UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

TESIS

Diagnóstico integral de Ciberseguridad, basado en estándares internacionales de seguridad de NIST CSF, para el Programa Nacional de Inversiones en Salud

Para optar el Título profesional de:

INGENIERA EN COMPUTACIÓN E INFORMÁTICA

Autor:

Bach. Carla Vivian Aguirre Segura

Asesor:

Dr. Gilberto Carrión Barco.
ORCID: 0000-0002-1104-6229

Lambayeque-Perú

2023

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

TESIS

Diagnóstico integral de Ciberseguridad, basado en estándares internacionales de seguridad de NIST CSF, para el Programa Nacional de Inversiones en Salud

Aprobado por los Miembros del Jurado

Dr. Ing. Armando José Moreno Heredia
Presidente

Dr. Ing Nilton César Germán Reyes
Secretario

M.Sc. Ing. Denny John Fuentes Adrianzén
Vocal

Lambayeque-Perú

2023

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

TESIS

Diagnóstico integral de Ciberseguridad, basado en estándares internacionales de seguridad de NIST CSF, para el Programa Nacional de Inversiones en Salud

Para optar el Título profesional de:

INGENIERA EN COMPUTACIÓN E INFORMÁTICA

Bach. Carla Vivian Aguirre Segura
Autor

Dr. Gilberto Carrión Barco
Asesor

DEDICATORIA

A Dios,
Por haberme dado la vida, guiarme en el camino correcto y por regalarme cada día.

A mis padres, Elmar y Dercy
Que en todo momento me brindan su amor, apoyo y comprensión.

A mi hermano Max
Por ser mi compañero y apoyo durante todo mi proceso universitario.

A mis pequeños ángeles, Lucero y Adrían
Por su amor, inocencia y dulzura que llenan de alegría mi vida.

A mi Clarisa
Que a pesar que hoy no esté conmigo, fue mi guía, mi motivación y mi aliento en mis momentos débiles.

AGRADECIMIENTO

A mi Dios quién supo guiarme por el buen camino para seguir adelante y no desmayar ante los problemas que se presentaban, enseñándome a encarar las adversidades sin desfallecer en el intento.

A mis padres por su apoyo, comprensión, amor, ayuda en los momentos difíciles, por ayudarme con los recursos necesarios para estudiar, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia para lograr mis objetivos.

A mis hermanos por ser fuente de mi motivación para superarme cada día

A mi esposo Alberth por su comprensión, apoyo, consejos y palabras de aliento para que siguiera adelante con mis ideales.

Un agradecimiento muy especial a mi asesor Dr. Gilberto Carrión, por su guía, seguimiento, tiempo y motivación durante el desarrollo de la tesis.

RESUMEN

"DIAGNÓSTICO INTEGRAL DE CIBERSEGURIDAD, BASADO EN ESTÁNDARES INTERNACIONALES DE SEGURIDAD DE NIST CSF, PARA EL PROGRAMA NACIONAL DE INVERSIONES EN SALUD"

La siguiente investigación presenta el DIAGNÓSTICO INTEGRAL DE CIBERSEGURIDAD, BASADO EN ESTÁNDARES INTERNACIONALES DE SEGURIDAD DE NIST CSF, PARA EL PROGRAMA NACIONAL DE INVERSIONES EN SALUD, la cual proporciona una forma consistente de determinar los controles necesarios para mitigar los riesgos de ciberseguridad en el Programa Nacional de Inversiones en Salud.

Los activos informáticos que se encuentran en el Programa Nacional de Inversiones en Salud, son susceptibles a múltiples tipos de vulnerabilidades, y usuarios mal intencionados hacen uso inaprovechado logrando explotarlas, provocando pérdidas irrecuperables de información, ante esta realidad, se plantea de identificar los riesgos del proceso de Tecnologías de la Información.

Tomando la importancia de la visibilidad de riesgos y como parte estratégica de las organizaciones, las incidencias de ciberseguridad están latentes en cualquier tipo de empresa, esta problemática no es ajeno al Programa Nacional de Inversiones en Salud, que maneja información pública sobre proyectos de inversión en infraestructura de los diferentes hospitales a nivel Nacional. En ese sentido, se propone implementar un modelo de Diagnóstico Integral de Ciberseguridad, basado en los estándares internacionales de seguridad de NIST CSF, que permitirá determinar los controles necesarios para mitigar los riesgos de ciberseguridad de los activos críticos de la Organización.

Palabras Clave: NIST CSF, Estándares Internacionales, Ciberseguridad

ABSTRACT

"COMPREHENSIVE CYBERSECURITY DIAGNOSIS, BASED ON NIST CSF INTERNATIONAL SECURITY STANDARDS, FOR THE NATIONAL HEALTH INVESTMENT PROGRAM"

The following research presents the COMPREHENSIVE CYBER SECURITY DIAGNOSIS, BASED ON NIST CSF INTERNATIONAL SECURITY STANDARDS, FOR THE NATIONAL HEALTH INVESTMENT PROGRAM, which provides a consistent way to determine the controls necessary to mitigate cybersecurity risks in the National Program of Investments in Health.

The computer assets that are in the National Program of Investments in Health, are susceptible to multiple types of vulnerabilities, and ill-intentioned users make inappropriate use, managing to exploit them, causing irrecoverable loss of information. Information Technology process.

Taking the importance of risk visibility and as a strategic part of organizations, cybersecurity incidents are latent in any type of company, this problem is not alien to the National Health Investment Program, which manages public information on investment projects in infrastructure of the different hospitals nationwide. In this sense, it is proposed to implement a Comprehensive Cybersecurity Diagnosis model, based on the international security standards of NIST CSF, which will allow the determination of the controls necessary to mitigate the cybersecurity risks of the Organization's critical assets.

Keywords: NIST CSF, International Standards, Cybersecurity

INDICE

CAPÍTULO I

ASPECTO INFORMATIVO

1.1 Título

Diagnóstico Integral de Ciberseguridad, basado en estándares internacionales de seguridad de NIST CSF, para el Programa Nacional de Inversiones en Salud.

1.2 Autor

Aguirre Segura Carla Vivian

Bachiller de ingeniería en Computación e Informática

1.3 Asesor de especialidad

Dr. Gilberto Carrión Barco.

1.4 Línea de investigación

Gestión de Tecnología de la Información

1.5 Lugar de investigación

Programa Nacional de Inversiones en Salud – Lima

CAPÍTULO II

2 PLANTEAMIENTO DE LA INVESTIGACIÓN

2.1 Síntesis de la situación problemática.

Al 2020, la transformación tecnológica ha cambiado el modo de operar en las organizaciones, de modo que la información se ha convertido en el principal y más importante activo.

Las vulnerabilidades son las debilidades en un sistema de información que pone en riesgo la seguridad informática de esta, por su parte, una amenaza es la acción de aprovechar las vulnerabilidades para comprometer la seguridad del sistema de información.

La falta de controles de seguridad informática en las empresas, pueden generar daños en la organización que, además de la pérdida de datos, van desde la pérdida de dinero y confianza, hasta la pérdida de su imagen que no es recuperable en el corto plazo.

Un claro ejemplo es lo que aconteció al Banco Central de Bangladés en el 2016, con la pérdida de aproximadamente ochenta y un millón de dólares, el Banco Central de Bangladés fue perpetrado por personas mal intencionadas, logrando acceder a la información y los sistemas informáticos, y transferir cantidades de dinero a varios destinos en Filipinas. (INCIBE, 2016)

El 3 de marzo de 2020, el Equipo Nacional de Respuesta a Incidentes de Seguridad Digital alertó sobre el envío de código malicioso de tipo Ransomware, conocido como Net Walker, a varios usuarios que trabajan en hospitales de España, Estados Unidos y Francia, aprovechando la propagación del Coronavirus. (COVID-19). Este ransomware se propaga a través de correos

electrónicos de estilo phishing, que están relacionados con la propagación del coronavirus o covid 19 que se ha desatado en los últimos años. El correo electrónico incluía un archivo malicioso llamado CORONAVIRUS_COVID19.vbs., el cual se caracteriza por cifrar los datos de las víctimas y después pedir una recompensa para recuperar los datos. Para la distribución, los atacantes suplantan la identidad de usuarios de las organizaciones de confianza, luego envían correos electrónicos a los usuarios para ser influenciados por el contenido del mensaje y descarguen el archivo adjunto. Si el usuario abre el archivo adjunto inicia el cifrado de datos e información. (PERCERT, 2020)

Recientemente en nuestro país acontecieron una serie de ataques cibernéticos en las que se encuentran implicadas las empresas públicas, un claro ejemplo lo evidencia el equipo de respuesta de nuestro país ante incidentes de seguridad digital nacional, que, a través de las funciones de monitoreo e investigación en el ciberespacio, identificó un portal web fraudulento que suplanta al portal institucional del Ministerio de Educación (MINEDU). Se observó que el portal web tiene contenido no autorizado por el MINEDU y cuenta con enlaces de imágenes y texto que el usuario al hacer clic re direcciona a otras páginas web sospechosas. (PERCERT, 2020)

Como parte de la planificación estratégica, las organizaciones ponen como objetivo, velar por la seguridad de la información, salvaguardando la disponibilidad, integridad y confidencialidad de este.

La seguridad económica de las organizaciones, estriba del trabajo confiable realizado a la infraestructura crítica de la organización. Las amenazas de ciberseguridad aprovechan la complejidad de los sistemas de información, poniendo la información, economía y reputación en riesgo, afectando la capacidad de la organización para transforma e innovar los ingresos, dar valor,

ganar y mantener a los clientes; dado esto, es importante tener una visibilidad de riesgos de ciberseguridad, que debe abordarse de manera integral a través de personas, procesos y tecnología, para identificar oportunamente las vulnerabilidades de los sistemas de información, de forma que sean identificadas y así predecir las potenciales amenazas a los sistemas.

A fin de abordar estas amenazas, en el año 2019, en los Estados Unidos de Norte América, el presidente. emitió la Orden Ejecutiva N°13636 “la mejora de la ciberseguridad de las infraestructuras Críticas”, donde se indica que la regulación de desempeño requiere el desarrollo de un marco de seguridad cibernética que incluya un conjunto de estándares y mejores prácticas para ayudar a las organizaciones a administrar los riesgos de seguridad cibernética (AWS & Organización de los Estados Americanos, 2019)

Tomando la importancia de la visibilidad de riesgos y como parte estratégica de las organizaciones, los hechos acontecidos no segregan el rubro de sector público o sector privado, las incidencias de ciberseguridad están latentes en cualquier tipo de empresa, esta problemática no es ajeno al Programa Nacional de Inversiones en Salud de siglas PRONIS, que maneja información pública sobre proyectos de inversión destinados a la infraestructura de los diferentes hospitales a nivel Nacional. Al respecto, se propone implementar un modelo de Diagnóstico Integral de Ciberseguridad, basado en los estándares internacionales de seguridad de NIST CSF, que proporciona una forma consistente de determinar los controles necesarios y adecuados para mitigar los riesgos de ciberseguridad.

2.2 Formulación del problema de investigación

¿El diagnóstico Integral de Ciberseguridad, basado en estándares internacionales de seguridad de NIST CSF, permitirá identificar los riesgos de ciberseguridad en el Programa Nacional de Inversiones en Salud?

2.3 Justificación

A continuación. explicaré el por qué y la importancia de la justificación

Justificación Económica: Porque una vez terminado el proyecto de investigación, el Programa Nacional de Inversiones en Salud permitirá ajustar el presupuesto destinado a personal especializado en Seguridad Informática.

Justificación Operativa: Porque permitirá identificar, inventariar y gestionar riesgos informáticos de los activos críticos del Programa Nacional de Inversión en Salud.

Justificación Académica: Porque mediante este proyecto, se aplicará conceptos sobre estándares internacionales de seguridad de Nist CSF.

Justificación Tecnológica: Para proteger la infraestructura del Programa Nacional de Inversiones en Salud y visualizar los riesgos Informáticos previendo de un enfoque priorizado, flexible, repetible, neutral que se adapte al PRONIS, Así como también mejorar el nivel de entendimiento del Equipo de Trabajo de Tecnologías de la Información y Comunicación sobre la Ciberseguridad y su importancia.

2.4 Hipótesis

Mediante el Diagnóstico Integral de Ciberseguridad, basado en estándares Internacionales de Seguridad de NIST CSF, permitirá determinar controles necesarios para mitigar los riesgos de ciberseguridad en el Programa Nacional de Inversiones en Salud.

2.5 Tipo de estudio y diseño de la investigación

Teniendo como objetivo, determinar los controles necesarios mediante el diagnóstico Integral de ciberseguridad, basado en estándares internaciones de seguridad de NIST CSF para mitigar los riesgos de ciberseguridad en el Programa Nacional de Inversiones en Salud, el diseño de contrastación de la hipótesis es **no experimental- propositiva**, dado que se fundamenta en la necesidad de proponer controles para la mitigación de riesgos.

Se medirá el impacto de la variable independiente: Modelo de gestión de ciberseguridad basado en NIST CSF, sobre la variable dependiente: mitigación de riesgos

de la hipótesis se formula a continuación:

Ge: O1 X O2

Dónde:

O1: La observación 1(O1) evalúa el estado actual de la seguridad cibernética del

Programa Nacional de Inversiones en Salud.

X: Representa el modelo de gestión ciberseguridad basado en los estándares de

seguridad internacional de NIST CSF.

O2: La observación 2 (O2) evalúa el estado de seguridad cibernética luego del diagnóstico integral de Ciberseguridad basado en NIST CSF del Programa Nacional de Inversiones en Salud propuesto.

2.6 Objetivos de la Investigación

2.6.1 Objetivo General

Determinar los controles necesarios mediante el Diagnóstico Integral de ciberseguridad basado en estándares internacionales de seguridad de NIST CSF para mitigar los riesgos de ciberseguridad en el Programa Nacional de Inversiones en Salud.

2.6.2 Objetivos Específicos

- Describir la situación actual de ciberseguridad del Programa Nacional de Inversiones en Salud por medio de recolección de datos mediante una ficha de observación.
- Determinar el alcance de la propuesta para determinar el nivel de capacidad de ciberseguridad.
- Aplicar el marco internacional de NIST CSF para el Programa nacional de Inversiones en Salud con respecto al procesos de Tecnologías de la Información.
- Emitir recomendaciones de los controles que permitan mitigar los riesgos encontrados.

CAPÍTULO III

DISEÑO TEÓRICO

3.1.Antecedentes de la Investigación

Según (Gómez Suarez, 2019), su investigación cuyo objetivo fue diseñar una estrategia de seguridad informática en una empresa basada en el marco de trabajo NIST, haciendo uso de estándares internacionales del marco de ciberseguridad NIST CSF, tomando como estudio los servicios y tipos de servicios de infraestructura informática, muestra resultados en base a la implementación teórica del framework de ciberseguridad NIST, aplicando la seguridad cibernética a la empresa en la que realizan su proyecto de tesis, mediante las cinco (5) fases del marco que son: identificar, detectar, proteger, responder y recuperar, para implementación de medidas y controles de refuerzo efectiva a todos los servicios y tipos de servicios de infraestructura informática de la empresa.

(Lara Guijarro, 2019), en su proyecto de investigación, desarrolló modelos de seguridad de la información para la Universidad Regional Autónoma de los Andes, Tulcán basados en modelos de seguridad de la información como: OSSTMMv3 (Versión de Open Source Security Test Methodology) 3), NIST 800 - 30 (Instituto Nacional de Estándares y Tecnología) e ISO 27001. Seguridad de datos. Logró corroborar el estado de la seguridad de la información, mediante la recolección de datos mediante encuestas aplicadas a usuarios de la red de la Universidad Regional Autónoma de los Andes, para posteriormente aplicar la política de seguridad, la identificación de activos, la implementación de controles y la evaluación de programas de seguridad.

2.6.3 Antecedentes Nacionales

Según (Guillinta Chavez & Merino Rivera, 2016), en su proyecto de investigación que tiene como objetivo la implementación de un modelo de prevención y defensa frente a ataques cibernéticos, basado en estándares de seguridad internacional en la empresa IT Expert, a través del uso de estándares internacionales NIST SP 800-30 y NIST 800-115, aplicado a los activos TI. Los autores obtienen como resultado, un progreso notable con relación a la protección de los sistemas críticos de la empresa contra ataques informáticos, remediación de las vulnerabilidades de infraestructura crítica comprometida, y al establecimiento de niveles de riesgo óptimos en IT-Expert, de acuerdo a la aplicación del modelo propuesto en sus operaciones de TI basado en la seguridad de estándares internacionales, y el considerar el análisis de vulnerabilidades en cada uno de sus despliegues, el monitoreo incesante de los niveles de riesgo, y la remediación de vulnerabilidades en cada uno de sus activos de TI.

Citando a (Vilcamorro Zubiate & Vilchez Linares, 2018) Su investigación tiene como objetivo proporcionar un marco de ciberseguridad para el área SOC de telecomunicaciones de EP, que permita: implementar, operar, monitorear, revisar y mejorar los controles de seguridad. La ciberseguridad se basa en los estándares internacionales de ciberseguridad.

Los autores hicieron uso del Marco Nist CSF, aplicado a las infraestructuras críticas de la Empresa de Telecomunicaciones EP, mostrando como resultado la creación de estrategias de ciberseguridad basado en el análisis de experiencias y publicidades, ayudando a identificar los servicios críticos para la empresa Telecomunicaciones EP.

2.6.4 Antecedentes Locales

Según (Leiva Peña, 2016) , en su proyecto de investigación, se refiere al diseño de un sistema de gestión de seguridad de la información, guiándose en estándares internacionales haciendo uso de la norma ISO IEC 27001 y 27002 y la metodología PDCA, con el objetivo de mejorar la entrega de medicamentos en la Red de Servicios de Salud de Lambayeque, ayudando a asegurar los sistemas la información utilizada.

Su proyecto resume en el desarrollo de un plan de tratamiento de riesgos en el marco del documento de la ISO, que condujo al desarrollo de políticas, procedimientos y controles que la organización puede aplicar para lograr la certificación.

2.7 Bases teóricas

2.7.1 Seguridad de la Información

La seguridad de la información, implica la implementación de estrategias y tácticas que incluyen operaciones en las que la información es el activo más significativo, las mismas que corresponden incluir principalmente el establecimiento de políticas, directivas o controles de seguridad, técnicas y procedimientos para detectar amenazas y vulnerabilidades de seguridad y así evitar poner en riesgo los activos, salvaguardando los sistemas que almacenan y administran la información.

La seguridad de la información, trata de conservar la confidencialidad, así como integridad y disponibilidad de la información mediante el proceso de gestión del análisis de riesgo, y garantiza que los riesgos sean manejados adecuadamente mediante la ISO 27001, es una norma internacional

donde se indica a detalle los requisitos necesarios, y procesos para la implementación, mantenimiento y mejora continua del sistema de seguridad de la información en una organización.

La norma internacional ISO 27001, presenta también requisitos para la evaluación y el manejo de los riesgos informáticos mediante el tratamiento de los mismos, adecuados a la necesidad de las organizaciones. La norma está elaborada para implementarse en cualquier industria empresarial, en todo tipo de organización.

Como se detalla líneas arriba, la seguridad de la información de forma puntual tiene la protección de la información como finalidad general, basado en el control de uso y accesos, protección de divulgación, y destrucción no autorizada de información. Entre la definición de "seguridad de la información" y "Seguridad Informática" tienen diferencias muy pequeñas, las mismas que radican en la orientación y el enfoque, la utilización de metodologías y zonas de concentración (Muñoz, cortez, & Bustamante, 2011).

2.7.2 Seguridad Informática.

Alrededor del año 1980, nació la seguridad Informática como medida de respuesta para contrarrestar y evitar las consecuencias que producen los diferentes ataques informáticos.

Todo empezó a cobrar relevancia, cuando la información utilizada por los sistemas informáticos, necesitaban cada ves de más privilegios para su acceso, o era de suma importancia para los usuarios de primera línea, conllevando así a convertirse en un activo para la organización. Es así como la seguridad informática

Así es como la seguridad informática crece por a la necesidad de proteger información sensible que podría impactar negativamente al negocio de una organización.

Hoy en el mundo, todas las organizaciones procesan los datos utilizados en equipos informáticos para el desarrollo de su negocio. Organizaciones públicas y privadas manejan información sensible, no solo de manera interna o nacional, también para países enteros, como ejemplo está el registro civil, donde se manejan datos de ciudadanos tratados y visto en todo un país. Ante ello surge la pregunta, ¿Qué pasaría si los datos que se encuentran en un sistema son alterados por un pirata informático siendo modificados o eliminados? Se desencadenaría un caos impactando a todo tipo de industria, viendo esta problemática, se debe otorgar la más alta importancia de seguridad informática en todas las organizaciones que consideren a la información como un activo privilegiado. (Aimacaña, 2015)

Con el pasar de los tiempos personas mal intencionadas han venido desarrollando ataques más sofisticados para explotar las vulnerabilidades de los sistemas informáticos conectados a internet, los usuarios, trabajadores y empresas aún no son conscientes que el funcionamiento correcto de los sistemas es consecuencia de la protección y seguridad de datos y equipos de información, sin embargo, la mayoría de las organizaciones no tienen a la seguridad informática entre sus prioridades.

Se entiende como seguridad, el estado o situación de cualquier sistema sea informático o no, que está libre de daño, peligro o riesgo. Es imposible que se aspire a un sistema total mente fiable, ya que según expertos en la materia opinan que la seguridad informática es utópico, dado que no existe un sistema al 100% seguro (Domínguez Chávez, 2015)

Para Chanaluiza, Meza y Tasipanta (Chanaluiza , Meza, & Tasipanta, 2012)la seguridad informática se enfoca en garantizar o salvaguardar la información contenida en los diversos sistemas, es un método que se usa para examinar adecuadamente los problemas y vulnerabilidades en la administración de una organización.

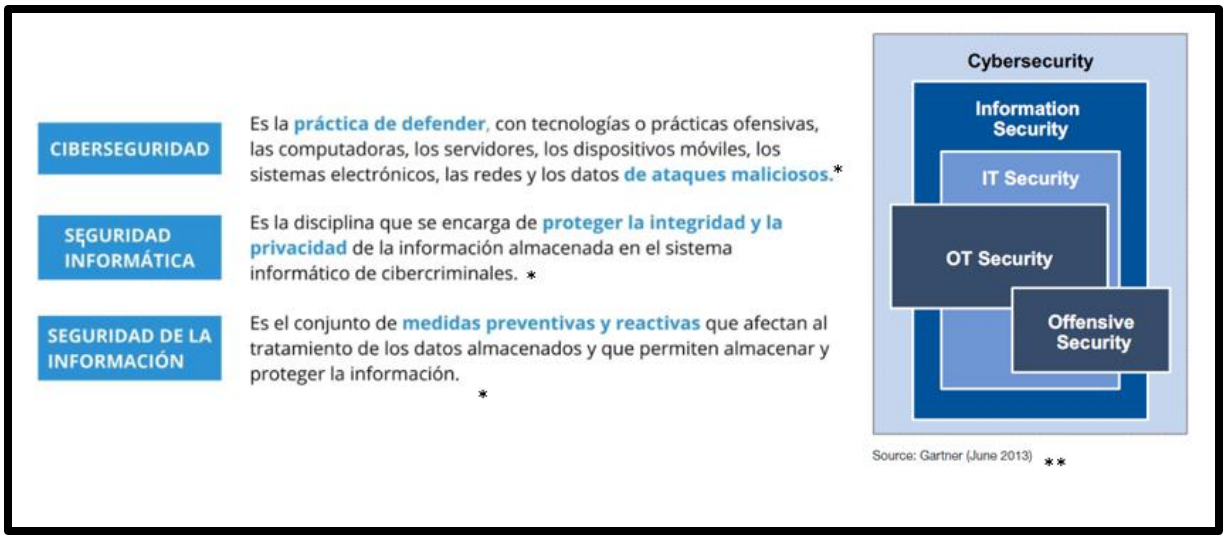
Según expertos de la seguridad informática, opinan que la seguridad informática protege y/o resguarda al sistema informático, asegurando la integridad y privacidad de la información que contiene. Por ello, en las organizaciones deberán implementar medidas que salvaguardan la infraestructura, aplicaciones, servicios de comunicación, hardware y software, entre otros servicios que sobrellevan la operación de la empresa. (ISOTools Excellence, 2017)

2.7.3 Ciberseguridad

La ciberseguridad se orienta a la información en los sistemas interconectados digitales que lo procesan, transmiten o almacenan, por lo que está directamente relacionado con la seguridad informática.

La ciberseguridad es denominada como la defensa de activos de información, realizada mediante el proceso de tratamiento de amenazas que pone en riesgo la información, transportada y almacenada y almacenada y transportada por interconectados (ISACA, 2020)

Figura 1Cuadro comparativo de Seguridad de la Información, Seguridad Informática y ciberseguridad



** Fuente: Elaboración propia*

**Fuente: Cuadrante Gartner 2013

2.7.4 Amenaza Informática

Una amenaza es un accidente, circunstancia o acontecimiento que pueda tener un impacto negativo en los activos y operaciones en cualquier tipo de organización (National Institute of Standards and Technology, 2012).

En relación a tecnologías de la información, una amenaza se define a todo elemento y acción que atenta a la seguridad de la información. La presencia de vulnerabilidades en los sistemas digitales, es hallazgo de amenaza, lo que significa que la amenaza existe siempre que haya una vulnerabilidad y esta sea explotada.

El perfeccionamiento e incremento de las técnicas de tendencia como ingeniería social, la falta de sensibilización y concientización a las personas en el uso de la tecnología y la creciente

rentabilidad y ganancia de los ataques, han sido causantes del incremento de amenazas intencionales en el mundo. (Departamento de Seguridadd Informática, 2018)

2.7.5 Riesgo

Se define el riesgo como el "efecto de incertidumbre sobre los objetivos", siendo el resultado positivo o negativo de lo esperado. (ISO 31000, 2018)

(Deloitte, 2016) Los riesgos de Tecnologías de la Información, podrían surgir en cualquier jerarquía dentro de la estructura orgánica. En primer lugar, los riesgos podrían surgir de prioridades que compiten entre el objetivo de hacer crecer el negocio, reducir costos, generar ganancias y otros similares

En segundo lugar, los riesgos de Tecnologías de la Información, pueden permanecer dentro de estar amplificados por un modelo o prototipo incorrecto del manejo de las herramientas y tecnología, administración del riesgo, inefectivo gobierno y vigilancia, políticas y estándares, métrica del riesgo y cultura del riesgo.

2.7.5.1 Riesgo inherente

Se llama riesgo inherente, al riesgo especifico producto de cada trabajo y proceso. El riesgo se encuentra en todos los ambientes y afecta a las múltiples categorías de las operaciones de una empresa. Mediante el plan de Gestión la empresa debe identificar los riesgos y así mitigarlos.

Este tipo de riesgo, proviene de los factores externos e internos, las empresas deben estar preparadas para minimizar el impacto y las consecuencias de ocurrir una eventualidad de este tipo.

A continuación, se detallan algunas fuentes de riesgo inherente

Factores externos, como normativas y regulaciones.

Características, políticas y normas de la empresa.

Estrategias y métodos de trabajo.

Área financiera.

Sistemas de control interno.

Hay varios métodos para identificar los riesgos inherentes e incluso programas creados específicamente para ello, independiente del método que se utilice el procedimiento reside en:

Recabar información de la empresa, así como los métodos utilizados para el control interno, que permita hallar el riesgo inherente.

Sistematizar la información para evaluar e identificar riesgos inherentes.

Relacionar riesgos inherentes con áreas y procesos de la empresa.

Clasificar los riesgos inherentes de acuerdo con la actividad.

2.7.5.2 Riesgo Residual

Centralmente en toda la organización para la evaluación de riesgos, se inicia detectando el riesgo inherente. El efecto después de haber propuesto los controles necesarios y medidas preventivas sobre los riesgos inherentes, viene a ser el riesgo residual. Es decir, es el riesgo remanente tras el tratamiento del riesgo.

Se denomina también riesgo inherente, al riesgo existente sin que se haya tomado alguna acción con el fin de modificar la probabilidad e impacto de un hecho, y el riesgo residual viene a ser el que permanece luego de la respuesta del riesgo inherente.

En resumen, los riesgos inherentes vienen a ser los riesgos sin tener en cuenta los controles, el residual viene a ser el riesgo que se le da un tratamiento aplicando los controles, y por último existe un riesgo que es el Riesgo tratado, es el riesgo eliminado mediante la aplicación de controles.

Figura 2: Evaluación del Riesgo

Fuente: ISO/IEC 27001:2013-Seguridad de la Información-GESCAM & ERCA

2.7.6 Control

Se define como control a la medida o acción que regula, modifica o cambia el riesgo. (ISO 31000, 2018), es la base para mitigar, implementar y/o controlar lo ser necesario para el riesgo.

Los controles no siempre producen el efecto pensado, previsto o asumido, no se limitan a cualquier política, dispositivo, práctica o proceso y acciones que modifique el riesgo.

2.7.7 Diagnóstico Integral de Ciberseguridad

El diagnóstico integral realiza un análisis de riesgos a nivel profesional para detectar las amenazas a las que están expuestos los activos críticos de la empresa, su probabilidad de ocurrencia e impacto con el fin de gestionar la seguridad de la información para salvaguardar su integridad, confidencialidad y tenerla disponible siempre que se le necesite.

El diagnostico se basa en la recopilación de información objetiva y subjetiva a través de entrevistas, cuestionario y observación, reuniones con personas clave para entender la situación general, identificación de causas de los problemas experimentados o riesgos inherentes a su empresa, plan de acción.

Al finalizar un diagnóstico integral se señalan los escenarios de riesgo, así como las recomendaciones para minimizarlos y disminuir su probabilidad de ocurrencia e impacto a la organización.

2.7.8 NIST

NIST, es el acrónimo de Instituto Nacional de Estándares y Tecnología, con siglas en inglés (National Institute of Standards and Technology), es una dependencia de los Estados Unidos de América, que aprueba estándares sobre productos y servicios relacionados a la tecnología.

Nist es un marco para la gestión de riesgos de ciberseguridad, que se ajusta a cualquier tipo de organización pequeña o grande, pública o privada (no importa tamaño o rubro). Se basa en estándares aceptados por el entorno de la ciberseguridad como ejemplo está NIST SP 800-53, COBIT 5, ISO/IEC 27001:2013, CIS CSC, entre otros).

Entre todas sus publicaciones, son particularmente relevantes los de serie SP 800 que se refiere a la Seguridad de la Información.

El Marco de Ciberseguridad de NIST- Cybersecurity Framework CSF, brinda procedimientos para seguir las mejores prácticas de gestión de riesgo en ciberseguridad para luego estructurar hojas de rutas que mitiguen los riesgos en la organización (Shackelford, Craig, & Martell, 2015)

El marco de NIST, sirve como asistencia a las empresas para comprender, administrar y reducir los riesgos de ciberseguridad internos como externos para proteger redes, datos e información. Brindando una reseña de mejores prácticas para ayudar a decidir protección de ciberseguridad.

El Nist fue inventado, para identificar las directrices y normas de la seguridad, aplicables en la infraestructura crítica de las organizaciones proveyendo un enfoque flexible y repetible, que prioriza actividades y permite conseguir el buen rendimiento de las infraestructuras críticas.

2.7.9 Marco de seguridad cibernética (CSF) de NIST

Debido al incremento de incidentes de ciberseguridad en los Estados Unidos de Norte América, en ese entonces Barack Obama como presidente , emite la orden ejecutiva (OE)13636, el 12 de febrero del 2013, que establece que "Es la política de los Estados Unidos mejorar la seguridad y resiliencia en las infraestructuras Críticas y mantener un entorno cibernético que fomente la eficiencia, la innovación y la prosperidad económica al mismo tiempo que promueve la seguridad, la confidencialidad, comercial, la privacidad y las libertades civiles", según NIST 2018 (NIST, 2018).

La característica principal del NIST CSF, es dejar de lado los estándares rígidos; el NIST CSF comenzó por crear una iniciativa para la protección de infraestructuras críticas, como la OTAN, que ha desarrollado manuales orientados en la protección de infraestructuras críticas destinadas para la defensa nacional. Su manual se llama "Manual del Marco de Trabajo de Ciberseguridad Nacional" (OTAN, 2012)."

Decreto Supremo N° 066-2011-PCM, Plan para el Desarrollo de la Sociedad de la Información en el Perú - Perú Agenda Digital 2.0 El Objetivo 7 establece "promover prácticas de justicia pública de calidad" y "mejorar la implementación de la seguridad de la información" de los Mecanismos de la Estrategia de seguridad cibernética, protección de la infraestructura crítica, lucha contra el delito cibernético y asistencia en el despliegue y desarrollo de marcos de seguridad cibernética.

La definición de seguridad digital en el artículo 2 del Decreto Supremo N° 050-2018-PCM indica que la seguridad digital doméstica es un estado de confianza en el dominio digital, en consecuencia, adoptando y gestionando todas las correspondencias, estamos

tomando medidas proactivas. Para hacer frente a los riesgos que afectan los objetivos de seguridad, económicos, sociales y ambientales nacionales antes descritos.

Está respaldado por alianzas entre gobiernos, el sector público, el sector privado y otros actores que ayudan a implementar acciones, medidas y controles. Considere los siguientes puntos:

a) Nota 1: La confianza en el entorno digital, también conocida como confianza digital, es el resultado de intercambios predecibles, honestos, seguros y confiables creados entre individuos, empresas y cosas.

b) Nota 2: Las acciones reactivas y preventivas incluyen programas de políticas, gestión, tecnología, capacitación y concientización. Mantener la tríada de seguridad: mantener la confidencialidad, integridad y disponibilidad de la información en el entorno digital.

c) Nota 3: El riesgo de seguridad digital, o riesgo en el entorno digital, es el resultado de una combinación de amenazas y vulnerabilidades en el entorno digital. La gestión de los riesgos de seguridad en los medios digitales le permite tomar acciones y medidas que se alinean con sus objetivos económicos y sociales.

d) Nota 4: El bienestar económico y social incluye la innovación, la creación de riqueza, la competitividad y las características relacionadas con la libertad personal, la educación cultural, la salud, la participación, la ciencia, la participación democrática, etc.

2.7.9.1 Estructura del CSF

Este marco proporciona un camino para reducir el riesgo de amenazas cibernéticas, incluida la seguridad de la información. El marco consta de tres partes:

comienzo: núcleo de marco, intermedio: nivel de implementación del marco y finalmente perfil del marco.

2.7.9.2 Framework Core o Núcleo del Marco

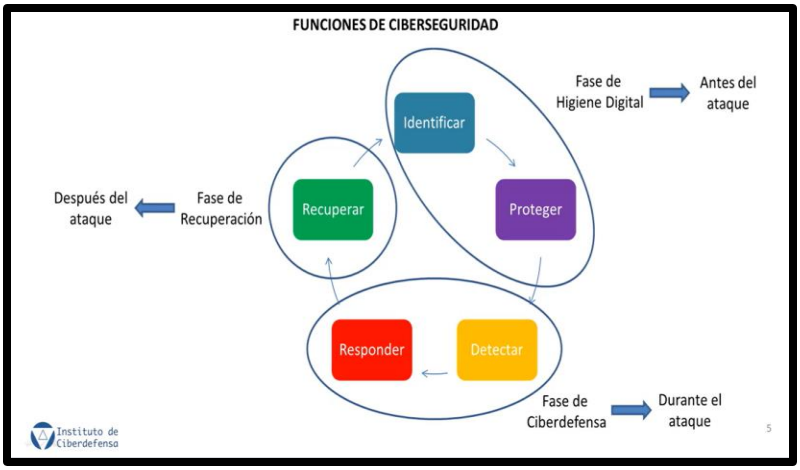
Un núcleo es un conjunto de actividades y resultados de ciberseguridad deseados, organizados en categorías y alineados con referencias informadas a los estándares aceptados de la industria. Diseñado para ser intuitivo, actúa como una capa de traducción, lo que permite la comunicación entre equipos multidisciplinarios utilizando un lenguaje simple y no técnico.

- Está compuesto por tres partes las cuales son: Funciones, Categorías y Subcategorías y Referencias Informativas.

2.7.9.2.1 Funciones

Las funciones organizan las actividades del entorno de ciberseguridad al más alto nivel, las funciones son cinco: Antes del ataque (Identificar, Proteger) durante el ataque (Detectar y Responder), después del ataque (Recuperar).

Figura 3: Funciones de la Ciberseguridad



Fuente: ISO/IEC 27001:2013-Seguridad de la Información-GESCAM & ERCA

Las funciones ayudan a las organizaciones a expresar y mostrar la gestión del riesgo del entorno de ciberseguridad, abordando amenazas, delegando decisiones de gestión, organizando la información y mejorando el aprendizaje de las actividades previas.

Contiene cinco funciones de alto nivel: identificación, protección, detección, respuesta y recuperación.

Tabla 1 Funciones de NIST CSF

FUNCIONES	DESCRIPCIÓN
Identificar	Permite la identificación organizacional de activos, datos, sistemas, recursos, contexto comercial y riesgos de ciberseguridad que afectan el entorno de una organización Como identificador, el acrónimo ID.AM se divide en Gestión de activos, Entorno empresarial, Gobernanza, Evaluación de riesgos, Estrategia de gestión de riesgos y Gestión de riesgos de la cadena de suministro.
Proteger	Esto permite el desarrollo e implementación de las medidas necesarias para limitar y/o prevenir el impacto de posibles eventos de ciberseguridad. Estos se dividen en Gestión de Identidad y Control de Acceso, Concientización y Capacitación, Seguridad de Datos, Procesos y Procedimientos de Protección de la Información y Tecnologías de Protección y Mantenimiento.
Detectar	Esto permite el desarrollo y despliegue de actividades para determinar la ocurrencia de eventos de ciberseguridad a través de un monitoreo continuo. Se divide en anomalías y eventos, monitoreo continuo de seguridad y procesos de detección.
Responder	Aprobar la definición e implementación de acciones para responder y mitigar el impacto de los eventos de ciberseguridad identificados. Esto se divide en planificación de respuesta, comunicación, análisis, mitigación y remediación.

Recuperar	Esta es una capacidad que permite el desarrollo de actividades de gestión de la resiliencia y el desarrollo de operaciones normales después de un incidente. Se divide en planificación, mejora y comunicación.

Fuente: Elaboración propia

El núcleo del marco presenta una lista de partes de características, categorías, subcategorías e información de referencia para describir las operaciones de seguridad cibernética en áreas de infraestructura crítica.

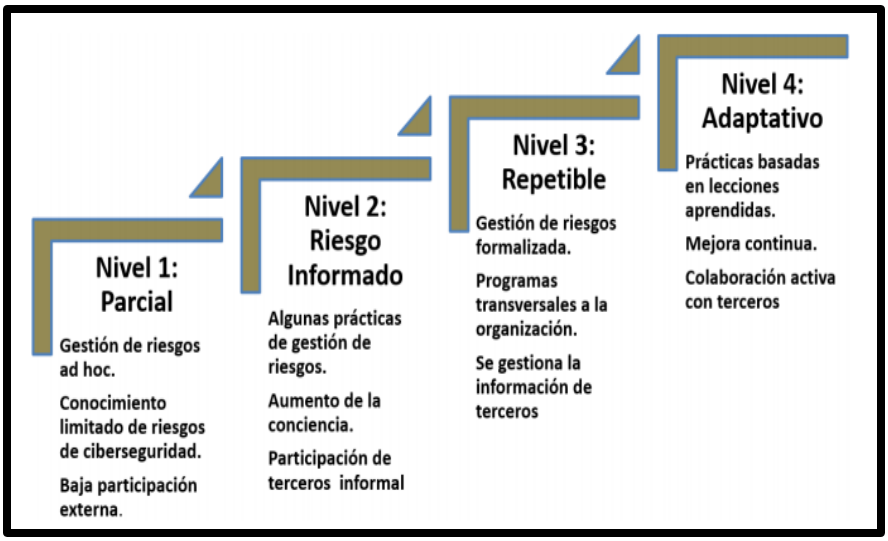
El Marco, ayuda utilizar subcategorías, referencias informáticas eficientes y rentables que ayuda administrar los riesgos de seguridad cibernética en los diferentes sectores y organizaciones públicos y privados.

Los resultados identificados en el núcleo del marco por medio de sus partes: funciones, categorías y subcategorías, son los mismos identificados en la guía de seguridad de los sistemas de control industrial conocido con abreviaturas de ICS.

2.7.9.2.2 Niveles de implementación del NIST CSF

El núcleo del marco presenta una lista de partes de características, categorías, subcategorías e información de referencia para describir las operaciones de seguridad cibernética en áreas de infraestructura crítica.

Figura 4: Niveles de implementación del NIST CSF



Fuente: National Institute of Standards and Technology (NIST)

Nist señala que los niveles de NIST no son una indicación precisa de los niveles de madurez dentro de una organización y, en realidad, son relativamente similares. Es importante para una organización determinar el nivel deseado. (Los controles no tienen que implementarse al más alto nivel), asegúrese de que el nivel que elija cumpla con los objetivos de su organización y ayude a reducir el riesgo de ciberseguridad a un nivel aceptable.

Tabla 2: *Descripción de los Niveles de Implementación de Nist CSF.*

N°	NIVEL	DESCRIPCIÓN
NIVEL 1	PARCIAL	Durante este nivel, los esfuerzos se realizan de manera aislada, y hay iniciativas básicas de ciberseguridad. Se desarrollan implementaciones de puntos de vista ad-hoc. Hay dependencia alta,

		del personal responsable de llevar las tareas no documentadas. Se desarrolla la actitud reaviva frente a los incidentes de seguridad.
NIVEL 2	RIESGO INFORMADO	Establecimiento de pautas y/o lineamientos para el desarrollo de tareas. Hay dependencia del conocimiento individual. Se documenta el desarrollo de tareas, y existe progreso para el desarrollo de procesos.
NIVEL 3	REPETIBLE	En este nivel se formaliza y documenta las políticas y procedimientos. Las implementaciones complejas se automatizan y centralizan, permitiendo iniciar la gobernanza. Los procedimiento y políticas implementadas ayudan a establecer los controles y métricas. El enfoque se basa en el esfuerzo de procesos, las personas y la tecnología.
NIVEL 4	ADAPTATIVO	Las actividades relacionadas con el control interno son realizadas por el RIS (Gerente de Seguridad de la Información), quien es responsable de verificar y mejorar el sistema de gestión de seguridad de la información, coordinando con las desviaciones y/o revisiones de cumplimiento. La experiencia obtenida de los controles definidos puede conducir a actividades de mejora continua. La comunicación es periódica, las partes interesadas se informan continuamente.

	Alineamiento, de estrategias, esfuerzos y tecnología de ciberseguridad, con la misión y visión de la entidad.

Fuente: Elaboración Propia

Un perfil es una combinación única de roles, categorías y subcategorías con los requisitos comerciales, la tolerancia al riesgo y los recursos de una organización. Los perfiles permiten a las organizaciones establecer una hoja de ruta para la reducción de riesgos de ciberseguridad que refleje las prioridades comerciales, gestione los riesgos de seguridad y se alinee con los objetivos de la organización y la industria. Esta hoja de ruta tiene en cuenta los requisitos legales o reglamentarios y las mejores prácticas de la industria. Debido a la complejidad de muchas organizaciones, pueden optar por tener múltiples perfiles para adaptarlos a componentes básicos específicos y satisfacer sus necesidades individuales.

Definir un perfil actual permite a las organizaciones realizar una evaluación objetiva de su programa de seguridad cibernética contra el CSF (no relacionado con revisiones formales o técnicas de otro tipo) y qué esperar de su estado de seguridad actual se puede saber con precisión. Objetivos que brindan información sobre reclutamiento, capacitación, cambios de políticas, cambios de procedimientos y estrategias y prioridades de liderazgo tecnológico en comparación con el perfil actual dada la evaluación de riesgos, los requisitos de cumplimiento y los objetivos organizacionales.

2.7.9.2.3 Categorías

Las categorías son divisiones funcionales en grupos de resultados de ciberseguridad estrechamente relacionados con necesidades prácticas y actividades específicas. Ejemplos de categorías son "gestión de activos", "gestión de identidad y control de acceso" y, finalmente, "proceso de descubrimiento".

2.7.9.2.4 Referencias Informativas.

Estas son secciones específicas de estándares, lineamientos y prácticas comunes en áreas críticas de infraestructura que guían cómo lograr buenos resultados en cada subcategoría.

2.7.9.3 Implementación del marco NIST CSF

Ayuda a identificar y priorizar acciones para mitigar los riesgos de seguridad cibernética y puede usarse como una herramienta para alinear los enfoques de políticas, negocios y tecnología para la gestión de riesgos.

Las organizaciones pueden utilizar este marco como parte clave de un proceso sistemático para identificar, evaluar y gestionar los riesgos de ciberseguridad. Este marco no está diseñado para reemplazar los procesos organizacionales.

Las organizaciones pueden usar marcos y superposiciones actuales para identificar brechas en su enfoque actual del riesgo de seguridad cibernética y desarrollar una hoja de ruta para mejorar.

Aquí hay algunas secciones donde las organizaciones pueden usar el marco:

2.7.9.3.1 Revisión básica de las prácticas de ciberseguridad en la Organización.

Con este marco, puede comparar las prácticas de ciberseguridad actuales de su organización con las descritas en el marco de referencia.

Al crear un perfil existente, las organizaciones pueden probar el rendimiento en categorías y subcategorías clave y probar cinco capacidades de alto nivel: identificación, protección, detección, respuesta y recuperación. La ciberseguridad se puede administrar en función de los riesgos conocidos de una manera que permita a las organizaciones lograr los resultados deseados y determinar si pueden mejorar. Las organizaciones pueden usar esta información para desarrollar planes de acción para fortalecer las medidas de ciberseguridad existentes y mitigar los riesgos de ciberseguridad.

La organización puede usar esta información para reasignar recursos para fortalecer otras prácticas de ciberseguridad.

2.7.9.3.2 Establecimiento o mejora de un programa de ciberseguridad.

Los siguientes pasos describen cómo una entidad puede fortalecer el marco para crear un programa de seguridad cibernética o modificar un programa.

PASO 1. Priorizar y Alcance.

Una organización define sus objetivos de negocio, misión y prioridades de alto nivel. Con la información obtenida, la organización desarrolla una estrategia de toma de decisiones de implementación de ciberseguridad y define el alcance de los sistemas y activos que soportan el proceso o área de actividad seleccionada.

Los marcos se pueden adaptar para admitir diferentes áreas comerciales o procesos dentro de

una organización. Sus necesidades comerciales y la tolerancia al riesgo asociada pueden variar. La capacidad de aceptar el riesgo se refleja en el nivel de desempeño objetivo.

Con esta información, las organizaciones desarrollan estrategias de toma de decisiones para la implementación de la ciberseguridad y determinan el alcance de los sistemas y activos que respaldan los procesos o áreas comerciales seleccionadas. Este marco se puede adaptar para admitir diferentes áreas comerciales o procesos dentro de una organización, que pueden tener diferentes necesidades comerciales y tolerancias de riesgo asociadas. Su tolerancia al riesgo se refleja en su nivel de consecución de objetivos.

PASO 2. Orientación.

Orientación. Una vez que se determina el alcance de un programa de ciberseguridad empresarial o de procesos, la organización define su enfoque holístico de los sistemas y los activos relacionados, los requisitos reglamentarios y los riesgos. Luego, las organizaciones consultan fuentes de información para identificar amenazas y vulnerabilidades que se aplican a esos sistemas y activos

PASO 3. Crear un Perfil Actual.

Cree un perfil existente. La organización desarrolla un perfil actual que muestra los resultados principales y de subcategoría del marco que se están logrando actualmente. Tenga en cuenta que si una sección tiene éxito, ese hecho ayudará a respaldar sus próximos pasos al proporcionar información de antecedentes.

PASO 4. Realizar una evaluación de riesgos.

Realice una evaluación de riesgos. Esta evaluación puede guiarse por el proceso general de gestión de riesgos de la organización o por actividades previas de evaluación de riesgos. Las organizaciones analizan su entorno operativo para distinguir entre la probabilidad de un evento de ciberseguridad y su impacto en la organización. Es fundamental que las organizaciones identifiquen los riesgos emergentes y utilicen información sobre amenazas de seguridad cibernética de fuentes internas y externas para comprender mejor la probabilidad y el impacto de estas amenazas y eventos de seguridad de la red.

PASO 5: Crear un perfil objetivo.

Cree un perfil de destino. La organización desarrolla un perfil objetivo centrado en la evaluación de categorías y subcategorías del marco que describen los resultados de ciberseguridad que desea la organización. Las organizaciones también pueden crear sus propias categorías y subcategorías adicionales para reflejar sus riesgos únicos. Las organizaciones también pueden considerar la influencia y los requisitos de las partes interesadas externas, como asociaciones comerciales, clientes y socios comerciales, al desarrollar un perfil objetivo. Los registros de goles deben demostrar plenamente los criterios para marcar goles.

PASO 6: Determinar, analizar y priorizar brechas

Las organizaciones deben comparar sus perfiles actuales y objetivo para identificar brechas, desarrollar un plan de acción priorizado para llenar las brechas (que refleje los impulsores de la misión, los costos, los beneficios y los riesgos) y proporcionar

resultados.

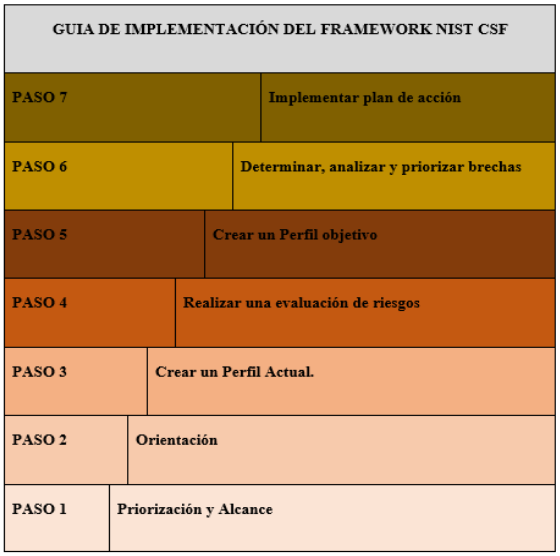
Luego, la organización determina los recursos necesarios para llenar el vacío, incluidos los recursos financieros y humanos. El uso de registros de esta manera puede ayudar a las organizaciones a tomar decisiones informadas sobre sus actividades de seguridad cibernética, ayudar a administrar el riesgo y realizar mejoras específicas y efectivas en las minas de su red.

PASO 7: Implementar plan de acción.

La organización identifica los próximos pasos para abordar las vulnerabilidades identificadas en el paso anterior y adapta las medidas de ciberseguridad actuales para cumplir con el perfil objetivo. Para brindar orientación adicional, el Marco define ejemplos de referencias de información para categorías y subcategorías, pero se alienta a las organizaciones a definir estándares, pautas y prácticas, incluidos los estándares específicos de la industria que mejor se adapten a sus necesidades.

Las organizaciones ensayan los pasos necesarios para evaluar y mejorar continuamente la ciberseguridad. Por ejemplo, las organizaciones pueden encontrar que repetir los pasos de orientación a menudo mejora la calidad de sus evaluaciones de riesgos. Además, las organizaciones pueden realizar un seguimiento del progreso actualizando repetidamente el perfil actual y comparándolo con el perfil de destino. Las organizaciones también pueden usar este proceso para alinear sus programas de seguridad cibernética al nivel deseado de implementación del marco.

Figura 5: *Guía de Implementación del Framework NIST CSF*



Fuente: Elaboración propia

2.7.9.3.3 Comunicación de requisitos de ciberseguridad a las partes interesadas.

Este marco proporciona un lenguaje común para comunicar los requisitos entre las partes interesadas interdependientes responsables de la entrega de productos y servicios de infraestructura crítica. A continuación, se muestra un ejemplo. Las organizaciones pueden usar perfiles de destino para exponer sus requisitos de gestión de riesgos de ciberseguridad a proveedores de servicios externos, como proveedores de nube a los que la organización exporta datos.

Las organizaciones pueden demostrar su estado de seguridad cibernética a través de registros actuales y comunicar los resultados y los requisitos de adquisición estándar. Después de identificar a los socios externos de los que depende su infraestructura, los propietarios u operadores de infraestructura crítica pueden usar perfiles de destino para comunicar sus categorías y listas.

Un dominio de infraestructura crítica puede establecer un perfil de destino que se puede usar entre componentes como un perfil base inicial para crear perfiles de destino personalizados. Mediante el uso de jerarquías para evaluar la infraestructura crítica y su lugar en la economía digital más amplia, las organizaciones pueden gestionar mejor los riesgos de ciberseguridad entre las partes interesadas.

La comunicación entre todas las partes de la cadena de suministro es especialmente importante. Una cadena de suministro es un conjunto complejo de recursos y procesos, distribuidos globalmente e interconectados en múltiples niveles de la organización.

La cadena de suministro comienza con la provisión de productos y servicios y se extiende a través del diseño, desarrollo, producción, procesamiento, manejo y entrega de productos y servicios al usuario final. Dadas estas relaciones complejas e interrelacionadas, la gestión de riesgos de la cadena de suministro (SCRM) es una función organizacional crítica. Cyber SCRM es el conjunto de actividades necesarias para gestionar los riesgos de ciberseguridad relacionados externamente. Específicamente, la red SCRM aborda tanto el impacto de la seguridad cibernética de la organización en las partes externas como el impacto de la seguridad cibernética de las partes externas en la organización.

Uno de los objetivos principales de la red SCRM es eliminar "los productos y servicios que contienen una funcionalidad potencialmente maliciosa, están falsificados o son susceptibles de exportación inapropiada o desarrollo de la cadena de suministro en línea". Identificar, evaluar y mitigar. (NIST 800161, 2015)

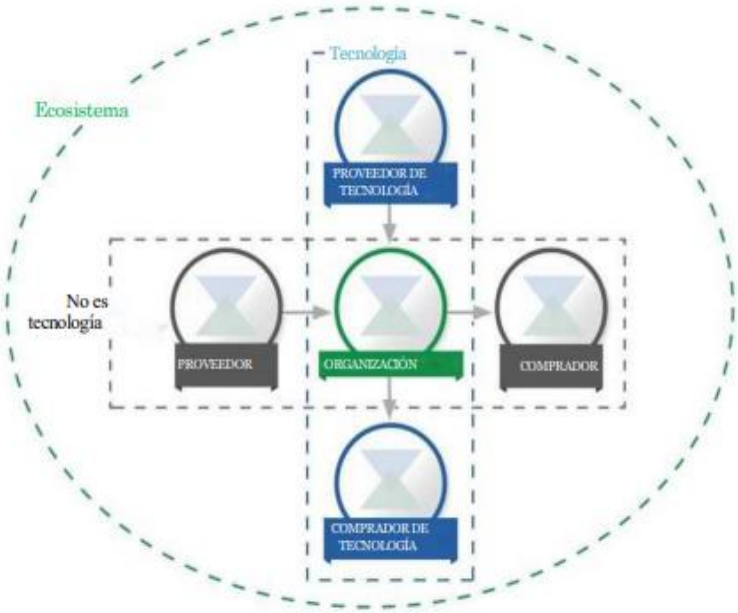
Las actividades de CyberSCRM pueden incluir lo siguiente:

1. Definir los requisitos de ciberseguridad para los proveedores.
2. Aprobar requisitos de ciberseguridad a través de un acuerdo formal (por ejemplo, contrato).
3. Informar a los proveedores cómo se verificarán y autenticar estos requisitos de ciberseguridad.

Asegúrese de que los requisitos de seguridad cibernética se cumplan a través de una variedad de métodos de evaluación.

Dirigir y gestionar las actividades anteriores. Cyber SCRM incluye proveedores y compradores de tecnología y proveedores y compradores de no tecnología, donde la tecnología incluye tecnología de información mínima (TI), sistemas industriales de sistemas de control público (ICS), sistemas físicos de red (CPS) y conectividad general que incluye Internet de Cosas (IoT).

Figura 6: Ecosistema de ciberseguridad en una organización Tecnología, proveedores y procesos.



Fuente: National Institute of Standards and Technology (NIST)

La figura Nº6, representa una organización en un momento dado. Sin embargo, en el curso normal de los negocios, la mayoría de las organizaciones serán tanto proveedoras como compradoras de otras organizaciones o usuarios finales.

La sección que se muestra en la Figura 3 muestra el ecosistema de ciberseguridad de una organización. Estas relaciones resaltan el papel fundamental que desempeñan las redes SCRM en la gestión del riesgo de ciberseguridad en la infraestructura crítica y la economía digital más amplia. Estas relaciones, los productos y servicios que ofrecen y los riesgos que plantean deben identificarse e integrarse en las capacidades de detección y protección y los protocolos de aplicación de su organización. En el diagrama anterior, "comprador" se refiere a una persona u organización que consume un producto o servicio en particular de una organización, incluidas las organizaciones comerciales y sin fines de lucro. "Proveedor" incluye proveedores de productos y

servicios (como infraestructura de TI) utilizados internamente por una organización o integrados en productos o servicios proporcionados por una organización.

Estos términos se aplican a productos y servicios tecnológicos y no tecnológicos. Ya sea que busque subcategorías principales individuales o perfiles completos, este marco brinda a las organizaciones y sus socios una forma de garantizar que los nuevos productos o servicios satisfagan sus necesidades.

.Al seleccionar resultados críticos para la seguridad que son principalmente relevantes para el contexto (p. (por ejemplo, envíos de información de identificación personal (PII), provisión de servicios críticos, servicios de verificación de datos, servicios de integridad de productos o servicios), las organizaciones pueden evaluar a los socios en función de estos criterios.

2.7.9.3.4 Identificación de oportunidades para información nueva o revisada.

Una organización que implemente una subcategoría en particular o desarrolle una nueva subcategoría puede encontrar pocas o ninguna referencia útil a actividades relacionadas. Para satisfacer esta necesidad, las organizaciones pueden trabajar con líderes tecnológicos y organismos de estándares para crear, desarrollar y coordinar estándares, pautas o prácticas. Para probar la efectividad de una inversión, una organización primero debe establecer una comprensión clara de sus objetivos, la relación entre esos objetivos y los resultados de ciberseguridad relevantes, y cómo se implementarán y gestionarán esos resultados de ciberseguridad individuales. Aunque medir todos estos puntos está más allá del alcance del marco, los hallazgos clave de seguridad cibernética del marco respaldan la autoevaluación de la inversión en seguridad cibernética y la efectividad operativa para:

Una organización que implemente una subcategoría en particular o desarrolle una nueva subcategoría puede encontrar pocas o ninguna referencia útil a actividades relacionadas. Para satisfacer esta necesidad, las organizaciones pueden trabajar con líderes tecnológicos y organismos de estándares para crear, desarrollar y coordinar estándares, pautas o prácticas.

Para probar la efectividad de una inversión, una organización primero debe tener una comprensión clara de sus objetivos, la relación entre esos objetivos y los resultados de ciberseguridad relevantes, y cómo se implementarán y gestionarán esos resultados de ciberseguridad individuales. Si bien medir todos estos puntos está más allá del alcance del marco, los hallazgos clave de seguridad cibernética del marco respaldan la autoevaluación de la inversión en seguridad cibernética y la efectividad operativa para:

La evolución de las métricas de rendimiento de la ciberseguridad está evolucionando. Las organizaciones deben ser reflexivas, creativas y vigilantes en la forma en que utilizan las métricas para optimizar su uso, pero no deben confiar en indicadores artificiales del estado actual y el progreso de los riesgos de seguridad de la red. Las evaluaciones de riesgos cibernéticos requieren disciplina y deben reevaluarse periódicamente. Siempre que se utilicen métricas como parte de un proceso marco, se alienta a las organizaciones a definir y comprender claramente por qué las métricas son importantes y cómo contribuyen a la gestión de riesgos. Riesgo general de seguridad de la red. También debemos ser claros acerca de las limitaciones de los medios que utilizamos.

Por ejemplo, el seguimiento de las medidas de seguridad y el rendimiento puede proporcionar información valiosa sobre cómo los cambios en los controles de seguridad detallados afectan el logro de los objetivos de la organización. Validar el logro de objetivos organizacionales específicos requiere el análisis de datos solo después de que se hayan alcanzado los objetivos. Este

tipo de retraso es más absoluto. Sin embargo, puede ser más útil predecir la probabilidad y el impacto de los riesgos de seguridad cibernética utilizando métricas que brindan predicciones. Se alienta a las organizaciones a innovar y personalizar la forma en que integran las métricas adoptando el marco con una comprensión completa de su utilidad y limitaciones. A continuación, se muestra una lista informativa de referencias que describen características, categorías, subcategorías y prácticas específicas de ciberseguridad comunes a todos los dominios de infraestructura crítica.

El núcleo se compone de cuatro elementos.

- Cinco (05) Funciones
- Veintitrés (23) Categorías
- Ciento ocho (108) Subcategorías
- Referencias

Figura 7: Identificación de funciones del Framework NIST CSF

Fuente: National Institute of Standards and Technology (NIST)

Figura 8: Identificación de función y categoría del Framework

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

*Fuente: National Institute of Standards and Technology (*NIST*)*

El anexo N.º 3, adjunto a este proyecto de investigación, proporciona una lista de las funciones, categorías y subcategorías principales del marco, así como también una lista de información de referencia que describe las actividades individuales de seguridad de la red para todas las áreas críticas de la infraestructura.

2.7.10 Programa Nacional de Inversiones en Salud-PRONIS

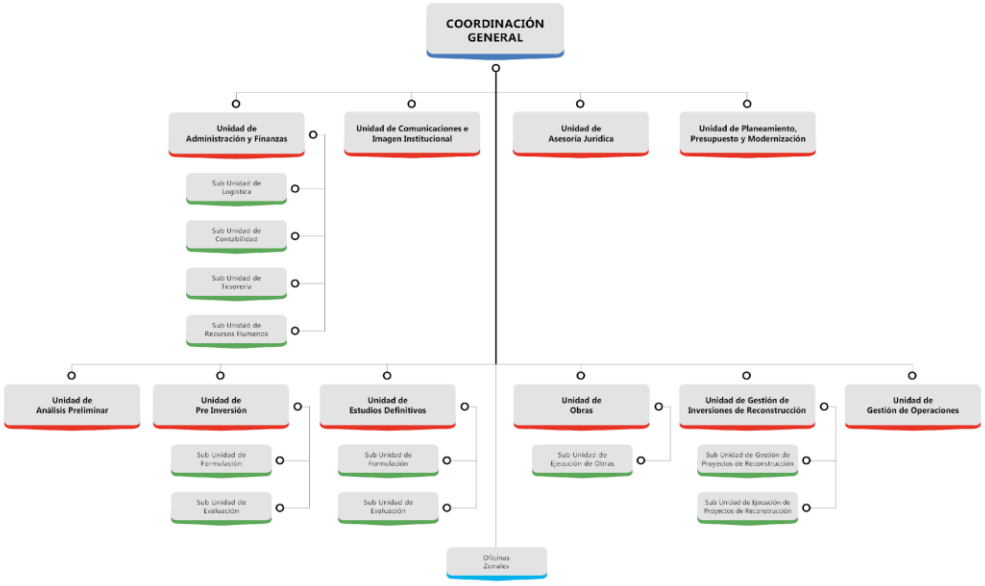
El Programa Nacional de Inversión en Salud, abreviado como PRONIS, es una organización del sector público dependiente del Ministerio de Salud (MINSA) del Perú, responsable de la concepción, desarrollo e implementación de proyectos de inversión pública en el sector salud de este país relacionados con infraestructura hospitalaria. a escala nacional.

Los proyectos se ejecutan bajo cualquier fuente de financiamiento y se coordinan con los gobiernos locales y regionales, en el marco de los convenios firmados.

2.7.10.1 Misión

Formular, evaluar e implementar proyectos de inversión en salud de todos los niveles de complejidad a nivel nacional, en el marco de los convenios suscritos. Brindar apoyo técnico a los organismos regionales, locales y del MINSA en la fase de reinversión e inversión en salud, y gestionar y monitorear el cumplimiento de sus obligaciones contractuales, proyectos de inversión en los términos de la asociación público-privada y actividades tributarias. , de acuerdo con la normativa.

Figura 9 *Organigrama del Programa Nacional de Inversiones de Salud.*



Fuente: Intranet PRONIS

2.7.10.2 Equipo de trabajo de tecnologías de la información y comunicación.

El Equipo de Tecnologías de la Información y las Comunicaciones, abreviado como ETTIC, pertenece a la Unidad Administrativo-Financiera del PRONIS, establecida mediante Resolución de Coordinación General N° N° 004-2018-PRONIS-CG , de fecha 30 de noviembre de 2018, se da aprueba la creaciòn del Departamento de Tecnologías de la Información y las Comunicaciones, creado como equipo de Trabajo, asimismo se precisa las siguientes responsabilidades:

a) Administrar recursos de hardware y software, así como programas de telecomunicaciones.

b) Elaboración e implementación de un plan de Gobierno Digital y demás herramientas técnicas normativas relacionadas con las tecnologías de la información, en el marco de la normatividad vigente.

c) Proponer planes, proyectos y procedimientos para los escenarios de seguridad, mantenimiento y contingencia de los servicios de información y comunicaciones, en el marco de la normatividad aplicable.

d) Implementar, mantener y actualizar los sistemas informáticos y/o aplicaciones desarrolladas para realizar las funciones y operaciones del Programa.

e) Ejecutar, monitorear y calibrar el florecimiento de proyectos de implementación de soluciones de Tecnologías de la Información (TI) en protección a las áreas usuarias de la entidad.

f) Brindar anaquel técnico, sostenimiento preventivo y correctivo, respecto de los posibles equipos de hardware y sistemas que utiliza el Programa.

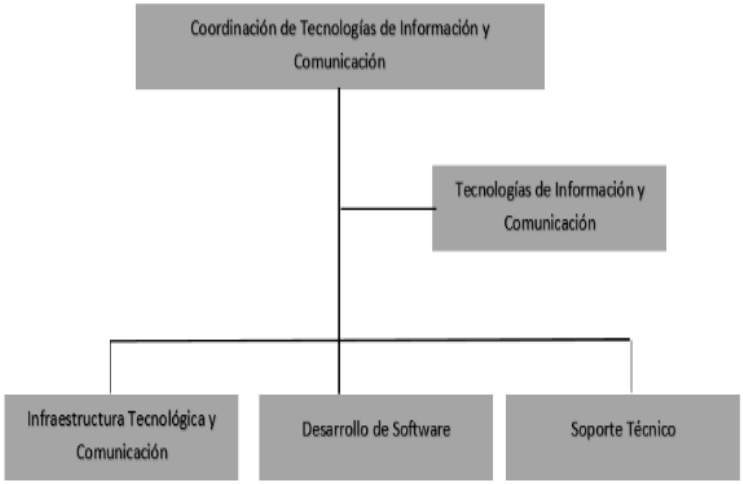
g) Emitir crítica técnica en asuntos de su competencia, sometidos a su instrucción y resolver las consultas que se formulen al respecto.

h) Velar por la integridad, disponibilidad y resguardo de la Base de Datos del Programa; gestionar las redes de datos y comunicaciones locales y remotas del Programa.

i) Establecer protocolos de seguridad y tramitar en coordinación con las unidades usuarias la habilitación, creación y baja de los operadores autorizados de los sistemas informáticos y tecnológicos.

j) Registrar de manera oportuna y consistente los datos e información en los aplicativos informáticos institucionales y nacionales de su competencia.

Figura 10 *Estructura del ETTIC*



Fuente: Elaboración propia

CAPÍTULO IV

DISEÑO METODOLÓGICO

2.8 Población y Muestra

Según Hernández, Fernández y Baptista indican que, una población es la suma total del fenómeno estudiado cuyas unidades tienen características comunes, son estudiadas y dan lugar a los datos de investigación.

La muestra es una parte o subconjunto de un conjunto, generalmente elegido de tal manera que revele sus propiedades. Su característica más importante es la representatividad, es decir, es una parte típica de la población en términos de características o características relevantes para la encuesta. (Hernandez Sampieri, Fernandez Collado, & Baptista , 2010)

2.9 Población:

Para el caso de este proyecto, se tomará en cuenta al personal que trabaja en el Programa Nacional de Inversiones en Salud, los mismos que pertenecen a diferentes unidades del Ponis.

2.10 Muestra:

Para el presente proyecto se tomará como muestra al personal del Equipo de Trabajo de Tecnologías de la Información y Comunicación dado que el proceso seleccionado corresponde a Tecnologías de la Información explicado más adelante en el desarrollo de la propuesta.

2.10.1 Determinación de la Muestra

Para determinar la muestra se tuvo en cuenta el alcance del presente proyecto, dado que está acotado al proceso de Tecnologías de la Información y Comunicación, y este proceso está a cargo del Equipo de Trabajo de Tecnologías de la Información y Comunicación.

2.10.2 Métodos y Procedimientos para la recolección de Datos.

Como principal método que se empleará en la presente investigación, se considera la

encuesta, la cual permitirá recabar la información necesaria sobre la percepción en relación a la ciberseguridad en el Programa Nacional de Inversiones en Salud.

Para la presente investigación, se ha empleado el cuestionario y checklist que se realizó al personal del Equipo de Trabajo de Tecnologías de la Información y Comunicación del Programa Nacional de Inversiones en Salud, que ha sido desarrollado de acuerdo a la investigación teórica propuesta.

2.10.2.1 Tipo de encuesta

Para la presente investigación, se utilizará la encuesta individual, se utilizará sobre la base de un cuestionario cerrado y preguntas con escala de intervalo (Kendall y Kendall, 1997), aplicados a una muestra definida.

CAPÍTULO V

DESARROLLO DE LA PROPUESTA

Para el desarrollo de la propuesta de la presente investigación, se hará uso del Marco y/o Programa de Ciberseguridad NIST CSF.

Los siguientes pasos de la figura 9, ilustra cómo una organización podría utilizar el Marco de Ciber Seguridad NIST, para crear un nuevo programa de ciberseguridad o mejorar uno existente. Estos pasos deben repetirse según sea necesario para mejorar continuamente la seguridad de la red.

Figura 11: Pasos de utilización del Marco NIST CSF

Fuente: Control-IT, septiembre del 2019

A Fin de cumplir con el objetivo planteado en la propuesta “Determinar los controles necesarios mediante el Diagnóstico Integral de ciberseguridad basado en estándares internacionales de seguridad de NIST CSF para la mitigar los riesgos de ciberseguridad en el Programa Nacional de Inversiones en Salud”, se menciona a continuación los puntos desarrollados:

2.11 PRIORIZACIÒN Y ALCANCE:

En este punto se identificará los objetivos y prioridades organizacionales, para tomar decisiones estratégicas con respecto a las implementaciones de ciberseguridad; se determinará el alcance que implica seleccionar un proceso; se identificarán los activos de información que respaldan el flujo de proceso seleccionado y se adaptará el núcleo del marco de ciberseguridad NIST CSF.

2.11.1 Misión y visión del Programa Nacional de Inversiones en Salud

2.11.1.1 Misión y Visión

Formular, evaluar e implementar proyectos de inversión en salud de todos los niveles de complejidad a nivel nacional, en el marco de los convenios suscritos.

Brindar apoyo técnico a los gobiernos regionales y locales y organismos del Minsa durante la fase de preinversión e inversión en salud, y gestionar y monitorear el cumplimiento de las obligaciones contractuales de los proyectos de inversión en la modalidad de asociación público-privada y obra por impuesto.

Su visión es contribuir a ejecutar los proyectos de inversión en Salud para mejorar la calidad de vida de todos los peruanos.

2.11.1.2 Alcance

Se establece el alcance que está acotado al proceso de Tecnologías de la Información (Activos de información)

Las Tecnologías de la Información, está a cargo del Equipo de Trabajo de Tecnologías de la Información y Comunicación de la Unidad de Administración y finanzas.

2.11.2 Inventario de activos de información.

A continuación, se presenta el inventario de activos de información críticos, los cuales fueron preferidos en relación al proceso seleccionado (Tecnologías de la Información) y obtenidos en la encuesta realizada con el coordinador del Equipo de trabajo de Tecnologías de la Información y Comunicación, basado en el análisis de las actividades cotidianas y activos sensibles que administra y se usa en el Programa Nacional de Inversiones en Salud para lograr los objetivos institucionales.

2.11.2.1 Activos Informáticos

- Equipos de comunicaciones (switch, router)
- Equipos Servidores.

2.11.2.2 Activos de Información

- Topología de red.
- Internet.
- Sistema SIA.
- Bases de Datos.

2.11.3 Listado de subcategorías del núcleo del marco aplicables al alcance.

En este punto, los miembros del Grupo de Trabajo de NIST CSF sobre Tecnologías de la Información y la Comunicación desarrollaron una línea de base del Marco de Ciberseguridad de NIST CSF a través de una serie de actividades de ciberseguridad que incluyeron todas las infraestructuras y sectores críticos identificados. Para el desarrollo de la propuesta se consideraron las características y elementos que se describen a continuación en la Figura 12.

Figura 12: Puntos considerados para la implementación del Núcleo del Marco NIST CSF

FUNCIÓN	CATEGORÍA
IDENTIFICAR(ID)	
	ID.GV Gobernanza
	ID.AM Gestión de Activos
	ID.RA Evaluación de riesgos
PROTEGER (PR)	PR.AC Gestión de identidad, autenticación y control de acceso.
	PR.DS Seguridad de datos.
DETECTAR(DE)	DE.CM Monitoreo Continuo de la seguridad
RESPONDER(RS)	RS.RP Planificación de la respuesta
RECUPERAR(RC)	RC.RP Planificación de la recuperación

Fuente: Elaboración Propia

Las subcategorías del núcleo del Marco de Ciberseguridad NIST CSF, fueron seleccionadas según la información y análisis brindada por el Coordinador de Tecnologías de la Información y Comunicación del proceso de Tecnologías de la Información como se detalla en la figura 13.

Figura 13: Selección de Categorías del Núcleo del Marco de Ciberseguridad NIST CSF

ANÁLISIS DEL COORDINADOR DE ETTIC	FUNCIÓN	CATEGORÍA	SUBCATEGORÍA
Revisar el inventario de software y hardware del Equipo de Trabajo de Tecnologías de la Información y Comunicación se alinea con la gestión del riesgo de ciberseguridad.	IDENTIFICAR (ID)	ID.AM Gestión de Activos	ID.AM-1 Los dispositivos y sistemas físicos dentro del la Organización están inventariados.
			ID.AM-2 Las Plataformas de software y aplicaciones dentro de la organización están inventariadas
La identificación, a través de la coordinación con las áreas internas, sobre el cumplimiento regulatorio.		ID.GV Gobernanza	ID.GV-1 Se establece y se comunica la política de seguridad cibernética Organizacional.
La organización comprende los riesgos de seguridad cibernética para sus operaciones (incluida su misión, función, imagen o reputación), activos y personas		ID.RA Evaluación de riesgos	ID.RA-1 Se identifican y documentan las vulnerabilidades de los activos
El acceso a los activos físicos y lógicos y las instalaciones relacionadas está restringido a usuarios, procesos y dispositivos autorizados, y se administra de manera consistente con el riesgo evaluado de acceso no autorizado a actividades y transacciones autorizadas.	PROTEGER (PR)	PR.AC Gestión de identidad, autenticación y control de acceso.	PR.AC-2 Se gestiona y se protege el acceso físico a los activos.
La segregación de la Infraestructura tecnológica de soporte al desarrollo y operación.		PR.DS Seguridad de datos.	PR.DS-7 Los entornos de desarrollo y pruebas están separados del entorno de producción.
El monitoreo y detección de código malicioso que pueda ser inyectado por un atacante.	DETECTAR (DE)	DE.CM Monitoreo Continuo de la seguridad	DE.CM-4 Se detecta el código malicioso
La inclusión de las acciones necesarias en el Plan de respuestas a incidentes de ciberseguridad.	RESPONDER (RS)	RS.RP Planificación de la respuesta	RS.RP-1 El plan de respuesta se ejecuta durante o después de un incidente.
La inclusión de las acciones necesarias en el Plan de recuperación a incidentes de ciberseguridad	RECUPERAR (RC)	RC.RP Planificación de la recuperación	RC.RP-1 El plan de recuperación se ejecuta durante o después de un incidente.

Fuente: Elaboración propia

2.12 ORIENTACIÒN

Determinado el alcance, en este punto se define un enfoque de riesgo basado en las amenazas y vulnerabilidades aplicables a los activos informáticos relacionados, realizaremos las siguientes acciones:

- Identificación del enfoque y requisito regulatorio relacionados a la seguridad.
- Inventario de amenazas y vulnerabilidades aplicables a los activos informáticos.

En cumplimiento de los requisitos regulatorios se cita a la Norma Técnica Peruana NTP-ISO 17799-2007, ISO NTP/IEC 27001:2014 y Política Nacional de Ciberseguridad.

- NTP-ISO 17799-2007 Norma que fue aprobada mediante Resolución Ministerial N° 246-2007-PCM. EDI. Tecnologías de la información. concebido como una guía práctica para la gestión de la seguridad de la Tecnologías de la Información, nos sirve como una guía práctica para desarrollar los estándares organizacionales de Seguridad Informática.
- ISO NTP/IEC 27001:2014: : Norma aprobada bajo la Resolución Ministerial N° 002016 Tecnologías de la Información PCM. Técnicas de seguridad. Un sistema de gestión de seguridad de la información, que ayude a generar confianza en el proceso nacional de normalización de la competitividad y el uso de buenas prácticas internacionales en seguridad de la información.

Según las encuestas realizadas a los involucrados del proceso es decir al personal de ETTIC, se obtuvo el cuadro de vulnerabilidades y amenazas de cada activo de información. Considerando que una vulnerabilidad es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, mientras que una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

A continuación, se detalla el cuadro de Vulnerabilidades y Amenazas de cada activo crítico del Programa Nacional de Inversiones en Salud.

Tabla 3: *Identificación de Vulnerabilidades y Amenazas del PRONIS.*

ACTIVO	ID	VULNERAVILIDAD	ID	AMENAZA
Equipo de Comunicación y Topología de red	V1	Ausencia de copias de seguridad oportunas del router core	A1	Incumplimiento en la generación de copias de Seguridad del equipo router core.
	V2	Carencia de seguridad física (sin vigilantes, sin llaves, número de identificación)	A2	Accesos no autorizados
	V3	Inadecuada seguridad del cableado.	A3	Intromisión por parte de elementos inoportunos a la red de datos interna de la institución
	V4	Fallas de equipos de Telecomunicaciones y servidores.	A4	Falta de mantenimiento
	V5	Contraseñas predeterminadas no modificadas.	A5	Interceptación, escucha o alteración del tráfico de red.
	V6	Punto único de fallas y red plana	A6	Incumplimiento de enlaces redundantes
	V7	Fuga de Información	A7	Falta de control y monitoreo a la información
	V8	Falta de distribución de permisos de internet	A8	No asignación de permisos en la red hacia internet
Equipos Servidores	V9	Permisos no mapeados	A9	Protección débil desde el punto de vista de confidencialidad en los servidores
	V10	carencia de procedimientos o plan de continuidad que cubran a la información y activos de información.	A10	Falla de operaciones ejecutadas mediante Outsourcing
	V11	Procedimientos no documentados de la administración de equipos servidores	A11	Pérdida o ausencia de personal clave
internet	V12	Ausencia de mecanismos de monitoreo de niveles de acceso a internet	A12	Accesos innecesarios a usuarios para navegación a internet.
	V13	Descarga y uso no controlado desde internet	A13	Ataque por virus, malware y gusanos
	V14	Limitar accesos en puertos de servidores publicados	A14	Ataque de denegación de servicio (DoS / DDoS).
	V15	Falta de sensibilización en temas de Seguridad Informática	A15	Falta de controles, procedimientos y/o directivas.
Sistema SIA	V16	Segregación inadecuada o insuficiente de ambientes de producción y de pruebas.	A16	Incumplimiento de relaciones contractuales
	V17	Mal uso del SIA en la gestión y carga de documentos	A17	Uso indebido de los sistemas de información.
	V18	Falta de identificación del usuario y mecanismo de autenticación.	A18	Manejo de información sensible por usuario no autorizado.

Base de Datos	V19	Inadecuada gestión de capacidad del sistema.	A19	Falsificación de registros.

Fuente: Elaboración propia

2.13 IDENTIFICACIÓN DEL PERFIL ACTUAL

En este punto se busca desarrollar el perfil actual basado en la situación actual del PRONIS, según el alcance planteado, es decir, lo que actualmente existe en la institución en relación a la gestión de riesgos en la organización del proceso informático. mediante el documento de trabajo que funciona con la identificación actual de registros (AS-IS) de la organización.

Para este punto, se hará uso de los perfiles que se explican en el Programa de Ciberseguridad de NIST CSF de la tabla 2.

Siendo que el proceso de Tecnologías de la Información, según la identificación del perfil actual (AS-IS) del PRONIS, en su mayoría se encuentra en el Nivel 1, como se muestra en el punto 5.3.1 a continuación.

2.13.1 Papel de trabajo con la identificación del perfil actual (AS-IS) del PRONIS.

A continuación, se muestra el papel de trabajo desarrollado según las Funciones, categorías y sub categorías del núcleo del marco. Cada papel de trabajo tiene su nivel de implementación (AS-IS) es decir tal como está el PRONIS en estos Momentos.

Figura 14: ID.AM Gestión de Activos-Subcategoría 1

ID.AM Gestión de Activos

Los datos, las personas, los equipos, los sistemas y las instalaciones que permites a la organización alcanzar sus objetivos definidos y gestionados son coherentes con su materialidad para los objetivos y estrategia de riesgo de la información.

Función	ID	Categoría
IDENTIFICAR (ID)	ID.AM	Gestión de activos
	ID.BE	Ambiente de negocios
	ID.GV	Gobierno
	ID.RA	Evaluación de riesgos
	ID.RM	Estrategia de gestión de Riesgos
	ID.SC	Gestión de riesgos de la cadena de suministros

ID. GV	Subcategorías
1	Se inventarían los dispositivos físicos y los sistemas de la organización.
2	Se inventarían las plataformas y aplicaciones de software en la organización.
3	Comunicación organizacional y flujos de datos mapeados.
4	Sistemas de información mapeados y flujos de datos
5	Los recursos (p. ej., hardware, equipo, datos, tiempo, personal y software) se priorizan en función de su clasificación, importancia y valor comercial
6	Roles y responsabilidades responsabilidad en materia de ciberseguridad para toda la fuerza y terceros interesados.

Niveles de Implementación			
(1) Parcial	(2) Riesgo Informático	(3) Repetible	(4) Adaptativo
Durante esta sesión, el equipo de Trabajo de Tecnologías de la Información y Comunicación, el equipo de soporte, equipo de Infraestructura Tecnológica y el equipo de desarrollo, han presentado herramientas que permite llevar el control de dispositivos en la institución.			

Perfil Actual

Fuente: Elaboración pronta

Figura 15: ID.AM Gestión de Activos-Subcategoría 2

ID.AM Gestión de Activos

Los datos, las personas, los equipos, los sistemas y las instalaciones que permiten a la organización alcanzar sus objetivos definidos y gestionados son coherentes con su materialidad para los objetivos y la estrategia de riesgo de la organización.

Función	ID	Categoría	#Sub cat.
IDENTIFICAR (ID)	ID.AM	Gestión de activos	6
	ID.BE	Ambiente de negocios	5
	ID. GV	Gobierno	4
	ID.RA	Evaluación de riesgos	6
	ID.RM	Estrategia de gestión de Riesgos	3
	ID.SC	Gestión de riesgos de la cadena de suministros	5

ID. GV	Subcategorías
1	Se inventarían los dispositivos físicos y los sistemas de la organización.
2	Se inventarían las plataformas y aplicaciones de software en la organización.
3	Comunicación organizacional y flujos de datos mapeados.
4	Sistemas de información mapeados y flujos de datos
5	Los recursos (p. ej., hardware, equipo, datos, tiempo, personal y software) se priorizan en función de su clasificación, importancia y valor comercial
6	Roles y responsabilidades responsabilidad en materia de ciberseguridad para toda la fuerza y terceros interesados.

Niveles de Implementación			
(1) Parcial	(2) Riesgo Informático	(3) Repetible	(4) Adaptativo
Durante esta sesión, el equipo de Trabajo de Tecnologías de la Información y Comunicación, el equipo de soporte, equipo de Infraestructura Tecnológica y el equipo de desarrollo, han presentado información sobre el software y aplicaciones organizadas mediante hojas de cálculo.			

Perfil Actual

Fuente: Elaboración propia

Figura 16: ID. GV GOBIERNO- Subcategoría 1

ID. GV GOBIERNO

Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización comprenden y se informan a la gestión del riesgo de seguridad Cibernética

Función	ID	Categoría	#Sub cat.
IDENTIFICAR (ID)	ID.AM	Gestión de activos	6
	ID.BE	Ambiente de negocios	5
	ID.GV	Gobierno	4
	ID.RA	Evaluación de riesgos	6
	ID.RM	Estrategia de gestión de Riesgos	3
	ID.SC	Gestión de riesgos de la cadena de suministros	5

ID.GV	Subcategorías
1	Se establece y comunica la política de seguridad cibernética organizacional
2	Las funciones y responsabilidades de ciberseguridad están coordinadas y alineadas con las funciones internas y con los socios externos.
3	Los requisitos legales y reglamentarios relacionados con la ciberseguridad, incluidas las obligaciones de privacidad y libertades civiles, se comprenden y gestionan.
4	Los procesos de gobierno y gestión de riesgos abordan los riesgos de ciberseguridad.

Niveles de Implementación			
(1) Parcial	(2) Riesgo Informático	(3) Repetible	(4) Adaptativo
No hay política de seguridad organizacional que pueda ser aplicada y ayude a sensibilizar los riesgos cibernéticos a los usuarios del PRONIS.			

Perfil Actual

Fuente: Elaboración propia

Figura 17: ID.RA EVALUACION DE RIESGO-subcategoría 1

ID.RA EVALUACION DE RIESGO

La organización comprende los riesgos de ciberseguridad para las operaciones de la organización (incluida la misión, funciones, imagen o reputación), los activos de la organización y las personas.

Función	ID	Categoría	#Sub cat.
IDENTIFICAR (ID)	ID.AM	Gestión de activos	6
	ID.BE	Ambiente de negocios	5
	ID.GV	Gobierno	4
	ID.RA	Evaluación de riesgos	6
	ID.RM	Estrategia de gestión de Riesgos	3
	ID.SC	Gestión de riesgos de la cadena de suministros	5

ID. GV	Subcategorías
1	Las vulnerabilidades de los activos se identifican y documentan
2	La ciberinteligencia se obtiene de foros y fuentes de intercambio de información.
3	Las amenazas, tanto internas como externas, se identifican y registran.
4	Impactos comerciales probables y probables identificados.
5	Las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para identificar los riesgos.
6	Respuestas al riesgo identificadas y priorizadas.

Niveles de Implementación			
(1) Parcial	(2) Riesgo Informático	(3) Repetible	(4) Adaptativo
No se aplica un marco de gestión de riesgos que aborde objetivos de cumplimiento regulatorio o normativo con respecto a tecnología, seguridad de la información, No existe registro de vulnerabilidades			

Perfil Actual

Fuente: elaboración propia

Figura 18: PR.DS SEGURIDAD DE DATOS- subcategoría 2

PR.DS SEGURIDAD DE DATOS
La información y los registros (datos) se gestionan de acuerdo con la política de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.

Función	ID	Categoría	#Sub cat.
IDENTIFICAR (ID)	PR.AC	Gestión de identidad y control de accesos	7
	PR.AT	concientización y Entrenamiento	5
	PR.DS	Seguridad de Datos	8
	PR. IP	Procesos y procedimientos de protección de la información y seguridad de los datos	12
	PR.MA	Mantenimiento	2
	PR.PT	Tecnología Protectora	5

ID. GV	Subcategorías
1	Las identidades y las credenciales se emiten, administran, verifican, revocan y auditan para dispositivos, usuarios y procesos autorizados.
2	Se gestiona y protege el acceso físico a los activos.
3	Se gestiona el acceso remoto.
4	Los derechos de acceso y la descentralización se gestionan combinando los principios de privilegio mínimo y separación de funciones.
5	La integridad de la red está protegida (por ejemplo, segregación de red, segmentación de red)
6	La identidad se verifica, reconoce y confirma en las interacciones.
7	Los usuarios, dispositivos y otros activos se autentican (p. ej., factor único y factor múltiple) en función de los riesgos de la transacción (p. ej., riesgos de seguridad y privacidad personal y otros riesgos).

Niveles de Implementación			
(1) Parcial	(2) Riesgo Informático	(3) Repetible	(4) Adaptativo
No se aplica un marco de gestión de riesgos que aborde objetivos de cumplimiento regulatorio o normativo con respecto a tecnología, seguridad de la información,			

Perfil Actual

Fuente: elaboración propia

Figura 19: PR.DS SEGURIDAD DE DATOS- subcategoría 1

PR.DS SEGURIDAD DE DATOS

La información y los registros (datos) se gestionan de acuerdo con la política de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.

Función	ID	Categoría	#Sub cat.
IDENTIFICAR (ID)	PR.AC	Gestión de identidad y control de accesos	7
	PR.AT	concientización y Entrenamiento	5
	PR.DS	Seguridad de Datos	8
	PR. IP	Procesos y procedimientos de protección de la información y seguridad de los datos	12
	PR.MA	Mantenimiento	2
	PR.PT	Tecnología Protectora	5

ID. GV	Subcategorías
1	Datos en reposo protegidos
2	Datos en tránsito protegidos
3	Los activos se gestionan oficialmente durante su eliminación, transferencia y eliminación.
4	Se mantiene una capacidad adecuada para garantizar la disponibilidad.
5	Se implementan protección
6	El mecanismo de compromiso de integridad se implementa para verificar la integridad del software, el firmware y los datos.
7	Los entornos de desarrollo y prueba están separados del entorno de producción.
8	El mecanismo de integridad de confirmación se utiliza para verificar la integridad del hardware.

Niveles de Implementación			
(1) Parcial	(2) Riesgo Informático	(3) Repetible	(4) Adaptativo
El marco de gestión de riesgos no está establecido para cumplir con los objetivos de cumplimiento regulatorio o regulatorio relacionados con la tecnología o la seguridad de la información.			

Perfil Actual

Fuente: elaboración propia

2.14 EVALUACIÓN DE LOS RIESGOS.

Toda organización está sujeta a riesgos; porque no hay un ambiente 100% seguro, el riesgo es constante. Por ello, toda organización debe estar atenta a cualquier cambio o situación extraña que crea que pueda afectar negativamente a un activo, a un área o toda su organización (Lucero Gómez & Valverde Padilla, 2012)

En esta etapa, el objetivo es evaluar los riesgos asociados a los sistemas de información y/o activos periféricos, también se analizará el entorno operativo para analizar la probabilidad de un evento de ciberseguridad y el impacto que el evento pueda tener en la organización.

Al haber identificado las amenazas y vulnerabilidades se procederá a definir los riegos basado en lo siguiente:

RIESGO = Amenaza + Vulnerabilidad. Es decir, el riesgo es el resultado de la identificación de una amenaza y Vulnerabilidad.

Para este paso se hará uso del inventario de activos de información, el catálogo de vulnerabilidades y amenazas.

Tabla 4: *Identificación del riesgo.*

ACTIVO	ID	VULNERAVILIDAD	ID	AMENAZA	RIESGO
Equipo de Comunicación y Topología de red	V1	Ausencia de copias de seguridad oportunas del router core	A1	Incumplimiento en la generación de copias de Seguridad del equipo router core.	Pérdida de la configuración de los equipos de Core
	V2	Carencia de seguridad física (sin vigilantes, sin llaves, número de identificación)	A2	Accesos no autorizados	Malversación de equipos físicos y acceso indebido a instalaciones del

					centro de gabinetes
	V3	Inadecuada seguridad del cableado.	A3	Intromisión por parte de elementos inoportunos a la red de datos interna de la institución	Pérdida de paquetes de red.
	V4	Fallas de equipos de Telecomunicaciones y servidores.	A4	Falta de mantenimiento	Fallas en el levantamiento de hardware por fallas técnicas.
	V5	Contraseñas predeterminadas no modificadas.	A5	Interceptación, escucha o alteración del tráfico de red.	Manipulación y uso malintencionado de los equipos de comunicación.
	V6	Punto único de fallas y red plana	A6	Incumplimiento de enlaces redundantes	inoperatividad de la red
	V7	Fuga de Información	A7	Falta de control y monitoreo a la información	Compartimiento con terceros a datos sensibles o privados
	V8	Falta de distribución de permisos de internet	A8	No asignación de permisos de red hacia internet	Inestabilidad de conexión de red hacia internet
Equipos Servidores	V9	Permisos no mapeados	A9	Protección débil desde el punto de vista de confidencialidad en los servidores	Abuso en el acceso a recursos compartidos dentro de la institución, Exfiltración de información crítica y/o Sensible.
	V10	carencia de procedimientos o plan de continuidad que cubran a la información y activos de información.	A10	Falla de operaciones ejecutadas mediante Outsourcing	Inoperatividad de servicios Outsourcing
	V11	Procedimientos no documentados de la administración de equipos servidores	A11	Pérdida o ausencia de personal clave	Procedimientos no documentados de la

					administración de equipos servidores
internet	V12	Ausencia de mecanismos de monitoreo de niveles de acceso a internet	A12	Accesos innecesarios a usuarios para navegación a internet.	Abuso de accesos de navegación hacia internet.
	V13	Descarga y uso no controlado desde internet	A13	Ataque por virus, malware y gusanos	Ataque por virus, malware y gusanos debido a la descarga y uso descontrolado desde internet
	V14	Limitar accesos en puertos de servidores publicados	A14	Ataque de denegación de servicio (DoS / DDoS).	Inoperatividad de los sistemas publicados del PRONIS por ataque de fuerza bruta.
	V15	Falta de sensibilización en temas de Seguridad Informática	A15	Falta de controles, procedimientos y/o directivas.	Acceso indebido a equipos de cómputo por usuarios con malas intenciones.
Sistema SIA	V16	Segregación inadecuada o insuficiente de ambientes de producción y de pruebas.	A16	Incumplimiento de relaciones contractuales	Robo de Información Interna.
	V17	Mal uso del SIA en la gestión y carga de documentos	A17	Uso indebido de los sistemas de información.	Uso de claves genéricas y acceso indebido de usuarios en los perfiles de otros usuarios
	V18	Ausencia de mecanismos de identificación y autenticación de usuario	A18	Manejo de información sensible por usuario no autorizado.	Robo de Información por ausencia de mecanismos de identificación y autenticación

Base de Datos	V19	Inadecuada gestión de capacidad del sistema.	A19	Falsificación de registros.	No confidencialidad de la Información de la base de datos

Fuente: Elaboración propia

2.14.1 Evaluación del riesgo

Esta se hace de manera cualitativa creando una comparación en la que se analiza la probabilidad de ocurrencia de un riesgo en relación a su impacto, obtenida al final de la matriz denominada "Matriz de Calificación, Evaluación y respuesta a los Riesgos", con la cual la guía describe cómo identificar los riesgos con niveles preestablecidos de impacto y probabilidad, y las áreas de riesgo presentan las posibles medidas de tratamiento que pueden conducir a este riesgo, como se muestra en la siguiente imagen:

Figura 20: Matriz de calificación, evaluación y respuesta a los riesgos

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía de Riesgos DAFP

Al visualizar los riesgos existentes y potenciales, puede evaluar su impacto e identificar los riesgos de mayor prioridad y poder ser tratados.

2.14.1.1 Análisis preliminar

A partir de un análisis probabilístico del riesgo y sus consecuencias o impactos, se pretende determinar la zona de riesgo inicial (RIESGO INHERENTE) de los riesgos identificados en el Programa Nacional de Inversión en Salud.

El riesgo inherente es el riesgo que existe en ausencia de cualquier acción que la gerencia pueda tomar para modificar la probabilidad o el impacto del riesgo.

RIESGO INHERENTE = PROBABILIDAD inh * IMPACTO inh

Impacto Inh: el impacto de un evento, excluyendo las medidas de mitigación y control.

Probabilidad Inh: La probabilidad de que ocurra un evento adverso sin tener en cuenta las medidas de mitigación y control.

Se trata de determinar la gravedad mediante una combinación de probabilidad e impacto. En la matriz de calor se definen se definen 4 zonas de severidad, zona baja, zona moderada, zona alta y zona Extrema.

2.14.1.2 Criterios de probabilidad e Impacto

La probabilidad se puede expresar como un porcentaje, número o frecuencia de ocurrencia e impacto en términos de costo, codificado por colores por categorías, impacto en el logro de objetivos, impacto en la calidad de un producto o servicio, impacto en los resultados operativos, dañar la imagen de marca o cualquier otro factor importante para la organización.

Como criterio para medir la probabilidad e impacto en el presente proyecto, se consideró medir mediante clasificación numérica y por colores según categorías clasificadas realizadas mediante preguntas abiertas realizadas al personal del Equipo de Trabajo de Tecnologías e Información involucrado, tomando en cuenta los siguientes conceptos:

2.14.1.2.1 Impacto

Insignificante: el riesgo no genera consecuencias negativas reales ni representa una amenaza significativa para la organización o sus objetivos específicos.

Menor: el riesgo tiene poco potencial de consecuencias negativas, pero no afectará significativamente el éxito general.

Moderado: es probable que el riesgo tenga consecuencias negativas, lo que representa una amenaza moderada para la organización y sus objetivos específicos de la organización.

Crítico: Riesgo de consecuencias negativas significativas que tendrán un impacto material en el éxito de la organización o sus objetivos específicos.

Catastrófico: El riesgo de consecuencias negativas graves que podrían llevar al fracaso de toda la organización o afectar gravemente las operaciones diarias. Estos son los riesgos de mayor prioridad que deben abordarse.

2.14.1.2.2 Probabilidad

Raro. El riesgo es extremadamente raro, con una probabilidad de ocurrencia cercana a cero.

Improbable: Riesgos que son relativamente raro, pero poco probable.

Posible: riesgo más típico, con una probabilidad de 50/50 de que suceda.

Probable: Es muy probable que suceda algo.

Casi seguro: Los riesgos que seguramente ocurrirán deben abordarse de inmediato.

Una vez identificados los riesgos inherentes del Programa Nacional de Inversiones en Salud, se deben identificar los controles de mitigación y de ahí resulta el riesgo residual como consecuencia.

El riesgo residual es el riesgo que existe después de la respuesta de gestión de riesgos.

2.15 IDENTIFICACIÓN DE CONTROLES

La evaluación de riesgos se aplica primero al riesgo inherente. Una vez que se han desarrollado respuestas al riesgo inherente a través de un control, este se considera riesgo residual.

En esta etapa se busca tener en cuenta la valoración realizada en el cuadro anterior, para así para seleccionar controles que permitan disminuir los valores de riesgo, encontrando así un nivel de riesgo aceptable en cada proceso de seguridad. problema.

2.15.1 Valoración de controles:

Conceptualmente, el control se define como una medida para reducir o minimizar el riesgo. Para la evaluación de los controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo mediante entrevistas con los responsables e involucrados de procesos seleccionador. En este caso sí aplica el criterio experto.
- Los responsables de establecer y monitorear las medidas de control son los que impulsan el proceso con el apoyo de su grupo de trabajo.

La clave es que las organizaciones determinen el nivel deseado de desempeño del control (no todos los controles deben estar en el nivel más alto), asegurando que el nivel elegido cumpla al menos con los objetivos de la organización y reduzca los riesgos de ciberseguridad a un nivel aceptable y rentable de implementar.

En esta etapa se busca que el control definido sea aplicado más adelante por los responsables de los activos a fin de convertir el riesgo inherente a un riesgo residual aceptable. En base a los datos obtenidos, se determinará un control de riesgo para cada Item (ID RIESGO), este control de riesgo va a ser el inicio para mitigar e implementar y controlar los riesgos más impactantes o categorizados como un nivel de alto impacto, es decir a los que están sobre la zona de riesgo moderado. Los riesgos de menor impacto no serán analizados, porque su control puede ser innecesario realizarlo.

Tabla 5: *Análisis del Riesgo*

ANALISIS DEL RIESGO				
RIESGO	ID RIESGO	EVALUACIÒN	Medidas de Respuesta	CONTROL
		Zona de Riesgo		

Pérdida de la configuración de los equipos de Core	R1	Moderada	Asumir o reducir el Riesgo	Actualización frecuente de respaldos
Malversación de equipos físicos y acceso indebido a instalaciones del centro de gabinetes	R2	Alta	Reducir el riesgo, evitar, compartir o transferir.	Implementar medidas de acceso físico y lógico como lector de huella biométrico, huella o lector facial.
Pérdida de paquetes de red.	R3	Extrema	Reducir el riesgo, evitar, compartir o transferir.	Implementar cableado estructurado en las estaciones finales.
Fallas en el levantamiento de hardware por fallas técnicas.	R4	Moderada	Asumir o reducir el Riesgo	Realizar mantenimiento preventivo y correctivo por lo menos de vez al año de los equipos de comunicación.
Manipulación y uso malintencionado de los equipos de comunicación.	R5	Alta	Reducir el riesgo, evitar, compartir o transferir.	Mejorar los niveles de seguridad a las instalaciones y equipos de comunicaciones a través de políticas y/o directivas
inoperatividad de la red	R6	Alta	Reducir el riesgo, evitar, compartir o transferir.	Segmentar la red del PRONIS
Compartimiento con terceros a datos sensibles o privados	R7	Extrema	Reducir el riesgo, evitar, compartir o transferir.	Implementar herramienta DLP y directiva de niveles de acceso y uso de la información.
Inestabilidad de conexión de red hacia internet	R8	Extrema	Reducir el riesgo, evitar, compartir o transferir.	Optimizar y distribuir el ancho de banda de la navegación a internet
Abuso en el acceso a recursos compartidos dentro de la institución, Exfiltración de información crítica y/o Sensible.	R9	Moderada	Asumir o reducir el Riesgo	Directiva de determinación de accesos a carpetas compartidas bajo responsabilidad
Inoperatividad de servicios Outsourcing	R10	Moderada	Reducir el riesgo, evitar, compartir o transferir.	Establecer claramente en los términos de referencia los puntos sobre obligaciones en el Servicio outsourcing.
Procedimientos no documentados de la administración de equipos servidores	R11	Extrema	Reducir el riesgo, evitar, compartir o transferir.	Documentar procedimientos sobre la configuración y administración de servidores y tener personal de contingencia.

Abuso de accesos de navegación hacia internet.	R12	Alta	Reducir el riesgo, evitar, compartir o transferir.	Elaboración y ejecución de directiva de acceso a internet
Ataque por virus, malware y gusanos debido a la descarga y uso descontrolado desde internet	R13	Alta	Reducir el riesgo, evitar, compartir o transferir.	Bloqueo de acceso a descargas de aplicativos desde internet.
Inoperatividad de los sistemas publicados del PRONIS por ataque de fuerza bruta.	R14	Alta	Reducir el riesgo, evitar, compartir o transferir.	Limitar los accesos de los puertos TCP/UP en el equipo Firewall.
Acceso indebido a equipos de cómputo por usuarios con malas intenciones.	R15	Alta	Asumir o reducir el Riesgo	Desarrollar y crear conciencia sobre las directrices y políticas de seguridad de TI.
Robo de Información Interna.	R16	Alta	Reducir el riesgo, evitar, compartir o transferir.	Brindar capacitaciones periódicas a los usuarios de la importancia de la seguridad informática
Uso de claves genéricas y acceso indebido de usuarios en los perfiles de otros usuarios	R17	Alta	Reducir el riesgo, evitar, compartir o transferir.	Políticas de determinación y control de acceso al SIA.
Robo de Información por ausencia de mecanismos de identificación y autenticación	R18	Moderada	Asumir o reducir el Riesgo	Control de acceso robustas con id usuario y contraseña y cambio periódicamente.
No confidencialidad de la Información de la base de datos	R19	Alta	Reducir el riesgo, evitar, compartir o transferir.	Políticas de gestión de la base de datos y Encriptación de datos

Fuente: Elaboración propia

2.16 INFORME DE RECOMENDACIONES.

- Riesgo Nº 1: Pérdida de la configuración de los equipos de Core.
  - Observación: Por medio de la entrevista y checklist aplicados al coordinador del ETTIC, se detectó ausencia de copias de seguridad oportuna en el router core, debido al incumplimiento en la generación de copias de Seguridad
  - Evaluación: Moderada
  - Medidas de respuesta: Reducir el riesgo
  - Control: Actualización frecuente de respaldos
  - Recomendación: Ejecutar y llevar inventario de respaldos periódicos del equipo de comunicación core del PRONIS.
- Riesgo Nº 2: Malversación de equipos físicos y acceso indebido a instalaciones del centro de los gabinetes
  - Observación: Mediante el recorrido en los pisos 13, 15 y 16 de las instalaciones del PRONIS, se observó que en cada piso existe un cuarto de gabinetes de comunicaciones, los mismos que no cuentan con un registro de acceso y seguridad física, sin vigilancia, sin llaves u otro medio que permita el acceso.
  - Evaluación: Alta
  - Medidas de respuesta: Reducir el Riesgo
  - Control: Implementar medidas de acceso físico y lógico como lector de huella biométrico, huella o lector facial.
  - Recomendación: Se recomienda que en los pisos 13, 14, 15 y 16 del Programa Nacional de Inversiones en Salud, en los cuartos de los gabinetes de

comunicaciones, se implemente un equipo de control de acceso físico y lógico como lector biométrico, lector de huella, lector facial, a fin de llevar el control de accesos a los equipos switches que se encuentran dentro de los gabinetes, y estos no sean hurtados y/o dados un mal uso.

- Riesgo Nº 3: Pérdida de paquetes de red.
- Observación: Por medio de la entrevista, y checklist al equipo de soporte del ETTIC, se corroboró que existen puntos de red que están conectados en switches genéricos tipo cascada, así cómo se evidenció que el cableado estructurado no llega a todas las estaciones finales de los usuarios, lo que implica la pérdida de paquetes de red y/o conectividad a una velocidad de 100Mbs.
- Evaluación: Extrema
- Medidas de respuesta: Reducir el riesgo.
- Control: Implementar cableado estructurado en estaciones finales
- Recomendación: Se recomienda implementar cableado estructurado en las estaciones finales de los usuarios del PRONIS, a fin de evitar demora en los procesos y desarrollo de actividades de los usuarios de las diferentes Unidades del PRONIS.

- Riesgo Nº 4: Fallas de equipos de Telecomunicaciones y servidores.
  - Observación: Mediante la entrevista realizada al equipo de redes del ETTIC, se corroboró que hay equipos servidores que partes de hardware no están funcionando en su totalidad, debido a la falta de mantenimiento, así como también no existe hardware de contingencia.

- Evaluación: Moderada
- Medidas de respuesta: Reducir el riesgo
- Control: Realizar mantenimiento preventivo en los equipos de comunicaciones al menos 1 vez al año.
- Recomendación: Se recomienda que se realice mantenimiento preventivo, así como también correctivo, de por lo menos 1 ves al año, esto permitirá garantizar la correcta funcionalidad física y lógica del equipo hardware como servidor y equipos de telecomunicaciones Switch.

- Riesgo Nº 5: Manipulación y uso malintencionado de los equipos de comunicación.
  - Observación: Según el checklist, realizado al equipo de redes del ETTIC, se puede analizar que existen equipos de comunicación Switches que son parte de un servicio de alquiler, estos tienen una clave administradora genérica, esto permite una interceptación, escucha o alteración del tráfico de red por parte de un tercero.
  - Evaluación: Alta
  - Medidas de respuesta: Reducir el riesgo
  - Control: Mejorar los niveles de seguridad a las instalaciones y niveles de accesibilidad a equipos de comunicaciones a través de políticas y/o directivas
  - Recomendación: Se recomienda que se establezca niveles de seguridad y accesibilidad a los equipos de comunicación que son parte del alquiler del servicio de Switches, se refuercen las contraseñas de acceso administrador lógico, así como se implementen políticas y/o directivas referidas a seguridad de la información que involucre claves de acceso al software.

- Riesgo Nº 6: Inoperatividad de Red
  - Mediante la entrevista al personal del ETTIC, y realizando trabajo de campo en el PRONIS, se evidenció que la red es una red plana, la red de datos tiene una máscara de sub red tipo B, que ocasiona tormentas de broadcast, con ello se saturan los equipos de comunicaciones y se consume ancho de banda de la red de datos, Se evidenció que no existe enlaces redundantes, existiendo punto único de fallas.
  - Evaluación: Alta
  - Medidas de respuesta: Reducir el riesgo.
  - Control: Segmentar la red del PRONIS.
    - Recomendación: Se recomienda que como parte del diseño de la red lógica del PRONIS, se logre segmentar la red dado que el acceso a la información en una red plana (sin segmentación), facilita los ataques de intrusión y supone un riesgo para la confidencialidad, disponibilidad e integridad de la información, debiendo los servidores estar lógicamente separados del resto de equipos de la red de datos.
- Riesgo Nº 7: Compartimiento con terceros a datos sensibles o privados
  - Observación: Por medio de la entrevista y checklist realizada al personal del ETTIC, se corroboró que no se realiza el monitoreo sobre salida de la información, si bien existen niveles de acceso para la salida a internet de los usuarios, pero, no se logra ver si el personal del PRONIS saca la información por algún medio extraíble o envío en la nube.
  - Evaluación: Extrema

- Medidas de respuesta: Reducir el riesgo
- Control: Implementar herramienta DLP y directiva de niveles de acceso y uso de la información.
- Recomendación: Se recomienda que se implemente una herramienta DLP (Data Loss Prevention) que evita la fuga de información. Se recomienda también que se implemente la directiva sobre niveles de acceso y uso de la información.

- Riesgo Nº 8: Inestabilidad de conexión de red hacia internet.
  - Observación: Mediante la entrevista desarrollada al equipo de redes del ETTIC, se pudo analizar que la red de datos del PRONIS hacia internet no cuenta con una distribución de ancho de banda hacia los servicios básicos de internet en los equipos firewall de última generación y optimizador de ancho de banda, así como no cuenta con políticas y directivas de niveles de acceso.
  - Evaluación: Extrema
  - Medidas de respuesta: Reducir el riesgo
  - Control: Optimizar y distribuir el ancho de banda de la navegación a internet
  - Recomendación: Se recomienda optimizar el tráfico de ancho de banda a servicios dedicados en el optimizador de ancho de banda, así como establecer traffic shaping en el fortigate, así como establecer políticas y directivas de niveles de acceso hacia internet.

- Riesgo Nº 9: Abuso en el acceso a recursos compartidos dentro de la institución, exfiltración de información crítica y/o sensible.

- Observación: De acuerdo a las encuestas realizadas y a la revisión de documentación realizada, con el equipo de desarrollo y el equipo de redes, se pudo observar que no se cuenta con un control de permisos mapeados en los sistemas y protección débil desde el punto de vista de confidencialidad en los servidores, permitiendo el abuso en el acceso a recursos compartidos dentro de la institución, y exfiltración de información crítica y/o sensible.
  - Evaluación: Moderada
  - Medidas de respuesta: Reducir el riesgo.
  - Control: Elaboración y ejecución de una directiva de determinación de accesos a carpetas compartidas bajo responsabilidad
  - Recomendación: Se recomienda que se elabore una directiva sobre determinación de acceso a carpetas compartidas donde se precise políticas y determinen procedimientos o acciones que debe realizarse en cumplimiento de disposiciones legales vigentes de la directiva en mención.
- Riesgo Nº 10: Establecer claramente en los términos de referencia los puntos sobre obligaciones en el Servicio outsourcing.
  - Observación: Mediante la entrevista realizada al coordinador del Equipo de Trabajo de Tecnologías de la información y Comunicación, se detectó que servicios Outsourcing no responden eficientemente en las incidencias reportadas, y como consecuencia a ello hay retraso en la solución a las incidencias.
  - Evaluación: Moderada
  - Medidas de respuesta: Reducir el riesgo

- Control: Establecer claramente en los términos de referencia los puntos sobre obligaciones en el Servicio outsourcing.
- Recomendación: Se debe establecer en los términos de referencia los puntos de respuesta de atención ni bien se reporte una incidencia, se debe establecer también que se cuente con una lista del personal en atención inmediata, entre otras obligaciones que ayuden a mejorar los servicios Outsourcing.

- Riesgo Nº 11: Procedimientos no documentados de la administración de equipos servidores
  - Observación: Por medio de la entrevista y checklist, realizada al equipo de redes de Tecnologías de la Información y Comunicación, se identificó que dos personas conforman el equipo de Redes, un administrador y un analista, los mismos que cumplen roles diferentes. El personal clave que es el administrador de red, faltó un día a laborar y se detuvieron las actualizaciones y configuraciones priori en los servidores, dado que no existen procedimientos documentados, y personal de contingencia.
  - Evaluación: Extrema
  - Medidas de respuesta: Reducir el riesgo.
  - Control: Documentar procedimientos sobre la configuración y administración de servidores y tener personal de contingencia.
  - Recomendación: Se debe documentar los procedimientos de la configuración y administración de los servidores. También se debe contar con personal de contingencia que realice actividades del personal clave.

- Riesgo Nº 12: Abuso de accesos de navegación hacia internet.
  - Observación: Mediante la entrevista realizada al equipo de Trabajo de Tecnologías de la Información y Comunicación, se evidenció que no existe una autorización para los usuarios ingresen a internet, es decir estos no son aprobados por un jefe, así como se evidenció que no existen restricciones en los accesos a internet.
  - Evaluación: alta
  - Medidas de respuesta: Reducir el riesgo
  - Control: Elaboración y ejecución de directiva de acceso a internet.
  - Recomendación: Se recomienda elaborar una directiva que indique los tipos y niveles de acceso que debe tener cada usuario de acuerdo a las actividades que realiza.
- Riesgo Nº 13: Ataque por virus, malware y gusanos debido a la descarga y uso descontrolado desde internet.
  - Observación: Mediante el checklist realizada al personal del Equipo de Trabajo de Tecnologías de la Información y Comunicación, los usuarios conectados a la wifi, tienen permisos de descarga de aplicaciones en sus laptops personales.
  - Evaluación: Alta
  - Medidas de respuesta: Reducir el riesgo.
  - Control: Bloqueo de acceso a descargas de aplicativos desde internet.

- Recomendación: Se recomienda que se cree una regla en el firewall que bloquee la descarga y ejecución de aplicativos ejecutables en la red de Wifi, dado que las laptops conectadas al wifi de los usuarios son personales.

- Riesgo Nº 14: Inoperatividad de los sistemas publicados del PRONIS por ataque de fuerza bruta.
  - Observación: Por medio de una revisión a las configuraciones de las reglas del equipo Firewall del PRONIS, se evidenció que existen puertos abiertos en los servicios publicados, los mismos que se podrían comprometerse mediante un ataque de denegación de Servicio DOS o DDoS.
  - Evaluación: Alta
  - Medidas de respuesta: Reducir el riesgo.
  - Control: Limitar los accesos de los puertos TCP/UP en el equipo Firewall.
  - Recomendación: Se recomienda deshabilitar o limitar los accesos de los puertos que navegan a internet en los servicios publicados.
- Riesgo Nº 16: Acceso indebido a equipos de cómputo por usuarios con malas intenciones.
  - Observación: Mediante la entrevista al equipo de soporte del Equipo de Trabajo de Tecnología de la Información y Comunicación, debido a que no existe cultura informática en los usuarios del PRONIS. Se ha evidenciado que los usuarios al momento de retirarse de sus equipos de trabajo dejan sin bloquear las PC, provocando que personas terceras con intensiones mal intencionadas puedan realizar trámites, firmar documentos entre otras actividades, comprometiendo la información que se maneja en el PRONIS.

- Evaluación: Alta
- Medidas de respuesta: Reducir el riesgo.
- Control: Elaboración de directivas y políticas de Seguridad informática, y sensibilización de las mismas.
- Recomendación: Se recomienda que se elaboren directivas sobre pantallas limpias y escritorios limpios (que incluye bloqueo de pantallas), así como se deberá sensibilizar a los usuarios del PRONIS sobre estas directivas implementadas.

- Riesgo Nº 17: Uso de claves genéricas y acceso indebido de usuarios en los perfiles de otros usuarios
  - Observación: Mediante el checklist, realizado al jefe de desarrollo del ETTIC, se concluye que en su mayoría los usuarios de las unidades del PRONIS, usan la contraseña por defecto para ingresar a la Suite integral de Aplicaciones -SIA, lo que como consecuencia trae suplantación de ingreso por parte de un tercero a una cuenta no correspondiente.
  - Evaluación: Alta
  - Medidas de respuesta: Reducir el riesgo.
  - Control: Implementar el forzado de cambio de contraseña en el SIA y brindar capacitaciones periódicas a los usuarios en la importación del manejo de la Información.
  - Recomendación: Se recomienda que se desarrolle un algoritmo que permita que los usuarios cambien su contraseña de lo contrario no puedan avanzar a desarrollar sus actividades en el SIA, este algoritmo deberá validar que la

contraseña sea una contraseña fuerte. Así mismo se sugiere que se realicen capacitaciones periódicas sobre el correcto manejo de información y accesos a los sistemas.

- Riesgo Nº 18: Robo de información por ausencia de mecanismos de identificación y autenticación.
  - Observación: Mediante el checklist realizada al Equipo de Trabajo de Tecnología de la Información y Comunicación, se identificó la ausencia de mecanismos de identificación y autenticación de usuario en las sesiones del PRONIS, asì como también existe manejo de información sensible por usuarios no autorizados, haciendo movimiento de expedientes sin ser autorizados.
  - Evaluación: Moderada
  - Medidas de respuesta: Reducir el riesgo.
  - Control: Medidas de acceso robustas con id usuario y contraseña.
  - Recomendación: Se recomienda se desarrolle un algoritmo que permita que los usuarios cambien su contraseña cada 60 o 90 días, las mismas que no deben tener similitud con información del usuario y deban contener.
- Riesgo Nº 19: No confidencialidad de la Información de la base de datos.
  - Observación: Mediante el checklist que se realizó al personal de desarrollo, sub equipo de trabajo que es responsable sobre la administración de la Base de Datos del PRONIS, se pudo observar que los registros pueden ser alterados sin que exista una gestión de aprobación de responsables del sistema, lo cual involucra a un fácil ingreso de registros por usuarios que puedan tener las credenciales.

- Evaluación: Alta
- Medidas de respuesta: Reducir el riesgo.
- Control: Políticas de gestión de la base de datos y Encriptación de datos
- Recomendación: Se recomienda se implemente directivas que incluyan políticas sobre la gestión de cambios de registros en la base de datos, es decir que de existir algún cambio o actualización de registros estos deban ser autorizados y aprobados. También se recomienda que los datos sensibles de los usuarios root de la base de datos sean encriptados.

CAPÍTULO VI

RESULTADOS

Se debe tener en cuenta que la muestra en estudio está constituida por el personal del Equipo de Trabajo de Tecnologías de la Información y las Comunicaciones, es decir de 09 personas distribuidos de la siguiente manera: 01 personal en jefatura, 03 en soporte técnico, 02 en desarrollo de software, 02 en redes e infraestructura. Los resultados aplicados se muestran a través de la aplicación de los controles establecidos en el Informe de Recomendaciones.

Ge: O1 X O2

Dónde:

O1: La observación 1(O1) evalúa el estado actual de la seguridad cibernética del Programa Nacional de Inversiones en Salud.

X: Representa el modelo de gestión ciberseguridad basado en los estándares de seguridad internacional de NIST CSF.

O2: La observación 2 (O2) evalúa el estado de seguridad cibernética luego del diagnóstico integral de Ciberseguridad basado en NIST CSF del Programa Nacional de Inversiones en Salud propuesto.

O1: Evalúa el estado actual de la seguridad cibernética del Programa Nacional de Inversiones en Salud.

Antes de la aplicación de controles se determinó que existían 19 Riesgos Inherentes.

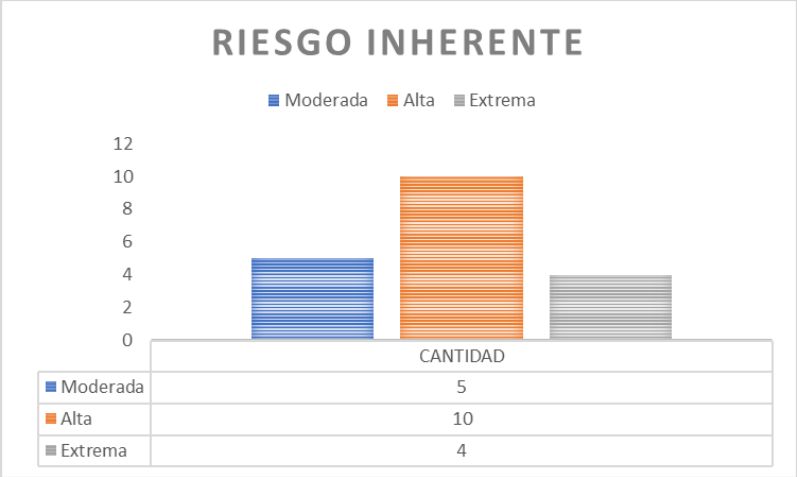
Figura 21: Determinación del Riesgo Residual

RIESGO	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
R1	3	2	Moderada
R2	4	3	Alta
R3	4	4	Extrema
R4	3	2	Moderada
R5	1	4	Alta
R6	1	5	Alta
R7	3	4	Extrema
R8	3	5	Extrema
R9	3	4	Moderada
R10	3	2	Moderada
R11	3	4	Extrema
R12	3	5	Alta
R13	4	2	Alta
R14	3	3	Alta
R15	3	3	Alta
R16	2	2	Alta
R17	4	2	Alta
R18	3	3	Moderada
R19	3	3	Alta

Fuente: Elaboración propia

De los cuales, se clasificó por zonda de riesgo, de los que se obtiene 10 riesgos en Zona 5 riesgos en zona moderada, 10 riesgos en zona alta y 4 riesgos en zona extrema.

Figura 22: Cuadro de Riesgo inherente



Fuente: Elaboración propia

X: Representa el modelo de gestión ciberseguridad basado en los estándares de seguridad internacional de NIST CSF aplicado en un periodo de 3 meses.

O2: Evalúa el estado de seguridad cibernética luego del diagnóstico integral de Ciberseguridad basado en NIST CSF del Programa Nacional de Inversiones en Salud propuesto.

Luego de la aplicación de controles establecidos en el Informe de Recomendaciones en el corto tiempo de 3 meses se observó que de los riesgos identificados bajaron un escalón dentro del nivel de evaluación de la zona de riesgo, obteniéndose de la siguiente manera:

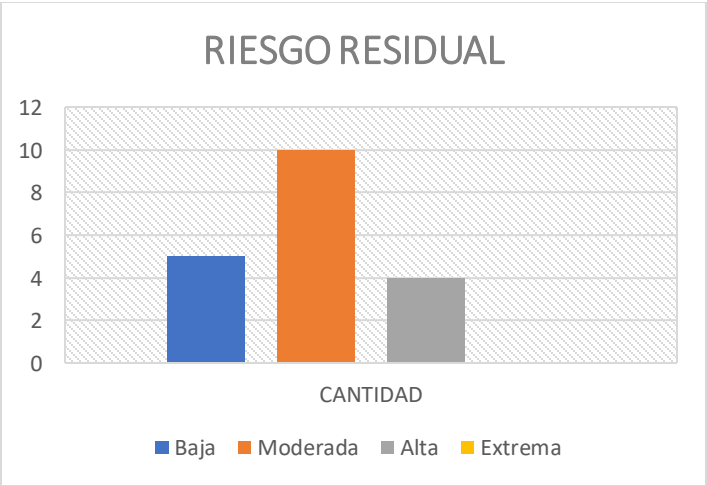
Figura 23: Determinación de Cuadro de Riesgo Residual

RIESGO	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
R1	3	2	Baja
R2	2	3	Moderada
R3	4	3	Alta
R4	3	2	Baja
R5	1	3	Moderada
R6	1	3	Moderada
R7	3	3	Alta
R8	3	3	Alta
R9	2	2	Baja
R10	3	2	Baja
R11	3	3	Alta
R12	3	2	Moderada
R13	3	2	Moderada
R14	3	2	Moderada
R15	3	2	Moderada
R16	2	2	Moderada
R17	3	2	Moderada
R18	3	2	Baja
R19	3	2	Moderada

Fuente: Elaboración propia

Obteniéndose, el riesgo residual de 5 riesgos en zona baja, 10 riesgos en zona moderada y 4 riesgos en zona alta.

Figura 24: Cuadro de Riesgo Residual



Fuente: Elaboración propia

CONCLUSIONES

- Aplicando encuestas, entrevistas y checklist se pudo determinar cuál es la situación actual de ciberseguridad del Programa Nacional de Inversiones en Salud, encontrándose como principales problemas el no contar con el personal suficiente en el Equipo de Trabajo de Tecnologías de la Información y Comunicación, así mismo no existe un proceso que permita mantener las habilidades y competencias del personal del ETTIC. Además, que no se tienen definidos esquemas de análisis de riesgos, identificación de amenazas y vulnerabilidades, los cuales permitan clasificarlos y se les dé una eficaz y eficiente tratamiento.

- Se determinó el alcance de la propuesta en el Proceso de Tecnologías de la Información para determinar el nivel de capacidad de ciberseguridad que a través de la aplicación del el Marco Nist CSF, se identificó los activos críticos de la organización del Proceso de Tecnologías de la Información.

- La aplicación del Marco Nist CSF, permitió identificar las vulnerabilidades y Amenazas de los activos críticos de la Organización del Proceso de Tecnologías de la información, permitiendo identificar los riesgos los cuales se detallaron a lo largo del capítulo V.

- Se detectaron 19 riesgos Inherentes, y posteriormente se empleó un control específico, obteniéndose el Riesgo Residual para mitigar el riesgo.

- Se elaboró un informe de recomendaciones para disminuir el riesgo, a fin de ser aplicado, luego de 3 meses se pudo evidenciar que el nivel de riego aplicado al control disminuyo una escala, obteniéndose 15 riesgos Residuales.

- Se determinó los controles necesarios relacionados a los activos críticos del proceso de tecnologías de la Información, mediante un diagnóstico integral de ciberseguridad basado en estándares internacionales de seguridad de NIST CSF para mitigar los riesgos de ciberseguridad en el Programa Nacional de Inversiones en Salud.

- Se emitió recomendaciones de los controles para mitigar los 19 riesgos encontrados en el Programa Nacional de Inversiones en Salud, a fin que sean considerados para disminuir el riesgo.

CAPITULO VII

RECOMENDACIONES

- Se recomienda aplicar los controles del proceso seleccionado, específicamente en el Equipo de Trabajo de Tecnologías de la Información y Comunicación para poder cumplir con las actividades de mitigación de riesgos, además de mantener las habilidades y competencias de dicho personal de manera constante.

- Se sugiere supervisar la implementación de los controles constantemente en la entidad por un especialista, ya que estas solo se encuentran documentadas mas no aplicados.

- Se sugiere monitorear el rendimiento del Equipo de Trabajo de Tecnologías de la Información y Comunicación con respecto al tema de ciberseguridad, mediante evaluaciones periódicas, dado que son los principales interesados en impartir conocimiento de confidencialidad, integridad y disponibilidad de la información; e informar los resultados a la Unidad de Administración y Finanzas, ya que no se hace dicho procedimiento.

- Se recomienda se disponga de recurso humano y tecnológico para la mitigación de riesgos en el Equipo de Tecnologías de la Información y las Comunicaciones.

- Se recomienda planificar y tomar iniciativas de aseguramiento que permitan diagnosticas el riesgo e identificar procesos críticos de TI en el Equipo de Trabajo de Tecnología de la Información y Comunicación.

CAPÌTULO VIII

REFERENCIA BIBLIOGRAFICA

Bibliografía

Aimacaña, F. (2015). *Esquema de Seguridad perimetral y control de incidencias de la red de datos para la Universidad Técnica de Cotopaxi. Ecuador.* Obtenido de dspace UNIANDES: http://dspace.uniandes.edu.ec/bitstream/123456789/415/1/TUAMEIE006-2015.pdf

AWS, & Organización de los Estados Americanos . (2019). Ciberseguridad Marco NIST. *Un abordaje Integral de la Ciberseguridad*, 20. Recuperado el 10 de julio de 2020

Chanaluiza , D., Meza, A., & Tasipanta, J. (2012). *Implementación del sistema de gestión y administración de seguridad para la dirección de tecnologías de la Universidad Central del Ecuador (DTIC).* Quito, Quito, Ecuador.

Deloitte. (2016). *Los riesgos de la tecnología.*

Departamento de Seguridadd Informática. (2018). Amenazas a la Seguridad de la Información. Obtenido de www.seguridadinformatica.unlu.edu.ar

Domínguez Chávez, J. (2015). *Seguridad Informática Personal y Corporativa.* Venezuela.

Gómez Suarez, Á. (2019). *Diseño de un Programa de Ciberseguridad de una empresa basado en el Marco de Trabajo NIST.* Jaen, España, España.

Guillinta Chavez, O., & Merino Rivera , J. (2016). *Modelo de prevención y defensa contra ataques cibernéticos basado en estándares de seguridad internacionales para IT-Expert.* Lima, Lima, Perú.

Hernandez Sampieri, Fernandez Collado, & Baptista , L. (2010). *Población, muestra, informantes clave, variable, unidad de análisis.*

INCIBE. (2016). Ranking de los 10 principales incidentes de Ciberseguridad a nivel mundial del 2016.

ISACA. (2020). *CYBERSECURITY NEXUS (CSX) Cybersecurity Fundamentals*. Obtenido de https://www.isaca.org/training-and-events/cybersecurity.

ISO 31000. (2018). *Administración/Gestión de riesgos-Norma Internacional.* Estados Unidos.

ISOTools Excellence. (2017). *Blog especializado en Sistemas de Gestiòn de Seguridad de la Información*. Obtenido de https://www.pmg-ssi.com/

Lara Guijarro, E. (2019). *Diseño de un modelo de Seguridad de la Información, basado en OSSTMMv3, NIST SP800-30 E ISO 27001 para centros de Educación: Caso de Estudio Universidad Regional Autónoma de los Andes, extensión Tulcán.* Quito, Quito, Ecuador.

Leiva Peña, R. (2016). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015.* Lambayeque, Lambayeque, PERÚ.

Lucero Gómez, A., & Valverde Padilla, J. (2012). *Análisis y gestión de riesgos de los sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo, utilizando la metodología MAGERIT*. Ecuador.

Muñoz, cortez, & Bustamante. (2011). *Seguridad de la Información.*

National Institute of Standards and Technology. (2012). Guide for Conducting risk assessments. Estados Unidos. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST 800-161. (2015). Prácticas de gestión de riesgo de la cadena de suministro para sistemas y organizaciones federales de la información. Obtenido de https://doi.org/10.6028/NIST.SP.800-161

NIST, C. (2018). *Estándares Internacionales NIST CSF.* (Vol. 1.1).

OTAN. (2012). National cyber security framework Manual. Obtenido de https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

PERCERT. (05 de abril de 2020). Reporte de Alerta Integrada de Seguridad Digital realizada por el equipo de Respuestas ante incidentes de seguridad Digital Nacional. *Alerta Integrada de Seguridad Digital*.

Shackelford, Craig, A., & Martell. (2015). *"Toward a global cybersecurity standard of care? Exploring the implicatons of the 2014 NIST cybersecurity framework on shaping.* Recuperado el 21 de febrero de 2021

Vilcamorro Zubiate, L., & Vilchez Linares , E. (2018). *Propuesta de implementación de un modelo de Gestión de Ciberseguridad para el Centro de operaciones de Seguridad (SOC) de una empresa de Telecomunicaciones.* Lima, Lima, Perú.

ANEXOS

ANEXO N°1: Encuesta aplicada al personal del ETTIC

Encuesta Aplicada al Coordinado del Equipo de Trabajo de Tecnologías de la Información y comunicación, al personal de redes, desarrollo y soporte del Equipo de Trabajo de Tecnologías de la Información y Comunicación.

El objetivo de la presente encuesta es obtener información para determinar las vulnerabilidades y amenazas correspondiente al proceso de Tecnologías de la Información del Programa Nacional de Inversiones en Salud.

1. Los dispositivos físicos y sistemas dentro de la organización son inventariados.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca

2. Las plataformas de software y las aplicaciones dentro de la organización son inventariadas.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
3. Se mapea la comunicación organizacional y los flujos de datos.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
4. Se catalogan los sistemas de información externos.
    a. Siempre
    b. Casi siempre

    c. Algunas veces
    d. Nunca
5. Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan según su clasificación, criticidad y valor en el negocio.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
6. Realizan Backup de sus sistemas Informàticos? Si es Sí, que tiempo dura la recepción de información.
7. Se establecen los roles y responsabilidades de ciberseguridad para todos los colaboradores y terceros interesados (por ejemplo, proveedores, clientes, socios).
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
8. Se establecen dependencias y funciones críticas para la entrega de servicios críticos.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
9. Los requisitos de resiliencia para apoyar la entrega de servicios críticos se establecen para todos los estados operativos (por ejemplo, bajo coacción/ataque, durante la recuperación, operaciones normales).
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
10. Los procesos de gobierno y gestión de riesgos abordan los riesgos de ciberseguridad.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
11. Se identifican y documentan las vulnerabilidades de los activos.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
12. Los procesos de gestión de riesgos son establecidos, gestionados y acordados por las partes interesadas de la organización.
    a. Siempre

b. Casi siempre
c. Algunas veces
d. Nunca

13. La determinación de la tolerancia al riesgo de la organización se basa en su infraestructura crítica y en el análisis de riesgo específico del sector.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
14. Los interesados de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión de riesgos de la cadena de suministro cibernética.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
15. Se identifican, priorizan y evalúan los proveedores y socios externos de los sistemas de información, componentes y servicios mediante un proceso de evaluación de riesgos de la cadena de suministro cibernética.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
16. Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir los objetivos del programa de ciberseguridad de una organización y el Plan de gestión de riesgos de la cadena de suministro cibernética.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
17. Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
18. La planificación y las pruebas de respuesta y recuperación se llevan a cabo con suministradores y proveedores externos.
    a. Siempre
    b. Casi siempre
    c. Algunas veces

    d. Nunca
19. Las identidades y las credenciales se emiten, administran, verifican, revocan y auditan para dispositivos, usuarios y procesos autorizados.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
20. Se gestiona y protege el acceso físico a los activos.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
21. Se gestiona el acceso remoto.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
22. Los permisos de acceso y las autorizaciones se gestionan, incorporando los principios de mínimo privilegio y segregación de funciones.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
23. Las identidades se comprueban y están sujetas a credenciales y se afirman en las interacciones.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
24. Los usuarios, dispositivos y otros activos se autentican (por ejemplo, factor único y multifactor) de acuerdo con el riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de los individuos y otros riesgos organizacionales).
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
25. Todos los usuarios son informados y entrenados.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca

26. Los usuarios privilegiados entienden sus roles y responsabilidades.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
27. Las partes interesadas externas (por ejemplo, proveedores, clientes, socios) entienden sus roles y responsabilidades.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca
28. Los ejecutivos senior entienden sus roles y responsabilidades.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca

29. El personal de seguridad física y ciberseguridad entiende sus roles y responsabilidades.
    a. Siempre
    b. Casi siempre
    c. Algunas veces
    d. Nunca

ANEXO N° 2: Checklist aplicada a ETTIC

Checklist, realizado al personal del Equipo de Trabajo de Tecnologías de la Información y Comunicación.

		PREGUNTA	SI	NO	NO APLICA	OBSERVACIÓN
ID	Cód. Categoría	ID.AM				
	Nombre Categoría	Gestión de activos				
	ID.AM-1	Los dispositivos físicos y sistemas dentro de la organización son inventariados.				
	ID.AM-2	Las plataformas de software y las aplicaciones dentro de la organización son inventariadas.				
	Cód. Categoría	ID.GV				
	Nombre Categoría	Gobierno				
	ID.GV-1	Se establece la política de ciberseguridad de la organización.				
	Cód. Categoría	ID.RA				
	Nombre Categoría	Evaluación de riesgos				
	ID.RA-1	Se identifican y documentan las vulnerabilidades de los activos.				
PR	Cód. Categoría	PR.AC				

	Nombre Categoría	**Control de accesos**				
	PR.AC-2	Se gestiona y protege el acceso físico a los activos.				
	Cód. Categoría	**PR.DS**				
	Nombre Categoría	**Seguridad de datos**				
	PR.DS-7	Los entornos de desarrollo y prueba están separados del entorno de producción.				
DE	**Cód. Categoría**	**DE.AE**				
	Nombre Categoría	**Anomalías y eventos**				
	DE.CM-4	Se detecta código malicioso.				
RS	**Cód. Categoría**	**RS.RP**				
	Nombre Categoría	**Planificación de respuesta**				
	RS.RP-1	El plan de respuesta se ejecuta durante o después de un incidente.				
	Cód. Categoría	**RC.RP**				
	Nombre Categoría	**Planificación de recuperación**				
	RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad.				

ANEXO N° 3: Núcleo del Marco.

Identificación de función (05), categoría (23), Subcategoría (108) y Referencias

Función	Categoría	Subcategoría	Referencias informativas
		ID.RA-3: Se identifican y se documentan las amenazas, tanto internas como externas.	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** Cláusula 6.1.2 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Se identifican los impactos y las probabilidades del negocio.	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Se identifican y priorizan las respuestas al riesgo.	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Cláusula 6.1.3 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Estrategia de gestión de riesgos (ID.RM): Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	**ID.RM-1:** Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: La tolerancia al riesgo organizacional se determina y se expresa claramente.	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3 **NIST SP 800-53 Rev. 4** PM-9

Función	Categoría	Subcategoría	Referencias informativas
		ID.RM-3: La determinación de la tolerancia del riesgo de la organización se basa en parte en su rol en la infraestructura crítica y el análisis del riesgo específico del sector.	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3 **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	Gestión del riesgo de la cadena de suministro (ID.SC): Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	**ID.SC-1:** Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético.	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2

Función	Categoría	Subcategoría	Referencias informativas
			NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
PROTEGER (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-1:** Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Se gestiona y se protege el acceso físico a los activos.	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009 4.3.3.3.2**, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Se gestiona el acceso remoto.	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1

Función	Categoría	Subcategoría	Referencias informativas
			NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9

Función	Categoría	Subcategoría	Referencias informativas
			ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Concienciación y capacitación (PR.AT): El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	**PR.AT-1:** Todos los usuarios están informados y capacitados.	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades.	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2

Función	Categoría	Subcategoría	Referencias informativas
			A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción.	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53 Rev. 4** SA-10, SI-7
	Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-1:** Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3

Función	Categoría	Subcategoría	Referencias informativas
			ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Los datos son eliminados de acuerdo con las políticas.	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53 Rev. 4** MP-6

Función	Categoría	Subcategoría	Referencias informativas
		PR.IP-7: Se mejoran los procesos de protección.	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 9, Cláusula 10 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Se comparte la efectividad de las tecnologías de protección.	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).	**CIS CSC** 19 **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Se prueban los planes de respuesta y recuperación.	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal).	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21

Función	Categoría	Subcategoría	Referencias informativas
			NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Las redes de comunicaciones y control están protegidas.	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o "hot swap") para lograr los requisitos de resiliencia en situaciones normales y adversas.	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
DETECTAR (DE)	**Anomalías y Eventos (DE.AE):** se detecta actividad anómala	**DE.AE-1:** Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3

Función	Categoría	Subcategoría	Referencias informativas
	y se comprende el impacto potencial de los eventos.	los usuarios y sistemas.	**ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Cos datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Se determina el impacto de los eventos.	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Se establecen umbrales de alerta de incidentes.	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Monitoreo Continuo de la Seguridad (DE.CM): El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia	**DE.CM-1:** Se monitorea la red para detectar posibles eventos de seguridad cibernética.	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

Función	Categoría	Subcategoría	Referencias informativas
	y se comprende el impacto potencial de los eventos.	los usuarios y sistemas.	**ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Cos datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Se determina el impacto de los eventos.	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Se establecen umbrales de alerta de incidentes.	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Monitoreo Continuo de la Seguridad (DE.CM): El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia	**DE.CM-1:** Se monitorea la red para detectar posibles eventos de seguridad cibernética.	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

Función	Categoría	Subcategoría	Referencias informativas
			COBIT 5 BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5
	Procesos de Detección (DE.DP): Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	**DE.DP-1:** Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.	**CIS CSC** 19 **COBIT 5** APO01.02, DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Se prueban los procesos de detección.	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Se comunica la información de la detección de eventos.	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: los procesos de detección se mejoran continuamente.	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA- 5, SI-4, PM-14

Función	Categoría	Subcategoría	Referencias informativas
	de las medidas de protección.	**DE.CM-2:** Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Se detecta el código malicioso.	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: Se detecta el código móvil no autorizado.	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Se realizan escaneos de vulnerabilidades.	**CIS CSC** 4, 20

Función	Categoría	Subcategoría	Referencias informativas
RESPONDER (RS)	**Planificación de la Respuesta (RS.RP):** Los procesos y procedimientos de respuesta se ejecutan y se mantienen a fin de garantizar la respuesta a los incidentes de seguridad cibernética detectados.	**RS.RP-1:** El plan de respuesta se ejecuta durante o después de un incidente.	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Comunicaciones (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley).	**RS.CO-1:** El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Cláusula 7.4, Cláusula 16.1.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética.	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15

Función	Categoría	Subcategoría	Referencias informativas
			NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Los incidentes son mitigados.	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Mejoras (RS.IM): Las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y respuesta actuales y previas.	**RS.IM-1:** Los planes de respuesta incorporan las lecciones aprendidas.	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Se actualizan las estrategias de respuesta.	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECUPERAR (RC)	**Planificación de la recuperación (RC.RP):** Los procesos y procedimientos de recuperación se ejecutan y se mantienen para asegurar la restauración de los sistemas o activos afectados por incidentes de seguridad cibernética.	**RC.RP-1:** El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Mejoras (RC.IM): La planificación y los procesos de recuperación se mejoran al incorporar en las actividades futuras las lecciones aprendidas.	**RC.IM-1:** Los planes de recuperación incorporan las lecciones aprendidas.	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Se actualizan las estrategias de recuperación.	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

Función	Categoría	Subcategoría	Referencias informativas
	Comunicaciones (RC.CO): Las actividades de restauración se coordinan con partes internas y externas (por ejemplo, centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores).	**RC.CO-1:** Se gestionan las relaciones públicas.	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Cláusula 7.4
		RC.CO-2: La reputación se repara después de un incidente.	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Cláusula 7.4
		RC.CO-3: Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4

ANEXO N° 4: Política Nacional de Ciberseguridad

A continuación, se presenta la política Nacional de ciberseguridad que se aplica en las entidades de la administración Pública.

PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno Digital

Año del Buen Servicio al Ciudadano

POLÍTICA NACIONAL DE CIBERSEGURIDAD

Objetivo

Proteger la infraestructura de información, los datos e información del Estado y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las propuestas legislativas, y en general la normatividad relacionada con la seguridad de la información o ciberseguridad comprendida en esta Política, identificando los recursos involucrados y las partidas presupuestales correspondientes.

Mantener la Política Nacional de Ciberseguridad actualizada, a efectos de asegurar su vigencia y por ende su eficacia, promoviendo la participación de las entidades de sector público y privado, así como representantes de la sociedad civil y la academia.

I. Alcance

La presente Política se aplica a todas las entidades de la Administración Pública a que hace referencia el Artículo I del Título Preliminar de la Ley N° 27444, así como a todos sus recursos y procesos sean estos internos o externos.

II. Referencias Internacionales

La presente Política cuenta con los siguientes marcos de referencia:

- Resolución Ministerial N° 246-2007-PCM, que aprueba la Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática, o la que haga sus veces.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, o la que haga sus veces.
- Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.

III. Marco Normativo

- Constitución Política del Perú.
- Decreto Legislativo N° 604.
- Ley N° 29158: Ley Orgánica del Poder Ejecutivo.

PÁGINA 1 | 8

- Ley Nº 27658: Ley Marco de Modernización de la Gestión del Estado.
- Ley Nº 27806: Ley Transparencia y Acceso a la Información Pública.
- Ley N° 27444: Ley de Procedimiento Administrativo General.
- Ley N° 27269: Ley de Firmas y Certificados Digitales.
- Ley N° 27291: Ley que modifica el código civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica.
- Ley N° 28493: Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM).
- Ley N° 29733: Ley de Protección de Datos Personales.
- Ley N° 28530: Ley de Promoción de Acceso a Internet para personas con discapacidad y adecuación del espacio físico en cabinas públicas de internet.
- Ley N° 29904: Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica.
- Ley N° 30096 y su modificatoria Ley 30171: Ley de Delitos Informáticos.
- Decreto Legislativo N° 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses.
- Decreto Supremo N° 022-2017-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
- Decreto Supremo N° 066-2011-PCM: Aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0".
- Decreto Supremo N° 004-2013-PCM: Aprueba la Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo N° 081-2013-PCM: Aprueba la Política Nacional de Gobierno Electrónico 2013-2017.
- Resolución Ministerial N° 179-2004-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2004 Tecnología de la Información. "Procesos del Ciclo de Vida del Software, 1ª Edición" en entidades del Sistema Nacional de Informática.
- Resolución Ministerial N° 246-2007-PCM, que aprueba la Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 197-2011-PCM, que establece fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información".
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

- Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.

IV. Términos y Definiciones

a) Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

- *Confidencialidad*: Garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- *Integridad*: Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.
- *Disponibilidad*: Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

- *Autenticidad*: Asegurar que la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- *Auditabilidad*: Definir que todos los eventos de un sistema puedan ser registrados para su control posterior.
- *Protección a la duplicación*: Asegurar que una transacción sólo se realice una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- *No repudio*: Evitar que una entidad que haya enviado o recibido información o intercambiado datos, alegue ante terceros que no los envió o no los recibió.
- *Legalidad*: Cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- *Confiabilidad de la Información*: Que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

- *Información*: Toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- *Sistema de Información*: Conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- *Tecnología de la Información*: Hardware y software operados por la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
- *Propietario de la Información*: Persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.

b) Evaluación de Riesgos

Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma; la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

c) Tratamiento de Riesgos

Proceso de selección e implementación de medidas para modificar el riesgo.

d) Gestión de Riesgos

Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo.

NOTA. La gestión de riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

e) Comité de Seguridad de la Información

Colegiado integrado por representantes de todas las áreas sustantivas de la entidad, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

f) Responsable de Seguridad de la Información

Persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la entidad que así lo requieran.

g) Incidente de Seguridad

Evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de quebrar los mecanismos de seguridad existentes.

h) Riesgo

Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

i) Amenaza

Causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

j) Vulnerabilidad

Debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

k) Control

Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal.

V. Política Nacional de Ciberseguridad

1. ***Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el de la ciberseguridad, creando un entorno y las condiciones necesarias que permitan brindar protección en el ciberespacio.***

Para lograr este objetivo es necesario involucrar a todos los sectores y entidades del Estado con responsabilidad en el campo de ciberseguridad y ciberdefensa, creando un ambiente participativo en el que participen representantes del sector privado, sociedad y la academia, donde cada quien aporte y actúe a propósitos comunes, estrategias concertadas y esfuerzos coordinados. Asimismo, es de vital importancia crear conciencia y sensibilizar a la población respecto de la importancia de la seguridad de la información (ciberseguridad); así como, fortalecer los niveles de cooperación y colaboración internacional en aspectos de ciberseguridad y ciberdefensa; apoyar investigaciones relacionadas con ataques informáticos y proteger a la ciudadanía de las consecuencias de estos ataques.

2. ***Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en materia de ciberseguridad dentro de la Administración Pública.***

Este objetivo permitirá generar y fortalecer las capacidades existentes en materia de seguridad cibernética, con el propósito de afrontar las amenazas que atentan contra los propósitos planteados.

Inicialmente, se capacitará a los funcionarios y servidores que estén directamente involucrados en la atención y manejo de incidentes cibernéticos. Gradualmente se extenderá esta capacitación a las demás entidades del Estado. Entre los planes de capacitación, el Pe-CERT con el apoyo del Comité Interamericano Contra el Terrorismo (CICTE) de la OEA, entre otros, elaborará un Plan de Capacitación para los demás funcionarios y servidores del Estado, así como programas de sensibilización y concienciación para los ciudadanos en general. De la misma forma, el Ministerio del Interior (MININTER) buscará la implementación gradual de asignaturas en seguridad de la información, ciberseguridad y ciberdefensa (teórico-prácticas) en las escuelas de formación y de capacitación de oficiales y suboficiales.

3. ***Desarrollar un Plan de sensibilización y capacitación a todos los ciudadanos respecto a la Ciberseguridad.***

Se busca que la sociedad civil tome consciencia sobre la ciber-seguridad, identificar posibles vulnerabilidades o amenazas y tomar acciones oportunas para su seguridad.

El Plan contará con una Estrategia de difusión que incluya la organización de conferencias para instituciones educativas (de nivel primario a universitario), y tareas de divulgación entre ciudadanos y otras entidades públicas y privadas del país.

Así mismo, se realizarán foros que permitan intercambiar opiniones y experiencias entre todas las entidades públicas y privadas, sociedad civil y academia, con el objeto de compartir las mejores prácticas en Ciberseguridad y Ciberdefensa.

Parte de la sensibilización en temas de Seguridad de la Información, radica en socializar la Normatividad vigente, como la Ley N° 27933 de Protección de Datos Personales, que ampara a todos los ciudadanos y la Ley N° 30096 modificada por la Ley N° 30171 – Ley de Delitos Informáticos, entre otros.

4. ***Fortalecer la legislación en materia de ciberseguridad, la cooperación internacional y propiciar la adhesión del Perú a los diferentes organismos internacionales en esta temática.***

Este objetivo busca desarrollar las herramientas jurídicas necesarias para una efectiva y eficiente prevención, investigación y judicialización de los delitos informáticos.

Así, se propenderá por la expedición de la normatividad necesaria para dar cumplimiento a los tratados internacionales sobre ciberseguridad, ciberdelincuencia, en la medida que hagan parte del bloque de constitucionalidad, así como por la debida reglamentación de lo dispuesto en la legislación nacional. Las entidades responsables de la ciberseguridad y ciberdefensa deberán buscar y evaluar la participación en diferentes redes y mecanismos internacionales de cooperación (Consejo de Europa, OEA y Forum Of Incident Response Security Teams - FIRST), que permitan preparar al país para afrontar los crecientes desafíos del entorno internacional en el área de ciber-seguridad, así como responder de una forma más eficiente a incidentes y delitos de seguridad cibernética.

De manera especial el Perú deberá gestionar la adhesión al Convenio de Ciberdelincuencia suscrito en Budapest el 23 de noviembre del 2001, adhesión que permitirá combatir la ciber-delincuencia de manera coordinada y globalizada, lo cual a su vez, se orienta al cumplimiento del Compromiso al que se arribó en la Cumbre Mundial sobre Sociedad de la información en Túnez 2005, enmarcados dentro de los Objetivos de Desarrollo del Milenio, (ahora denominados Objetivos de Desarrollo Sostenible), que disponen incrementar la confianza y la seguridad en cuanto a la utilización de las Tecnologías de la Información y de la Comunicación (TIC), y a su vez, se encuentra dentro de los alcances de lo establecido en el Política Nacional de Gobierno Electrónico 2013-2017, aprobada mediante Decreto Supremo N° 081-2013-PCM , y en plena concordancia con la Ley de Delitos Informáticos aprobada mediante Ley N° 30096, modificada mediante Ley N° 30171.

5. ***Afianzar la integración y coordinación eficaz, entre las diversas Coordinadoras de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública y el sector privado.***

   Según lo establecido en la Resolución Ministerial N° 360-2009-PCM, se hace necesario que cada Ministerio o la que haga sus veces, coordine con el Pe-CERT, para hacer cumplir sus objetivos.

   Es importante que dicha coordinación se realice permanentemente y que la misma tenga un carácter de prioridad ante cualquier amenaza que vulnere la seguridad de la Nación.

6. **Elaborar un Plan de Acción Nacional en Ciberseguridad**

   Este Plan deberá realizarse de forma multisectorial y multidisciplinaria, entre representantes de las entidades del sector público, sector privado, sociedad y la academia.

7. **Crear el Comité Nacional de Ciberseguridad**

   Este Comité tendrá como parte de sus funciones, el velar por el fiel cumplimiento de las políticas y lineamientos que se establezcan respecto a la Ciberseguridad.

   El Comité está conformado por las siguientes entidades:

   1. Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital (SEGDI)
   2. Poder Judicial
   3. Dirección Nacional de Inteligencia (DINI)
   4. Ministerio de Defensa (MINDEF)
   5. Ministerio del Interior (MININTER)
   6. Policía Nacional del Perú (PNP)
   7. Asociación de Gobiernos Regionales
   8. Sociedad Nacional de Industrias (SNI)
   9. Cámara de Comercio de Lima (CCL) (OBS)
   10. Cámara Nacional de Comercio, Producción, Turismo y Servicios – PERUCÁMARAS
   11. Colegio de Abogados de Lima (CAL)
   12. Colegio de Ingenieros del Perú (CIP)
   13. NAP (Network Access Point) Peru
   14. Confederación Nacional de Institucionales Empresariales Privadas (CONFIEP)
   15. Asociación de Bancos del Perú (ASBANC)
   16. Asociación para el Fomento de la Infraestructura Nacional (AFIN)
   17. Red Científica Peruana (RCP)
   18. Otros (Definir)

ACTA DE SUSTENTACIÓN

ACTA DE SUSTENTACIÓN VIRTUAL Nº 004-2023-D/FACFyM

Siendo las 11:00 am del día miércoles 18 de enero del 2023, se reunieron vía plataforma virtual, httpa//meet.google.com/xqu-rihx-mmk los miembros del jurado evaluador de la Tesis titulada: "DIAGNÓSTICO INTEGRAL DE CIBERSEGURIDAD, BASADO EN ESTÁNDARES INTERNACIONALES DE SEGURIDAD DE NIST CSF, PARA EL PROGRAMA NACIONAL DE INVERSIONES EN SALUD"

Designados por Decreto N° 003-2020-VIRTUAL-UI/FACFyM de fecha 05 de setiembre de 2020

Con la finalidad de evaluar y calificar la sustentación de la tesis antes mencionada, conformada por los siguientes docentes:

Dr. Ing. Armando José Moreno Heredia Presidente
Dr. Ing Nilton César Germán Reyes Secretario
Dr. Ing. Denny John Fuentes Adrianzén Vocal

La tesis fue asesorada por el Dr. Ing. Gilberto Carrión Barco nombrado por Decreto N° 003-2020-VIRTUAL-UI/FACFyM de fecha 05 de setiembre de 2020

El Acto de Sustentación fue autorizado por Resolución N°º 005-2023-VIRTUAL-D/FACFyM de fecha 3 de Enero de 2023

La Tesis fue presentada y sustentada por la Bachilleres: Aguirre Segura Carla Vivian, y tuvo una duración de 40 minutos.

Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado se procedió a la calificación respectiva, otorgándole el Calificativo de 17 (diecisiete) en la escala vigesimal, mención Bueno.

Por lo que queda apta para obtener el Título Profesional de **Ingeniera en Computación e informática** de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ciencias Físicas y Matemáticas y la Universidad Nacional Pedro Ruiz Gallo.

Siendo las 11:45 am se dio por concluido el presente acto académico, dándose conformidad al presente acto con la firma de los miembros del jurado.

Dr. Ing. Armando José Moreno Heredia
Presidente

Dr. Ing Nilton César Germán Reyes
Secretario

M.Sc. Ing. Denny John Fuentes Adrianzén
Vocal

Dr Ing. Gilberto Carrión Barco
Asesor

CARÁTULA DEL INFOME FINAL POR TURNITIN

DR. GILBERTO CARRIÓN BARCO
DNI: 16720146
Docente asesor

CARÁTULA DEL INFORME FINAL EVALUADO POR TURNITIN

DIAGNÓSTICO INTEGRAL DE CIBERSEGURIDAD, BASADO EN ESTÁNDARES INTERNACIONALES DE SEGURIDAD DE NIST CSF, PARA EL PROGRAMA NACIONAL DE INVERSIONES EN SALUD

por Carla Vivian Aguirre Segura

Nombre del archivo:	INFORME_FINAL_V20_para_Turniting.docx
Tamaño del archivo:	2.31M
Total páginas:	82
Total de palabras:	12,922
Total de caracteres:	73,384
Fecha de entrega:	23-dic.-2022 07:03p. m. (UTC-0500)
Identificador de la entre...	1986295212

DR. GILBERTO CARRIÓN BARCO

DNI: 16720146
Docente asesor

turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Karla Aguirre
Título del ejercicio:	Tesis - UNPRG
Título de la entrega:	Tesis_Turnitinv20
Nombre del archivo:	INFORME_FINAL_V20_para_Turniting.docx
Tamaño del archivo:	2.31M
Total páginas:	82
Total de palabras:	12,922
Total de caracteres:	73,384
Fecha de entrega:	23-dic.-2022 07:03p. m. (UTC-0500)
Identificador de la entre...	1986295212


UNIVERSIDAD NACIONAL

"PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FÍSICAS

Y MATEMÁTICAS (FACFYM)

"DIAGNÓSTICO INTEGRAL DE CIBERSEGURIDAD, BASADO EN ESTANDARES INTERNACIONALES DE SEGURIDAD DE NIST CSF, PARA EL PROGRAMA NACIONAL DE INVERSIONES EN SALUD"

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO EN COMPUTACIÓN E INFORMÁTICA

AUTOR:

Bach. Carla Vivian Aguirre Segura

ASESOR:

Dr. Gilberto Carrión Barco.

LIMA-PERÚ

2022

DR. GILBERTO CARRIÓN BARCO
DNI: 16720146
Docente asesor

ANEXO 01

CONSTANCIA DE VERIFICACIÓN DE ORIGINALIDAD
(RESOLUCIÓN N° 626-2021-CU DEL 30 DE DICIEMBRE 2021)

Yo, GILBERTO CARRIÓN BARCO, usuario revisor del documento titulado: DIAGNÓSTICO INTEGRAL DE CIBERSEGURIDAD, BASADO EN ESTÁNDARES INTERNACIONALES DE SEGURIDAD DE NIST CSF, PARA EL PROGRAMA NACIONAL DE INVERSIONES EN SALUD, Cuyo autor es, CARLA VIVIAN AGUIRRE SEGURA; Identificado con Documento de Identidad 16720146, declaro que la evaluación realizada por el Programa Informático, ha arrojado un porcentaje de similitud de **16 %**, verificable en el Resumen de Reporte automatizado de similitudes que se acompaña.

El suscrito analizó dicho reporte y concluyó que cada una de las coincidencias detectadas dentro del porcentaje de similitud permitido no constituyen plagio y que el documento cumple con la integridad científica y con las normas para el uso de citas y referencias establecidas en los protocolos respectivos.

Se cumple con adjuntar el Recibo Digital a efectos de la trazabilidad respectiva del proceso.

Lambayeque, 23 de diciembre de 2022

DR. GILBERTO CARRIÓN BARCO
DNI: 16720146
Docente asesor

Se adjunta:
*Resumen de Reporte automatizado de similitudes
*Recibo Digital