Revista de investigación de sistemas e informática
17(2): 205-219 (2024)
DOI: https://doi.org/10.15381/risi.v17i2.29671

ISSN: 1815-0268 (Impreso) / ISSN: 1816-3823 (Electrónico)
Facultad de Ingeniería de Sistemas e Informática - UNMSM

Postura de Ciberseguridad en Instituciones Educativas Digitales: Una Evaluación Usando el CyberSecurity Rubric basado en el NIST CSF 2.0.

Cybersecurity Posture in Digital Educational Institutions: An Assessment Using the CyberSecurity Rubric Based on the NIST CSF 2.0.

Handz Valentin Huiza
handz.valentin@unmsm.edu.pe
Universidad Nacional Mayor de San Marcos,
Lima, Perú

Recibido: 06/12/2024 - Aceptado: 15/12/2024 - Publicado: 31/12/2024

RESUMEN

Durante la pandemia y post-pandemia, todo el sistema educativo se vio en el desafío de mejorar las condiciones de continuidad y calidad en los aprendizajes adaptándose a la educación remota de emergencia que obligó a muchas instituciones a realizar inversiones en plataformas educativas digitales, herramientas para clases virtuales, equipos tecnológicos, material virtual y capacitación docente. Los ataques cibernéticos, que aumentan cada año, suponen un desafío para el sector educativo, debido principalmente a una nula o baja conciencia de ciberseguridad y por carecer de un plan de gestión de seguridad de la información. Este artículo se centra en un caso de estudio realizado a un Centro de Educación Técnico Productivo (CETPRO) que pertenece a la UGEL 02, y que cuenta con aplicaciones, servicios y dispositivos digitales para realizar sus actividades diarias. El CETPRO nunca ha elaborado ni aplicado un plan de gestión de la ciberseguridad que le permita cumplir con la Ley de protección de datos personales (29733) y proteger sus activos digitales. Para abordar estas preocupaciones, se propone el uso de una rúbrica de ciberseguridad alineado al NIST CSF 2.0 y que ha sido ajustado para evaluar la postura de ciberseguridad de cualquier institución educativa. Esta rúbrica permite medir el nivel de madurez general en las seis funciones del NIST: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar. Se espera que la I.E. pueda conocer el estado actual de su postura de ciberseguridad permitiéndole tomar decisiones a futuro para implementar un plan de gestión de ciberseguridad y mejorar su nivel de madurez.

Palabra clave: Ciberseguridad, NIST, CSF, Educación, Educación superior.

ABSTRACT

During the pandemic and post-pandemic, the entire educational system was challenged to improve the conditions of continuity and quality of learning by adapting to remote emergency education, which forced many institutions to invest in digital educational platforms, tools for virtual classes, technological equipment, virtual material and teacher training. Cyber attacks, which are increasing every year, pose a challenge to the education sector, mainly due to no or low cybersecurity awareness and lack of an information security management plan. This article focuses on a case study conducted to a Technical-Productive Education Center (CETPRO) that belongs to UGEL 02, and that relies on digital applications, services and devices to carry out its daily duties. The CETPRO has never developed or implemented a cybersecurity management plan that would allow it to comply with the Personal Data Protection Law (29733) and protect its digital assets. To address these concerns, the use of a cybersecurity rubric aligned to NIST CSF 2.0 is proposed and has been adjusted to assess the cybersecurity posture of any educational institution. This rubric allows for measuring the overall maturity level in the six NIST functions of Govern, Identify, Protect, Detect, Respond, and Recover. It is expected that the I.E. will be able to know the current state of its cybersecurity posture allowing it to make future decisions to implement a cybersecurity management plan and improve its maturity level.

Keywords: Cybersecurity, NIST CSF, Education, Higher education.

I. INTRODUCCIÓN

Internet es la red más grande y usada del mundo y ha transformado radicalmente nuestras vidas. Hoy, dependemos de esta gran red para diferentes actividades cotidianas como buscar información, recibir y enviar correos electrónicos, jugar en línea, conectarse por videollamadas con los amigos, enviar mensajes instantáneos y mucho más (Wempen, 2014).

La infraestructura de Internet está compuesta por millones de dispositivos interconectados a nivel mundial, creando lo que llamamos la “red de redes” que facilita la comunicación y el intercambio de información de personas, instituciones, empresas y gobiernos (Meyers, 2023).

Aunque Internet ha traído incontables beneficios para la humanidad, esta interconexión también representa diferentes amenazas de ciberseguridad que pueden ser aprovechadas por los ciberdelincuentes para robar credenciales, dar seguimiento a los movimientos de los usuarios, o mantener secuestrada la información (Microsoft, 2023).

Los ciberdelincuentes emplean diferentes técnicas y estrategias para engañar y manipular a sus víctimas, con el objetivo de acceder a información valiosa, como datos personales o credenciales de usuario, lo cual puede comprometer seriamente a las organizaciones (ESED Cyber Security, 2024). Un informe de investigación de la Universidad de Maryland expone que una computadora conectada a Internet puede recibir, en promedio, un ataque cada 39 segundos (Thakur & Khan Pathan, 2020). El Informe de Investigación de Brechas de Datos del 2024 de Verizon presenta un análisis exhaustivo del panorama actual de amenazas y vulnerabilidades en ciberseguridad. Según este informe, el robo de credenciales sigue siendo el método comúnmente más usado por los atacantes para obtener acceso no autorizado a las organizaciones, seguido del phishing y la explotación de vulnerabilidades. Además, revela que más del 60% de todas las brechas de seguridad a nivel global involucran el factor humano debido a errores accidentales o con conocimiento de causa (Verizon, 2024).

En América Latina, el panorama de ciberseguridad es alarmante, solo en el año 2022, la región registró más de 137 mil millones de intentos de ciberataques (Fortinet, 2022). En el 2024, se registraron en la región más de 16 mil ciberataques por segundo siendo Brasil y México los países más afectados (Cyber Security for Critical Assets, 2024). Un estudio de Kaspersky reporta que 3 de cada 10 empresas sufrieron al menos un incidente de ciberseguridad en los últimos dos años (Kaspersky, 2024). Además, el informe X-Force de IBM señala que el ransomware constituye el 31% de todos los ciberataques dirigidos a América Latina, evidenciando el crecimiento de este tipo de amenaza en la región (IBM, 2024).

En el año 2024, un informe de Microsoft reveló que los sectores más atacados son el de TI, educación e investigación y el sector gubernamental. Principalmente, el sector educativo y de investigación representa el 21% de los ataques, posicionándose como el segundo más atacado. Además, el informe destaca que los ciberdelincuentes utilizan este sector con frecuencia como un entorno de entrenamiento antes de atacar otros objetivos estratégicos (Microsoft, 2024). Es importante señalar que estos ataques se incrementaron considerablemente a partir de la pandemia, impulsado por la rápida

transición a plataformas digitales en la educación (ver Figura 1).

Con la llegada del virus SARS-CoV-2 (COVID-19), los gobiernos a nivel mundial se vieron obligados a suspender las clases presenciales debido al aislamiento social, afectando a más de mil millones de estudiantes en casi todos los países (Tecnológico de Monterrey, 2021). Durante la pandemia, aquellos países que no contaban con infraestructura tecnológica ni sistemas de aprendizaje digital adecuados sufrieron las mayores interrupciones y pérdidas en los procesos educativos (UNESCO, 2024). Es importante destacar que los Objetivos de Desarrollo Sostenible (ODS) instan a los países a garantizar una educación de calidad, según el objetivo 4. Para lograrlo, la financiación de la educación debe ser una prioridad (Naciones Unidas, 2024). Ante estos desafíos, se adoptaron soluciones tecnológicas para no postergar el aprendizaje de los estudiantes, implementando en pocas semanas estrategias de educación virtual para diferentes niveles educativos sin un plan de transformación digital. (Dirección de Gestión del Conocimiento - UPC, 2023).

Durante este periodo, numerosas instituciones educativas (I.E.) se vieron forzadas a acelerar su transformación digital, adoptando rápidamente diversas tecnologías para sus procesos críticos, como plataformas de aprendizaje, servicios de gestión documental y trabajo colaborativo, correo electrónico, Wi-Fi, entre otros. Sin embargo, esta rápida adopción dejó poco tiempo para establecer medidas de ciberseguridad adecuadas, lo que incrementó significativamente la exposición a ataques cibernéticos en el sector educativo (Kaspersky, 2020). La comunidad educativa a menudo carece de plena conciencia sobre la importancia de la ciberseguridad y de la adopción de buenas prácticas seguras en el uso de sus dispositivos y aplicaciones que en su mayoría no están bajo una adecuada gestión. A esto se suma la falta de personal en ciberseguridad lo que agrava la vulnerabilidad de este sector (Microsoft, 2024).

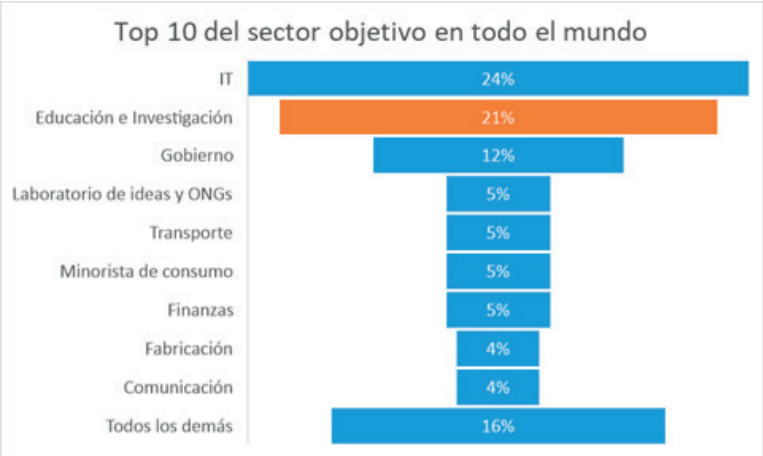
¿Qué buscan los ciberdelincuentes al atacar al sector educativo? Este sector resulta particularmente atractivo para los ciberdelincuentes ya que les permiten probar y perfeccionar sus habilidades técnicas. Además, las instituciones educativas manejan gran cantidad de datos sensibles como los repositorios de investigación, información sobre empresas proveedoras, e información personal y sensible de estudiantes, docentes y administrativos (Canvia, 2023).

En el Perú, las I.E. recopilan y almacenan una cantidad significativa de información personal tanto de sus estudiantes como del personal docente y administrativo. Para el proceso de matrícula en instituciones públicas, se solicita información personal como el Documento Nacional de Identidad (DNI) del estudiante y de sus padres, partida de nacimiento, correo electrónico, teléfono, fotografía, certificado de discapacidad, informe médico, y otros datos sensibles (MINEDU, 2024). En el caso del sector privado, la información recopilada puede incluir detalles adicionales como el nivel socioeconómico y el ingreso mensual de los padres.

La Ley 29733, conocida como la Ley de Protección de Datos Personales (PDP), garantiza el derecho fundamental a la privacidad de los datos personales. Según el artículo 2, inciso 4, del Reglamento de

Figura 1

El sector educativo y de investigación representa el 21% de los ataques



la Ley PDP, se consideran datos personales aquellos que identifican o hacen identificable a una persona natural. Estos datos incluyen no solo su nombre, sino también su imagen, dirección de correo electrónico, número telefónico, hasta sus perfiles de redes sociales (Ley N° 29733, 2011).

Cabe destacar que el sector educativo también ocupa las primeras posiciones entre los sectores más sancionados en los últimos años por incumplimiento en la protección de datos personales, lo que resalta la necesidad de reforzar las políticas de privacidad y seguridad para cumplir con la norma vigente (Payet Rey Cauvi Perez, 2022).

Las I.E. cuentan con diversos activos tecnológicos como computadoras, impresoras, equipos de red, sistemas y servicios, que son esenciales para sus actividades diarias. La Ley General de Educación (LGE) y el Proyecto Educativo Nacional (PEN) al 2036, enfatizan el uso universal e intensivo de las tecnologías digitales en el ámbito educativo. Por ello, es fundamental implementar una planificación estratégica para proteger tanto los activos tecnológicos como a los usuarios que interactúan con ellos, considerando estar expuestos a tantas amenazas en la red.

El objetivo de este artículo es evaluar el nivel de madurez de una I.E. de la Unidad de Gestión Local (UGEL) 02, dedicada a la educación técnica productiva (CETPRO) y mostrar el estado actual (as-is) de su postura de seguridad usando el Cybersecurity Rubric 2.0 (CR) que fue previamente traducido, ajustado por el autor, con el permiso de la organización desarrolladora de la rúbrica, y validado por juicio experto. El CR es una herramienta desarrollada por el Cybersecurity Coalition for Education y avalada por diferentes organizaciones internacionales (Cybersecurity Rubric, 2024). Esta herramienta está basada en el NIST Cybersecurity Framework (CSF) 2.0 de los Estados Unidos, un marco de trabajo abierto para que cualquier organización, sin importar su tamaño o la industria a la que pertenece, pueda aplicarlo según sus necesidades u objetivos estratégicos.

Después de obtener los resultados, se espera a futuro aplicar un modelo de ciberseguridad desarrollado por el autor, para comprobar el fortalecimiento de la postura de seguridad objetiva.

1.1. Definiendo la Postura de ciberseguridad

La postura de seguridad es un término ampliamente utilizado en documentación técnica, libros, artículos y productos relacionados a la seguridad de la información y la ciberseguridad. Para comprender su significado, es importante analizar la definición de *postura*. Según el diccionario Oxford, el término se refiere a la actitud o posición que tomamos ante una situación en particular o de qué manera decidimos gestionarla (Oxford University Press, 2024).

En el ámbito digital, podemos estar expuestos a diferentes amenazas cibernéticas que pueden traer consecuencias negativas. Tomar una postura, implica decidir de qué manera podemos enfrentarnos a estas situaciones mediante la implementación de diferentes estrategias.

El término *postura de seguridad* está definido en el glosario de términos del *Committee on National Security Systems* (CNSS), un organismo gubernamental de los Estados Unidos que diseña políticas, directivas, instrucciones y procedimientos operativos relacionados con la ciberseguridad a nivel nacional. Muchos de los términos que contiene son adoptados por el *National Institute of Standards and Technology* (NIST) en sus documentos técnicos.

Según el CNSS, la postura de seguridad se refiere al estado de seguridad de las redes, información y sistemas de una organización, determinado por la eficacia de sus recursos empleados para garantizar la seguridad de la información. Estos recursos incluyen personas, dispositivos de hardware, aplicaciones y políticas. Asimismo, incluye las capacidades implementadas para defenderse contra las amenazas y adaptarse a situaciones cambiantes del entorno de seguridad (CNSS, 2015).

Además, el Australian Signals Directorate define la postura de seguridad como el nivel de riesgo de seguridad al que está expuesto un sistema. Una postura de seguridad sólida se traduce en una exposición significativamente reducida a los riesgos, lo que ayuda a resistir a amenazas potenciales (ASD, 2024).

En el informe Report on the Cybersecurity Posture of the United States del 2024, se utiliza el término Postura de Ciberseguridad como la capacidad para **identificar, proteger, detectar, responder y recuperarse** de una intrusión, principalmente en escenarios donde un ciberataque ha comprometido los sistemas de información (National Cyber Director, 2024). Es importante destacar que los conceptos de *postura de seguridad* y *postura de ciberseguridad* suelen usarse indistintamente, aunque pueden resaltar ciertas diferencias según el contexto de seguridad de la información y ciberseguridad.

La seguridad de la información extiende su alcance protector no solo a los datos almacenados digitalmente, sino también otras formas de información, como documentos físicos en papel (Forbes, 2024). La principal diferencia entre ambos conceptos es que la seguridad de la información abarca la protección de la información independientemente del medio. Mientras que la ciberseguridad se enfoca en los datos en entornos digitales y cibernético (ST. John's University, 2024). Un análisis de búsquedas en Google revela que el término “Ciberseguridad” ha superado en popularidad a “Seguridad de la información” (Amine Agalit y otros, 2023). Esto indica una mayor preocupación por parte de los usuarios hacia aspectos relacionados específicamente con el ámbito digital y los riesgos cibernéticos.

En términos generales, la postura de seguridad se refiere a la madurez general del programa de ciberseguridad de una organización incluyendo su capacidad para protegerse de amenazas cibernéticas (Check Point, 2024). Para fines de este artículo, se usará el término postura de ciberseguridad de aquí en adelante.

Comprender la definición de postura de ciberseguridad nos lleva a reflexionar sobre nuestra propia postura. **¿Conocemos nuestra postura de ciberseguridad actual? ¿Tenemos una visión clara de cómo debe ser en el futuro?** Responder a estas preguntas puede brindar un diagnóstico de la situación actual y permite adoptar e implementar estrategias para mejorar o fortalecer una postura de seguridad a futuro en la organización. En muchas I.E., principalmente en aquellas del sector público, puede que no exista un entendimiento claro de su postura de ciberseguridad. Entonces, **¿Cómo puede hacer una institución educativa para evaluar su postura de ciberseguridad actual?**

Al revisar la definición del NIST Cybersecurity Framework (CSF) 2.0 se entiende que este marco de trabajo puede ser utilizado para describir la postura de ciberseguridad actual y futura de cualquier organización. Este marco es la base de la rúbrica de ciberseguridad propuesta en este artículo.

1.2. Conocer el NIST CSF 2.0

NIST CyberSecurity Framework (CSF) 2.0 es un marco de trabajo (framework) diseñado para ayudar a las organizaciones de cualquier tamaño e industria a gestionar y reducir los riesgos de ciberseguridad. Este framework ha sido reconocido internacionalmente por su adaptabilidad y efectivad en diferentes sectores. Esto se debe a que recopila diversos estándares, directrices y buenas prácticas adoptadas por diferentes organizaciones a nivel mundial.

Un framework es definido como un conjunto de creencias, ideas o reglas que se utilizan como base para guiar juicios, tomar decisiones, etc. (Oxford University Press, 2024). El NIST CSF 2.0 es considerado un marco de trabajo porque proporciona una serie de pautas que pueden ser aplicadas por las organizaciones para lograr uno o varios objetivos claves, como la capacidad de prevención, detección y respuesta frente a los riesgos de ciberseguridad.

A diferencia del ISO 27001, cuyo enfoque está basado en la seguridad de la información, el NIST CSF tiene un enfoque más amplio pues incluye la seguridad de la información y la ciberseguridad. Además, NIST CSF es más flexible, cuenta con niveles de madurez, y no necesita de un proceso de certificación formal (Amine Agalit y otros, 2023).

Figura 2

Comparación entre ISO 27001 y NIST CSF

ISO 27001	NIST CSF
• Seguridad de la Información • Prescriptivo • Certificación disponible • No tiene niveles de madurez	• Ciberseguridad • Flexible • No hay certificación • Tiene niveles de madurez

NIST CSF 2.0 es una nueva versión del framework que incluye tres componentes principales: el CSF Core, los perfiles organizativos del CSF y los niveles de CSF.

1.2.1. Núcleo del CSF (CSF Core):

El núcleo principal tiene como objetivo proporcionar una estructura organizada que permita a las organizaciones lograr resultados (*outcomes*) claros y efectivo en la gestión de riesgos de ciberseguridad. Para ello, el marco se enfoca en un sistema jerárquico que incluyen **funciones**, **categorías** y **subcategorías** que describen los resultados que las organizaciones aspiran poder lograr. Por ejemplo, las instituciones educativas pueden querer lograr el cumplimiento de la Ley 29733, fortalecer la cultura de ciberseguridad, o planificar una recuperación efectiva ante un ciberataque.

La nueva versión del CSF 2.0 ahora presenta seis funciones: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar. De estas, la función Go-

bernar es la base fundamental por lograr y priorizar los resultados de las otras cinco funciones. Cada una desempeña roles de vital importancia relacionados a la gestion de incidentes de ciberseguridad. Los resultados asociados a Gobernar, Identificar y Proteger están orientados a la prevención y preparacion frente a posibles incidentes, mientras que los resultados de Gobernar, Detectar, Responder y Recuperar se enfocan en la deteccion y gestion efectiva de los mismos (como se muestra en la figura 3)

Cada función en el CSF 2.0 está dividido en múltiples categorías que representan los resultados específicos de cada función. La Figura 3, muestra la lista de categorías por cada función:

1.2.2. Perfiles Organizativos

El perfil organizativo se utiliza tanto para describir la postura de ciberseguridad actual (as-is) como para definir la postura de ciberseguridad objetivo (to-be), tomando como referencia los resultados establecidos en el núcleo del CSF.

Un perfil organizativo puede ser adaptado según las necesidades de cada organización y puede incluir un perfil actual y/o un perfil objetivo.

1.2.3. Niveles

Permite evaluar la rigurosidad con la que una organización aborda las prácticas de gobernanza y gestión de riesgos de ciberseguridad. El marco propone cuatro niveles, que pueden ser adaptados a las necesidades de cualquier organización. Los niveles son: Parcial, Conocimiento de los riesgos, Repetible y Adaptable. Estos niveles deben ser aplicados a su perfil organizativo (ver Figura 4).

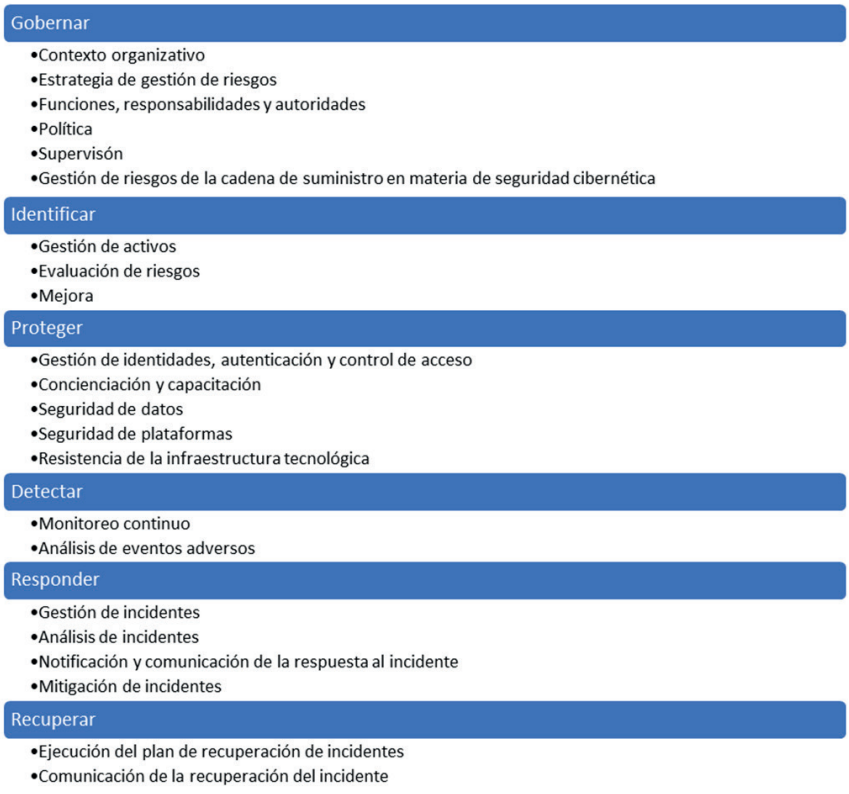
1.3. Cybersecurity Rubric for Education

El Cybersecurity Rubric for Education (CRE) es una herramienta de autoevaluación que ayuda a los líderes educativos a evaluar sus prácticas actuales en ciberseguridad. Fue desarrollado en el 2023 por el Cybersecurity Coalition for Education (CCE), una alianza formada por tres grandes organizaciones internacionales: ClassLink, ENA by Zayo y SecurityStudio. Durante ese año, se unieron dos nuevos miembros: Caetra.io y CDWG.

El CRE está basado en el NIST CSF 2.0 tomando en cuenta las necesidades específicas para la educación con un enfoque innovador para autoevaluar y mejorar la ciberseguridad en las instituciones educativas.

Figura 3

Funciones del NIST CSF 2.0 y sus respectivas categorías



Fuente: Elaboración propia.

1.3.1. Categorías del CRE

Debido a que el CRE está basado en el NIST CSF 2.0, este utiliza el núcleo del CSF a través de sus seis funciones y las 22 categorías. Todas ellas, perfiladas al sector educativo.

1.3.2. Obtener el CRE

El CRE está en idioma inglés y es gratuito para que cualquiera pueda descargarlo y usarlo. No existe ningún pre-requisito, sin embargo, puede llevar un entrenamiento sin costo para saber cómo sacarle provecho a la rúbrica de evaluación. Para descargar la rúbrica en formato de Excel, use este enlace: https://www.cybersecurityrubric.org/use-the-rubric#

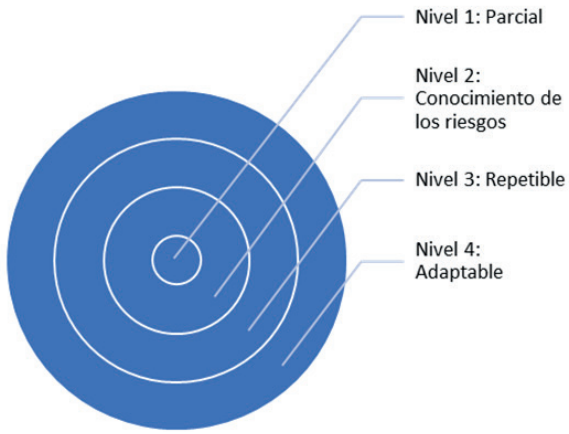
1.3.3. Conocer el Modelo de Madurez

El CRE confía en un Modelo de Madurez que evalúa cada categoría de las seis funciones del NIST de una manera escalonada. Este modelo presenta cinco niveles de madurez que van desde un enfoque reactivo a uno proactivo. La Figura 5 muestra los cinco niveles de madurez del CRE.

- **Inicial:** Identifica las prácticas de ciberseguridad que son reactivas, poco controladas e impredecibles.
- **Repetible:** Identifica las prácticas de ciberseguridad que se documentan, realizan y supervisan a nivel de proyecto con procesos.
- **Definido:** Identifica las prácticas de ciberseguridad que son proactivas y se entienden con procesos, herramientas y normas en vigor.
- **Gestionado:** Identifica las prácticas de ciberseguridad que se controlan mediante técnicas estadísticas y cuantitativas.
- **Optimizado:** Identifica las prácticas de ciberseguridad que mejoran continuamente a través de mejoras tecnológicas incrementales e innovadoras.

Figura 4

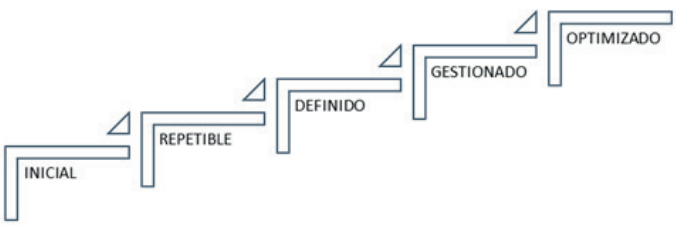
Niveles de perfil organizativo



Fuente: Elaboración propia.

Figura 5

Niveles de madurez



Fuente: Elaboración propia.

1.3.4. El Certified Cybersecurity Rubric Evaluator (CCRE)

El CRE es una rúbrica que puede ser descargado y utilizado por cualquier I.E. sin costo alguno y pueden realizar una autoevaluación interna de sus riesgos en ciberseguridad. Sin embargo, para mantener una evaluación objetiva, la institución educativa podría contratar a un evaluador certificado externo o también llamado un Certified Cybersecurity Rubric Evaluator (CCRE).

Un CCRE es un profesional certificado y acreditado por el Cybersecurity Coalition para evaluar instituciones educativas de manera sistemática, sin sesgos y de forma independiente usando el CRE (ver Figura 6).

1.3.5. Ajustes para instituciones educativas digitales en Perú

En el Perú, una institución educativa es la primera y principal instancia de gestión del sistema educativo descentralizado, encargada de brindar servicios educativos a la comunidad. Estas instituciones incluyen los centros de educación básica (inicial, primaria y secundaria), los de educación técnico-productiva y las instituciones de educación superior (Ley 28044, 2003).

La LGE promueve la integración de nuevas tecnologías en los procesos educativos. En este contexto, el Perú cuenta con un PEN al 2036 que enfatiza el uso universal e intensivo de tecnologías digitales como recursos educativos para potenciar las labores de enseñanza-aprendizaje, de aprendizaje autónomo y la investigación (Ministerio de Educación, 2020). Por tal motivo, muchas instituciones educativas han implementado Aulas de Innovación Pedagógica (AIP) para integrar las Tecnologías de Información y Comunicación (TIC) en las actividades pedagógicas.

Considerando la LGE y el PEN, así como el compromiso de cumplir con la Ley PDP, se ha obtenido el permiso para usar el CRE como base y ajustarlo a las necesidades de cualquier institución educativa peruana, sin importar su nivel educativo.

El CRE es un documento en formato de hoja de cálculo que cuenta con las siguientes hojas: Instrucciones, Resultados del nivel de madurez, y cada función del NIST (ver Figura 7).

II. METODOLOGÍA

La evaluación de la postura de ciberseguridad se realizó en un CETPRO del distrito de San Martin de Porres perteneciente a la UGEL 02, siguiendo la metodología propuesta por el Cybersecurity Coalition que consta de seis pasos claves (ver Figura 8).

2.1. Paso 1: Llamada a la acción

El primer paso es tener un acercamiento con la I.E. y conversar sobre el propósito y los beneficios de hacer una evaluación para conocer la postura de ciberseguridad actual. Para ello, se realizó una breve entrevista con los líderes educativos, para conocer la opinión sobre el proceso que se llevará a cabo y cómo trabajan dentro de la I.E. con el tema de la ciberseguridad. De estas entrevistas, se puede resumir en la siguiente información:

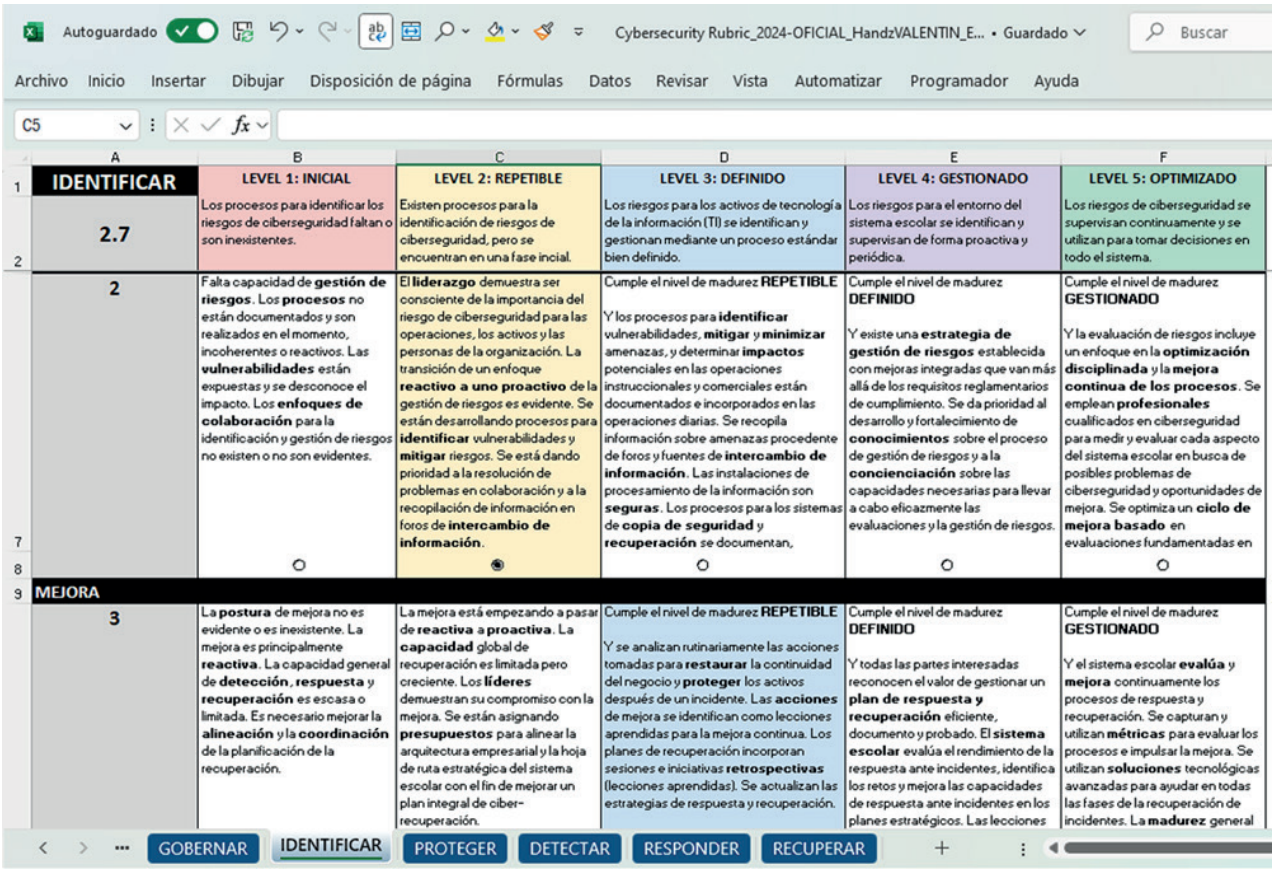
Figura 6

Certificado oficial de un CCRE

Fuente: Elaboración propia.

Figura 7

Rúbrica de Ciberseguridad ajustada por el autor



Autoguardado · Cybersecurity Rubric_2024-OFICIAL_HandzVALENTIN_E... • Guardado · Buscar

Archivo Inicio Insertar Dibujar Disposición de página Fórmulas Datos Revisar Vista Automatizar Programador Ayuda

C5

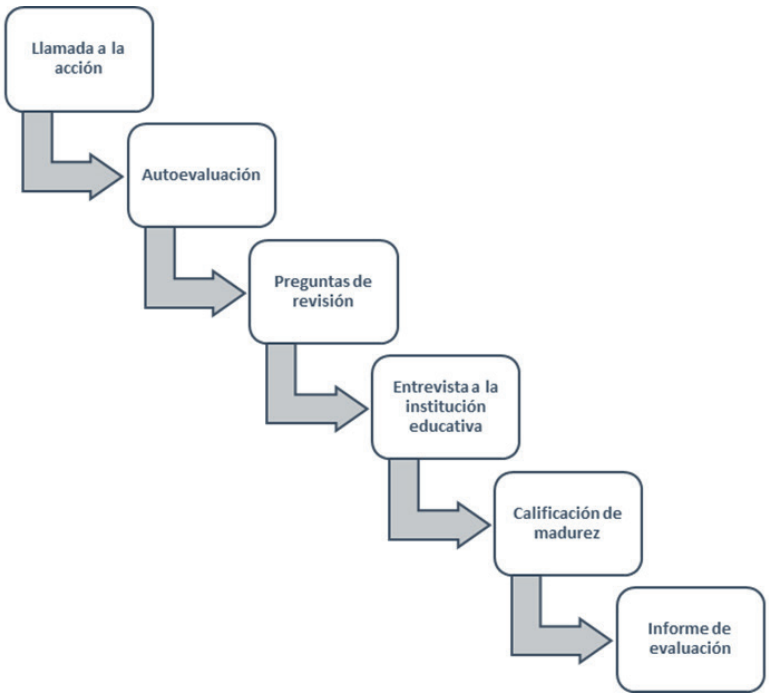
	A	B	C	D	E	F
1	**IDENTIFICAR**	**LEVEL 1: INICIAL**	**LEVEL 2: REPETIBLE**	**LEVEL 3: DEFINIDO**	**LEVEL 4: GESTIONADO**	**LEVEL 5: OPTIMIZADO**
2	**2.7**	Los procesos para identificar los riesgos de ciberseguridad faltan o son inexistentes.	Existen procesos para la identificación de riesgos de ciberseguridad, pero se encuentran en una fase incial.	Los riesgos para los activos de tecnología de la información (TI) se identifican y gestionan mediante un proceso estándar bien definido.	Los riesgos para el entorno del sistema escolar se identifican y supervisan de forma proactiva y periódica.	Los riesgos de ciberseguridad se supervisan continuamente y se utilizan para tomar decisiones en todo el sistema.
7	**2**	Falta capacidad de **gestión de riesgos**. Los **procesos** no están documentados y son realizados en el momento, incoherentes o reactivos. Las **vulnerabilidades** están expuestas y se desconoce el impacto. Los **enfoques de colaboración** para la identificación y gestión de riesgos no existen o no son evidentes.	El **liderazgo** demuestra ser consciente de la importancia del riesgo de ciberseguridad para las operaciones, los activos y las personas de la organización. La transición de un enfoque **reactivo a uno proactivo** de la gestión de riesgos es evidente. Se están desarrollando procesos para **identificar** vulnerabilidades y **mitigar** riesgos. Se está dando prioridad a la resolución de problemas en colaboración y a la recopilación de información en foros de **intercambio de información**.	Cumple el nivel de madurez **REPETIBLE** Y los procesos para **identificar** vulnerabilidades, **mitigar** y **minimizar** amenazas, y determinar **impactos** potenciales en las operaciones instruccionales y comerciales están documentados e incorporados en las operaciones diarias. Se recopila información sobre amenazas procedente de foros y fuentes de **intercambio de información**. Las instalaciones de procesamiento de la información son **seguras**. Los procesos para los sistemas de **copia de seguridad** y **recuperación** se documentan,	Cumple el nivel de madurez **DEFINIDO** Y existe una **estrategia de gestión de riesgos** establecida con mejoras integradas que van más allá de los requisitos reglamentarios de cumplimiento. Se da prioridad al desarrollo y fortalecimiento de **conocimientos** sobre el proceso de gestión de riesgos y a la **concienciación** sobre las capacidades necesarias para llevar a cabo eficazmente las evaluaciones y la gestión de riesgos.	Cumple el nivel de madurez **GESTIONADO** Y la evaluación de riesgos incluye un enfoque en la **optimización disciplinada** y la **mejora continua de los procesos**. Se emplean **profesionales** cualificados en ciberseguridad para medir y evaluar cada aspecto del sistema escolar en busca de posibles problemas de ciberseguridad y oportunidades de mejora. Se optimiza un **ciclo de mejora basado** en evaluaciones fundamentadas en
8		○	◉	○	○	○
9	**MEJORA**					
	3	La **postura** de mejora no es evidente o es inexistente. La mejora es principalmente **reactiva**. La capacidad general de **detección**, **respuesta** y **recuperación** es escasa o limitada. Es necesario mejorar la **alineación** y la **coordinación** de la planificación de la recuperación.	La mejora está empezando a pasar de **reactiva** a **proactiva**. La **capacidad** global de recuperación es limitada pero creciente. Los **líderes** demuestran su compromiso con la mejora. Se están asignando **presupuestos** para alinear la arquitectura empresarial y la hoja de ruta estratégica del sistema escolar con el fin de mejorar un plan integral de ciber-recuperación.	Cumple el nivel de madurez **REPETIBLE** Y se analizan rutinariamente las acciones tomadas para **restaurar** la continuidad del negocio y **proteger** los activos después de un incidente. Las **acciones** de mejora se identifican como lecciones aprendidas para la mejora continua. Los planes de recuperación incorporan sesiones e iniciativas **retrospectivas** (lecciones aprendidas). Se actualizan las estrategias de respuesta y recuperación.	Cumple el nivel de madurez **DEFINIDO** Y todas las partes interesadas reconocen el valor de gestionar un **plan de respuesta y recuperación** eficiente, documento y probado. El **sistema escolar** evalúa el rendimiento de la respuesta ante incidentes, identifica los retos y mejora las capacidades de respuesta ante incidentes en los planes estratégicos. Las lecciones	Cumple el nivel de madurez **GESTIONADO** Y el sistema escolar **evalúa** y **mejora** continuamente los procesos de respuesta y recuperación. Se capturan y utilizan **métricas** para evaluar los procesos e impulsar la mejora. Se utilizan **soluciones** tecnológicas avanzadas para ayudar en todas las fases de la recuperación de incidentes. La **madurez** general

GOBERNAR | IDENTIFICAR | PROTEGER | DETECTAR | RESPONDER | RECUPERAR

Fuente: Elaboración propia.

Figura 8

Metodología para aplicar la evaluación de la rúbrica de ciberseguridad



- Se tiene poco conocimiento sobre la ciberseguridad, pero se cree que es importante.
- No existe o no se tiene conocimiento de haber sufrido un ataque en los últimos meses.
- No se conocen ni aplican normativas enfocadas a la ciberseguridad y protección de datos personales.
- Debido a que no conocen las normativas sobre ciberseguridad y protección de datos personales, no se han implementado medidas para mitigar los riesgos.
- La I.E. no cuenta con un equipo de ciberseguridad específico.
- La I.E. solo utiliza antivirus no licenciados.
- Cada persona entrevistada tiene una percepción diferente de qué activos físicos y/o digitales son críticos para la institución.
- No existen procesos para identificar activos físicos y virtuales.
- La I.E. cuenta con socios y proveedores con acuerdos formales de colaboración, pero no se especifica el intercambio de datos.
- Debido a que hay poco conocimiento del tema de ciberseguridad y las leyes no son severas con instituciones educativas públicas, los líderes educativos no están muy involucrados en las decisiones relacionadas con la ciberseguridad.
- No existen programas de capacitación interna sobre ciberseguridad.
- La I.E. no cuenta con presupuesto del estado para temas de ciberseguridad.
- No existe un plan de continuidad de negocio ni de recuperación ante desastres. Las operaciones digitales no son resilientes.
- Hasta el momento, no existen planes a futuro para implementar medidas de seguridad.

2.2. Paso 2: Autoevaluación

Debido a que la institución no cuenta con un personal enfocado a la ciberseguridad y nunca han aplicado una evaluación sobre su postura de seguridad, se ha tenido que acompañar a los líderes de la I.E. durante su autoevaluación aclarando algunos criterios de la Rúbrica de Ciberseguridad.

Tabla 1

Detalles de la Autoevaluación

Autoevaluación realizada por:	**Coordinador Administrativo**
Inicio de la autoevaluación:	03/12/2024
Final de la autoevaluación:	06/12/2024

Durante la autoevaluación se obtuvieron los siguientes resultados:

Tabla 2

Resultados de la función Gobernar

GOBERNAR	
Categorías	**Puntaje**
Contexto Organizativo	1
Estrategia de Gestión de Riesgos	1
Funciones, Responsabilidades y Autoridades	1
Política	1
Supervisión	1
Gestión de Riesgos de la Cadena de Suministro de Ciberseguridad	2
PROMEDIO	1.2

Tabla 3

Resultados de la función Identificar

IDENTIFICAR	
Categorías	**Puntaje**
Gestión de Activos	2
Evaluación de Riesgos	1
Mejora	1
PROMEDIO	1.3

Tabla 4

Resultados de la función Proteger

PROTEGER	
Categorías	**Puntaje**
Gestión de Identidad, Autenticación y Control de Acceso	1
Conciencia y Entrenamiento	1
Seguridad de Datos	1
Seguridad de la Plataforma	1
Resiliencia de la Infraestructura Tecnológica	1
PROMEDIO	1

Tabla 5

Resultados de la función Detectar

DETECTAR	
Categorías	**Puntaje**
Monitoreo Continuo	1
Análisis de Eventos Adversos	1
PROMEDIO	1

Tabla 6

Resultados de la función Responder

RESPONDER	
Categorías	**Puntaje**
Gestión de Incidentes	1
Análisis de Incidentes	1
Informe y Comunicación de Respuesta ante Incidentes	1
Mitigación de Incidentes	1
PROMEDIO	1

Tabla 7

Resultados de la función Recuperar

RECUPERAR	
Categorías	**Puntaje**
Ejecución del Plan de Recuperación de Incidentes	1
Comunicación de Recuperación ante Incidentes	1
PROMEDIO	1

2.3. Paso 3: Preguntas de revisión

Una vez completada la autoevaluación, se utilizó y se ajustaron las preguntas por cada categoría y función del NIST sugeridas por el Cybersecurity Rubric y proporcionadas a los CCRE. Estas preguntas son necesarias para iniciar la entrevista con la institución educativa.

2.4. Paso 4: Entrevista con la I.E.

La persona encargada para la entrevista fue la coordinadora administrativa con apoyo de la docente de mayor nivel en la I.E.

Entrevista realizada por:	Handz Valentin (CCRE)
Entrevista realizada a:	Coordinador Administrativo
Apoyo:	Docente (Sexta Escala)
Inicio de las entrevistas:	09/12/2024
Fin de las entrevistas:	17/12/2024

2.4. Paso 5: Calificación de la madurez

Con la entrevista, se logró entender mejor cómo trabaja la I.E. en diferentes aspectos relacionados con las funciones del NIST CSF 2.0. Los resultados encontrados se visualizan en las Tablas 8-12.

Tabla 8

Resultados del CCRE en la función Gobernar

GOBERNAR		
Categorías	**Criterios de evaluación**	**Puntaje**
Contexto Organizativo	Las defensas para **mitigar los riesgos** no están claramente definidas. Los acuerdos de **intercambio de datos con terceros** no son formales. Los procesos de **datos sensibles** necesitan mejoras. Las decisiones de **gestión de riesgos** no están incluidas en la planificación de iniciativas de ciberseguridad.	1
Estrategia de Gestión de Riesgos	Las **prioridades, restricciones, tolerancias** y **suposiciones** de la organización en materia de riesgos no están claramente definidas. Falta o no existe una **estrategia integral de gestión de riesgos**. Los procesos no están documentados ni alineados para respaldar la **arquitectura** y la **hoja de ruta** estratégica.	1
Funciones, Responsabilidades y Autoridades	Deben definirse los **roles y responsabilidades** para el desarrollo e implementación de las políticas y prácticas de privacidad y ciberseguridad de datos. Se deben asignar **recursos** y presupuestos para satisfacer las necesidades de privacidad de ciberseguridad y datos del sistema escolar.	1
Política	La escuela carece de **políticas** para gestionar los riesgos de ciberseguridad. Las políticas no se documentan, comunican ni aplican.	1
Supervisión	Es evidente la **falta de supervisión** en la revisión de las directrices, procesos o políticas de ciberseguridad por parte de la dirección ejecutiva. Los **resultados** de la gestión de riesgos de ciberseguridad no se revisan ni ajustan para garantizar la cobertura de los requisitos y riesgos del sistema escolar.	1
Gestión de Riesgos de la Cadena de Suministro de Ciberseguridad	Los procesos para gestionar los riesgos de los **proveedores** no están documentados y son realizados en el momento, incoherentes o reactivos. Falta o no existe un **inventario** exhaustivo de proveedores y socios terceros, así como la identificación de los sistemas de información, componentes y servicios prestados.	1
PROMEDIO		1

Tabla 9

Resultados del CCRE en la función Identificar

IDENTIFICAR		
Categorías	**Criterios de evaluación**	**Puntaje**
Gestión de Activos	Los procesos de **inventario de activos** son realizados en el momento, incoherentes y/o reactivos y pueden estar desfasados. Faltan **controles** para la protección de activos o es necesario mejorarlos.	1
Evaluación de Riesgos	Falta capacidad de **gestión de riesgos**. Los **procesos** no están documentados y son realizados en el momento, incoherentes o reactivos. Las **vulnerabilidades** están expuestas y se desconoce el impacto. Los **enfoques de colaboración** para la identificación y gestión de riesgos no existen o no son evidentes.	1
Mejora	La **postura** de mejora no es evidente o es inexistente. La mejora es principalmente **reactiva**. La capacidad general de **detección**, **respuesta** y **recuperación** es escasa o limitada. Es necesario mejorar la **alineación** y la **coordinación** de la planificación de la recuperación.	1
PROMEDIO		1

Tabla 10

Resultados del CCRE en la función Proteger

PROTEGER		
Categorías	**Criterios de evaluación**	**Puntaje**
Gestión de Identidad, Autenticación y Control de Acceso	Los procesos y protocolos de **control de acceso** físico y remoto no están establecidos ni documentados. No se ha implementado la **autenticación multifactor**. Las medidas de **protección de datos** son incoherentes. No están definidos los procesos de **integridad de la red**. No están definidos los procesos de **revisión de cuentas** de usuario, proveedor y sistema. No están definidas las condiciones de **pertenencia a grupos y roles**.	1
Conciencia y Entrenamiento	Los procesos para garantizar que todo el personal y los estudiantes con cuentas de **identificación de usuario** no están documentados y son realizadas en el momento, incoherentes o reactivos. La **formación** sobre concienciación en ciberseguridad no es obligatoria ni está programada para los usuarios nuevos o existentes. La formación en seguridad **basada en roles específicos** para el personal designado es incoherente o inexistente. El **personal** encargado de documentar y monitorear las actividades de formación en seguridad de los sistemas de información no está definido ni designado. No se ha definido una **política de retención de registros**.	1
Seguridad de Datos	Los procesos para gestionar y proteger los **datos almacenados** y **transmitidos** no están documentados o son realizados en el momento, incoherentes o reactivos. Se carece o son inexistentes los procesos y políticas para **proteger** la **confidencialidad**, **integridad** y **disponibilidad** de la información y los registros. La dirección demuestra una comprensión incompleta de la protección de datos y la gestión de riesgos.	1
Seguridad de la Plataforma	Faltan procesos para **mantener** y **reparar** los sistemas de información y las aplicaciones de acuerdo con las especificaciones y requisitos del proveedor. Los **sistemas** y **herramientas** de mantenimiento no están controlados. Las **actividades** de mantenimiento son principalmente reactivas y esporádicas y/o inconsistentes. Los **controles de seguridad** para verificar la funcionalidad tras el mantenimiento carecen de definición. Los registros de las actividades de mantenimiento son realizados en el momento, incoherentes o incompletos. Los procesos para impedir el **acceso no autorizado** necesitan definición y/o mejora.	1
Resiliencia de la Infraestructura Tecnológica	Faltan procesos para proteger los **dispositivos** de los estudiantes y el personal, o son realizados en el momento, incoherentes o reactivos. Faltan o no existen **tecnologías de protección** avanzadas para proteger los dispositivos de las amenazas identificadas y potenciales. Las **actualizaciones de seguridad** no se realizan de forma oportuna y programada. El personal de tecnologías de la información (TI) dispone de poco **tiempo** para capturar y revisar los registros de auditoría o no dispone de él. Se necesitan medidas de protección adicionales para los **medios extraíbles** y los **componentes de la infraestructura** de red.	1
PROMEDIO		1

Tabla 11

Resultados del CCRE en la función Detectar

DETECTAR		
Categorías	**Criterios de evaluación**	**Puntaje**
Monitoreo Continuo	Los procesos para gestionar activamente todos los **activos** son inexistentes o incompletos. Los procesos para detectar, eliminar y/o remediar **activos no autorizados y no gestionados** son realizados en el momento, incompletos o reactivos. No se realizan consistentemente **revisiones** de cuentas, reglas de firewall y pruebas de penetración de los sistemas externos. Los **escaneos de vulnerabilidades** externas no se realizan al menos trimestralmente.	1
Análisis de Eventos Adversos	Los procesos para recopilar, revisar y correlacionar **datos de eventos** de un ataque de ciberseguridad no están documentados o son realizados en el momento, incoherentes o reactivos. No existe o falta una **línea base** de las operaciones de red y flujos de datos esperados para el personal, los estudiantes y los sistemas. Se necesita personal tecnológico asignado al análisis del **impacto** de los eventos. Falta capacidad para detectar **anomalías**.	1
PROMEDIO		1

Tabla 12

Resultados del CCRE en la función Responder

RESPONDER		
Categorías	**Criterios de evaluación**	**Puntaje**
Gestión de Incidentes	Los procesos aprobados para mantener un **plan integral de respuesta a incidentes** de ciberseguridad faltan o son inexistentes. No se ha identificado ni formado **al personal** responsable de elaborar y aplicar el plan de respuesta a incidentes.	1
Análisis de Incidentes	Los procesos de **análisis** de incidentes son insuficientes. La respuesta adecuada y el apoyo a las **actividades de recuperación** son realizados en el momento, incoherentes o reactivos.	1
Informe y Comunicación de Respuesta ante Incidentes	Los procesos para definir las **actividades de respuesta** ordenada faltan o son inexistentes. Los criterios para el **reporte de incidentes** no están claramente definidos o son principalmente reactivos. Los procesos de comunicación para el **reporte de incidentes** son poco claros o inexistentes.	1
Mitigación de Incidentes	Falta o no existe un enfoque sistemático para prevenir la **expansión** de un suceso. Los procesos o tecnologías para **mitigar** los efectos de un incidente y erradicarlo no están definidos, y las prácticas son realizadas en el momento, incoherentes y reactivas.	1
PROMEDIO		1

Tabla 13

Resultados del CCRE en la función Recuperar

RECUPERAR		
Categorías	**Criterios de evaluación**	**Puntaje**
Ejecución del Plan de Recuperación de Incidentes	Los **planes de incidentes** faltan o son inexistentes. No se han determinado las medidas de **recuperación** para la continuidad de la educación. Si existe un plan, no se ajusta a las **hojas de ruta** estratégicas ni a los **objetivos** de ciberseguridad.	1
Comunicación de Recuperación ante Incidentes	Falta o no existe un enfoque sistemático para comunicar las **actividades de restauración**. No están definidas ni documentadas las **condiciones** y **responsabilidades** en las que se invocará el plan de recuperación.	1
PROMEDIO		1

2.4. Paso 6: Informe de evaluación

Al concluir con la evaluación, se elaboró un informe detallado que recopila información clave tanto de la autoevaluación como de la evaluación realizada por el CCRE. Este informe incluye los hallazgos identificados por cada función del NIST y recomendaciones proporcionadas por parte del CCRE.

III. CONCLUSIONES

Después de culminar con la evaluación por parte del CCRE y presentado el informe a las autoridades correspondientes, se concluye con la siguiente puntuación en el nivel de madurez sobre ciberseguridad en la institución educativa:

- **Nivel de madurez de la autoevaluación:** 1.1
- **Nivel de madurez de la evaluación por CCRE:**1.0

Se debe tomar en cuenta las siguientes recomendaciones a nivel general:

- La evaluación basada en el NIST CSF 2.0 reveló brechas significativas en las seis funciones del marco (Identificar, Proteger, Detectar, Responder y Recuperar). Estas brechas ponen en manifiesto diferentes áreas críticas que necesitan atención principal, como la gestión de riesgos en ciberseguridad, la protección de datos sensibles alineados a la ley 29733 y llevar un control adecuado de sus activos digitales.
- El análisis evidenció que la I.E. está en un nivel inicial de madurez con controles inexistentes o realizados solo cuando la situación lo amerita. En el informe final se recomienda mejorar estos aspectos pasando de algo reactivo a un enfoque proactivo.
- La conciencia en ciberseguridad es un aspecto importante para fortalecer los planes de ciberseguridad en la I.E. Es crucial implementar capacitaciones más frecuentes que permita a la comunidad educativa comprender la gravedad de las vulnerabilidades que existe en el mundo digital y adoptar prácticas seguras para mitigar los riesgos.
- Para mejorar la postura de ciberseguridad de la I.E., pueden utilizar modelos de ciberseguridad basado en enfoques más actuales como Zero Trust.

REFERENCIAS

[1] Wempen, F. (2014). Computing Fundamentals IC3 Edition. Wiley.

[2] Meyers, M. (2023). CompTIA A+ Certification Exam Guide. MC Graw Hill.

[3] Microsoft. (11 de Abril de 2023). What are the most common threats to your online security? https://www.microsoft.com/en-us/edge/learning-center/common-threats-online-security?form=MA13I2.

[4] ESED Cyber Security. (31 de 10 de 2024). Las 15 técnicas de hacking más comunes. https://www.esedsl.com/blog/15-tecnicas-de-hacking-mas-comunes.

[5] Thakur, K., & Khan Pathan, A. (2020). Cybersecurity Fundamentals A Real-World Perspective. CRC Press.

[6] Verizon. (2024). 2024 Data breach Investigations Report. https://www.verizon.com/business/resources/T14a/reports/2024-dbir-data-breach-investigations-report.pdf.

[7] Fortinet. (18 de agosto de 2022). Fortinet registró 137 mil millones de intentos de ciberataques en América Latina en la primera mitad del año. fortinet.com: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortinet-registro-137-mil-millones-de-intentos-de-ciberataques-e

[8] Cyber Security for Critical Assets. (2024). LatAm Cyber Summit 2024 Annual Report. https://latam.cs4ca.com/wp-content/uploads/LatAm-Cyber-Summit-2024-Annual-Report.pdf

[9] Kaspersky. (16 de octubre de 2024). El 67% de los ciberataques a empresas latinoamericanas fueron considerados graves. https://latam.kaspersky.com/about/press-releases/el-67-de-los-ciberataques-a-empresas-latinoamericanas-fueron-considerados-graves?srsltid=AfmBOoqPybamIW-tI-6H0AVLRAnyX7H_Iq0fXfOzUpk8oWJBaPo603jM

[10] IBM. (2024). X-Force Threat Intelligence Index. https://www.ibm.com/downloads/documents/us-en/107a02e952c8fe80

[11] Microsoft. (octubre de 2024). Microsoft Digital Defense Report 2024. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

[12] Tecnológico de Monterrey. (21 de junio de 2021). Instituto para el Futuro de la Educación. ¿Cómo la pandemia por COVID-19 cambió la industria de la educación para siempre?: https://observatorio.tec.mx/edu-bits-blog/la-pandemia-cambio-la-industria-de-la-educacion-para-siempre/

[13] UNESCO. (6 de febrero de 2024). Qué necesita saber acerca del aprendizaje digital y la transformación de la educación. https://www.unesco.org/es/digital-education/need-know

[14] Naciones Unidas. (26 de enero de 2024). Objetivos de Desarrollo Sostenible. Objetivo 4: Educación de Calidad: https://www.un.org/sustainabledevelopment/es/education/

[15] Dirección de Gestión del Conocimiento - UPC. (29 de marzo de 2023). La digitalización de la educación en la pandemia. https://repositorioacademico.upc.edu.pe/handle/10757/667528

[16] Kaspersky. (04 de 09 de 2020). Digital Education: The cyberrisks of the online classroom. Securelist.com: https://securelist.com/digital-education-the-cyberrisks-of-the-online-classroom/98380/

[17] Microsoft. (10 de octubre de 2024). Cyber Signals Edición 8 | Educación bajo asedio: Cómo los cibercriminales atacan nuestras escuelas. news.microsoft.com: https://news.microsoft.com/source/latam/noticias-de-microsoft/cyber-signals-edicion-8-educacion-bajo-asedio-como-los-cibercriminales-atacan-nuestras-escuelas/

[18] Canvia. (25 de abril de 2023). Sector educativo: Ciberataques más comunes en Perú. canvia.com: https://www.canvia.com/ciberataques-educacion/

[19] MINEDU. (12 de marzo de 2024). Matrícula general. https://www.gob.pe/: https://www.gob.pe/20776-matricula-general

[20] Ley N° 29733. (3 de julio de 2011). Ley de Protección de Datos Personales (Ley 29733). https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf?v=1618338779

[21] Payet Rey Cauvi Perez. (2022). PRCP.com.pe. https://prcp.com.pe/wp-content/uploads/2022/03/Tratamiento-de-datos-personales-en-entornos-escolares.pdf

[22] ANPDP. (2024). Resoluciones de los procedimientos sancionadores. https://www.gob.pe/institucion/anpd/colecciones/1801-resoluciones-de-los-procedimientos-sancionadores

[23] Oxford University Press. (2024). Oxford Learner's Dictionaries. https://www.oxfordlearnersdictionaries.com/us/definition/english/posture_1?q=Posture

[24] CNSS. (6 de Abril de 2015). Committee on National Security Systems. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

[25] ASD. (2024). Australian Signals Directorate. https://www.cyber.gov.au/glossary/security-posture

[26] National Cyber Director. (5 de 2024). 2024 Report on the Cybersecurity Posture of the United States. whitehouse.gov: https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf

[27] Forbes. (28 de Marzo de 2024). Information Security Vs. Cybersecurity: What's The Difference? https://www.forbes.com/advisor/education/it-and-tech/information-security-vs-cybersecurity/

[28] ST. John's University. (25 de marzo de 2024). Information Security vs Cyber Security: Are They the Same? https://www.stjohns.edu/news-media/johnnies-blog/information-security-vs-cyber-security-are-they-same

[29] Amine Agalit, M., Chakir, E., Issam, T., & Khamlichi, Y. (2023). A Review of Cybersecurity Management Standards Applied in Higher Education . International Journal of Safety and Security Engineering, 13(6), 1109-1116. https://doi.org/http://iieta.org/journals/ijsse

[30] Check Point. (2024). What is Security Posture? https://www.checkpoint.com/cyber-hub/cyber-security/what-is-security-posture/

[31] Oxford University Press. (2024). Oxford Learner's Dictionaries. https://www.oxfordlearnersdictionaries.com/us/definition/english/framework?q=framework

[32] Ley 28044. (2003). Ley General de Educación (Ley 28044). https://www.minedu.gob.pe/p/ley_general_de_educacion_28044.pdf

[33] Ministerio de Educación. (2020). Proyecto Educativo Nacional (PEN 2036). https://cdn.www.gob.pe/uploads/document/file/1915017/CNE-%20proyecto-educativo-nacional-al-2036.pdf.pdf?v=1679434080