red de Comando y Control (una clase de ataque cibernético) que había sido atacada por el ransomware CryptoDefense. La investigación posterior al ataque reveló que el 2,9% de las víctimas, de un total de 68 mil infecciones pagaron por el rescate. también

Tesis publicada con autorización del autor
No olvide citar esta tesis

372.600 millones de ataques de ransomware a consumidores, empresas y pymes. De ellos, el 17% estaban dirigidos a todo tipo de empresas, y los consumidores o usuarios representaban la mayoría de los ataques.

León, (2021) nos dice que lamentablemente existe el acceso no autorizado por parte de ciberdelincuentes, que roban el conocimiento esencial de las instituciones. Esto teniendo en cuenta que todas las organizaciones requieren y exigen el uso de tecnologías, pero muchas de ellas no saben manejarlo; en cuanto a ciberseguridad se refiere, esto significa que no cuentan con una metodología para la detección de incidentes.

Santos (2020) Indica que hay una gran preocupación por los riesgos que están expuestas las instituciones gubernamentales, empresas y sobre todo los ciudadanos.

El NIST CSF pretende básicamente ser una guía de las actividades de ciberseguridad. El Framework está formado por tres componentes (Ilustración 3): El núcleo del marco de trabajo, los niveles de implementación del framework

Ilustración 3: Componentes de Ciberseguridad del NIST (2018)



Fuente: NIST v.1 (2018)

Tesis publicada con autorización del autor
No olvide citar esta tesis

y los perfiles del framework. En 2023 lanzan en evaluación la nueva versión donde se visualiza mayor integración con todos los componentes en la ilustración 4.

Ilustración 4: Componentes de Ciberseguridad NIST (2023)



Fuente: NIST v.2 (2023)

El núcleo del marco abarca un conjunto de tareas y recursos informativos acerca de ciberseguridad para infraestructuras esenciales. Los niveles de ejecución proporcionan contexto acerca de cómo una entidad maneja los riesgos de ciberseguridad. Al contrastar el perfil vigente con el perfil deseado, los perfiles del marco reflejan tanto la situación actual como la situación anhelada de una organización y permiten identificar oportunidades para mejorar la ciberseguridad.

Justificación

La elección de llevar a cabo mi investigación en torno a la “Aplicación de la Metodología NIST en la Mejora de la Ciberseguridad de la empresa TPX, 2023” se justifica por varias razones fundamentales:

Tesis publicada con autorización del autor
No olvide citar esta tesis

Justificación Teórica

La creciente amenaza de ciberataques y la complejidad de los entornos tecnológicos actuales requieren que las empresas adopten metodologías sólidas y comprobadas para garantizar la ciberseguridad. En este contexto, la metodología del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) se ha destacado como un marco fundamental para la gestión de riesgos de ciberseguridad.

El Marco de Ciberseguridad del NIST (NIST CSF) ofrece una perspectiva estructurada para detectar, protegerse, responder, recuperarse y establecer medidas de protección ante ciberamenazas. Según el NIST (2018), “el Marco de Ciberseguridad se ha convertido en una herramienta ampliamente adoptada que apoya a las instituciones en la gestión y disminución eficiente de los riesgos relacionados con la ciberseguridad” (NIST, 2018, p. iv). Este marco se fundamenta en cinco funciones clave que permiten a las organizaciones manejar sus riesgos de ciberseguridad de forma integral y continua.

La relevancia de implementar la metodología NIST en las organizaciones se centra en su orientación fundamentada en riesgos. Según Ross et al. (2018), “la gestión de riesgos de ciberseguridad debe ser un componente integral de la estrategia organizacional, y el NIST CSF proporciona una base sólida para lograrlo” (Ross & McEvilley, 2018). Este enfoque permite a las organizaciones

Tesis publicada con autorización del autor
No olvide citar esta tesis

priorizar sus recursos y esfuerzos en función de los riesgos más críticos, lo cual es esencial en un entorno donde los recursos son limitados.

Además, el NIST CSF promueve la mejora continua de la ciberseguridad a través de su ciclo de vida de gestión de riesgos. “El marco enfatiza la necesidad de evaluar y ajustar continuamente las estrategias de ciberseguridad en respuesta a la evolución de las amenazas y las vulnerabilidades” (Bowen, P., Hash, J., & Wilson, M., 2018, p. 4). Esta capacidad de adaptación es crucial para mantener la resiliencia frente a ciberamenazas dinámicas y sofisticadas.

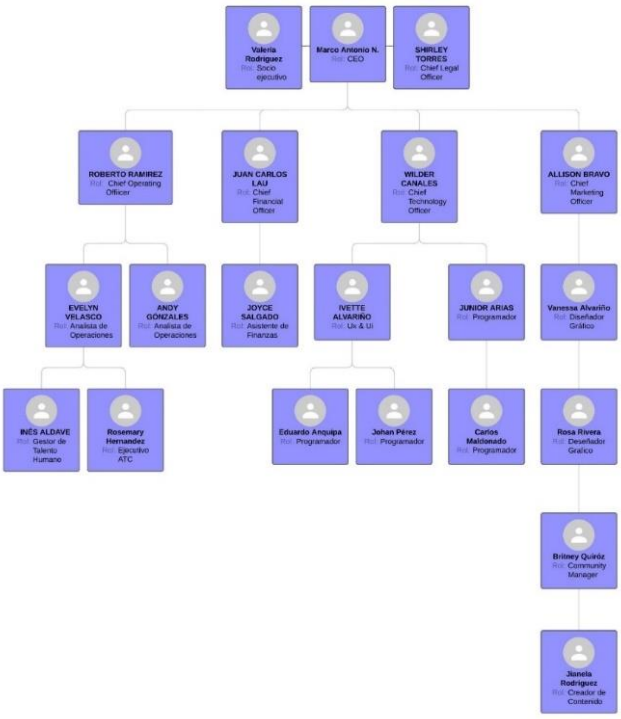
En el caso de la empresa TPX, la aplicación de la metodología NIST permitió una evaluación detallada de sus activos críticos de información y la implementación de controles de seguridad adecuados. Según Johnson et al. (2019), “la identificación y protección de los activos de información críticos es fundamental para la continuidad del negocio y la protección de los datos sensibles” (Johnson & Dempsey, 2019). La metodología NIST proporciona un marco para llevar a cabo esta evaluación de manera sistemática y eficaz.

Por último, la adopción de estándares y marcos reconocidos internacionalmente, como el NIST CSF, puede mejorar la confianza de los clientes y socios comerciales en la capacidad de la empresa para gestionar riesgos de ciberseguridad. Como señala Lipner (2018), “la alineación con marcos de ciberseguridad reconocidos puede fortalecer la reputación de una empresa y proporcionar una ventaja competitiva en el mercado” (Lipner, 2018).

Tesis publicada con autorización del autor
No olvide citar esta tesis

Podemos inferir entonces que, la aplicación de la metodología NIST en la empresa TPX no solo mejorará su postura de ciberseguridad, sino que también proporcionará una base sólida para la gestión continua de riesgos y el fortalecimiento de la confianza de sus partes interesadas.

Ilustración 5: Estructura organizativa de la empresa TPX



Fuente: Elaboración propia

Justificación Práctica

La ciberseguridad se ha convertido en una parte muy importante del mundo empresarial actual, donde la interconexión global y la constante evolución tecnológica han incrementado significativamente la exposición de las organizaciones a riesgos cibernéticos. La amenaza de ataques cibernéticos, la

Tesis publicada con autorización del autor
No olvide citar esta tesis

pérdida de datos confidenciales y la interrupción de las operaciones empresariales plantean desafíos críticos que requieren una atención inmediata y efectiva.

La aplicación de la metodología NIST en la mejora de la ciberseguridad de la empresa TPX se justifica por su foque holístico, su reconocimiento global, su flexibilidad en diversos contextos empresariales y su aptitud para ofrecer un marco organizado para la administración de riesgos y facilitar la ejecución de controles de seguridad.

Sin embargo, a pesar de la reconocida eficacia de NIST, la implementación exitosa de esta metodología no está exenta de desafíos. Las empresas se enfrentan a limitaciones que van desde restricciones presupuestarias hasta la falta de acceso a datos de incidentes cibernéticos, lo que dificulta la aplicación práctica de estrategias basadas en datos.

Es en este contexto que surge la necesidad de esta investigación. Este trabajo “Aplicación de la Metodología NIST en la Mejora de la Ciberseguridad de la Empresa TPX, 2023” busca abordar la constante evolución de ataques con equipos tecnológicos y con mejores desarrollos en ciberataques donde la evolución con distintos tipos de ataques por ejemplo ahora con ayuda de la I.A., en diferentes lenguajes, para determinados servidores y hasta para el uso de nuevos sistemas operativos con nuevas brechas de seguridad; se tiene que planificar estrategias de recuperación pero que sean eficientes para la continuidad de la operación.

Tesis publicada con autorización del autor
No olvide citar esta tesis

La relevancia de esta investigación radica básicamente en su capacidad para proporcionar a la empresa TPX soluciones prácticas y estrategias adaptadas a las condiciones del entorno empresarial actual dejando el conocimiento de cómo se encuentra la ciberseguridad de la empresa. Se espera siempre que los hallazgos de esta investigación beneficien tanto a las organizaciones que buscan mejorar su seguridad cibernética como para los profesionales y académicos abocados en el campo de la ciberseguridad empresarial.

Así de esta manera la investigación aborda los desafíos específicos que enfrentan las empresas, y contribuirá al desarrollo de enfoques más flexibles y aplicables de la metodología NIST. Además, ofrece al final las recomendaciones concretas para superar obstáculos y mejorar la ciberseguridad en un entorno empresarial en constante evolución y cada vez más digitalizado.

Problemas

Primeramente, la empresa era consciente de que tenía vulnerabilidades frente a sus activos críticos de información en torno a la ciberseguridad que después de un análisis la empresa TPX era sobre todo afectada por la ausencia de una metodología estructurada que permitiría gestionar de manera eficaz los riesgos cibernéticos. A medida que las amenazas digitales se incrementan y diversifican, la empresa carece de un sistema robusto que integre los procesos de identificación, prevención, detección, respuesta y recuperación ante incidentes de ciberseguridad. Si esto no es atendido, se pone en riesgo la integridad, confidencialidad y disponibilidad de sus activos de información, afectando su continuidad operativa y la confianza de sus clientes.

Tesis publicada con autorización del autor
No olvide citar esta tesis

En este contexto, surge la necesidad de analizar de qué manera la aplicación efectiva de la metodología NIST puede mejorar la ciberseguridad de la empresa TPX, optimizando sus capacidades en cada una de las dimensiones mencionadas y permitiéndole enfrentar los desafíos actuales en materia de ciberseguridad.

De acuerdo con el trabajo de investigación y al no tener catalogado el activo critico dentro de la empresa, se desarrolló un catálogo de activos críticos realizando así una matriz de información. Todo esto con la finalidad de detectar activos críticos, para colocar los controles del NIST.

Siempre teniendo en cuenta que "Los activos de información son datos, sistemas y otra información valiosa que las organizaciones necesitan proteger. Esto incluye información física y electrónica, propiedad intelectual y secretos comerciales" (ISO/IEC, 2018).

Tabla 2: Matriz de Información crítica de la empresa TPX

Nombre del Activo	Descripción	Confidencial	Integridad	Accesibilidad	Niveles de Riesgo
					HIGH
		C	I	A	MEDIUM
					LOW
Servidor de Base de Datos	Contiene todos los datos críticos de clientes, operaciones y finanzas.	C3	I3	A1	ALTO
Sistemas de Gestión ERP	Plataforma central para la gestión de recursos empresariales y operaciones.	C2	I2	A3	ALTO
Red Interna Corporativa	Infraestructura de comunicación interna entre empleados y sistemas.	C3	I2	A3	ALTO
Servidor de Correo Electrónico	Maneja todas las comunicaciones	C2	I3	A3	ALTO

Tesis publicada con autorización del autor
No olvide citar esta tesis

	internas y externas.				
Plataforma de Comercio Electrónico	Portal en línea para ventas y servicios al cliente.	C3	I2	A3	ALTO
Sistema de Gestión de Clientes (CRM)	Base de datos y herramientas para gestionar las relaciones con los clientes.	C2	I2	A3	ALTO
Sistema de Backup y Recuperación	Soluciones para la copia de seguridad y recuperación de datos críticos.	C3	I2	A3	ALTO

Fuente: Elaboración Propia

Tabla 3: Matriz de Calor

		Baja	Medio	Alto
NIVELES DE RIESGO		1	2	3
Alto	3	**4**	**8**	**16**
Medio	2	**3**	**6**	**12**
Baja	1	**2**	**4**	**8**

Tabla 4: Principios básicos de la Información

INFORMACIÓN		
DISPONIBILIDAD	**INTEGRIDAD**	**CONFIDENCIALIDAD**
Garantizar que la información se encuentre a disposición de quienes deben acceder a ella.	Busca que la totalidad de la información esté protegida, para garantizar que este exenta de modificaciones de usuarios no autorizados	Prevenir la divulgación de información a personas no autorizadas.

Objetivos de la Investigación

Objetivo General

Implementar un modelo de ciberseguridad para mejorar la seguridad de la información, basada en NIST en la empresa TPX, 2023

Tesis publicada con autorización del autor
No olvide citar esta tesis

Objetivos Específicos

Para lograr alcanzar el objetivo principal como se debe, se plantean los siguientes objetivos específicos:

- Mejorar la identificación de riesgos y activos críticos en la empresa TPX mediante la metodología NIST.

- Fortalecer la protección de la información sensible a través de estrategias de seguridad de la metodología NIST.
- Optimizar la detección de amenazas con sistemas de monitoreo y alertas basados en NIST.
- Aumentar la eficiencia en la respuesta a incidentes mediante protocolos definidos en la metodología NIST.
- Garantizar una rápida recuperación y continuidad operativa con planes de contingencia basados en NIST.

Hipótesis de la Investigación

Basados en la revisión exhaustiva de la literatura y en la comprensión de las dinámicas actuales de las Tecnologías y la ciberseguridad empresarial, formulamos la siguiente hipótesis de investigación:

Tesis publicada con autorización del autor
No olvide citar esta tesis

Hipótesis General

El modelo de ciberseguridad permite mejorar la seguridad de la información, basada en NIST en la empresa TPX, 2023

Hipótesis Específicas

• La aplicación de la metodología NIST permite una mejor identificación de riesgos y activos críticos en la empresa TPX.

• La adopción de controles de ciberseguridad basados en NIST mejora significativamente la protección de la información en la empresa TPX.

• La implementación del modelo NIST incrementa la detección temprana de incidentes de ciberseguridad en la empresa TPX.

• La metodología NIST optimiza la capacidad de respuesta ante incidentes de seguridad en la empresa TPX.

• La aplicación de mecanismos de recuperación basados en NIST garantiza la continuidad operativa de la empresa TPX.

4 Materiales y Métodos

4.1 Tipo de la Investigación:

Aplicada Según, Baena (2017), el tipo de investigación aplicada trata de darle un desenlace a una cuestión específica dentro de una realidad convirtiendo la teoría en una experiencia para generar nueva información que sea de utilidad

Tesis publicada con autorización del autor
No olvide citar esta tesis

4.2 Diseño y Corte de la Investigación

El diseño de esta investigación es de tipo pre-experimental. Según Creswell presenta una visión práctica para investigadores: “cuando no es posible realizar un experimento verdadero, los diseños pre-experimentales (p. ej., estudio de un solo grupo) pueden usarse para explorar efectos preliminares, aunque recomienda pasos para mitigar sesgos y para justificar su uso." (Creswell J. W., 2014). Por otro lado el corte de la investigación es transversal; Cvetković nos dice que “El elemento clave que define a un estudio transversal es la evaluación de un momento específico y determinado de tiempo.” (Cvetković-Vega, 2021)

4.3 Enfoque de la Investigación

Se destacan que la investigación cuantitativa permite abordar problemas de investigación complejos, logrando una mayor profundidad y amplitud en la comprensión del fenómeno estudiado (Hernández-Sampieri, & Mendoza. 2018)

4.4 Nivel de Investigación

El nivel de investigación es explicativo, Según Sampieri nos dice ”El nivel explicativo se enfoca en dar respuesta a las causas de los fenómenos y eventos sociales o físicos. Se centra en describir por qué ocurre un fenómeno y bajo qué condiciones, o por qué dos o más variables están relacionadas.” *(Sampieri, Fernández & Baptista, 2014, p. 91)*

4.5 Población y Muestra

Según el autor Arias (2006, p. 81) define población como “un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Esta queda delimitada por el

Tesis publicada con autorización del autor
No olvide citar esta tesis

problema y por los objetivos del estudio". La población está compuesta por la totalidad de la empresa TPX que es un total de 30 empleados. Cabe señalar que los sujetos de estudió no van a sufrir ninguna afectación de su integridad científica.

Según el autor Arias (2006, p. 83) define muestra como "un subconjunto representativo y finito que se extrae de la población accesible". La muestra consistirá en una selección representativa de diferentes departamentos o divisiones dentro de la organización que aborden las temáticas relevantes para el estudio, en este caso son: departamento de operaciones, departamento de marketing, departamento legal, departamento de Ux & Ui, departamento de tecnología.

En esta investigación, se ha incluido a toda la población compuesta por el personal administrativo, de ventas, de soporte, de desarrollo, del área logística, del área contable, es decir todas las áreas; los cuales desempeñan cualquier tipo de riesgo frente a un ataque, el cual se necesita asegurar y es parte del análisis de mejora para el estudio. Es importante señalar que la población de estudio está compuesta por (30) profesionales que están familiarizados con y trabajan en la empresa TPX. En consecuencia, no se ha tomado en cuenta ningún tamaño de muestra, ni muestreo alguno en esta investigación, ya que se han incluido todos los elementos de la población analizada.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Ilustración 6: Calculadora de Muestra



Fuente: Questionpro

Variable Dependiente: Ciberseguridad. La ciberseguridad es la práctica de defender los sistemas, redes y programas de ataques digitales, que generalmente están dirigidos a acceder, cambiar o destruir información sensible (Hernández & Santos, 2019).

Variable Independiente: Aplicación de la Metodología NIST. Según la National Institute of Standards and Technology (NIST), Tiene que entenderse que es la metodología que se refiere a un marco que ayuda a las organizaciones a entender, gestionar y reducir sus riesgos de ciberseguridad, y protege la infraestructura crítica (NIST, 2018).

4.6 Instrumentos

El instrumento que se emplea es una encuesta de 20 preguntas sobre la variable dependiente la mejora en la postura de ciberseguridad de la empresa TPX y midiendo a las 5 dimensiones tales como: Identificación, Prevención, Detección, Respuesta, Recuperación. El *NIST Cybersecurity Framework* en sí mismo

Tesis publicada con autorización del autor
No olvide citar esta tesis

describe las cinco funciones clave (Identificar, Proteger, Detectar, Responder y Recuperar) como componentes esenciales para gestionar y reducir el riesgo cibernético; y como nos señala Marianne M.(2003) sobre la evaluación basada en cuestionarios: ASSET emplea un formato de cuestionario para evaluar la postura de seguridad de los recursos de tecnología de la información. Los evaluadores, incluidos los evaluadores primarios y secundarios, son responsables de garantizar que se respondan todas las preguntas del cuestionario. Este enfoque estructurado permite una evaluación integral de las medidas de seguridad utilizando NIST.

Por último, la encuesta fué evaluada por un veredicto de cuatro especialistas. Palella y Martins (2012) mencionan que el cuestionario es un instrumento que se encuentra dentro de una técnica de encuesta, la cual incluye instrucciones exactas y claras para facilitar una solución.

También se revisará se examinar políticas, procedimientos, informes de incidentes de seguridad y otros documentos.

Tabla 5: Análisis de fiabilidad para D1, D2, D3, D4, D5

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,976	20

La consistencia interna indica el grado de que los ítems diseñados del instrumento evalúen el mismo constructo con puntuaciones similares.

Se utiliza el alfa de Cronbach para determinar el nivel de consistencia interna del instrumento.

El Alpha de Cronbach posee valores entre 0 y 1 Mientras más cercano a 1 mejor es la confiabilidad del instrumento.

Análisis de fiabilidad (D1 D2 D3 D4 D5-p1 p2 p3 p4)

Tesis publicada con autorización del autor
No olvide citar esta tesis

Fuente: Elaborado de forma Propia a través del software IBM SPSS v.28

La confiabilidad de las variables D1 D2 D3 D4 D5 es muy satisfactoria

Tabla 6: Evaluación de Cuestionario

EXPERTO	INSTRUMENTO: CUESTIONARIO				EVALUACIÓN
	SUFICIENCIA	CLARIDAD	RELEVANCIA	SUFICIENCIA	
EXPERTO 1	Si	Si	Si	Si	Aplica
EXPERTO 2	Si	Si	Si	Si	Aplica
EXPERTO 3	Si	Si	Si	Si	Aplica
EXPERTO 4	Si	Si	Si	Si	Aplica

Fuente: Elaboración Propia

La tabla 6 Indica que se evaluó a cuatro expertos y que el cuestionario es aplicable en relación con la variable dependiente. También se ha examinado la matriz operacional y la matriz de consistencia.

Tabla 7: Escala Likert

Puntuación	Calificación
1	Totalmente Desacuerdo
2	En Desacuerdo
3	Indiferente
4	De Acuerdo
5	Totalmente de Acuerdo

Fuente: Elaboración Propia

En la **tabla 7** El instrumento elaborado en escala Likert se valida con una lista de veinte preguntas, numeradas del 1 al 5 y con su calificación correspondiente.

5 Procedimientos (pasos y aportes tecnológicos)

Evaluación Inicial

El primer paso consistió en realizar un análisis de sus activos críticos y el resultado se muestra en la tabla 2 (pág. 40) que es un catálogo de activos críticos realizando así una matriz de información. Para posteriormente pasar de cómo se encontraba la empresa y realizar un AS IS donde el resultado se muestra de la siguiente manera:

Tesis publicada con autorización del autor
No olvide citar esta tesis

Tabla 8: Matriz AS IS situación actual de Ciberseguridad en la empresa TPX

DIMENSIÓN	SITUACIÓN ACTUAL (AS IS)	PROBLEMÁTICA DETECTADA
Gestión de Activos	La empresa no cuenta con un inventario formal y actualizado de activos de información. No hay una gestión estructurada de activos críticos.	- Falta de un catálogo de activos críticos (bases de datos, servidores, dispositivos de red). - No se han clasificado los activos según su nivel de criticidad y confidencialidad. - No existe una matriz clara de riesgos asociados a cada activo. - Falta de asignación de propietarios responsables de cada activo.
Protección de Activos Digitales	Se han implementado medidas básicas de seguridad, pero son insuficientes para garantizar la protección de los activos digitales.	- Falta de cifrado de datos en reposo y en tránsito. - Uso de contraseñas débiles sin una política estricta de autenticación. - Controles de acceso inadecuados (accesos concedidos sin justificación ni revisión periódica). - Ausencia de un sistema centralizado de gestión de identidad y accesos (IAM).
Detección de Amenazas	La detección de incidentes es manual y reactiva, con herramientas insuficientes para la identificación temprana de amenazas.	- No se cuenta con un sistema de monitoreo en tiempo real para detectar accesos no autorizados. - Falta de correlación de eventos de seguridad (SIEM). - No existen mecanismos para la identificación proactiva de vulnerabilidades en la infraestructura. - Respuesta tardía ante incidentes debido a la falta de visibilidad de los activos expuestos.
Respuesta a Incidentes	La empresa tiene procedimientos básicos de respuesta a incidentes, pero no están estandarizados ni alineados con un marco de mejores prácticas.	- No existe un plan formal de respuesta a incidentes basado en NIST. - La gestión de incidentes depende de la experiencia del personal y no de procedimientos establecidos. - Falta de roles y responsabilidades definidas en caso de un ciberataque. - No se realizan simulacros ni entrenamientos en respuesta a incidentes.
Recuperación y Continuidad	No se han implementado estrategias adecuadas de recuperación y continuidad operativa tras incidentes de seguridad.	- No se han implementado planes de recuperación ante desastres (DRP). - Falta de respaldo regular de los datos críticos y ausencia de pruebas de restauración. - No existen estrategias de redundancia para minimizar el impacto de un ciberataque. - La empresa no tiene acuerdos de recuperación con proveedores externos.

Fuente: Elaboración propia

Tesis publicada con autorización del autor
No olvide citar esta tesis

Tras realizar una evaluación exhaustiva del estado actual (AS IS) de la ciberseguridad en la empresa TPX, se implementó un proceso de medición en dos fases. En primer lugar, se utilizó el Baldrige Cybersecurity Excellence Builder como herramienta de evaluación, midiendo la madurez de la ciberseguridad de la empresa en función de 4 ejes Enfoque, Implementación, Aprendizaje, Integración, Posteriormente, se aplicó el NIST Cybersecurity Framework (CSF) con el fin de profundizar en el análisis. Teniendo en cuenta que se realizó una previa identificación de activos críticos de información, para luego realizar el análisis de riesgos asociados para finalmente revisar las políticas y procedimientos de seguridad vigentes (NIST. 2018)

A continuación, procedemos con la evaluación del Baldrige Cybersecurity Excellence.

A) El Baldrige Cybersecurity Excellence Builder

Contexto Organizacional

Como empresa de marketing, TPX maneja datos sensibles de clientes, campañas publicitarias, y información de clientes relacionados con la segmentación de mercado. Esto implica que TPX debe garantizar la confidencialidad, integridad y disponibilidad de la información.

Entorno Operativo: TPX utiliza una infraestructura de TI que soporta actividades de marketing digital, CRM, almacenamiento de datos a nivel local on- premise y en la nube, plataformas de comunicación y colaboración

Tesis publicada con autorización del autor
No olvide citar esta tesis

con clientes, así como software de diseño gráfico y análisis de datos con ERP.

Enfoque

Nivel Actual: Es Reactivo. TPX está en una fase donde la ciberseguridad se aborda sin una estructura clara, aplicando medidas de seguridad principalmente en respuesta a incidentes.

Evaluación de Madurez: En esta etapa, TPX carece de una estrategia de ciberseguridad definida y se enfrenta a limitaciones debido a la falta de procedimientos estandarizados y una visión clara de ciberseguridad. En términos de madurez, TPX se encuentra en el inicio del ciclo de desarrollo.
Recomendación para Avanzar en Madurez: TPX debería trabajar en formalizar una estrategia de ciberseguridad documentada, creando procesos que incluyan políticas, roles y responsabilidades específicas. Esto les permitiría avanzar hacia un estado “En desarrollo” o incluso “Maduro”.

Implementación

Nivel Actual: Temprano. Los procesos de ciberseguridad en TPX son inconsistentes y no se aplican de manera uniforme en toda la organización.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Evaluación de Madurez: La implementación irregular indica que TPX aún no ha integrado la ciberseguridad en sus operaciones diarias de manera sistemática. En el marco de Baldrige, esto sugiere una etapa de inmadurez, donde la organización apenas está comenzando a aplicar procesos de ciberseguridad básicos.

Recomendación para Avanzar en Madurez: TPX debe establecer una práctica consistente de ciberseguridad en toda la organización, creando procedimientos estándar aplicables a todos los departamentos y sistemas críticos. Este paso los acercaría al nivel "En desarrollo".

Aprendizaje

Nivel Actual: En desarrollo para la mejora de procesos y Temprano en compartir mejoras.

Evaluación de Madurez: TPX aún no tiene un sistema formal para evaluar o mejorar sus procesos de ciberseguridad, y la difusión de mejoras dentro de la organización es limitada. En el modelo de Baldrige, esto indica una madurez incipiente.

Recomendaciones para Avanzar en Madurez: TPX debería instituir revisiones periódicas de ciberseguridad y prácticas de retroalimentación, asegurando que las mejoras se compartan de manera efectiva en la organización. Crear un proceso de aprendizaje y mejora continua ayudará a TPX a progresar hacia una madurez "Maduro" o "Líder".

Tesis publicada con autorización del autor
No olvide citar esta tesis

Integración

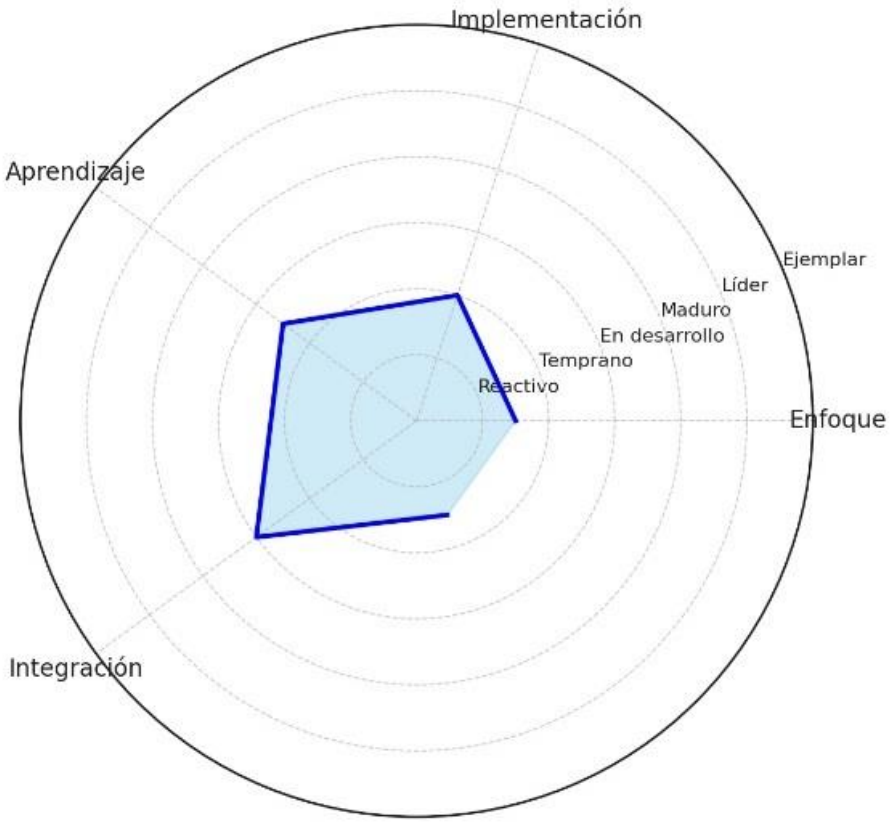
Nivel Actual: En desarrollo. Los procesos de ciberseguridad en TPX satisfacen algunas necesidades actuales, pero no hay un plan sólido para necesidades futuras.

Evaluación de Madurez: En el modelo de Baldrige, TPX se encuentra en una fase de madurez reactiva en términos de integración. La falta de una visión a futuro y la integración limitada indican que la organización aún no ha consolidado sus prácticas de ciberseguridad en todos los aspectos de su operación.

A continuación, se realiza un análisis inicial ya que no existía ningún análisis previo, para lograr mostrar el grado de madurez de la empresa TPX; y de esta manera tenemos el resultado de la evaluación del nivel de madures usando la herramienta Baldrige Cybersecurity Excellence Builder, que a su vez nos sirve como indicador en la investigación, y se puede visualizar lo siguiente:

Tesis publicada con autorización del autor
No olvide citar esta tesis

Ilustración 7: Evaluación de Madurez en Ciberseguridad de la Empresa TPX



Fuente: Elaboración propia

Y para este resultado se tiene que los 4 ejes comprenden:

- Implementación (20%): Representa que solo el 20% de las políticas o controles de ciberseguridad se encuentran implementados.
- Enfoque (25%): El enfoque es parcial, con políticas iniciales y un desarrollo limitado.
- Integración (20%): Solo el 20% de las políticas están integradas en los procesos organizacionales.
- Aprendizaje (30%): Los empleados han alcanzado un 30% de nivel de madurez en capacitación y aprendizaje.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Los datos numéricos y las preguntas de encuesta reflejan la base realista del gráfico radar. La información cuantitativa (porcentajes) asignada proviene de las respuestas obtenidas en las encuestas aplicadas a empleados y responsables de las áreas. Este enfoque estructurado permite medir el nivel de madurez de la ciberseguridad de forma objetiva.

Tabla 9: Matriz de madurez de Ciberseguridad de la empresa TPX

Dimensión	Nivel Actual	Valoración Cuantitativa (%)	Descripción / Observaciones	Preguntas de Encuesta
Implementación	Reactivo	20%	Las medidas implementadas son mínimas y no estructuradas.	1. ¿Se cuenta con un plan de implementación de políticas de ciberseguridad? (Sí/No/Parcial) 2. ¿Qué porcentaje de las medidas propuestas ha sido implementado en el último año? (0-25%, 26-50%, etc.)
Enfoque	Reactivo	25%	El enfoque está en etapas iniciales con objetivos muy minimos.	1. ¿Existen políticas formales para la detección y mitigación de amenazas? (Sí/No/Parcial) 2. ¿Qué tan alineado está el enfoque de ciberseguridad con los objetivos de la empresa? (Bajo/Medio/Alto)
Integración	Reactivo	20%	La integración de prácticas y políticas es escasa.	1. ¿Se integran prácticas de ciberseguridad en todos los departamentos? (Sí/No/Parcial) 2. ¿Qué nivel de integración tienen las medidas en procesos diarios? (Nulo/Bajo/Medio/Alto)
Aprendizaje	En desarrollo	30%	Existe algunas capacitaciones parciales, pero faltan procesos formales.	1. ¿Se realizan capacitaciones regulares sobre ciberseguridad? (Sí/No/Ocasionalmente) 2. ¿Qué nivel de aprendizaje han logrado los empleados en buenas prácticas de seguridad? (Bajo/Medio/Alto)

Fuente: Evaluación Propia

Evaluación Global de Madurez de TPX en Ciberseguridad

Madurez General: La empresa TPX se encuentra en un nivel de madurez Temprano en Desarrollo en la mayoría de las áreas del Baldrige Cybersecurity Excellence Builder. (Enfoque, Implementación,

Tesis publicada con autorización del autor
No olvide citar esta tesis

Aprendizaje, e Integración.) Su enfoque inicial y sus procesos básicos reflejan una estructura de ciberseguridad incipiente, orientada más hacia la respuesta reactiva que hacia una prevención y protección proactiva.

Recolección de Datos:

Se utilizó técnicas de recolección de datos cuantitativos; así mismo se revisó cierta documentación accesible, como también entrevistas dirigidas a los encargados que manejan el departamento de TI y que tienen toma de decisión; adicionalmente se realizó encuestas a todo el personal que trabaje en la empresa, para comprender el estado actual de la ciberseguridad. Según John Creswell en "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches" (2014), esto permitirá una visión completa y detallada de la situación actual.

Tabla 10: Baremo de las 5 dimensiones

Escala y valores		
1	Totalmente desacuerdo	
2	En desacuerdo	
3	Indiferente	
4	De acuerdo	
5	Totalmente de acuerdo	
Dimensiones		
D1	Identificación	4 ítems
D2	Prevención	4 ítems
D3	Detección	4 ítems
D4	Respuesta	4 ítems
D5	Recuperación	4 ítems
	Total	20 ítems

Fuente: Elaboración Propia

Tesis publicada con autorización del autor
No olvide citar esta tesis

En la **tabla 10** se aprecia la medición, la escala de valores y las 5 dimensiones del NIST (identificación, prevención, detección, respuesta y recuperación) donde cada una de ellas está compuesta por 4 ítems medidas por la escala de Likert

2 Establecimiento de Métricas

Tabla 11: Nivel y Rango Variable General

Numero de niveles: 3 (inicio, proceso, logrado)

BAREMOS			
Niveles y rangos	**Inicio**	**Proceso**	**Logrado**
Identificación	[4-9]	[10-15]	[16- 21]
Prevención	[4-9]	[10-15]	[16- 21]
Detección	[4-9]	[10-15]	[16- 21]
Respuesta	[4-9]	[10-15]	[16- 21]
Recuperación	[4-9]	[10-15]	[16- 21]

Fuente: Elaboración propia

En la **tabla 11** tenemos las variables y dimensiones que se midieron en 3 escalas (inicio, proceso y logrado). En el baremo de la variable general, cada dimensión se calcula el valor máximo, mínimo, rango y amplitud, de esta forma se calculan los intervalos de cada uno de ellos.

Alineación de KPIs con las funciones del marco NIST

Se estableció la alineación de los indicadores clave de rendimiento (KPIs) con las funciones del marco NIST específicos de ciberseguridad, como el inventario de activos, cifrado de datos sensibles, cobertura del monitoreo, plan de respuesta y el tiempo de recuperación. Este paso está basado en el trabajo de Ron S. Kenett y Silvia Salini en "Modern Analysis of Customer Surveys: With Applications Using R" (2012).

Tesis publicada con autorización del autor
No olvide citar esta tesis

Tabla 12:Alineación de los KPI's con las Funciones del NIST de la Empresa TPX

FUNCIÓN NIST	KPI'S	LÍNEA DE BASE	OBJETIVO
Identificar	Inventario de activos actualizado	3%	70% en 3 meses.
	Evaluación de riesgos completada	10%	80% en 6 meses.
	Cumplimiento de políticas de seguridad	20%	90% en 10 meses.
Proteger	Protección de endpoints	80%	70% en 6 meses.
	Cifrado de datos sensibles	20%	80% en 8 meses.
	Acceso controlado	25%	80% en 8 meses.
Detectar	Tiempo promedio de detección (MTTD)	24 horas	12 horas en 6 meses.
	Cobertura de monitoreo	10%	80% en 7 meses.
	Alertas de seguridad atendidas	25%	70% en 24 horas.
Responder	Tiempo promedio de respuesta (MTTR)	72 horas	24 horas en 6 meses.
	Plan de respuesta a incidentes probado	0 simulacros	2 simulacros trimestrales.
	Incidentes reportados a autoridades	5%	80% en el presente año.
Recuperar	Tiempo de recuperación (RTO)	72 horas	24 horas en 7 meses.
	Pruebas de recuperación realizadas	0 pruebas	2 pruebas anuales.
	Backups verificados	40%	95% en 7 meses.

Fuente: Elaboración Propia

En la **tabla 12** nos muestra la medición claramente del estado actual ("línea base") de cada KPI para saber en qué situación está la empresa TPX frente a las funciones del NIST. Pero también se hace la alineación de los KPI's con las dimensiones del NIST y de esta manera se plantean objetivos claros y

Tesis publicada con autorización del autor
No olvide citar esta tesis

cuantificables para mejorar en un tiempo determinado (3, 6 u 8 meses). Al distribuirse los KPIs en las funciones del NIST, se asegura que todas las dimensiones de la ciberseguridad sean cubiertas (no solo tecnología, sino también procesos, tiempos de respuesta, recuperación, etc.). Y siempre pensando en la mejora continua.

B) Implementación de la Metodología NIST

A continuación, en el siguiente cuadro se muestra la ejecución de la metodología NIST CSF que se le hace a la empresa TPX. El nivel encontrado de niveles existentes versus los niveles recomendados del NIST en la empresa TPX, teniendo un assessment dando como resultado nuevos ajustes abocados a la ciberseguridad para la empresa en mención.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

EVALUACIÓN DE ACUERDO A LA MÉTODOLOGÍA NIST - EMPRESA TPX

Tabla 13: Evaluación de acuerdo con la Metodología NIST - Empresa TPX

N°	Función	Categoría	Identificador de Categoría	Estado Actual	Observación Estado Actual	Perfil Objetivo	Observación Perfil Objetivo		Observación
1	IDENTIFICAR (ID): Se conocen los riesgos de seguridad cibernética actuales de la organización	Gestión de activos (ID.AM): Los activos (p. ej., datos, hardware, software, sistemas, instalaciones, servicios, personas) que permiten a la organización alcanzar sus objetivos empresariales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización	ID.AM-01: Se mantienen inventarios del hardware gestionado por la organización	**2**	Parcialmente Implementado	Algunos planes incluyen actividades posteriores a la finalización del acuerdo, pero no está estandarizado para todos los proveedores.	3	Completamente Implementado	Todos los planes de gestión de riesgos incluyen disposiciones claras para las actividades una vez que finaliza una relación contractual con proveedores.
			ID.AM-02: Se mantienen inventarios de software, servicios y sistemas gestionados por la organización	**1**	No Implementado	Se tiene un inventario parcial muy antiguo de software y servicios, pero no existe uno actualizado ni integrado.	3	Completamente Implementado	Todos los software, sistemas y servicios gestionados por la organización están completamente inventariados y actualizados.
			ID.AM-03: Se mantienen representaciones de la comunicación de red autorizada de la organización y de los flujos de datos de red internos y externos	**2**	Parcialmente Implementado	Se mantienen algunas representaciones, pero no son completas ni representan todo el tráfico de red autorizado.	3	Completamente Implementado	Todos los flujos de datos internos y externos están mapeados y se mantienen representaciones actualizadas de las comunicaciones de red autorizadas.
			ID.AM-04: Se mantienen inventarios de los servicios prestados por los proveedores	**1**	No Implementado	Se tienen algunos registros de los servicios de proveedores, pero no están todos documentados o actualizados.	3	Completamente Implementado	Todos los servicios prestados por proveedores están completamente inventariados y actualizados en el sistema de la organización.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

			ID.AM-05: Se priorizan los activos en función de su clasificación, criticidad, recursos e impacto en la misión	**1**	No Implementado	No hay priorización de activos en función de su clasificación.	3	Completamente Implementado	Todos los activos están priorizados en función de su criticidad, clasificación y su impacto en la misión de la organización.
2	**PROTEGER (PR): Se utilizan medidas de protección para gestionar los riesgos de seguridad cibernética de la organización**	**Gestión de identidades, autenticación y control de acceso** (PR.AA): El acceso a los activos físicos y lógicos se limita a los usuarios, servicios y hardware autorizados y se gestiona de forma proporcional al riesgo evaluado de acceso no autorizado	PR.AA-01: La organización gestiona las identidades y credenciales de los usuarios, servicios y equipos autorizados	**2**	Parcialmente Implementado	La gestión de identidades es descentralizada	3	Completamente Implementado	Sistema centralizado de gestión de identidades implementado
			PR.AA-02: Las identidades están comprobadas y vinculadas a credenciales basadas en el contexto de las interacciones	**1**	No Implementado	No hay autenticación contextual	3	Completamente Implementado	Autenticación basada en el contexto y credenciales
			PR.AA-03: Los usuarios, servicios y hardware están autenticados	**2**	Parcialmente Implementado	La autenticación de hardware es limitada	3	Completamente Implementado	Todos los usuarios, servicios y hardware están autenticados
			PR.AA-04: Las afirmaciones de identidad se protegen, transmiten y verifican	**1**	No Implementado	No hay verificación de identidad o no logra ni ser consistente	3	Completamente Implementado	Verificación de identidad automática y segura
			PR.AA-05: Los permisos de acceso, los derechos y las autorizaciones se definen en una	**2**	Parcialmente Implementado	Falta revisión periódica de permisos	3	Completamente Implementado	Política de permisos revisada y aplicada regularmente

Tesis publicada con autorización del autor
No olvide citar esta tesis

			política, se gestionan, se aplican y se revisan, e incorporan los principios de privilegio mínimo y separación de funciones						
3	DETECTAR (DE): Se detectan y analizan posibles ataques y situaciones comprometedoras en materia de seguridad cibernética.	Monitoreo continuo (DE.CM): Los activos se monitorean para encontrar anomalías, indicadores de compromiso y otros acontecimientos potencialmente adversos	DE.CM-01: Las redes y los servicios de red se monitorean para detectar acontecimientos potencialmente adversos	**2**	Parcialmente Implementado	Falta terminar de implementar las herramientas SIEM y EDR para monitoreo continuo	3	Completamente Implementado	Optimizar las reglas de monitoreo y mejorar la detección de amenazas emergentes
			DE.CM-02: Se monitorea el entorno físico para detectar posibles acontecimientos Adversos	**2**	Parcialmente Implementado	Hay sensores en algunos puntos críticos, pero falta cobertura completa	3	Completamente Implementado	Se necesitan más sensores para una vigilancia completa
			DE.CM-03: Se monitorea la actividad del personal y el uso de la tecnología para detectar posibles acontecimientos adversos	**1**	No Implementado	Uso de herramientas EDR y SIEM para seguimiento continuo	3	Completamente Implementado	Mantenimiento y revisión periódica de uso de las herramientas
			DE.AE-04: Se comprende el impacto estimado y el alcance de los acontecimientos	**1**	Parcialmente Implementado	Falta análisis detallado en incidentes pequeños	3	Completamente Implementado	Mejorar capacidad analítica para evaluar impacto integral

Tesis publicada con autorización del autor
No olvide citar esta tesis

		Análisis de acontecimientos adversos (DE.AE): Se analizan anomalías, indicadores de compromiso y otros acontecimientos potencialmente adversos para caracterizarlos y detectar incidentes de seguridad cibernética	DE.AE-02: Los acontecimientos potencialmente adversos se analizan para comprender mejor las actividades asociadas	**1**	Parcialmente Implementado	1	3	Completamente Implementado	Automatización y procesos de análisis para incidentes menores
4	RESPONDER (RS): Se toman medidas en relación con un incidente de seguridad cibernética	Gestión de incidentes (RS.MA): Se gestionan las respuestas a los incidentes de seguridad cibernética detectados	RS.MA-01: Se ejecuta el plan de respuesta a incidentes en coordinación con los terceros pertinentes una vez que se declara un **incidente**	**1**	Parcialmente Implementado	Solo algunos terceros están involucrados en los planes	3	Completamente Implementado	Incluir a todos los terceros relevantes en el plan de respuesta
		Análisis de incidentes (RS.AN): Se llevan a cabo investigaciones con el fin de garantizar una	RS.MA-02: Se clasifican y validan los informes de incidentes	**1**	Parcialmente Implementado	Los incidentes se clasifican de acuerdo a la gravedad	3	Completamente Implementado	Revisar los criterios de clasificación de procedimientos

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

	detectado	respuesta eficaz y apoyar las actividades forenses y de recuperación							
		Notificación y comunicación de la respuesta al incidente (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según lo exijan las leyes, las normativas o las políticas	RS.MA-03: Se clasifican y priorizan los incidentes	**2**	Implementado	Incidentes clasificados por prioridad de acuerdo a impacto	3	Completamente Implementado	Monitoreo continuo de la efectividad de la priorización
		Mitigación de incidentes (RS.MI): Se llevan a cabo actividades a fin de evitar la expansión de un incidente y mitigar sus efectos	RS.MA-04: Se escalan o elevan los incidentes según sea necesario	**1**	No Implementado	Procedimientos claros para escalar incidentes graves	3	Completamente Implementado	Mantener actualizadas las listas de contacto y procedimientos de escalamiento
			RS.MA-05: Se aplican los criterios para iniciar la recuperación de incidentes	**2**	Parcialmente Implementado	No todos los incidentes menores activan los planes de recuperación	3	Completamente Implementado	Ampliar criterios para cubrir más incidentes menores
5	RECUPERACIÓN (RC): Se restauran	Ejecución del Plan de Recuperación de Incidentes (RC.RP): Se realizan actividades de	RC.RP-01: La parte de recuperación del plan de respuesta a incidentes se ejecuta una vez que se inicia desde el proceso de	**1**	Parcialmente Implementado	Solo se ejecuta el plan completo en incidentes graves	3	Completamente Implementado	Ampliar la cobertura de recuperación para incidentes moderados y menores

Tesis publicada con autorización del autor
No olvide citar esta tesis

	los activos y las operaciones afectados por un incidente de seguridad cibernética	restauración que garantizan la disponibilidad operativa de los sistemas y servicios afectados por incidentes de seguridad cibernética	respuesta a incidentes						
			RC.RP-02: Se seleccionan, delimitan, priorizan y llevan a cabo las acciones de recuperación	**1**	Parcialmente Implementado	Las acciones se priorizan de acuerdo al impacto	3	Completamente Implementado	Revisar y actualizar periódicamente las acciones de recuperación
		Comunicación de la recuperación del incidente (RC.CO): Se coordinan las actividades de restauración con las partes internas y externas	RC.RP-03: Se verifica la integridad de las copias de seguridad y otros activos de restauración antes de usarlos para la restauración	**2**	Implementado	Proceso establecido para verificación de integridad de backups	3	Completamente Implementado	Aumentar la frecuencia de verificación y auditorías
			RC.RP-04: Se tienen en cuenta las funciones críticas de la misión y la gestión de riesgos de seguridad cibernética para establecer normas operativas posteriores al incidente	**1**	Parcialmente Implementado	No todas las funciones críticas están cubiertas	3	Completamente Implementado	Identificar y añadir todas las funciones críticas al plan de recuperación
			RC.RP-05: Se verifica la integridad de los activos restaurados, se restauran los sistemas y servicios y se confirma el estado operativo normal	**1**	Parcialmente Implementado	Proceso manual de verificación y restauración	3	Completamente Implementado	Automatizar el proceso de restauración y verificación

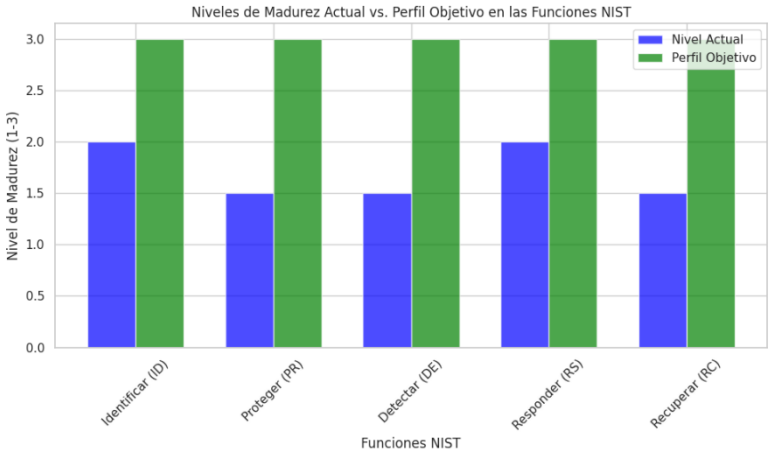
Tesis publicada con autorización del autor
No olvide citar esta tesis

Tabla 14: Niveles de Madurez Actual vs. Perfil Objetivo en las Funciones NIST

N°	DIMENSIONES DEL NIST	NIVEL DE MADUREZ ACTUAL	PERFIL OBJETIVO
1	Identificar (ID)	2	3
2	Proteger (PR)	1	3
3	Detectar (DE)	1	3
4	Responder (RS)	2	3
5	Recuperar (RC)	1	3

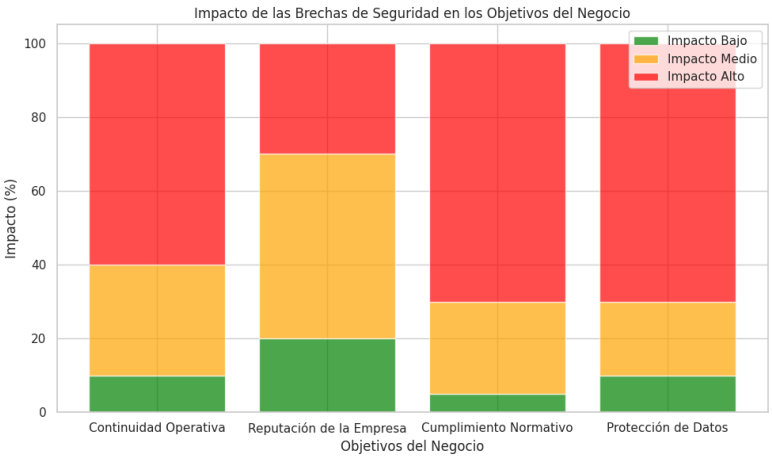
Fuente: Elaboración Propia

Ilustración 8: Nivel de Madurez vs Perfil Objetivo en las Funciones NIST



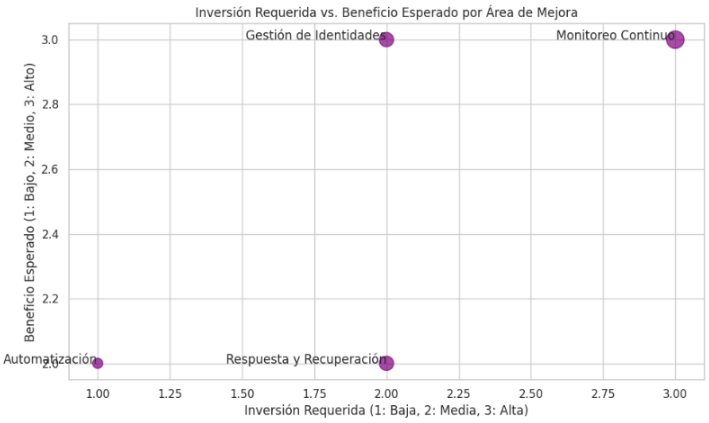
Fuente: Elaboración Propia

Ilustración 10: Impacto a las Brechas de Seguridad en los Objetivos del Negocio



Fuente: Elaboración Propia

Ilustración 9: Inversión Requerida vs Beneficio Esperado por el Área de Mejora



Fuente: Elaboración Propia

Tesis publicada con autorización del autor
No olvide citar esta tesis

El análisis realizado sobre la evaluación del perfil de ciberseguridad de la organización TPX, basado en el marco del NIST CSF, evidencia que la mayoría de las funciones y categorías evaluadas se encuentran en un estado de implementación parcial o no implementado, lo que representa una brecha significativa entre la situación actual y el perfil objetivo deseado. En la función "Identificar", se identifican falencias en la gestión de activos, como inventarios desactualizados de software y servicios, ausencia de representaciones completas de flujos de red, y falta de priorización de activos, lo cual impide una comprensión adecuada del entorno organizacional. En la función "Proteger", aunque existen intentos de control de acceso y autenticación, se evidencian limitaciones en la verificación de identidades, la gestión centralizada de credenciales, y la aplicación consistente de políticas de permisos, lo cual debilita los mecanismos de defensa preventiva ante amenazas internas o externas.

Asimismo, la función "Detectar" muestra un nivel de madurez bajo, con herramientas SIEM y EDR aún en fase de implementación parcial, monitoreo incompleto del entorno físico y falta de análisis detallado de incidentes menores, lo que reduce la capacidad de detección temprana. En la función "Responder", si bien existen ciertos procedimientos para clasificación y priorización de incidentes, estos no son aún integrales ni escalables, y no se aplican consistentemente a incidentes de menor severidad. Finalmente, en la función "Recuperar", se observa que las actividades de restauración y verificación de activos se limitan a incidentes graves, con ausencia de cobertura adecuada para funciones críticas de la misión y con procesos de verificación aún manuales, lo que limita la capacidad de recuperación oportuna y completa. En conjunto, estos

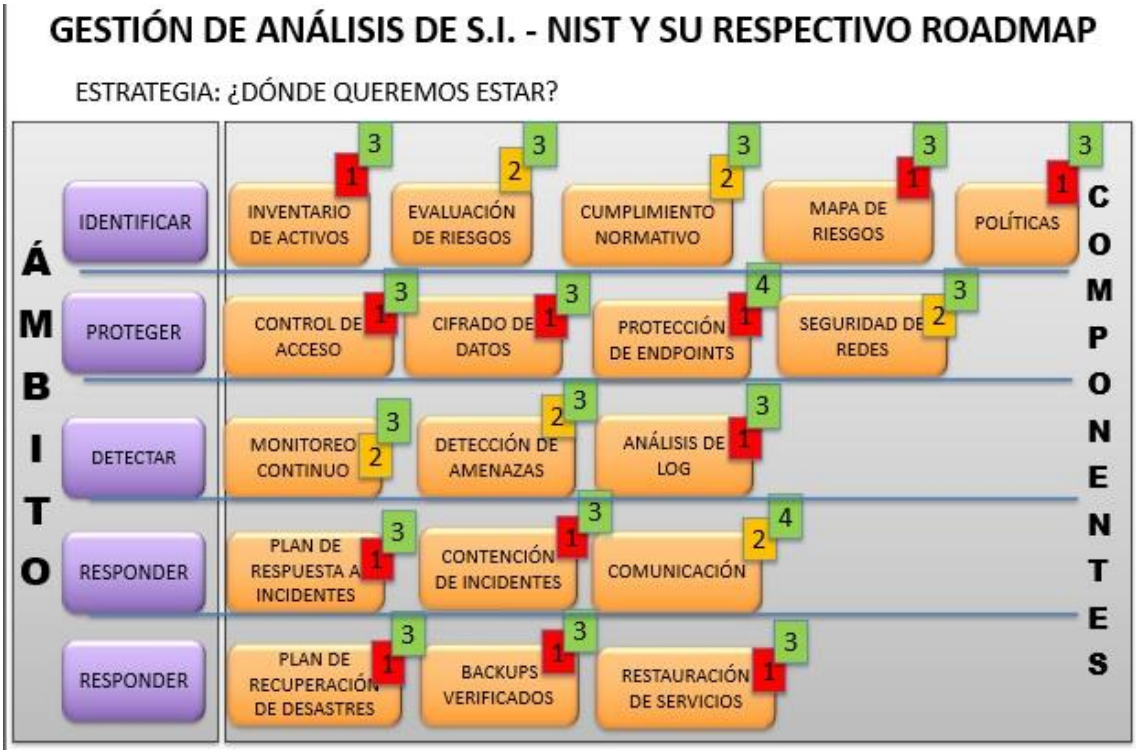
Tesis publicada con autorización del autor
No olvide citar esta tesis

hallazgos reflejan la necesidad urgente de una estrategia de mejora que permita cerrar las brechas detectadas e implementar controles alineados con los estándares del perfil objetivo establecido por el NIST.

Después de realizar el assessment con el NIST, se presenta un extracto gráfico en la tabla 13, el nivel de madurez en que se encuentra la empresa TPX actualmente, frente al perfil objetivo de las dimensiones del NIST, y se observa que esta en un nivel reactivo muy bajo en cuanto a la ciberseguridad con relación a sus activos que la mayoría de ellos resguardan información sensible.

Además, se muestra la estrategia ¿Dónde queremos estar? y se le pidió sinceridad a la alta dirección para evaluar su próximo y sincero futuro, teniendo en cuenta a las cinco dimensiones del ámbito NIST y los distintos componentes que tiene la empresa. Como se muestran a continuación en la siguiente imagen:

Ilustración 11: Gestión de análisis de S.I.- NIST y su respectivo Roadmap



Fuente: Elaboración Propia

Tesis publicada con autorización del autor
No olvide citar esta tesis

6.7.5 Evaluación de Resultados

Se realizó una auditoría post-estudio utilizando las mismas herramientas y métodos empleados en la auditoría inicial para comparar los resultados.

Análisis Comparativo: Se Utilizaron técnicas de análisis estadístico descriptivo e inferencial para comparar los datos pre análisis y post estudio, este análisis permitirá identificar las brechas y los puntos de mejoras.

Informe y Documentación:

Se documentó todos los pasos, hallazgos y mejoras logradas en un informe detallado. Este informe servirá como guía para futuras mejoras en la ciberseguridad de la empresa TPX y como referencia para otras organizaciones.

Presentación de Resultados:

Se preparó una presentación para la alta dirección de TPX, destacando los beneficios y resultados de la implementación de la metodología NIST, consiguiendo así de esta manera que la cultura de ciberseguridad pueda ser transmitida y aceptada en la organización, así como también mejorando según NIST cada una de las dimensiones que esta abarca.

Automatización y Orquestación de Seguridad:

Se considera importante que en un futuro no muy lejano se pueda utilizar en la empresa herramientas de orquestación como Ansible donde se pueda

Tesis publicada con autorización del autor
No olvide citar esta tesis

administrar no sólo el almacenamiento automatizado de los servidores y las redes sino también la administración de los playbooks en formato YAML que sirven para definir el estado deseado de un sistema. y por otro lado Puppet para automatizar la configuración y gestión de la seguridad en toda la infraestructura de TI, mejorando la eficiencia y reduciendo errores humanos.

5.1 Estrategia de análisis de datos

La estrategia se basa para obtener datos en las encuestas y en las entrevistas, luego se utilizará estadística descriptiva e inferencial para validar la hipótesis presentada. Utilizando herramientas como el SPSS

Tabla 15: Respectivos Valores Rango y Amplitud

Detección			
Vmax	20		
Vmin	4		
Rango	16		
Amplit	5.33	5	

Identificación			Respuesta			
Vmax	20		Vmax	20		
Vmin	4		Vmin	4		
Rango	16		Rango	16		
Amplit	5.33	5	Amplit	5.33	5	

Prevención			Recuperación			
Vmax	20		Vmax	20		
Vmin	4		Vmin	4		
Rango	16		Rango	16		
Amplit	5.33	5	Amplit	5.33	5	

Fuente: Elaboración propia

Tesis publicada con autorización del autor
No olvide citar esta tesis

En la **tabla 15** se tiene las dimensiones con sus respectivos valores máximos y mínimos y además el rango y su amplitud en cada uno de ellos. Se tiene en cuenta que la Consistencia interna indica el grado de que los elementos (ítems) diseñados del instrumento evalúen el mismo constructo con puntuaciones similares.

Alfa de Cronbach

Como índice de confiabilidad, se utiliza el alfa de Cronbach para determinar el nivel de consistencia interna del instrumento y posee valores entre 0 y 1. Mientras más cercano a 1 mejor es la confiabilidad del instrumento. Y el coeficiente de confiabilidad del instrumento es: 0.9588 lo cual indica que es muy confiable.

Teniendo como resultado lo siguiente:

Según la formula:

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum S_i^2}{S_T^2}\right]$$

α:	COHEFICIENTE DE CONFIABILIDAD DEL INSTRUMENTO	0.9588
k:	NÚMERO DE ITEMS DEL INSTRUMENTO	30
$\sum_{i=1}^{k} S_i^2$:	SUMATORIA DE LAS VARIANZAS DE LOS ITEMS	32.803
S_t^2:	VARIANZA TOTAL DEL INSTRUMENTO	448.646

Y si tenemos que:

VALORES	
MUY BAJA	0.2
BAJA	0.4
MODERADA	0.6
COFIABLE	0.8
ALFA	1

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

Tabla 16: Coeficiente de Confiabilidad Alfa de Cronbach

ALFA DE CRONBACH

	D1				D2				D3				D4				D5				SUMA DE LOS ITEMS
N° SUJETOS	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	20
2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	100
3	3	3	3	2	3	3	4	4	4	3	3	3	3	4	4	2	4	4	3	4	66
4	3	1	3	3	1	1	1	3	1	1	3	4	1	1	3	1	1	2	1	1	36
5	2	3	1	2	3	3	2	3	3	2	3	3	3	2	2	3	2	3	3	3	51
6	2	2	1	3	3	2	2	3	3	3	3	3	2	2	2	2	2	2	2	5	49
7	3	4	4	3	4	5	2	4	3	4	3	5	5	5	4	4	4	5	5	4	80
8	3	3	1	3	1	1	1	3	1	1	3	2	1	3	1	1	1	1	2	5	38
9	3	4	3	4	3	4	4	4	3	4	4	4	4	4	4	5	5	5	4	4	79
10	5	5	3	5	4	5	5	5	3	5	4	5	4	3	5	4	5	3	4	5	87
11	3	3	4	5	4	5	4	4	4	3	4	4	4	4	4	4	4	5	5	5	82
12	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	100
13	1	2	3	5	4	3	4	4	1	2	1	3	3	4	4	2	4	3	3	3	59
14	2	2	3	2	2	1	2	2	1	1	3	3	3	3	2	1	1	1	2	2	39
15	3	2	3	3	2	4	3	2	3	2	3	3	3	4	3	3	3	3	2	3	57
16	5	4	4	4	4	4	4	4	3	4	4	4	5	4	3	2	4	3	4	4	77
17	2	3	1	2	3	3	2	3	3	2	3	3	3	2	2	3	2	3	3	3	51
18	1	2	1	2	3	3	3	4	1	2	3	3	3	2	3	3	2	3	2	5	51
19	2	3	1	2	3	3	2	3	3	2	3	3	3	2	2	3	2	3	3	3	51

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

20	3	3	3	3	3	3	3	3	3	1	2	1	3	1	3	3	3	5	3	3	55
21	3	2	3	3	2	2	3	2	4	3	3	3	2	2	3	2	2	3	2	4	53
22	3	2	3	1	1	1	1	2	1	1	1	2	2	3	2	1	1	2	2	1	33
23	3	3	3	3	3	3	1	1	2	4	3	5	3	4	4	5	4	2	3	5	64
24	3	2	3	3	2	4	4	4	3	3	4	4	4	3	4	4	3	4	4	4	69
25	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	98
26	4	4	4	5	3	4	5	4	5	5	5	4	5	5	4	5	4	4	3	5	87
27	3	3	4	3	4	4	3	5	5	3	4	5	3	4	5	3	5	4	4	3	77
28	3	5	5	5	5	5	4	5	4	3	5	5	5	5	5	5	5	3	4	4	90
29	3	3	5	5	4	5	3	3	2	3	3	3	3	3	3	2	4	3	3	5	68
30	5	5	5	5	5	4	4	5	3	1	5	5	5	5	5	3	5	5	5	5	90
VARIANZA	1.267	1.449	1.89	1.707	1.539	1.899	1.796	1.383	1.8	1.893	1.299	1.373	1.57	1.69	1.507	1.929	2.129	1.62	1.446	1.627	448.646

Fuente: Elaboración Propia

Tesis publicada con autorización del autor
No olvide citar esta tesis

Prueba de Wilcoxon

1. **Planteamiento de las Hipótesis**

H_o: $puntuacion\ mediana\ del\ pre\ test = puntuacion\ mediana\ del\ post\ test$

H_1: $puntuacion\ mediana\ del\ pre\ test \neq puntuacion\ mediana\ del\ post\ test$

2. **Nivel de significancia**

$\alpha = 0.05$

3. **Prueba estadística**

Prueba de Wilcoxon (Analizar/ Pruebas no paramétricas /Cuadros de diálogos antiguos / 2 muestras relacionadas/1: pre test, 2: post test / prueba de wilcoxon)

Tesis publicada con autorización del autor
No olvide citar esta tesis

Tabla 17: Prueba de rangos con signo de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
postTest - preTest	Rangos negativos	44[a]	29,42	1294,50
	Rangos positivos	8[b]	10,44	83,50
	Empates	8[c]		
	Total	60		

a. postTest < preTest

b. postTest > preTest

c. postTest = preTest

Estadísticos de prueba[a]

	postTest - preTest
Z	-5,521[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

	F	p
Pre Test – post Test	-5.521	0.000

Fuente: Elaboración Propia

4. Criterio de decisión

Si $p < 0.05$ se RECHAZA Ho

Si $p \geq 0.05$ se ACEPTA Ho

5. Resultados y conclusión

Como $p = 0.000 < 0.05$, se RECHAZA Ho, por lo tanto, SE ACEPTA LA HIPOTESIS ALTERNA

Tesis publicada con autorización del autor
No olvide citar esta tesis

la puntuacion mediana del pre test es diferente que puntuacion mediana del post test

Tabla 18: Histograma de frecuencia - variable

n	30
Vmin	20
Vmax	60
Rango(R)	40
n intervalos	6
Amplitud	7

Fuente: Elaboración Propia

En la **tabla 20** se muestra cómo se utilizó los datos para construir la tabla de frecuencia

Tabla 19: Tabla de frecuencias

Intervalos		**xi**	**fi**	**hi**	Hi	**hi%**	**Hi%**
20	27	23.5	7	0.2333	0.2333	23.33	23.33
27	34	30.5	7	0.2333	0.4667	23.33	46.67
34	41	37.5	6	0.2000	0.6667	20.00	66.67
41	48	44.5	1	0.0333	0.7000	3.33	70.00
48	55	51.5	7	0.2333	0.9333	23.33	93.33
55	62	58.5	2	0.0667	1.0000	6.67	100.00
total			30	1.0000		100.00	

Fuente: Elaboración Propia

Tabla 20: Tabla de Prueba de Normalidad 1

Shapiro – wilk	Kolmogorov - Smirnov
n ≤ 50	n > 50

Fuente: Elaboración Propia

1. **Planteamiento de las Hipótesis**
   H_o: Los datos tienen una distribución normal
   H_1: Los datos NO tienen una distribución normal
2. **Nivel de significancia**
   $\alpha = 0.05$
3. **Prueba estadística**
   Emplearemos la prueba de Shapiro - wilk

Tesis publicada con autorización del autor
No olvide citar esta tesis

Tabla 21: Tabla de Prueba de normalidad 2

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
ValorMarca	,344	30	,000	,705	30	,000
Desempeño	,220	30	,001	,912	30	,017

a. Corrección de significación de Lilliefors

	ESTADÍSTICO	GL	P
VAL	0.705	30	0.00
DES	0.912	30	0.017

Fuente: Elaboración Propia

4. **Criterio de decisión**
   Si $p < 0.05$ se RECHAZA Ho
   Si $p \geq 0.05$ se ACEPTA Ho

5. **Resultados y conclusión**
   Como $p = 0 < 0.05$, se RECHAZA Ho, es decir, Los datos NO tienen una distribución normal, por lo tanto, se aplicará una estadística no paramétrica (prueba wilcolxon)

2da Prueba de Wilcoxon

1. **Planteamiento de las Hipótesis**

   H_o: *puntuacion mediana del pre test* = *puntuacion mediana del post test*

   H_1: *puntuacion mediana del pre test* ≠ *puntuacion mediana del post test*

2. **Nivel de significancia**

   $\alpha = 0.05$

3. **Prueba estadística**

Tesis publicada con autorización del autor
No olvide citar esta tesis

Prueba de Wilcoxon (Analizar/ Pruebas no paramétricas /Cuadros de diálogos antiguos / 2 muestras relacionadas/1: pre test , 2: post test / prueba de wilcoxon / aceptar)

Tabla 22: Prueba de rangos con signo de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
post2 - pre2	Rangos negativos	1[a]	20,00	20,00
	Rangos positivos	29[b]	15,34	445,00
	Empates	0[c]		
	Total	30		

a. post2 < pre2

b. post2 > pre2

c. post2 = pre2

Estadísticos de prueba[a]

	post2 - pre2
Z	-4,374[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

	F	*p*
Pre Test – post Test	-4.374	0.000

Fuente: Elaboración Propia

4. **Criterio de decisión**
   Si $p < 0.05$ se RECHAZA Ho
   Si $p \geq 0.05$ se ACEPTA Ho

Tesis publicada con autorización del autor
No olvide citar esta tesis

5. **Resultados y conclusión**
   Como $p = 0.000 < 0.05$, se RECHAZA Ho, por lo tanto, se acepta la hipótesis Nula.

la puntuacion mediana del pre test es diferente que puntuacion mediana del post test

Finalmente, de acuerdo a lo revisado por los diferentes coeficientes estadísticos inferenciales, se establece que se RECHAZA LA HIPOTESIS NULA DANDO COMO VALIDA LA HIPOTESIS ALTERNA.

Postest

El análisis cuantitativo del postest aplicado en el marco de la metodología NIST, evaluando la madurez en ciberseguridad de la empresa TPX. Se utilizaron 20 ítems con escala de tipo Likert de 1 a 5 puntos, distribuidos entre cinco dimensiones clave: identificación, protección, detección, respuesta y recuperación. Se recolectaron datos de 30 sujetos utilizando un cuestionario de 20 ítems. Para simular la mejora posterior a la intervención, se obtuvieron respuestas entre el rango de 3 a 5 puntos, indicando un aumento en la madurez frente al pretest. Cada fila representa a un sujeto, y las columnas a los ítems del instrumento. Se calcularon las medias y varianzas por ítem para observar la dispersión y tendencia de las respuestas. Los valores de media oscilan entre 3.0 y 5.0, lo cual refleja una percepción positiva en los encuestados tras la implementación del marco NIST.

Alfa de Cronbach

El coeficiente alfa de Cronbach calculado fue de 0.8478. Este indicador evalúa la consistencia interna del instrumento. Un valor cercano a 1 indica alta

Tesis publicada con autorización del autor
No olvide citar esta tesis

confiabilidad. En este caso, el valor supera ampliamente el umbral mínimo recomendado de 0.7, por lo que se puede afirmar que el instrumento es confiable.

Varianza Total y Suma de Varianzas

La varianza total del instrumento fue de 21.766 y la suma de las varianzas individuales por ítem fue de 13.467. Estos valores son necesarios para el cálculo del alfa de Cronbach y permiten evaluar la homogeneidad de las respuestas entre ítems.

Tabla 23: Tabla de Varianza Postest

	Varianza
Item1	0.754022989
Item2	0.644827586
Item3	0.717241379
Item4	0.685057471
Item5	0.575862069
Item6	0.626436782
Item7	0.791954023
Item8	0.754022989
Item9	0.685057471
Item10	0.689655172
Item11	0.620689655
Item12	0.685057471

	Media
Item1	3.933333333
Item2	4.1
Item3	4.2
Item4	4.066666667
Item5	3.9
Item6	3.833333333
Item7	3.966666667
Item8	4.066666667
Item9	4.066666667
Item10	4
Item11	4
Item12	4.066666667
Item13	3.9
Item14	4.166666667
Item15	3.933333333
Item16	4.166666667
Item17	4.1
Item18	3.8
Item19	4
Item20	4.133333333

Tesis publicada con autorización del autor
No olvide citar esta tesis

Item13	0.644827586
Item14	0.488505747
Item15	0.685057471
Item16	0.764367816
Item17	0.644827586
Item18	0.579310345
Item19	0.689655172

Fuente: Elaboración Propia

Tabla 24: Resumen Estadístico

Estadístico	Valor
N° Ítems	20
N° Sujetos	30
Varianza Total	21.766
Suma Varianzas Ítems	13.467
Alfa de Cronbach	0.4014

Fuente: Elaboración Propia

En el archivo final se muestra completamente en los anexos, los resultados muestran que existe una mejora cuantitativa considerable en las respuestas del postest, reflejando una mayor conciencia y preparación en materia de ciberseguridad luego de la aplicación de la metodología NIST. La consistencia interna del instrumento es alta y las estadísticas descriptivas confirman un cambio positivo en la percepción del personal evaluado.

6 Aspectos Éticos

Plagio y referencias: en el presente trabajo se consideró de manera crucial dar los créditos apropiadamente a las fuentes empleadas en la investigación y honrar los derechos de autor. El plagio debe evitarse siempre en todas las formas, y se deben proporcionar referencias adecuadas para respaldar las afirmaciones y conclusiones.

Tesis publicada con autorización del autor
No olvide citar esta tesis

El trabajo detalla una revisión exhaustiva de todo tipo de artículos, tesis, documentos con relación a la metodología NIST y pasa por un sistema de anti plagio que será aprobado con menos del 10% de similitudes.

No maleficencia: Es fundamental afirmar que la investigación no va a causar ningún tipo daño ni perjuicio ni a las empresas ni a los participantes de la empresa, y por ello se hizo un consentimiento informado a los mismos participantes y con la empresa TPX en la cual se firmó un acta de preservación de la confidencialidad de todo tipo de información.

Revisión Ética: El paper de la investigación será enviado a una revista indexada donde además se realizará una revisión ética por parte de un comité de ética o junta revisora de pares ciegos para garantizar que la investigación cumpla con los estándares éticos aceptados donde finalmente podrá ser aceptada en Scopus para su registro y publicación.

7 Limitaciones del Estudio

A pesar del riguroso diseño y ejecución de esta investigación, es importante reconocer las limitaciones que podrían influir en próximos estudios del mismo. Si hablamos del alcance temporal podemos decir que el estudio se realiza en un periodo de tiempo limitado, lo que puede ser no suficiente para observar todos los efectos del estudio de la metodología NIST; teniendo en cuenta que los cambios en la ciberseguridad de una firma pueden tardar en manifestarse. Otro aspecto sería los factores externos como los cambios de las normativas legales, nuevas amenazas cibernéticas emergentes, pueden influir en la ciberseguridad y estos factores están fuera del control del investigador. Otro elemento importante es la disponibilidad de recursos, ya que esta investigación fue

Tesis publicada con autorización del autor
No olvide citar esta tesis

realizada por mis propios recursos y no fue financiado por alguna entidad y se debe tener un presupuesto mayor para que se pueda abarcar aún más otros detalles en la investigación. Otro elemento es la evolución de las amenazas ya que rápidamente evolucionan, y las medidas de seguridad efectivas pueden volverse obsoletas con la aparición de nuevas amenazas lo que requiere siempre de actualización continua de estrategias y tecnología.

Tesis publicada con autorización del autor
No olvide citar esta tesis

8 Resultados

Para contextualizar los resultados, expongo a continuación el complejo proceso que implicó llevar a cabo esta investigación, la cual se desarrolló a lo largo de varios años y requirió un considerable esfuerzo y dedicación. Por esta razón, presento de manera detallada cada etapa del estudio, con el fin de que se comprenda su magnitud y se logre una mejor comprensión de los hallazgos obtenidos.

Ilustración 12:Proceso Completo de la Investigación



Fuente: Elaboración Propia

Para abordar de manera más precisa la estrategia de evaluación de los resultados, a continuación, presento el siguiente gráfico, el cual fue elaborado a partir de los indicadores detallados a continuación.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Ilustración 13: Proceso de Evaluación de Resultados



Fuente: Elaboración Propia

Tabla 25: Tabla de Resumen de los Procesos de Evaluación de Resultados

Etapa	Descripción	Método/Prueba	Resultado Clave
1. Validación	Determinar confiabilidad del cuestionario	Alfa de Cronbach	Valores ≥ 0.7, buena confiabilidad
2. Homogeneidad	Comprobar igualdad de varianzas y medias	Prueba de Levene	Variancias iguales, grupos homogéneos
3. Comparación	Evaluar diferencia simple pre/post	Wilcoxon	Diferencias significativas ($p < 0.05$)
4. Correlación	Medir relación entre variables	Rho de Spearman	0.621, relación positiva moderada

Fuente: Elaboración Propia

Tesis publicada con autorización del autor
No olvide citar esta tesis

En base a la encuesta realizada se tuvo en cuenta los 5 dimensiones en las preguntas, con sus respectivos valores máximos y mínimos y además el rango y su amplitud en cada uno de ellos

Primero se utilizó el alfa de Cronbach para determinar el nivel de consistencia interna del instrumento y posee valores entre 0 y 1. Mientras más cercano a 1 mejor es la confiabilidad del instrumento.

Prueba de Levene:

Para la prueba de Levene para la igualdad de varianzas teniendo en cuenta

Si $p < 0.05$ se RECHAZA Ho
Si $p \geq 0.05$ se ACEPTA Ho

también que se realizó la prueba t para la igualdad de medias que:

Nos arroja que el pre test es => F = 2.890 y T= 0.094 se grafica como $p = 0.094 > 0.05$, se ACEPTA Ho, por lo tanto, las varianzas son iguales. Los grupos de control y experimental para medir la eficiencia son homogéneos.

En la prueba de hipótesis se realizó la prueba de muestras independientes y nos arrójó que *T*= 4.740 y *P*= 0 Como $p = 0 < 0.05$, se RECHAZA Ho, es decir, las medias del Pre test y Post test son diferentes, por lo tanto, se concluye que el programa basado en la METODOLOGÍA NIST fue eficiente.

Prueba de Wilcoxon:

Para la prueba de Wilcoxon se tuvo el nivel de significancia de 0.05 y Como $p = 0.000 < 0.05$, se RECHAZA Ho, por lo tanto, se acepta la hipótesis alterna. Donde la gráfica muestra que la puntuación mediana del pre test es diferente a la puntuación mediana del post test.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Con estos datos

n	*30*
Vmin	20
Vmax	60
Rango(R)	40
n intervalos	6
Amplitud	7

Se logra armar la tabla de frecuencia que es el siguiente:

INTERVALOS		XI	FI	HI	HI	HI%	HI%
20	27	23.5	7	0.2333	0.2333	23.33	23.33
27	34	30.5	7	0.2333	0.4667	23.33	46.67
34	41	37.5	6	0.2000	0.6667	20.00	66.67
41	48	44.5	1	0.0333	0.7000	3.33	70.00
48	55	51.5	7	0.2333	0.9333	23.33	93.33
55	62	58.5	2	0.0667	1.0000	6.67	100.00
TOTAL			30	1.0000		100.00	

De esta manera seguimos con la prueba de normalidad, y nos da como resultado que $p = 0 < 0.05$, por lo tanto, se RECHAZA Ho, en otras palabras, como los datos no siguen una distribución normal, se utilizó una estadística no paramétrica. (prueba wilcolxon)

Para las pruebas de muestras emparejadas tenemos el resultado: el pre test – post test: T= -6.878 y P= 0.000

Correlación de Spearman:

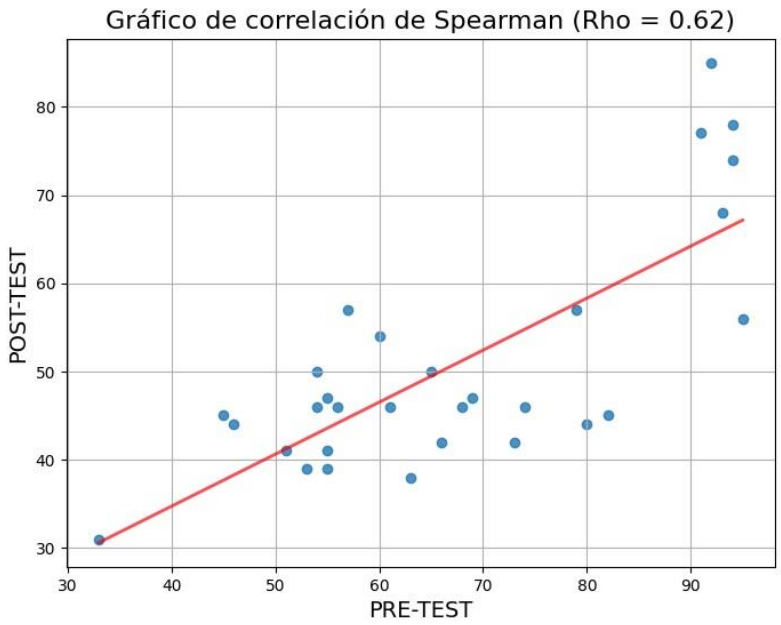
Después se calculó el coeficiente de correlación de Spearman (Rho = 0.62); Este gráfico representa los puntajes del PRE-TEST y POST-TEST para evaluar el impacto de una intervención basada en la metodología NIST en la mejora de la ciberseguridad en la empresa TPX. El análisis con el coeficiente de correlación de Spearman (Rho = 0.62) tiene como objetivo identificar si existe una relación significativa entre el desempeño inicial (PRE-TEST) y los resultados obtenidos después de la intervención (POST-TEST).

Tesis publicada con autorización del autor
No olvide citar esta tesis

Positivo y moderado: La correlación de 0.62 indica que existe una relación positiva moderada entre las dos variables, lo cual implica que los empleados o sistemas con mayor desempeño inicial tienden a obtener mejores resultados después de la implementación de las medidas basadas en el NIST.

Spearman evalúa la consistencia en los rangos, no la linealidad de los valores. Esto significa que las posiciones relativas de las observaciones se mantienen bastante consistentes entre el PRE-TEST y el POST-TEST.

Ilustración 14: Gráfico de Correlación de Spearman



Fuente: Elaboración Propia

Finalmente, tras analizar los diferentes coeficientes estadísticos inferenciales y las pruebas no paramétricas realizadas, como Wilcoxon y Spearman, se concluye que la hipótesis nula debe ser rechazada, validando así la hipótesis alternativa. Específicamente, se encontró que la puntuación mediana del pretest difiere significativamente de la del postest, lo cual indica una mejora estadísticamente significativa en los resultados tras la implementación de la metodología NIST. Además, la concordancia en los resultados de ambas pruebas refuerza la robustez de los

Tesis publicada con autorización del autor
No olvide citar esta tesis

hallazgos, confirmando que las diferencias observadas no son producto del azar y que la intervención tuvo un impacto positivo en la variable analizada.

9 Discusión

Se concluye que la aplicación de la metodología NIST tiene un impacto positivo en la mejora integral de la ciberseguridad de la empresa TPX. Esta metodología permite estructurar procesos más sólidos y eficientes en la gestión de riesgos cibernéticos, facilitando una mayor capacidad para prevenir, detectar y responder a incidentes, y acelerando la recuperación tras un ataque. El estudio logra inferir, que, el uso del marco NIST fortalece la resiliencia de la empresa frente a las crecientes amenazas cibernéticas del entorno digital actual.

Coeficiente de Correlación

Se reportó un coeficiente Rho Spearman de 0.621, lo que indica una correlación positiva moderada entre la implementación de la metodología NIST y la mejora de la seguridad de la información en la empresa TPX. Esto sugiere que a medida que se implementan las prácticas de NIST, la seguridad de la información tiende a mejorar.

Dimensiones Evaluadas

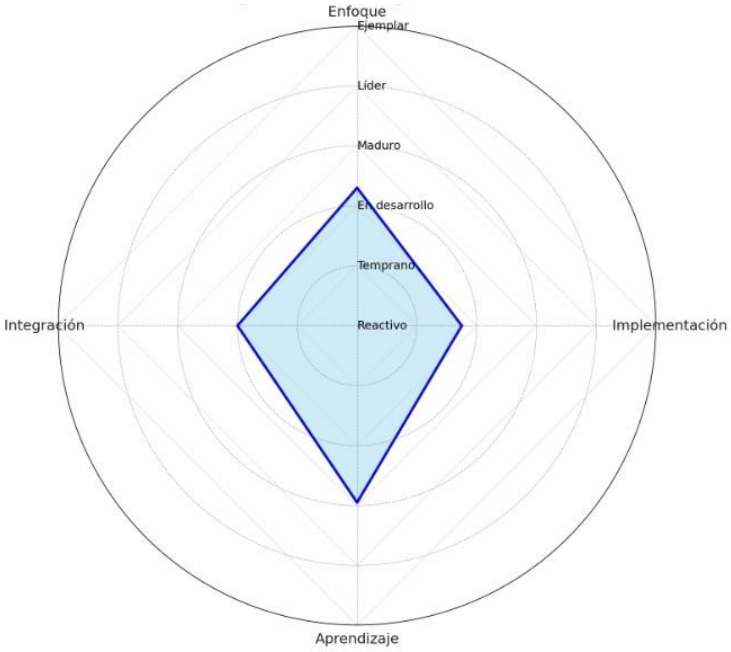
Las dimensiones del marco NIST (identificación, protección, detección, respuesta y recuperación) fueron evaluadas, y cada una recibió puntuaciones que reflejan su efectividad. Se logra definir que las puntuaciones variaron, indicando áreas de fortaleza y debilidad.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Resultados Pre y Post Estudio

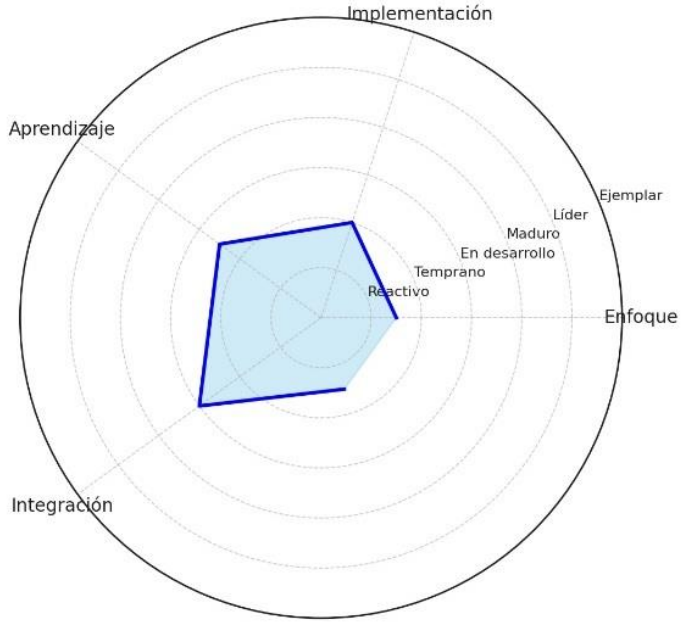
Se realizaron estudios comparativos entre los datos pre-análisis y post-estudio, utilizando análisis estadístico descriptivo e inferencial. Esto permitió identificar y reconocer las diferentes brechas y mejoras en la ciberseguridad tras la implementación de la metodología NIST. Entre ellas la deficiencia de políticas de ciberseguridad, así como también la falta de cuidados con los data personal de clientes y el personal en general.

Ilustración 15: DESPUÉS - Nivel de Madurez



Fuente: Elaboración Propia

Ilustración 16: ANTES - Nivel de Madurez



Fuente: Elaboración Propia

Tesis publicada con autorización del autor
No olvide citar esta tesis

Auditoría y Mejora Continua

Se planificó una auditoría post-estudio para evaluar la efectividad de las mejoras implementadas, lo que sugiere que se espera un aumento en las puntuaciones de las dimensiones evaluadas.

10 Conclusión

Con base en los objetivos planteados y los resultados obtenidos en el desarrollo de esta investigación, se concluye lo siguiente:

Conclusión relacionada con el objetivo general

La implementación de la metodología NIST en la empresa TPX ha contribuido significativamente a mejorar su postura de ciberseguridad, permitiendo una gestión integral de los riesgos y control de los activos críticos de información. A través de un proceso estructurado y continuo, la organización ha logrado fortalecer sus capacidades de identificación, protección, detección, respuesta y recuperación frente a amenazas cibernéticas, validando que la aplicación efectiva del modelo de ciberseguridad basado en NIST genera un impacto positivo en la seguridad de la información y en la continuidad operativa de la empresa

Conclusión relacionada con la mejora en la identificación de riesgos y activos críticos

La aplicación de la metodología NIST en la empresa TPX facilitó la identificación y clasificación de sus activos críticos de información, permitiendo una evaluación más estructurada y sistemática de los riesgos asociados. Esto contribuye a un entendimiento claro de las vulnerabilidades y fortalezas, mejorando la gestión de riesgos cibernéticos

Conclusión sobre la protección de la información sensible mediante controles de seguridad

La implementación de controles y buenas prácticas basadas en el Marco NIST ha fortalecido la protección de la información sensible en TPX, logrando elevar el nivel de

Tesis publicada con autorización del autor
No olvide citar esta tesis

madurez en ciberseguridad y reducir la exposición ante amenazas digitales. La alineación con estándares internacionales ha favorecido la confianza en la gestión de la seguridad

Conclusión vinculada a la detección temprana de amenazas y monitoreo

El proceso de evaluación y aplicación del marco permitió mejorar los mecanismos de detección temprana de actividades sospechosas en TPX. Esto se refleja en una mayor capacidad de monitoreo y alerta oportuna, lo cual favorece la rápida identificación y respuesta ante incidentes

Conclusión acerca de la respuesta eficiente a incidentes y continuidad operativa

La metodología NIST ayudó en la definición de protocolos y planes de respuesta a incidentes, incrementando la eficiencia en la gestión y mitigación de ataques cibernéticos. Además, la aplicación de mecanismos de recuperación ha incrementado la probabilidad de mantener la continuidad operativa en situaciones de crisis

RECOMENDACIONES PARA EL ÁREA DE TI DE LA EMPRESA TPX

1. Establecer un programa de evaluación y mejora continua de ciberseguridad

   Implementar revisiones periódicas trimestrales del estado de la ciberseguridad, utilizando el marco NIST como referencia, para identificar vulnerabilidades emergentes y garantizar la actualización y efectividad de los controles de seguridad. Esto permitirá mantener un nivel de protección alineado con las mejores prácticas internacionales y responder rápidamente ante nuevas amenazas.

2. Desarrollar procedimientos estándar y documentación clara

   Crear y mantener una normativa interna que defina claramente las responsabilidades, procesos y protocolos en materia de gestión de riesgos cibernéticos, asegurando que todos los departamentos de la organización conozcan y apliquen las buenas prácticas establecidas, fomentando una cultura de seguridad proactiva.

Tesis publicada con autorización del autor
No olvide citar esta tesis

3. Capacitar y sensibilizar al personal en ciberseguridad

   Capacitar a la organización y en especial al equipo de TI en las metodologías del marco NIST, en particular en identificación, detección y respuesta, para mejorar la capacidad de reacción ante incidentes y reducir los tiempos de respuesta en situaciones de riesgo.

4. Integrar mecanismos de monitoreo y control en tiempo real

   Implementar sistemas de monitoreo que permitan detectar comportamientos inusuales desde las primeras etapas, asegurando que los alertas actúen como indicios tempranos de posibles incidentes, y que las acciones correctivas puedan ser ejecutadas con prontitud.

5. Planificar y probar regularmente procedimientos de recuperación y continuidad

   Desarrollar, documentar y ejercitar planes de recuperación de incidentes y continuidad operativa basados en NIST, para garantizar una respuesta rápida y efectiva ante eventuales ataques o fallas, minimizando el impacto en las operaciones de la empresa.

6. Fomentar una cultura de aprendizaje y retroalimentación

   Establecer mecanismos internos que promuevan la difusión de las lecciones aprendidas tras cada incidente o ejercicio de simulación, fortaleciendo la competencia del equipo en la gestión de riesgos cibernéticos y ajustando las estrategias en función de los resultados obtenidos.

CONSIDERACIONES FINALES

Es importante considerar que la sostenibilidad de las mejoras requiere de un monitoreo continuo y actualizaciones periódicas del modelo de ciberseguridad, dado el dinamismo y la constante evolución del entorno digital y las amenazas cibernéticas. Se recomienda fortalecer la capacitación del personal y la automatización de procesos para mantener los logros alcanzados a largo plazo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Decir también que la integración del ciclo de vida del marco NIST ha promovido una cultura de mejora continua en la ciberseguridad de TPX, permitiendo una evaluación constante y ajustes necesarios frente a la evolución de amenazas, fortaleciendo la resiliencia de la organización

Tesis publicada con autorización del autor
No olvide citar esta tesis

11 Referencias Bibliográficas

Apaza Tineo, C. A. (2020). Implementación de políticas de ciberseguridad en empresas medianas del sector financiero en Perú. Lima, Lima, Perú: UNIVERSIDAD MAYOR DE SAN MARCOS.

Balasinorwala, & Bhagwani, V. (Febrero de 2023). Cyber Security. *Revista Internacional de Investigación Científica en Ingeniería y Gestión (IJSREM), 07*, 5.

Benavides, V. (2018). La ciberseguridad y el contexto actual. *Redalyc.org*, 7-10.

Bhagwani, V., & Balasinorwala, S. (2023). Cyber Security. *Revista científica india de investigación en ingeniería y gestión*, 2-7. doi:10.55041/ijsrem17691

BID. (2021). *Ciberseguridad en América Latina y el Caribe: Situación actual y recomendaciones.* Obtenido de https://publications.iadb.org

Böhme, R. &. (2020). The economics of cybersecurity: Principles and applications. *ACM Computing Surveys*, 52. doi:https://doi.org/10.1145/3316782

Bowen P. (Octubre de 2018). *NIST.* Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

Calderón Alarcón, R. (2018). Propuesta de un plan de seguridad de la información basado en la norma ISO 27001 para una empresa peruana de TI. *Propuesta de un plan de seguridad de la información basado en la norma ISO 27001 para una empresa peruana de TI*. Lima, Lima, Perú: Universidad Peruana de Ciencias Aplicadas.

CCL. (2022). *Informe sobre ciberseguridad en PYMEs limeñas.* LIMA: CCL.

Chinchilla, & Allende, &. (2017). Riesgo de Ciberseguridad en las Empresas. *Tecnología y Desarrollo*, 6-7.

Collins, & Hinds. (2021). Exploring workers' subjective experiences of habit formation in cybersecurity: A qualitative survey. *Cyberpsychology, Behavior, and Social Networking,*, 1-10. doi:https://doi.org/10.1089/cyber.2020.0631

Corletti, A. (2017). *Ciberseguridad. Una estrategia Informática Militar.* Madrid, España: DARFE. Obtenido de https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2018/LibroCiberseguridad_A.Corletti_nov2017.pd.pdf.

Creswell, J. W. (2014). Experimental and quasi-experimental designs for research on teaching. En J. W. Creswell, *Handbook of research on teaching.* SAGE Publications.

Creswell, J. W. (2014). *Qualitative, quantitative, and mixed methods approaches* (Vol. 4Th ed). SAGE Publications.

Cvetković-Vega, A. M. (2021). Estudios transversales / Cross-sectional studies. *Revista de la Facultad de Medicina Humana*, 179-185. doi:https://doi.org/10.25176/RFMH.v21i1.3069

Dedeke, A. (2017). Adopción del marco de ciberseguridad: uso de niveles de capacidad para niveles y perfiles de implementación. *doi: 10.1109/MSP.2017.3681063*, 47-54.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Delgado, M. F. (2021). Methodology Based on the NIST Cybersecurity Framework as a proposal for Cybersecurity Management in Government Organizations. *3C TIC. Cuadernos de desarrollo aplicados a las TIC*, 123-138.

Delgado, M. F., Esenarro, D., Juárez Regalado, F. F., & Díaz, R. M. (2021). Metodología basada en el marco de ciberseguridad del NIST como propuesta para la gestión de la ciberseguridad en organizaciones gubernamentales. *Metodología basada en el Marco de Ciberseguridad del NIST como propuesta para la gestión de la ciberseguridad en Organizaciones Gubernamentales*, 123-141.

Dempsey, K., & Nolan, R. (2014). NIST Special Publication (SP) 800-161: Supply chain risk management practices for federal information systems and organizations. *National Institute of Standards and Technology*. doi:10.6028

Diaz, & Puime Maroto, J. (2023). Marco Minimo de Ciberseguridad para PYMES en el contexto de la Industria 4.0. *Centro de Tecnología Avanzada CITAQ*, 47-48. Obtenido de https://dx.doi.org/10.5354/0719-3769.2021.57067

Dolezilek, D., & Hussey, L. (2011). Requirements or recommendations? Sorting out NERC CIP, NIST, and DOE cybersecurity. *3C TIC*, 328-333.

ESET. (2022). *Informe de amenazas cibernéticas en América Latina.* España: Pymes de TAI. Obtenido de https://www.eset.com

Ferreira, D. J., & São Mamede, H. (2022). Predicting Cybersecurity Risk - A Methodology for Assessments. *ARIS2 - Advanced Research on Information Systems Security*, 50-63. doi:10.56394/aris2.v2i2.23

Fisch, E., & White, G. (1999). Intrusion Detection Systems and Incident Response: Managing Cybersecurity Threats.

Forum, W. E. (2023). *World Economic Forum.* Cologny, Suiza: Grupo Editorial Holtzbrinck.

Gartner. (2023). *Top Security and Risk Management Trends for 2023.* Stamford, Connecticut EEUU: Gartner, Inc. Obtenido de https://www.gartner.com

Ghernaouti, S. (2013). *Ciberpoder: Una ciberseguridad global. Universidad de Lausanne.* EEUU: Presses Polytechniques et Universitaires Romandes (PPUR) .

Gordon, L. A. (2020). Investing in cybersecurity: Insights and implications from economics and accounting research. *Journal of Information Security*, 63-79. doi:https://doi.org/10.4236/jis.2020.112004

Hernández Sampieri, & R. Collado, L. L. (2014). Metodologia de la investigación. *MacGraw Hill*.

INEI. (2021). *Estadísticas de ciberseguridad en Perú.* LIMA: INEI.

Kamalanathan, K., Srinivas, S., & Krishnashree, A. (2021). Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations. *Digital Healthcare*, 12345-12349. doi:10.1109/access.2022.3145372

Kshetri. (2020). Cybersecurity in the post-COVID-19 era: Challenges and opportunities for startups. *Journal of International Technology and Information Management*, 1-15. Obtenido de https://doi.org/10.58729/1941-6679.1422

Tesis publicada con autorización del autor
No olvide citar esta tesis

León, J. (2021). Ciberseguridad y protección de datos personales en el Perú. 15-21. Lima, Lima, Perú.

Mendoza, S., & Vega, Gallegos. (2019). *Universidad Pacifico Escuela de Post Grado.* Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.up.edu.pe/bitstream/handle/11354/2250/Luis_Tesis_Maestria_2019.pdf?sequence=1&isAllowed=y

MTC. (2023). *Iniciativas de ciberseguridad en Perú.* LIMA: MTC.

MTC. (2023). *Iniciativas de ciberseguridad en Perú.* Lima.

NIST. (2018). *Marco para la mejora de la seguridad cibernética en infraestructuras críticas.* Whashinton: NIST. doi:10.6028/NIST.CSWP.04162018

NIST. (2021). *El Marco de Ciberseguridad del NIST.* Washington, DC: Departamento de Comercio de EEUU.

OEA. (2020). *Ciberseguridad en América Latina y el Caribe: Diagnóstico y recomendaciones.* Washington D. C., Estados Unidos: Revista Américas.

Peréz Ugarte, L. A. (2019). Evaluación de la seguridad de la información en empresas peruanas usando el marco NIST. *Evaluación de la seguridad de la información en empresas peruanas usando el marco NIST*. Lima, Lima, Perú: Pontificia Universidad Católica del Perú.

Ponemon Institute. (2022). Cost of a Data Breach Report 2022. IBM Security. *IBM Security*, 5. Obtenido de https://www.ibm.com/security/data-breach

Pontiroli, S. (2020). *Kaspersky Labs*. Obtenido de https://latam.kaspersky.com/about/press-releases/2020_kaspersky-america-latinaregistra-5-mil-ataques-de-ransomware-por-dia

PwC. (2023). Global Digital Trust Insights 2023. *PricewaterhouseCoopers*. Obtenido de https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html

Raynor, S. D. (2022). Cybersecurity. *Libros electrónicos de prensa de productividad*, 127-132. doi:10.4324/9781003304036-17

Rizzo, D., & Pagola, H. (2019). *"NIST CYBERSECURITY FRAMEWORK".* Obtenido de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1460_RizzoD.pdf

Ross, & McEvilley. (2018). NIST Special Publication (SP) 800-160. *NIST*. Obtenido de https://doi.org/10.6028/NIST.SP.800-160v1

Schneier, B. (2016). The Security Mindset. *Computadora IEEE*, 7-8.

Vivanco Toala, D., Bolaños Burgos, F., & Angulo Murillo , N. (2020). Estudio Exploratorio de las Estrategias para la Protección a las Redes Empresariales de las Infecciones Ransomware. *Revista Científica Multidisciplinaria Arbitrada YACHASUN*, 72-74. doi:DOI: https://doi.org/10.46296/yc.v4i7.0035

Yañez Intriago, J. (14 de Octubre de 2022). *Aplicación del NIST Cybersecurity Framework en el Instituto Superior Tenológico Sucre.* Obtenido de Repositorio.puce.edu.ec: https://repositorio.puce.edu.ec/items/ce4a629e-fce3-4167-9c65-095aea1cf0d3

Tesis publicada con autorización del autor
No olvide citar esta tesis

Zimroz, R. (2022). *Marco de Ciberseguridad del NIST y criterios de ciberseguridad.* Whashinton: Chapter. Obtenido de https://link.springer.com/: https://link.springer.com/chapter/10.1007/978-3-031-26845-8_5

Tesis publicada con autorización del autor
No olvide citar esta tesis

12 Anexos

ANEXO N°1 - MATRIZ DE CONSISTENCIA

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPOTESIS GENERAL	MÉTODO
¿En qué medida un modelo de ciberseguridad permite mejorar la seguridad de la información, basada en NIST en la empresa TPX, 2023?	Implementar un modelo de ciberseguridad para mejorar la seguridad de la información, basada en NIST en la empresa TPX, 2023	El modelo de ciberseguridad permitirá mejorar la seguridad de la información, basada en la metodología NIST en la empresa TPX, 2023	**DISEÑO:** El diseño de esta investigación es de tipo pre-experimental. Según Creswell presenta una visión práctica para investigadores: "cuando no es posible realizar un experimento verdadero, los diseños pre-experimentales (p. ej., estudio de un solo grupo) pueden usarse para explorar efectos preliminares, aunque recomienda pasos para mitigar sesgos y para justificar su uso." **TIPO:** Aplicada Según, Baena (2017), el tipo de investigación aplicada trata de darle un desenlace a una cuestión específica dentro de una realidad convirtiendo la teoría en una experiencia para generar nueva información que sea de utilidad **CORTE:** Transversal **ENFOQUE:** Cuantitativo **NIVEL DE INVESTIGACIÓN:** Explicativo. Para, Fernández & Baptista (2014) señalan que el nivel explicativo está dirigido a responder por las causas de los eventos y fenómenos físicos o sociales Se enfoca en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta, o por qué se relacionan dos o más variables.
PROBLEMAS ESPECIFICOS	**OBJETIVOS ESPECIFICOS**	**HIPOTESIS ESPECIFICAS**	
•¿En qué medida la implementación de un modelo de ciberseguridad basado en NIST mejora la identificación de riesgos y activos críticos en la seguridad de la información en la empresa TPX, 2023?	• Mejorar la identificación de riesgos y activos críticos en la empresa TPX mediante la metodología NIST.	• La aplicación de la metodología NIST permitirá una mejor identificación de riesgos y activos críticos en la empresa TPX.	
• ¿En qué medida la adopción de controles de ciberseguridad basados en NIST fortalece la protección de la información sensible en la empresa TPX, 2023?	• Fortalecer la protección de la información sensible a través de estrategias de seguridad de la metodología NIST.	• La adopción de controles de ciberseguridad basados en NIST mejora significativamente la protección de la información en la empresa TPX.	
• ¿En qué medida la implementación de un modelo de ciberseguridad basado en NIST	• Optimizar la detección de amenazas con sistemas de monitoreo y alertas basados en NIST.	• La implementación del modelo NIST incrementa la detección temprana de	

Tesis publicada con autorización del autor
No olvide citar esta tesis

optimiza la detección temprana de incidentes de seguridad en la empresa TPX, 2023? • ¿En qué medida la aplicación de estrategias de respuesta basadas en NIST mejora la eficiencia en la gestión de incidentes de seguridad en la empresa TPX, 2023? • ¿En qué medida la aplicación de mecanismos de recuperación basados en NIST mejora la continuidad operativa de la empresa TPX, 2023?	• Aumentar la eficiencia en la respuesta a incidentes mediante protocolos definidos en la metodología NIST. • Garantizar una rápida recuperación y continuidad operativa con planes de contingencia basados en NIST.	incidentes de ciberseguridad en la empresa TPX. • La metodología NIST optimiza la capacidad de respuesta ante incidentes de seguridad en la empresa TPX. • La aplicación de mecanismos de recuperación basados en NIST garantiza la continuidad operativa de la empresa TPX.	**POBLACIÓN:** 30 personas. Según el autor Arias (2006, p. 81) define población como "un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Esta queda delimitada por el problema y por los objetivos del estudio". La población está compuesta por la totalidad de la empresa TPX que es un total de 30 empleados. **MUESTRA:** 30 personas igual a la población. De acuerdo con un nivel de confianza del 99% con un margen de error del 5% la muestra es igual a la población. Según el autor Arias (2006, p. 83) define muestra como "un subconjunto representativo y finito que se extrae de la población accesible". La muestra consistirá en una selección representativa de diferentes departamentos o divisiones dentro de la organización que aborden las temáticas relevantes para el estudio, en este caso son: departamento de operaciones, departamento de marketing, departamento legal, departamento de Ux & Ui, departamento de tecnología, departamento contable.
			TECNICA DE RECOLECCIÓN DE DATOS: Encuestas y Entrevistas

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

ANEXO N°2 - MATRIZ DE OPERACIONALIZACIÓN

VARIABLES	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN	INSTRUMENTO
Variable Dependiente: **Ciberseguridad**	La ciberseguridad es la práctica de defender los sistemas, redes y programas de ataques digitales, que generalmente están dirigidos a acceder, cambiar o destruir información sensible (Hernández & Santos, 2019).	Identificación Protección Detección Respuesta Recuperación	El Baldrige Cybersecurity Excellence Builder (BCEB)	Escala Likert (1 = Totalmente Desacuerdo, 2 = desacuerdo, 3 = Indiferente, 4 = de Acuerdo, 5 = Totalmente de acuerdo)	Técnica: Cuestionario y Entrevista no estructurada Instrumento: Cedula del cuestionario y relación de preguntas. Herramientas: Cuantitativo = SPSS
Variable Independiente: **Aplicación de la Metodología NIST**	Según la *National Institute of Standards and Technology* (NIST), la metodología se refiere a un marco que ayuda a las organizaciones a entender, gestionar y reducir sus riesgos de ciberseguridad, y protege la infraestructura crítica (NIST, 2018).	No aplica	No aplica	No aplica	

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO N°3 - ENCUESTA / INSTRUMENTO DE EVALUACIÓN

La presente encuesta está orientado a la empresa TPX – Marketing Digital, las cuales todos los integrantes tienen conocimientos de informática, por el giro del negocio y la labor que realizan.

Totalmente Desacuerdo	En desacuerdo	Indiferente	De Acuerdo	Totalmente de acuerdo
1	2	3	4	5

Ítem	Pregunta	Valoración				
		1	2	3	4	5
D1: Identificación						
1	¿Cuál es su percepción sobre la importancia de identificar y evaluar activos críticos de información para garantizar la seguridad de la empresa?					
2	En su opinión, ¿es esencial revisar y actualizar regularmente las políticas internas de seguridad de la información en una empresa?					
3	Desde su perspectiva, ¿qué tan crucial es que el personal de una empresa tenga un alto nivel de conocimiento en prácticas de ciberseguridad?					
4	En su percepción, ¿cómo valoraría la eficacia actual de las medidas de seguridad implementadas por las empresas en general para identificar y mitigar amenazas cibernéticas?					
D2:	**Prevención**					
5	¿Cómo calificaría la efectividad general de los mecanismos de seguridad, en la prevención de amenazas cibernéticas en la empresa?					
6	¿Cómo evaluaría las políticas internas de seguridad de la información de la empresa ante amenazas cibernéticas?					
7	Desde su punto de vista, ¿cuál considera que es la importancia de la concientización del personal en la prevención de incidentes de seguridad de la información?					
8	¿Considera que la inversión en tecnologías avanzadas, puede mejorar significativamente la capacidad de una empresa para prevenir ataques cibernéticos?					
D3:	**Detección**					
9	Desde su punto de vista, ¿es importante establecer un monitoreo activo para identificar actividades sospechosas?					
10	En su perspectiva, ¿cómo calificaría usted la detección oportuna de amenazas cibernéticas?					
11	¿considera que la implementación de sistemas avanzados de detección, como análisis de comportamiento, mejora la capacidad de la empresa para identificar amenazas cibernéticas?					
12	¿Cuál es su percepción sobre la importancia de contar con un equipo de monitoreo activo (terceros) para evaluar comportamientos previos antes de detectar un incidente de seguridad?					
D4:	**Respuesta ante incidentes**					

Tesis publicada con autorización del autor
No olvide citar esta tesis

13	¿Usted considera que el tiempo de respuesta por algún tipo de incidentes es el adecuado?					
14	¿Qué nivel de madures tiene la organización frente a amenazas cibernéticas en la actualidad?					
15	En su opinión, ¿cómo evaluaría la eficacia de los planes de respuesta a incidentes de la empresa para mitigar los impactos de amenazas cibernéticas?					
16	¿Cuál es su percepción sobre la eficacia de la empresa en general para aprender de incidentes previos y mejorar sus estrategias de respuesta a ciberataques?					
D5:	**Recuperación**					
17	En su perspectiva, ¿cómo calificaría la eficacia de las estrategias de recuperación implementadas por la empresa para restablecer operaciones después de sufrir un incidente?					
18	¿Está de acuerdo sobre la importancia de contar con backups regulares y actualizados como parte de la estrategia de recuperación de una empresa frente a eventos de ciberseguridad?					
19	Desde su perspectiva, ¿considera que las inversiones significativas en tecnologías de recuperación son necesarias para garantizar la resiliencia de la empresa frente a incidentes cibernéticos?					
20	¿Está de acuerdo en que la colaboración con socios externos, como proveedores de servicios de ciberseguridad, es esencial para mejorar la capacidad de recuperación de una empresa?					

ANEXO 3A - VALIDACIÓN DEL ENVÍO DEL PROYECTO DE TESIS

Facultad de Ciencias Empresariales

UNIVERSIDAD CIENTÍFICA DEL SUR

ANEXO 3 A

VALIDACIÓN DEL ENVÍO DE PROYECTO DE TESIS

Lima, 25 de julio de 2024

Yo, CARLOS ENRIQUE LOPEZ SOVERO, docente a tiempo de la FACULTAD DE CIENCIAS EMPRESARIALES de la Carrera de INGENIERÍA DE SISTEMAS EMPRESARIALES, asesor del estudiante MARLON ENRIQUE NUÑEZ COSINGA estudiante de la Carrera de INGENIERÍA DE SISTEMAS EMPRESARIALES en la elaboración del proyecto de tesis titulado:

"APLICACIÓN DE LA METODOLOGIA NIST EN LA MEJORA DE CIBERSEGURIDAD DE LA EMPRESA TPX, 2023"

Confirmo que he revisado dicho proyecto y considero que la versión presentada puede ser sometida a evaluación por la Dirección General de Investigación, Desarrollo e Integridad Científica.

Atentamente,

Asesor de la tesis
Mg. LOPEZ SOVERO CARLOS ENRIQUE

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO N°4 - BASE DE DATOS

Data Pretest

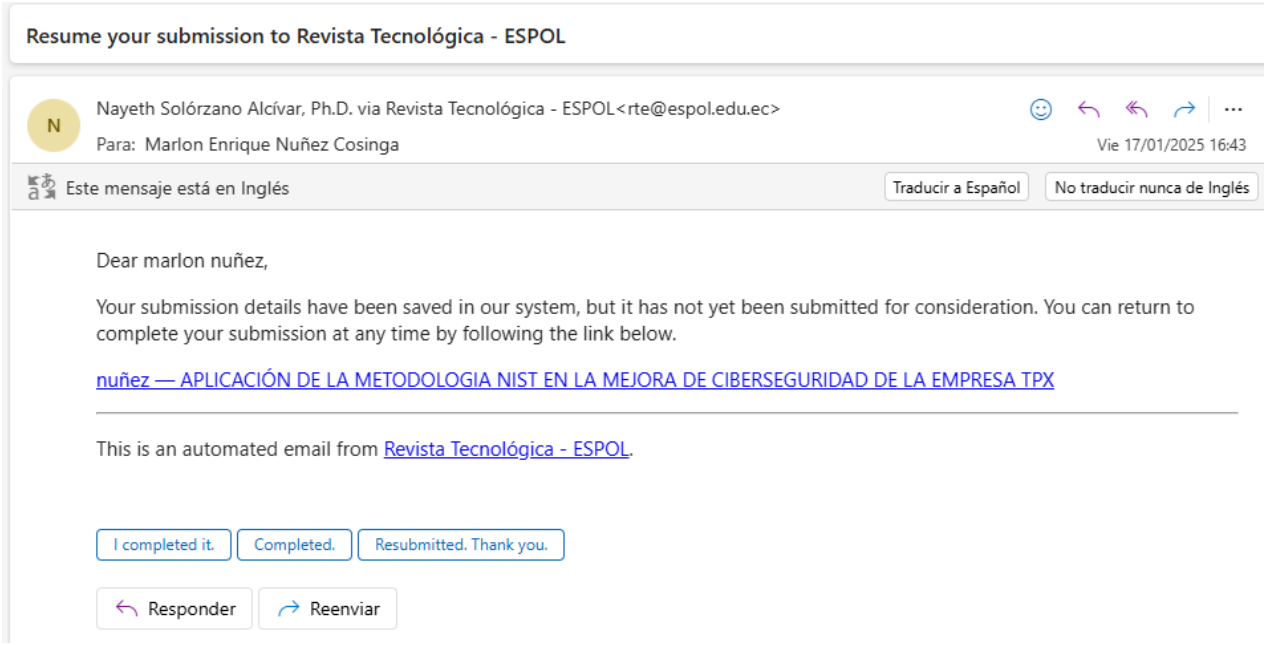
	VALORACIÓN DE LAS DIMENSIONES DEL NIST MEDIANTE LA ENCUESTA																								
	D1				D2				D3				D4				D5								
N°	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	D1	D2	D3	D4	D5	TOTAL
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	4	4	4	4	20
2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	20	20	20	20	20	100
3	3	3	3	2	3	3	4	4	4	3	3	3	3	4	4	2	4	4	3	4	11	14	13	13	15	66
4	3	1	3	3	1	1	1	3	1	1	3	4	1	1	3	1	1	2	1	1	10	6	9	6	5	36
5	2	3	1	2	3	3	2	3	3	2	3	3	3	2	2	3	2	3	3	3	8	11	11	10	11	51
6	2	2	1	3	3	2	2	3	3	3	3	3	2	2	2	2	2	2	2	5	8	10	12	8	11	49
7	3	4	4	3	4	5	2	4	3	4	3	5	5	5	4	4	4	5	5	4	14	15	15	18	18	80
8	3	3	1	3	1	1	1	3	1	1	3	2	1	3	1	1	1	1	2	5	10	6	7	6	9	38
9	3	4	3	4	3	4	4	4	3	4	4	4	4	4	4	5	5	5	4	4	14	15	15	17	18	79
10	5	5	3	5	4	5	5	5	3	5	4	5	4	3	5	4	5	3	4	5	18	19	17	16	17	87
11	3	3	4	5	4	5	4	4	4	3	4	4	4	4	4	4	4	5	5	5	15	17	15	16	19	82
12	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	20	20	20	20	20	100
13	1	2	3	5	4	3	4	4	1	2	1	3	3	4	4	2	4	3	3	3	11	15	7	13	13	59
14	2	2	3	2	2	1	2	2	1	1	3	3	3	3	2	1	1	1	2	2	9	7	8	9	6	39
15	3	2	3	3	2	4	3	2	3	2	3	3	3	4	3	3	3	3	2	3	11	11	11	13	11	57
16	5	4	4	4	4	4	4	4	3	4	4	4	5	4	3	2	4	3	4	4	17	16	15	14	15	77
17	2	3	1	2	3	3	2	3	3	2	3	3	3	2	2	3	2	3	3	3	8	11	11	10	11	51
18	1	2	1	2	3	3	3	4	1	2	3	3	3	2	3	3	2	3	2	5	6	13	9	11	12	51
19	2	3	1	2	3	3	2	3	3	2	3	3	3	2	2	3	2	3	3	3	8	11	11	10	11	51
20	3	3	3	3	3	3	3	3	3	1	2	1	3	1	3	3	3	5	3	3	12	12	7	10	14	55
21	3	2	3	3	2	2	3	2	4	3	3	3	2	2	3	2	2	3	2	4	11	9	13	9	11	53
22	3	2	3	1	1	1	1	2	1	1	1	2	2	3	2	1	1	2	2	1	9	5	5	8	6	33
23	3	3	3	3	3	3	1	1	2	4	3	5	3	4	4	5	4	2	3	5	12	8	14	16	14	64
24	3	2	3	3	2	4	4	4	3	3	4	4	4	3	4	4	3	4	4	4	11	14	14	15	15	69
25	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	18	20	20	20	20	98
26	4	4	4	5	3	4	5	4	5	5	5	4	5	5	4	5	4	4	3	5	17	16	19	19	16	87
27	3	3	4	3	4	4	3	5	5	3	4	5	3	4	5	3	5	4	4	3	13	16	17	15	16	77
28	3	5	5	5	5	5	4	5	4	3	5	5	5	5	5	5	5	3	4	4	18	19	17	20	16	90
29	3	3	5	5	4	5	3	3	2	3	3	3	3	3	3	2	4	3	3	5	16	15	11	11	15	68
30	5	5	5	5	5	4	4	5	3	1	5	5	5	5	5	3	5	5	5	5	20	18	14	18	20	90

Data Postest

ID	Item1	Item2	Item3	Item4	Item5	Item6	Item7	Item8	Item9	Item10	Item11	Item12	Item13	Item14	Item15	Item16	Item17	Item18	Item19	Item20	Total
1	5	4	5	5	3	5	5	4	5	4	5	4	3	4	5	4	3	5	3	4	85
2	5	4	3	3	3	3	4	5	3	5	3	3	4	3	4	3	3	3	5	4	73
3	4	5	5	5	4	3	3	5	4	3	5	5	5	5	4	5	3	4	3	5	85
4	3	5	4	5	3	5	5	3	5	4	5	4	4	5	3	3	4	3	5	4	82
5	4	3	4	4	3	3	4	5	4	4	4	5	3	5	5	4	5	5	4	5	83
6	3	5	5	4	4	5	5	3	4	4	3	4	3	4	5	5	3	4	4	4	81
7	3	4	4	3	5	4	5	3	4	3	5	3	3	5	3	5	4	3	3	3	75
8	3	3	3	4	3	3	3	5	5	4	4	3	5	5	4	5	5	3	5	3	78
9	3	4	5	4	4	3	4	4	5	3	4	4	3	5	4	4	5	4	5	5	82
10	5	4	4	5	5	5	4	4	5	5	3	3	5	4	5	5	4	4	5	5	89
11	4	5	3	3	3	3	4	3	3	3	4	5	4	4	4	3	4	3	5	5	75
12	3	3	5	4	4	4	4	4	5	5	4	5	3	4	3	4	4	5	4	5	82
13	3	5	4	4	3	4	3	5	3	4	4	5	3	3	3	4	3	4	3	4	74
14	5	5	5	3	4	3	3	5	3	5	4	3	5	5	3	5	4	3	4	3	80
15	4	5	5	5	5	5	5	4	3	3	4	4	5	5	4	4	5	3	4	5	87
16	4	5	5	4	4	4	4	4	4	4	4	4	4	4	5	5	4	4	4	3	83
17	5	3	5	3	5	3	3	5	5	5	4	5	4	3	3	5	5	4	5	4	84
18	5	4	3	4	4	4	5	5	5	3	5	4	4	5	5	3	4	3	3	5	83
19	5	4	5	4	4	3	5	5	4	3	5	5	5	5	5	3	5	4	3	5	87
20	4	3	5	5	4	5	3	5	3	4	4	3	3	4	3	5	4	4	3	3	77
21	3	3	4	5	4	4	5	3	3	4	3	4	4	3	3	3	3	3	5	3	72
22	5	4	4	3	5	3	3	4	4	3	5	4	4	4	5	5	5	4	4	4	82
23	5	5	5	4	4	4	3	3	5	5	4	5	5	4	4	5	3	4	3	5	85
24	5	4	3	5	3	5	5	3	5	3	3	4	5	4	3	5	5	3	3	5	81
25	3	4	5	3	4	4	3	3	4	5	3	5	3	3	3	3	4	5	5	5	77
26	3	4	5	3	3	3	5	4	5	5	5	3	4	4	4	5	3	5	5	3	81
27	4	3	4	5	3	4	3	3	4	4	5	3	4	4	4	3	4	3	4	4	75
28	3	5	3	5	5	4	3	5	3	5	3	5	4	4	3	5	5	5	4	5	84
29	3	5	3	5	5	3	3	3	4	5	3	5	3	4	5	4	5	3	3	3	77
30	4	3	3	3	4	4	5	5	3	3	3	3	3	4	4	3	5	4	4	3	73

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO N°5 - ENVÍO DEL ARTICULO



Resume your submission to Revista Tecnológica - ESPOL

N

Nayeth Solórzano Alcívar, Ph.D. via Revista Tecnológica - ESPOL<rte@espol.edu.ec>

Para: Marlon Enrique Nuñez Cosinga

Vie 17/01/2025 16:43

Este mensaje está en Inglés

Traducir a Español | No traducir nunca de Inglés

Dear marlon nuñez,

Your submission details have been saved in our system, but it has not yet been submitted for consideration. You can return to complete your submission at any time by following the link below.

nuñez — APLICACIÓN DE LA METODOLOGIA NIST EN LA MEJORA DE CIBERSEGURIDAD DE LA EMPRESA TPX

This is an automated email from Revista Tecnológica - ESPOL.

I completed it. | Completed. | Resubmitted. Thank you.

Responder | Reenviar

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO N°6 - CONSENTIMIENTO INFORMADO

ANEXO 19

FORMATO DE CONSTANCIA DE CONSENTIMIENTO INFORMADO DE ACCESO PÚBLICO (Empresa)

Por medio de la presente, informamos que la empresa TPX SAC autoriza al tesista MARLON ENRIQUE NUÑEZ COSINGA con código de matrícula 100058567 de la carrera profesional de INGENIERÍA DE SISTEMAS EMPRESARIALES de la Universidad Científica del Sur, hacer uso de la información que a continuación se detalla, con el consentimiento de la institución, para el desarrollo de su tesis de grado, la cual lleva por título: **APLICACIÓN DE LA METODOLOGIA NIST EN LA MEJORA DE CIBERSEGURIDAD DE LA EMPRESA TPX, 2023**

Información y/o permiso solicitado y a emplear en la tesis:

1. ~~REGISTRO DE LOS TRABAJADORES CONTRADOS~~
2. ~~REGIDSTRO DE ASISTENCIA D ELOS TRABAJORES DE LOS 2 AÑOS~~
3. ~~DATOS DE LA IMP´LEMENTACION DEL SISTEMA XX~~
4. PERMISO PARA REALIZAR ENCUESTA A LOS TRABAJADORES DE PLANTA

Dicha información, se recopilará en el Trabajo de Campo para posteriormente ser registrada en su investigación con fines netamente pedagógicos.

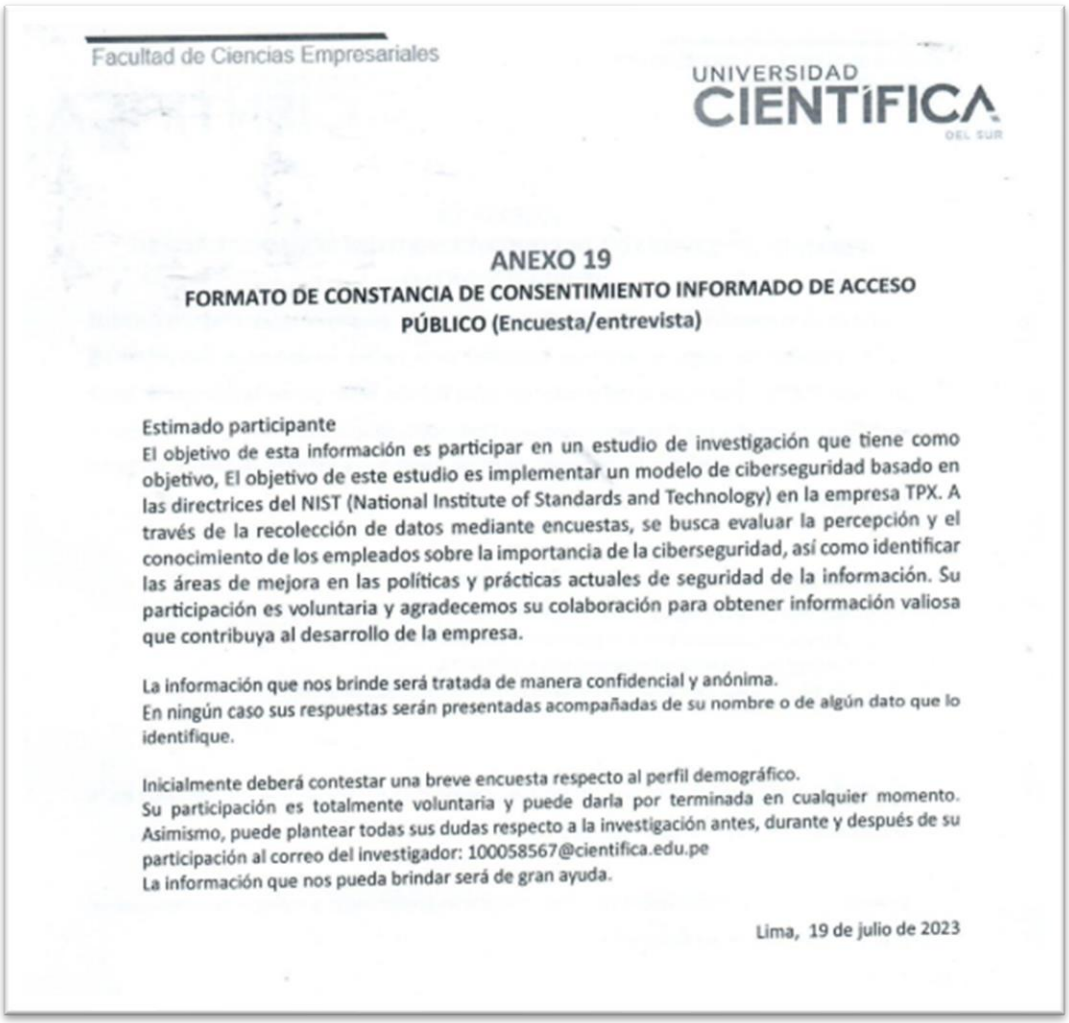
Se expide la presente CONSTANCIA DE CONSENTIMIENTO INFORMADO, a solicitud del interesado (a) para los fines que estime conveniente.

Lima, 14 de julio de 2023

Firma del Tesista
DNI: 10868433

Firma y sello de la Empresa
Razón Social de la Empresa: TPX SAC
RUC: 20608553089
Sitio web: www.grupotpx.com

Tesis publicada con autorización del autor
No olvide citar esta tesis



Facultad de Ciencias Empresariales

UNIVERSIDAD CIENTÍFICA DEL SUR

ANEXO 19

FORMATO DE CONSTANCIA DE CONSENTIMIENTO INFORMADO DE ACCESO PÚBLICO (Encuesta/entrevista)

Estimado participante
El objetivo de esta información es participar en un estudio de investigación que tiene como objetivo, El objetivo de este estudio es implementar un modelo de ciberseguridad basado en las directrices del NIST (National Institute of Standards and Technology) en la empresa TPX. A través de la recolección de datos mediante encuestas, se busca evaluar la percepción y el conocimiento de los empleados sobre la importancia de la ciberseguridad, así como identificar las áreas de mejora en las políticas y prácticas actuales de seguridad de la información. Su participación es voluntaria y agradecemos su colaboración para obtener información valiosa que contribuya al desarrollo de la empresa.

La información que nos brinde será tratada de manera confidencial y anónima.
En ningún caso sus respuestas serán presentadas acompañadas de su nombre o de algún dato que lo identifique.

Inicialmente deberá contestar una breve encuesta respecto al perfil demográfico.
Su participación es totalmente voluntaria y puede darla por terminada en cualquier momento. Asimismo, puede plantear todas sus dudas respecto a la investigación antes, durante y después de su participación al correo del investigador: 100058567@cientifica.edu.pe
La información que nos pueda brindar será de gran ayuda.

Lima, 19 de julio de 2023

ANEXO N°7 - LINK DE ACCESO A PAPER

Se pone a disposición el paper realizado, y enviado a la revista científica ESPOL según el formato que requiere.

https://drive.google.com/drive/folders/1DS1WkKFrqVhJ_4O-3heNvfekRVKRKTYQ?usp=sharing

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO 8 – PROCEDIMIENTO METODOLÓGICO DE APLICACIÓN DEL NIST EN LA EMPRESA TPX

1. Introducción

En el presente Anexo se describe cómo se aplicó la metodología NIST (CSF) en la empresa TPX, en el contexto del trabajo de investigación titulado: **"APLICACIÓN DE LA METODOLOGÍA NIST EN LA MEJORA DE CIBERSEGURIDAD DE LA EMPRESA TPX. 2023"**

La empresa TPX, dedicada a procesos tecnológicos estratégicos, requiere fortalecer su postura de ciberseguridad. Este procedimiento metodológico integra el análisis AS-IS y TO BE con los resultados de la evaluación de madurez con el Modelo Baldrige Cibersecurity desarrollados en el estudio, y define cómo el NIST (CSF) se utilizó para generar mejoras específicas en los procesos de seguridad de la organización.

2. Fundamentos de la Metodología NIST CSF

El NIST (CSF) es un estándar internacional que organiza las actividades de ciberseguridad en cinco funciones fundamentales:

Identify (Identificar): reconocer los activos, riesgos, contexto y recursos organizacionales.

Protect (Proteger): establecer controles y salvaguardas para limitar el impacto de incidentes.

Detect (Detectar): implementar capacidades para identificar eventos de seguridad oportunamente.

Respond (Responder): definir acciones para contener y mitigar incidentes.

Recover (Recuperar): restaurar servicios y operaciones después de un incidente.

Cada función se subdivide en categorías y subcategorías, que permiten estructurar las actividades de ciberseguridad. El NIST CSF ofrece flexibilidad para que las organizaciones definan su propio perfil de seguridad, ajustado a su contexto y objetivos estratégicos.

3. Contexto de Aplicación en la Empresa TPX

El trabajo realizado con TPX incluyó:

Tesis publicada con autorización del autor
No olvide citar esta tesis

Diagnóstico AS-IS: levantamiento de la situación actual en procesos, tecnología y gestión de seguridad.

Diagnóstico TO BE: El diagnóstico TO BE proyectado para la empresa TPX es propuesto como una visión sólida de madurez en ciberseguridad, dentro de sus posibilidades, orientada a implementar controles robustos, procesos bien definidos y capacidades de monitoreo continuo, alineados con el NIST, lo que permitirá reducir las brechas detectadas en el estado AS-IS y elevar significativamente la resiliencia operativa de la organización.

Evaluación de madurez (Modelo Baldrige): para medir el nivel de madurez de sus procesos de gestión y seguridad, dando como resultado un nivel muy bajo demasiado reactivo.

Estas fases revelaron brechas importantes en áreas como monitoreo, gestión de incidentes y planes de continuidad. A partir de este diagnóstico, se definió el procedimiento de aplicación del NIST CSF para cubrir esas brechas.

4. Procedimiento Metodológico de Aplicación del NIST CSF

La metodología aplicada en TPX se estructuró en las siguientes fases, enmarcadas en el ciclo de mejora continua:

Fase 1: Identificación (Identify)

En esta fase, TPX realizó:

Inventario de activos:

Se identificaron activos críticos de información relacionados también a sus endpoint (servidores, aplicaciones, bases de datos, procesos clave).

Análisis de contexto:

Se documentaron factores internos y externos que impactan la seguridad (clientes, regulaciones, amenazas específicas del sector).

Análisis de riesgos:

Tesis publicada con autorización del autor
No olvide citar esta tesis

Se determinó el nivel de exposición de cada activo, usando matrices de impacto y probabilidad.

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
Levantamiento de activos	Identificar y clasificar activos tecnológicos y procesos.	Área TI / Seguridad (se le asigna la responsabilidad)
Análisis de amenazas	Determinar amenazas más probables y sus impactos.	Comité de Seguridad (se determina un comité)
Matriz de riesgos	Evaluar vulnerabilidades y niveles de riesgo.	Seguridad de la Información (se le asigna la responsabilidad)

Fuente: Elaboración Propia

Esta primera fase me permitió construir el perfil actual (Current Profile) en el Framework NIST, alineado a las categorías de Identify, o identificación destacando deficiencias en documentación de activos y análisis de riesgos.

Fase 2: Protección (Protect)

Basándome en las brechas identificadas, se definió para TPX pueda implementar medidas para proteger sus activos. Entre ellas:

- ✓ Creación de políticas de seguridad actualizadas.
- ✓ Definición de controles de acceso basados en principios de mínimo privilegio.
- ✓ Capacitación al personal sobre ciberseguridad.

ACTIVIDAD	DESCRIPCIÓN	RESPONSABILIDAD
Desarrollo de Políticas	Redactar y aprobar políticas alienadas al NIST	Seguridad de la Información
Controles Técnicos	Configuración de firewalls, Segmentación de red	Área TI

Tesis publicada con autorización del autor
No olvide citar esta tesis

Programas de Capacitación	Sensibilización de empleados sobre amenazas comunes.	Recursos Humanos

Fuente: Elaboración Propia

Se priorizó la actualización de políticas de seguridad, especialmente en el manejo de información crítica, alineadas a la categoría Access Control (PR.AC) del Framework.

Fase 3: Detección (Detect)

Se propuso que la empresa TPX implemente capacidades de detección para identificar incidentes en forma temprana:

- ✓ Configuración de herramientas de monitoreo y correlación de eventos (SIEM).
- ✓ Definición de procesos de revisión de logs.

ACTIVIDAD	DESCRIPCIÓN	RESPONSABILIDAD
Configuración SIEM	Implementación de herramientas de monitoreo centralizado	Área TI / Seguridad
Revisión de Logs	Análisis periódico de registros	Seguridad de la Información

Fuente: Elaboración Propia

Se evidenció que TPX tenía capacidades muy limitadas en monitoreo. La adopción de un SIEM fue considerada prioritaria para mejorar su madurez en la función Detect.

Fase 4: Respuesta (Respond)

Se desarrollaron planes de acción para gestionar incidentes de seguridad:

- ✓ Definición de roles y responsabilidades durante un incidente.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- ✓ Procedimientos para comunicación interna y externa.
- ✓ Plantillas de gestión de incidentes.

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
Plan de Respuesta	Documentar procesos de gestión de incidente	Seguridad de la Información
Comunicación	Establecer protocolos de notificación	Gerencia / Seguridad (Asignación de responsabilidad)

Fuente: Elaboración Propia

Se estableció un plan de respuesta que contempla incidentes en sistemas críticos, con procedimientos escalonados según la gravedad.

Fase 5: Recuperación (Recover)

Se consideró la elaboraron planes para restablecer operaciones rápidamente tras un incidente:

- ✓ Se consideró la elaboración de planes de recuperación y continuidad.
- ✓ Ejercicios de simulacro para probar la eficacia de los planes.

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
Consideración de desarrollo de planes	Redactar planes de continuidad y recuperación.	Área de TI / Seguridad
Realizar Simulacros continuos	Ejercitar recuperación de sistemas críticos	Seguridad de la Información

Fuente: Elaboración Propia

Se consideró muy seriamente elaborar planes de diseño para restaurar operaciones en menos de 24 horas para los procesos críticos identificados durante el análisis AS-IS.

Tesis publicada con autorización del autor
No olvide citar esta tesis

5. Integración NIST CSF – Baldrige en TPX

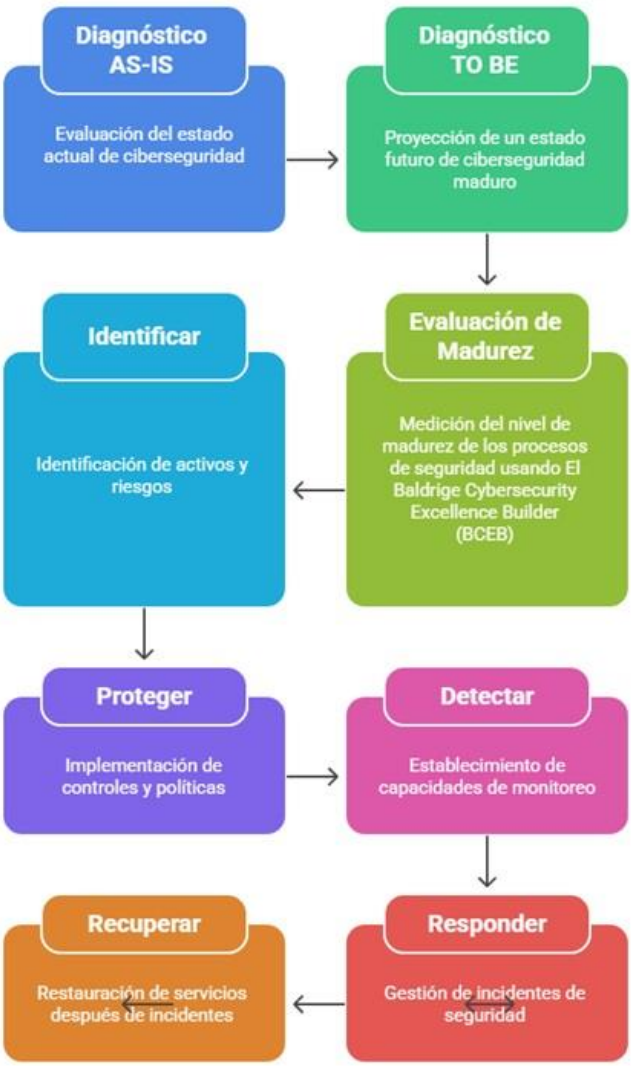
La aplicación del NIST CSF en TPX se vinculó estrechamente con el Modelo Baldrige El Baldrige Cybersecurity Excellence Builder (BCEB), usado en el trabajo como herramienta de medición de madurez. Esto permitió los siguiente:

- ✓ Se propuso asociar cada función NIST con áreas estratégicas de gestión.
- ✓ Se solicitó priorizar mejoras en liderazgo, estrategia, procesos y resultados.
- ✓ Se propuso traducir hallazgos técnicos en acciones de gestión empresarial.

6. Diagrama de Aplicación General del trabajo del NIST CSF a la empresa TPX

Se adjunta el siguiente diagrama para ilustrar el procedimiento de manera más global:

Ilustración 17: Diagráma General del Proceso



Fuente: Elaboración Propia

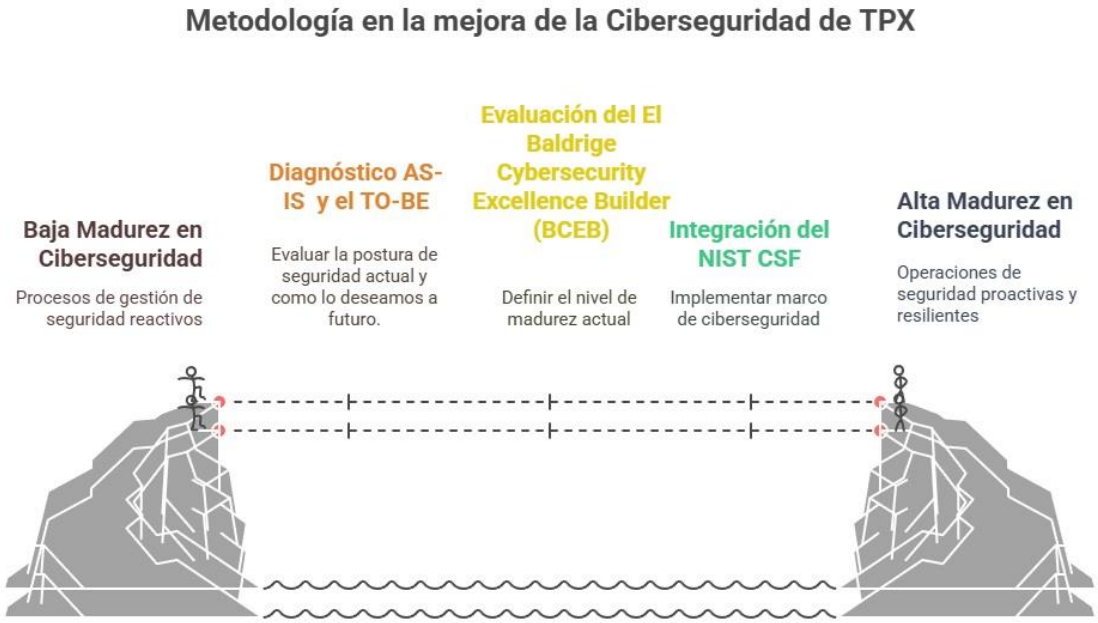
Tesis publicada con autorización del autor
No olvide citar esta tesis

La metodología NIST CSF aplicada a la empresa TPX y la aplicación de los aportes que considero importante como el uso del AS-IS el TO-BE además de ello también el Baldrige poco conocido pero muy importante para evaluar la madurez de una organización; todo ello considero que permitió traducir un diagnóstico técnico en acciones prácticas y medibles, reduciendo las brechas detectadas y fortaleciendo la postura de ciberseguridad de la empresa. Es importante destacar que la estructura metodológica desarrollada en esta tesis constituye, en términos analógicos, un puente que permite a cualquier organización cruzar el umbral de incertidumbre que, de no gestionarse adecuadamente, podría conducir al fracaso, especialmente en empresas jóvenes o en crecimiento. Si este fenómeno se replicara en numerosas organizaciones emergentes en países como Perú o en Latinoamérica, considerando además el creciente número de ciberataques que se producen a diario, podría derivar en una catástrofe económica a nivel nacional. Las empresas, más allá de aquellas dedicadas exclusivamente a la exportación de recursos naturales, representan un pilar fundamental para la economía de un país, y su protección frente a amenazas cibernéticas es esencial para garantizar la estabilidad y el desarrollo sostenible.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Entonces puedo afirmar que el trabajo expuesto y detallado va posicionar a la empresa TPX en un mejor nivel de madurez, con procesos más sólidos y capacidad de respuesta ante amenazas cibernéticas. Aquí se muestra a manera de resumen una gráfica que podría dar mayor claridad a la analogía que afirmo y sostengo.

Ilustración 18: Metodología en la mejora de la Ciberseguridad de TPX



Fuente: Elaboración Propia

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO 9 – INVERSIÓN EN CIBERESEGURIDAD

La inversión en ciberseguridad, especialmente orientada a incrementar el grado de madurez de los procesos, ha sido objeto de amplias discusiones en la literatura reciente. Si bien existe consenso sobre la necesidad de proteger los activos críticos, los autores discrepan respecto al nivel de inversión óptimo y el retorno esperado frente al riesgo de incidentes.

Gordon et al. (2020) sostienen que, si bien la inversión en seguridad es necesaria, existe un punto de rendimientos decrecientes, es decir, cada dólar adicional invertido en ciberseguridad genera menor retorno en términos de reducción de riesgo. Según su estudio, “los beneficios marginales de incrementar el nivel de madurez en seguridad tienden a disminuir una vez superado un umbral básico de protección” (Gordon et al., 2020, Journal of Information Security).

En contraste, Ponemon Institute (2022) revela que las empresas con niveles más altos de madurez cibernética no solo presentan menos incidentes, sino que logran costos significativamente más bajos cuando se produce un ataque. Su investigación muestra que “las organizaciones con una postura madura gastaron en promedio 58% menos en la contención de incidentes que aquellas con madurez básica” (Ponemon Institute, 2022, Cost of a Data Breach Report).

Tesis publicada con autorización del autor
No olvide citar esta tesis

Por su parte, Böhme y Moore (2020) cuestionan el supuesto de que una mayor madurez técnica siempre justifica costos elevados, señalando que en algunos sectores, especialmente en pequeñas y medianas empresas (PYMEs), el costo de alcanzar ciertos niveles de madurez puede ser desproporcionado respecto al valor de los activos protegidos. En palabras de los autores, “la estrategia óptima para muchas organizaciones podría ser aceptar un riesgo residual en lugar de aspirar a niveles altos de madurez que implican altos costos continuos” (Böhme & Moore, 2020, ACM Computing Surveys).

Finalmente, PwC (2023) adopta una visión pragmática y plantea que, aunque la inversión en ciberseguridad es creciente, debe estar alineada a objetivos de negocio y no simplemente guiada por estándares de madurez. Su reporte advierte que “las organizaciones deben evitar gastar excesivamente en áreas de seguridad que tienen bajo impacto en el negocio y priorizar inversiones que respalden la resiliencia operativa” (PwC, 2023, Global Digital Trust Insights).

En conclusión, podíamos indicar que, mientras algunos autores destacan que invertir en medidas preventivas de ciberseguridad genera beneficios económicos y reduce costos frente a posibles incidentes, otros señalan que aumentar demasiado el nivel de madurez puede implicar gastos elevados que no siempre se compensan con beneficios reales. Este debate pone de manifiesto la importancia de que las empresas evalúen cuidadosamente su contexto, los

Tesis publicada con autorización del autor
No olvide citar esta tesis

riesgos específicos que enfrentan y su capacidad financiera, antes de determinar cuánto invertir en fortalecer su ciberseguridad.

Tabla: Estimaciones de inversión en ciberseguridad

Tamaño de empresa	Inversión recomendada en ciberseguridad (% de IT)	Costo promedio anual en USD	Fuente / Autor
Pequeña (≤ 100 empleados)	7 % – 10 % del presupuesto IT	USD 10,000 – USD 50,000	Gordon et al. (2020)
Mediana (101 – 1,000 empleados)	6 % – 9 % del presupuesto IT	USD 50,000 – USD 500,000	PwC (2023)
Grande (> 1,000 empleados)	5 % – 8 % del presupuesto IT	USD 1 millón – USD 5 millones	Ponemon Institute (2022)
Empresas críticas (sector financiero, salud, energía)	≥ 10 % del presupuesto IT	USD 5 millones – USD 20 millones	Böhme & Moore (2020)

Fuente: Elaboración propia, con datos de distintos autores.

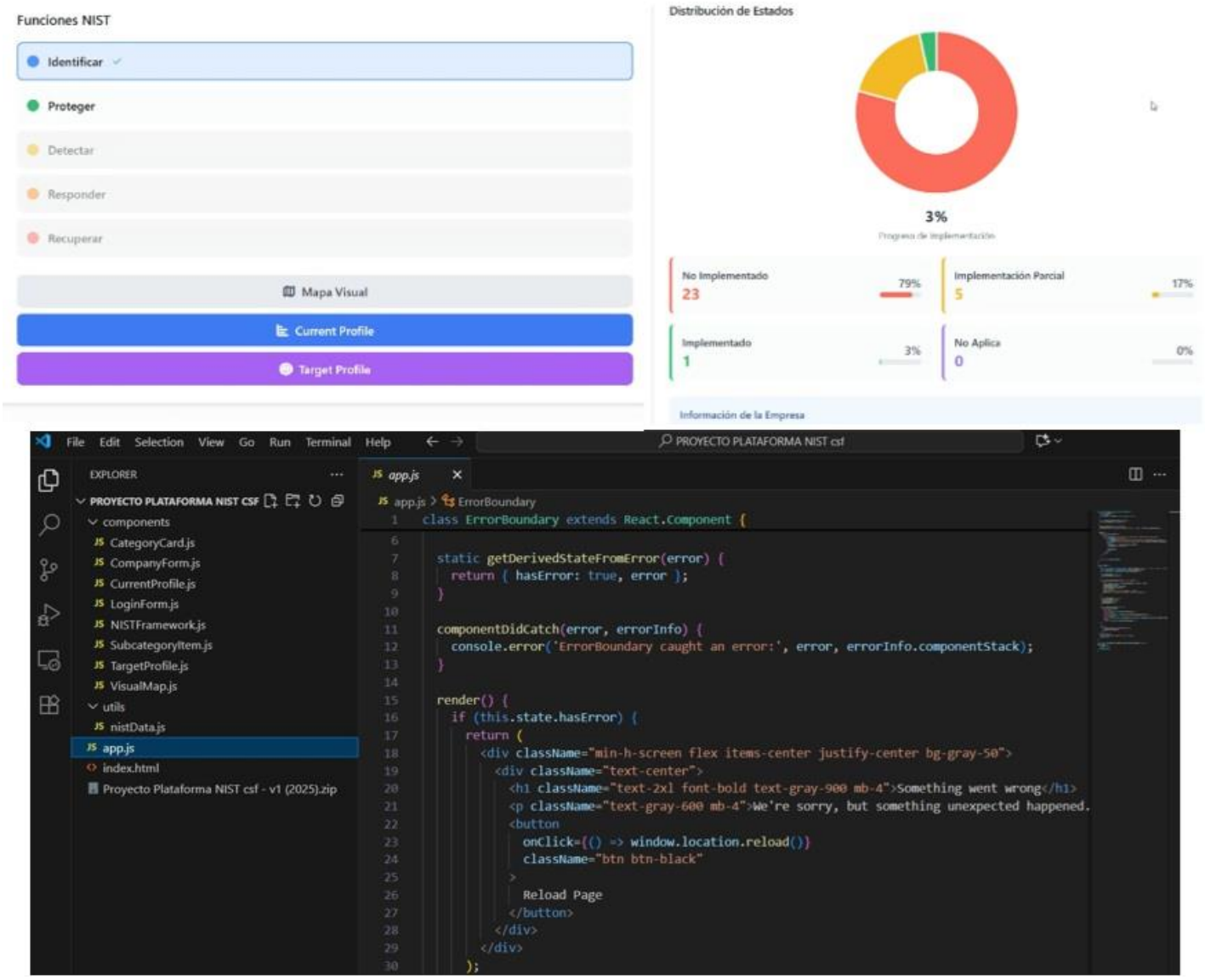
Con relación al NIST csf no se puede tener un costo exacto, ya que su implementación va a depender mucho de las consultorías para el análisis del AS-IS y del GAP, así como también de las adquisiones de herramientas como por ejemplo un SIEM o un EDR, los equipos para el backups; además también las capacitaciones que son muy importantes para el personal, el diseño de políticas, las auditorias periódicas entre muchas otras cosas que se necesitan, ya que debe entenderse que la implementación del NIST no es un producto, sino un conjunto de prácticas y controles.

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO 10 – IMÁGENES DE LA CREACIÓN DE LA HERRAMIENTA BASADA EN NIST

Dado que el marco NIST contempla cinco funciones, veintitrés categorías y ciento ocho subcategorías, su implementación puede resultar compleja. Por ello, diseñé una herramienta que facilita el proceso, permitiendo centrar todos los esfuerzos en la fase de evaluación. De este modo, es posible identificar con mayor precisión los gaps o brechas existentes entre el current profile y el target profile, optimizando así la gestión de la ciberseguridad organizacional para esta y cualquier empresa del mundo.

Ilustración 19: Herramienta creada basada en NIST CSF



Fuente: Elaboración Propia

Tesis publicada con autorización del autor
No olvide citar esta tesis

RESOLUCION DIRECTORIAL DE CARRERA: Ingeniería de Sistemas Empresariales -CI-DAFCE-U. CIENTIFICA-2020

CARRERA DE: Ingeniería de Sistemas Empresariales

Lima 05 de 09 del 2024

VISTO:

El informe de resolución independiente académico del proyecto de tesis titulado: APLICACIÓN DE LA METODOLOGIA NIST EN LA MEJORA DE CIBERSEGURIDAD DE LA EMPRESA TPX, 2023 presentado por:

-MARLON ENRIQUE NUÑEZ COSINGA //

CONSIDERADO:

Que, de acuerdo con el Reglamento General de la Universidad Científica del Sur y los reglamentos de para obtener el título profesional en la Carrera de Ingeniería de Sistemas Empresariales, se debe desarrollar un trabajo de investigación.

Que, de acuerdo normativa vigente de la Universidad Científica del Sur, en uso de las atribuciones conferidas al director académico de carrera.

SE RESUELVE:

Aprobar e inscribir el proyecto de tesis titulado: APLICACIÓN DE LA METODOLOGIA NIST EN LA MEJORA DE CIBERSEGURIDAD DE LA EMPRESA TPX, 2023 con Número de registro: PRE-12-2024-00559, y establecer el inicio del periodo de ejecución del mencionado proyecto.
Nombrar al docente Carlos Enrique López Sovero // como asesor para el desarrollo de tesis en cuestión
Regístrese, Comuníquese y archívese

Director Académico
Carrera de Ingeniería de Sistemas Empresariales

Dr. Wester Edison Zela Moraya Director de Departamento Académico de Ingeniería de Sistemas Empresariales	**Mg. Brian Andreé Meneses Claudio** Responsable de Investigación de Ingenierías de Ciencias Empresariales