FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

“MODELO DE CIBERSEGURIDAD PARA LA PREVENCIÓN DE ATAQUES CIBERNÉTICOS EN LA OFICINA DE SEGUROS DE LA DIRIS LIMA NORTE 2020”

Tesis para optar el título profesional de:

Ingeniera de Sistemas Computacionales

Autora:
Maylen Alida Alvines Villegas

Asesor:
Mg. Franchesca Fiorella Rodríguez Rivera

Lima - Perú

2021

DEDICATORIA

Dedico este trabajo a Dios, a mis padres, por ser los pilares de mi vida, por su apoyo y amor incondicional. A mi hermano menor, Moisés, por apoyarme todo el camino y siempre creer en mí.

AGRADECIMIENTO

A las oficinas de seguros DIRIS Lima Norte, en especial al supervisor Jeremy Castellanos por proporcionar toda la información necesaria para la presente tesis.

Tabla de contenidos

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ECUACIONES

RESUMEN

Se realizó un estudio cuyo objetivo fue precisar la influencia y diseñar un modelo de ciberseguridad en la Oficina de seguros de la DIRIS Lima Norte, se aplicó un diseño cuantitativo en el cual participaron 30 operaciones del área de Dirección de Monitoreo y Gestión Sanitaria de la Oficina de seguros de la DIRIS Lima Norte, las cuales fueron observadas en 2 ocasiones; el pre test, previo a la aplicación del modelo de ciberseguridad, para obtener los datos antes de la aplicación; el post test, fue después de la aplicación, para así obtener los datos de la eficiencia del modelo. Se utilizó como instrumento una hoja de observación, validado por 3 expertos. Los resultados evidenciaron El modelo de ciberseguridad previene de ataques cibernéticos a la oficina de seguros de la DIRIS Lima Norte 2020.

Palabras clave: Modelo de ciberseguridad, ciberseguridad, ciberataques, framework

CAPÍTULO I. INTRODUCCIÓN

1.1. Realidad problemática

Contemplando un panorama internacional, Vera (2020) indica que, en los últimos seis meses, durante la pandemia global de COVID-19, la cantidad ciberataques en el sector salud ha ido en aumento, especialmente los utilizando programas: ransomware y técnicas de ingeniería social, como el spear-phishing. IBM Security ha informado de un aumento del 600% en los ciberataques de spear-phishing en 2020, siendo la industria del cuidado de la salud de Estados Unidos el objetivo más común. Beazley, una compañía de seguros global, indicó que el sector salud experimentó el mayor número de ciberataques y violaciones de datos entre todas las industrias en 2019, con más del doble del número de ataques y violaciones de la industria.

Bajo este lineamiento. “Debido a la pandemia, las empresas e instituciones del sector Salud se han vuelto los blancos más buscados por los cibercriminales en toda América Latina. Tienen mucha información privada, que se puede usar para hacer extorsiones. Por ejemplo, los hospitales y clínicas poseen información altamente sensible, como las historias clínicas de pacientes, en donde se encuentran: nombres completos, fechas de nacimiento, DNI, huella digital, dirección, antecedentes clínicos, enfermedades, dolencias, marcadores genéticos, etc. Esta información puede ser vendida a compañías aseguradoras que podrían cambiar las pólizas utilizando esta información confidencial.” (Gestión, 2020).

Aprovechando estas vulnerabilidades, se han desarrollado nuevas formas de obtener acceso no autorizado a redes, programas y datos, comprometiendo de gran manera la

seguridad cibernética. Volviendo al sector salud, como lo comenta el diario Gestión, en uno de los sectores más afectados.

Evaluando el ámbito nacional, Perú no es ajeno a la situación. Según Carreón (2020), en el país es común esperar a ser víctima de un ciberataque, para empezar a plantear medidas y destinar un presupuesto para la ciberseguridad. En otras palabras, tiene que surgir una emergencia o problema para que las instituciones o empresas le presten importancia a este campo. Los expertos enfatizaron que debido a la información sensible y valiosa, uno de los más vulnerables del país a este tipo de ataques es el sector salud.

Según lo previamente mencionado, hoy en día es crítico emplear buenas prácticas para salvaguardar la ciberseguridad de cualquier institución o empresa. Sin embargo, si no se implementan buenas prácticas, el profesional de riesgos puede encontrar beneficioso adoptarlas formalmente o recurrir de manera informal a uno o varios estándares o marcos bien aceptados, que pueden ayudar a asegurar que la gestión de ciberseguridad sea completa y acreditada.

A continuación, se describe la institución donde se ha implementado el proyecto de tesis, la Oficina de seguros de la Dirección de Redes Integradas de Salud – DIRIS Lima Norte, conformando la Red Integrada de Salud (Hospitales y los Establecimientos de salud de primer nivel de atención), es un órgano desconcentrado del Ministerio de Salud; que opera, gestiona y articula los procesos de promoción, prevención, recuperación y rehabilitación en salud. (DIRIS,2020)

La estructura organizacional de la Oficina de seguros de la Dirección de Redes Integradas de Salud – DIRIS Lima Norte, está conformada de la siguiente manera:

Figura 1. Organigrama de la DIRIS Lima Norte

Fuente: Diris Lima Norte (s.f)

El costo de los modelos de ciberseguridad que hay en el mercado, su extensión y complejidad, más el aumento de la carga de trabajo, debido a la pandemia, ha conllevado al descuido de la ciberseguridad en el área de Dirección y Monitoreo de Gestión Sanitaria, ya que no cuentan con un marco de ciberseguridad, estándares o normas robustas, que aseguren la correcta gestión de ciberseguridad. Por ende, se desarrolló el siguiente diagrama de Ishikawa, en el cual se identifican las hipótesis por las que las instituciones del sector salud son vulnerables a ciberataques:

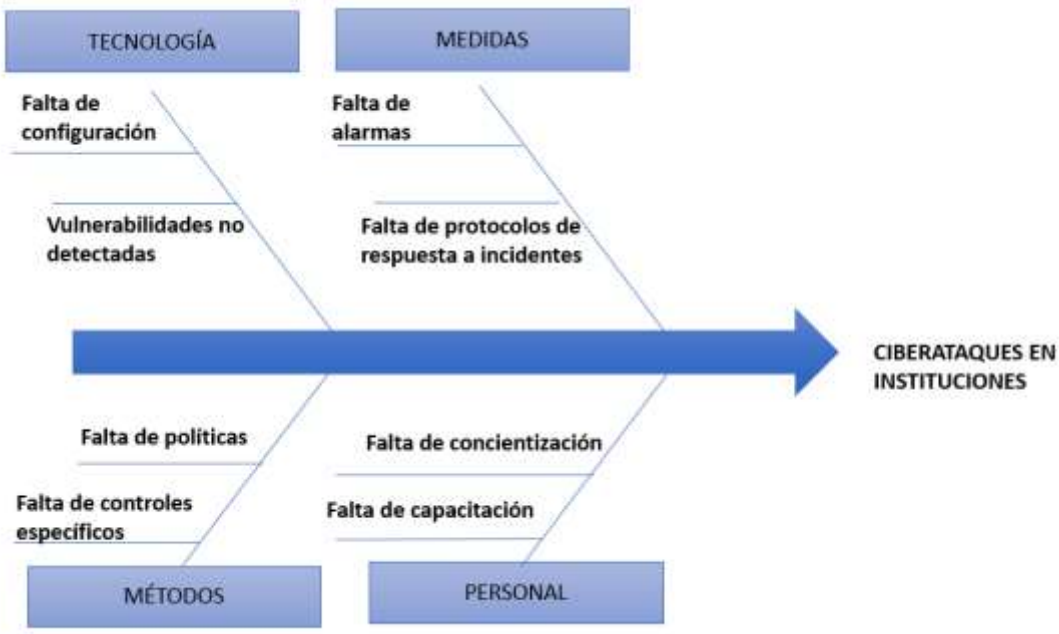

Figura 2. Diagrama de Ishikawa

Fuente: Elaboración propia

En la Figura 2, se presenta el diagrama de Ishikawa donde se describe la realidad problemática de la institución.

El personal debido a la falta de capacitación y concientización sobre el tema de ciberseguridad se toma muy a la ligera la información que manejan.

Se evidencia la falta de controles específicos y políticas dentro del área.

La institución no ha realizado una introspección, identificando sus vulnerabilidades o configuraciones necesarias para mantenerse protegidos.

No se toman las medidas correspondientes ante posibles amenazas, debido a que no se cuenta con alertas, o planes de respuesta, detección y recuperación ante amenazas.

1.2. Antecedentes de la investigación

A nivel nacional se tiene la investigación, Bruderer (2019) desarrolló la tesis: "Diseño de un modelo de ciberseguridad para dispositivos móviles en el sector empresarial", planteó como objetivo general: "Diseñar un modelo de ciberseguridad para dispositivos móviles en el sector empresarial". Su diseño fue experimental de enfoque cuantitativo. La muestra fue el sector empresarial. Concluyó que el modelo reducirá significativamente los riesgos de ciberseguridad asociados a los dispositivos, además permitirá facilitar la implementación del mismo al agrupar de un modo más ordenado los objetivos de los controles y los controles al usar la estructura de los componentes del marco de ciberseguridad de NIST.

En ese sentido, Rivera (2016), presentó la tesis "Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco 2016", planteó como objetivo general: "Conocer de qué manera los riesgos de ciberseguridad tienen consecuencias en la prevención de fraudes en las empresas industriales del distrito de Yanacancha". Su diseño fue experimental de enfoque cuantitativo. La muestra fue de 176 representantes y trabajadores de las empresas industriales del distrito de Yanacancha. Concluyó que la dirección de la ciberseguridad debe realizarse de manera centralizada. El estado debe establecer una agencia responsable de orientar la ciberseguridad nacional y coordinar las entidades públicas y privadas involucradas.

De la misma manera, Inoguchi y Macha (2017) desarrollaron la tesis: "Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las pymes del Perú, 2016", planteó como objetivo general: "Determinar la gestión de la ciberseguridad con la

prevención de los ataques cibernéticos en las PYMES del Perú, 2016.". Su diseño fue experimental de enfoque cuantitativo. La muestra a la empresa Transporte Zavala Cargo S.A.C. Concluyó que la indiferencia de temas como Ciberseguridad da como resultado la falta de apoyo económico al proceso de creación de medidas de seguridad informática dentro de una red privada, provocando así que la organización se exponga a mayores riesgos.

En cuanto a nivel internacional, Aguirre (2017), presentó la tesis: "Ciberseguridad en Infraestructuras Críticas de Información", planteó como objetivo general: "Presentar y analizar estrategias nacionales de ciberseguridad que están aplicando algunos países avanzados en la materia y su relación con las infraestructuras críticas". Su diseño fue experimental de enfoque cuantitativo. Concluyó que el modelo desarrollado representa el primer paso para proteger los servicios críticos de un país. Su aplicación debe integrar múltiples miradas e identificar las interdependencias entre sectores para determinar los impactos directos e indirectos.

De la misma manera Arias y Celis (2015), presentaron la tesis: "Modelo experimental de ciberseguridad y ciberdefensa para Colombia", planteó como objetivo general: "Construir el modelo de referenciación que garantice al estado colombiano parametrizar las condiciones de protección en el ciberespacio como respuesta a los ataques producidos por guerra de la información". Su diseño fue experimental de enfoque cuantitativo. La muestra fue la población de Colombia. Concluyó que El MCCPC, establece los valoradores de acción logística, como resultado de la interpretación analítica de los ejes de referenciación organizacional para controlar y formular procedimientos para la Ciberseguridad y para la Ciberdefensa,

fundamentados en la significancia de la administración moderna (P=planeación, O=organización, D=dirección, E=ejecución, R=revisión o control), significando que para implementar el modelo convencionalmente, el programa debe acercarse como consultor al MINTIC y MINDEFENSA.

Finalmente, Freire (2017), presenta en su tesis: "Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad" como objetivo general: "Realizar un análisis de los tipos y formas de ciberataques que han afectado a las instituciones y estados de América Latina en el siglo XXI.". Su diseño fue descriptivo de enfoque cuantitativo. La muestra fueron las empresas de Ecuador. Concluyó que debido a que los empleados carecen de conocimientos básicos sobre las políticas de seguridad de la red y la empresa no cumple con las políticas de seguridad de la red, se han provocado muchos ataques permanentes a la red.

1.3. Marco teórico

Norma. Según (Karron10, 2013): "Son reglas de conductas que nos imponen un determinado modo de obrar o de abstenernos. Las normas pueden ser establecidas desde el propio individuo que se el auto impone, y en este caso son llamadas normas autónomas, como sucede con las éticas o morales. Así, una persona ayuda a un necesitado porque se lo ordena su propia conciencia, y cuyo castigo también es personal, y está dado por el remordimiento. Una norma es una regla que debe ser respetada y que permite ajustar ciertas conductas o actividades. Las normas se enfocan más en los procesos por los que tienen que pasar los productos y los estándares especifican la calidad con la que debe contar los productos."

Estándar. Según (Karron10, 2013): "Es un conjunto de reglas que deben cumplir los productos, procedimientos o investigaciones que afirmen ser compatibles con el mismo producto. Los estándares ofrecen muchos beneficios, reduciendo las diferencias entre los productos y generando un ambiente de estabilidad, madurez y calidad en beneficio de consumidores e inversores. Los esfuerzos que se están realizando y los ya realizados han perseguido distintos objetivos que van desde la definición de API (Interface de Programación de Aplicaciones), los formatos de los ficheros con la información de parámetros biométricos, la encriptación de la información biométrica, la interacción entre dispositivos biométricos diferentes, etc."

Malware. El malware ("software maligno") se refiere a programas diseñados para infiltrarse computadoras sin el consentimiento de los usuarios e incluye amenazas como virus y programas de rescate. Mientras que las amenazas internas son problemas creados por los errores o acciones deliberadas de staff (por ejemplo, responder a correos electrónicos de phishing, un ataque de ingeniería social para extraer credenciales de acceso o lanzar un ataque de malware, configuraciones de seguridad erróneas, uso indebido de contraseñas, pérdida de ordenadores portátiles y envío de correos electrónicos no cifrados). (Coventry and Branley, 2018)

Ciberseguridad. se refiere a la seguridad del ciberespacio, abarca el paradigma de la CIA ("Confidencialidad", "Integridad" y "Disponibilidad") para las relaciones y los objetos dentro del ciberespacio y amplía ese mismo paradigma de la CIA para abordar

la protección de la privacidad de las entidades jurídicas (personas y empresas), y para abordar la resiliencia. (Nevmerzhitskaya 2018)

Vulnerabilidad. Un fallo o debilidad en un sistema informático, en sus procedimientos de seguridad, en sus controles internos o en su diseño e implementación, que podría ser explotado para violar la política de seguridad del sistema. (Jansen, Winograd and Scarfone, 2021)

Una debilidad en el diseño, implementación, operación o el control interno de un proceso que podría exponer al sistema a las amenazas. (Isaca, 2019)

Amenaza. Cualquier circunstancia o evento con el potencial de dañar un sistema de información a través del acceso no autorizado, la destrucción, la divulgación, la modificación de datos y/o la negación del servicio. Las amenazas surgen de acciones humanas y eventos naturales. (Jansen, Winograd and Scarfone, 2021). De la misma manera NIST, nos indica que se refiere a cualquier circunstancia o evento con el potencial de impactar negativamente en las operaciones de la organización (incluyendo la misión, las funciones, la imagen o la reputación), los activos de la organización o los individuos a través de un sistema de información mediante el acceso no autorizado, la destrucción, la divulgación, la modificación de la información y/o la denegación de servicio. También, el potencial de una fuente de amenaza para explotar con éxito una vulnerabilidad particular del sistema de información.

Ciberataque. Intento de comprometer e inhabilitar las computadoras, hurtar información o utilizar un sistema informático vulnerable para lanzar ataques adicionales; tienen como blanco un recurso, físico o lógico, que tiene una o más vulnerabilidades, las cuales pueden ser explotadas por un cibercriminal; como

resultado del ataque, la confidencialidad, integridad o disponibilidad del recurso se ve comprometida. Los ciberataques pueden ser:

Pasivo: En un ataque pasivo, un atacante obtiene acceso no autorizado a una base de datos privada para comprobar o escuchar su transmisión sin alteraciones.

Activo: Durante este tipo de ataques, un usuario no autorizado puede cambiar los datos o puede introducir datos erróneos en la red del hogar inteligente. Esto puede lograrse mediante la modificación de los datos transmitidos o guardados o mediante la inserción de nuevos flujos de datos en la red del hogar inteligente

Su origen puede ser:

Interno: Iniciado desde el interior del perímetro de seguridad de una organización, como una persona que tiene acceso autorizado a datos confidenciales que roba datos.

Externo: Lanzado desde fuera del límite de seguridad como un ataque distribuido de denegación de servicio (ataque DDoS) impulsado por una botnet.

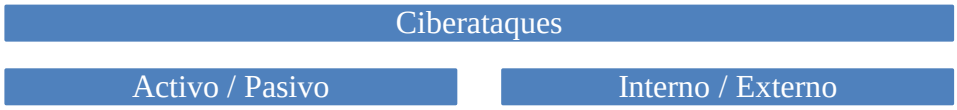

Figura 3. Tipos de ciberataques

Fuente: Elaboración propia

Cibercriminales. Motivados por el deseo de obtener beneficios económicos, estos individuos están involucrados en transacciones financieras fraudulentas. (Isaca, 2019). Cabe resaltar que Trend Micro (s.f) indica que son individuos o equipos de personas que utilizan la tecnología para cometer actividades maliciosas en sistemas o redes digitales con la intención de robar información sensible de la empresa o datos personales, y generar beneficios.

Riesgo. La combinación de la probabilidad de un evento y su consecuencia. El riesgo se mitiga a través del uso de controles o salvaguardas. (Isaca, 2019). Según NIST (s.f), se puede definir como la medida del grado en que una entidad se ve amenazada por una circunstancia o evento potencial, y suele ser una función de: (i) los impactos adversos que surgirían si la circunstancia o el evento ocurren; y (ii) la probabilidad de que ocurran.

Integridad. Propiedad que indica que algo está completamente libre de errores. (ISO,s.f). De la misma manera NIST (s.f) define el término "integridad" como la protección contra la modificación o destrucción indebida de la información, e incluye la garantía de no repudio y autenticidad de la información. Por último, Isaca (s.f) señala que el termino protección se refiere contra la modificación o destrucción indebida de la información, e incluye la garantía de no repudio y autenticidad de la información.

Confidencialidad. Propiedad de la información que puede ser accesada o compartida, solo por determinadas personas, entidades o procesos. (ISO,s.f). Según Isaca (s.f), se el término se define como la preservación de las restricciones autorizadas de acceso y divulgación, incluidos los medios para proteger la privacidad y la información de propiedad. Finalmente NIST (s.f), indica que la propiedad se encarga de que los datos o la información no se pongan a disposición o se revelen a personas o procesos no autorizados.

Norma ISO/IEC 27001. Según la OIN (Organización Internacional de Normalización) es una norma para salvaguardar la seguridad informática. Fue publicada el 15 de octubre de 2005 por la ISO, con base en la norma británica BS7799-2:2002, el estándar internacional ISO/IEC 27001:2005.

Pertenece a la serie "270xx", que consiste en un conjunto de estándares formulados o en desarrollo por ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional).

A continuación se muestra la cronología de ISO-27001:

Figura 4: Cronología de la ISO 27001
Fuente: Acevedo (2011)

i. Alcance de la ISO 27001

La política de seguridad de la información según ISO 27001: 2013 debe aplicarse a todos los activos de información. Estas políticas también se aplicarán a todos los empleados, consultores, contratistas, temporales o terceros que accedan a los activos de información. Los consultores, contratistas o terceros cumplirán requisitos de seguridad similares a los de los empleados.

Los empleados, contratistas, temporales o terceros estarán obligados a continuar protegiendo la información y cumplir con la política de seguridad incluso después de terminar la relación con la organización. (Estructura recomendada para el Documento De Políticas De Seguridad De La Información ISO 27001:2013, 2018).

ii. Propósito de la ISO 27001

Según (Estructura recomendada para el Documento De Políticas De Seguridad De La Información ISO 27001:2013, 2018), el propósito de la política de seguridad de la

información ISO 27001 debe ser proteger los activos de información de amenazas internas o externas, ya sean Intencional, natural o accidental. De la misma manera:

1. La **confidencialidad** debe prevalecer en la información, de modo que solo los usuarios que cuenten con autorización puedan acceder.
2. La **integridad** de la información para evitar alteraciones no autorizadas.
3. La **disponibilidad** de información para asegurar su existencia en todo momento a los usuarios debidamente autorizados, otorgándoles una respuesta en un plazo de tiempo razonable.
4. **Cumplimiento** con respecto a las regulaciones y leyes.
5. **Capacitación** a todos los empleados sobre cuestiones de seguridad de la información.
6. **Cumplir** con las obligaciones contractuales con los clientes y proveedores.

iii. Flujo

De acuerdo con Villa (2019), su implementación se basa en el ciclo PDCA y establece las siguientes fases:

• Fase de planificación (Plan): establecimiento de SGSI En esta etapa, se deben definir y establecer estrategias, objetivos, procesos y procedimientos de seguridad relevantes para gestionar los riesgos y mejorar la seguridad de la información con el fin de entregar resultados de acuerdo con la estrategia y los objetivos generales de la organización.

• Fase de implementación (Do): Implementación y operación del SGSI: En esta etapa, se deben implementar y operar las políticas, los controles, los procesos y los procedimientos del SGSI.

• Fase de verificación (Check): seguimiento y revisión del SGSI En esta etapa, el desempeño del proceso debe ser evaluado y medido de acuerdo con la estrategia y los objetivos de seguridad y la experiencia práctica, y los resultados deben ser reportados a la gerencia.

• Fase de actuación (Act): Mantenimiento y mejora continua del SGSI En esta etapa, se deben tomar medidas correctivas y preventivas basadas en los resultados de la auditoría interna y la revisión por la dirección del SGSI.

A continuación se detalla el flujo de procesos de la ISO 27001.

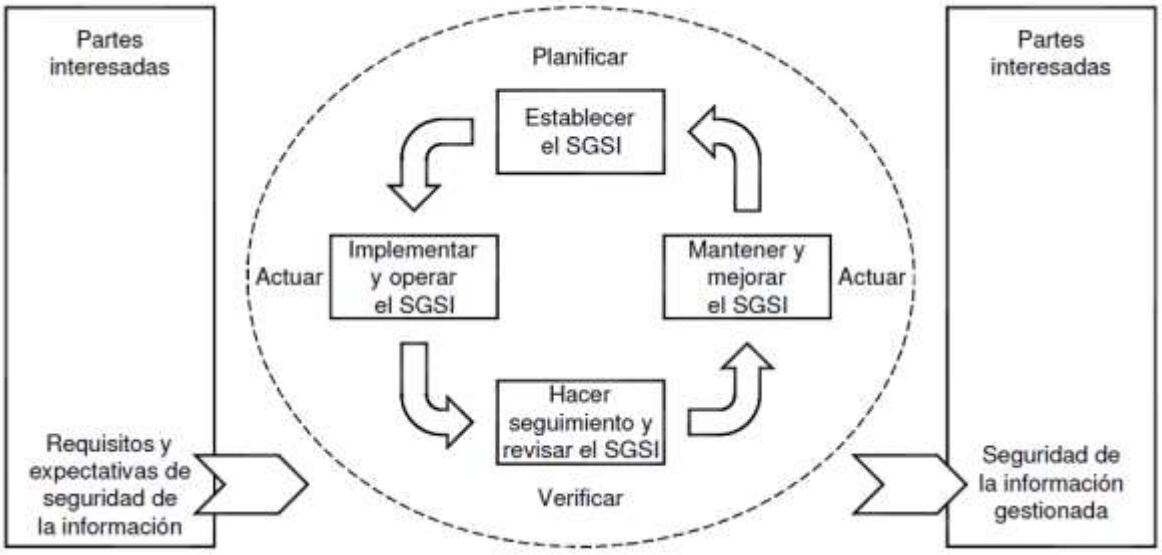

Figura 5: Diagrama de Flujo de Procesos ISO 27001
Fuente: ISO/IEC 27001. 2013

Además, la norma cuenta con un anexo técnico, el cual contiene 114 medidas de control que se deben implementar, las cuales se dividen en las siguientes áreas:

• Política de seguridad de la información: A. 5.

• Organización de seguridad de la información: A.6.

• Seguridad de los recursos humanos: A. 7.

• Gestión de activos: A.8. • Control de acceso: A.9.

• Criptografía-cifrado y gestión de claves: A.10.

• Seguridad física y ambiental: A.11.

• Seguridad operativa: A.12.

• Seguridad de las comunicaciones: A.13.

• Adquisición, desarrollo y mantenimiento de sistemas: A.14.

• Gestión de incidentes de seguridad de la información A.16.

• Cumplimiento: A.18.

NIST SP 800-30 Nació en el seno del National Institute of Standard Technology (Instituto Nacional de Estándares y Tecnología), agencia federal fundada en 1901 para la Administración de Tecnología de Departamento de Comercio de los Estados Unidos. El propósito de la Publicación Especial 800-30 es proporcionar orientación para la realización de evaluaciones de riesgos de los sistemas y organizaciones federales de información, ampliando la orientación de la publicación especial 800-39. (NIST, 2012)

i. Objetivos

Aseguramiento de los sistemas de Información que almacenan, procesan y transmiten información.

Gestión de Riesgos

Optimizar la administración de Riesgos a partir del resultado en el análisis de riesgos.

Proteger las habilidades de la organización para alcanzar su misión (no solamente relacionada a la IT, sino de toda la empresa)

Ser una función esencial de la administración (no solo limitada a funciones técnicas de IT)

ii. Fases

Según Tejena (2018), la metodología NIST SP 800: 30 consta de nueve etapas: caracterización del sistema, que puede determinar el alcance y los límites operativos de la evaluación de riesgos de una empresa; identificar amenazas es donde se define la motivación de las amenazas; identificar vulnerabilidades, donde La etapa enumerará los defectos o debilidades del sistema que pueden ser utilizados por las amenazas. Análisis de control; determinar la probabilidad; análisis de impacto; etapa de determinación de riesgos, que ayuda a evaluar los riesgos en el sistema de información, brinda recomendaciones de control y proporciona controles que pueden mitigar los riesgos identificados Medidas para reducir el riesgo a un nivel aceptable, y finalmente entregar un documento de resultado, generar una descripción de amenazas y vulnerabilidades, medir el riesgo y proponer la implementación de medidas de control..

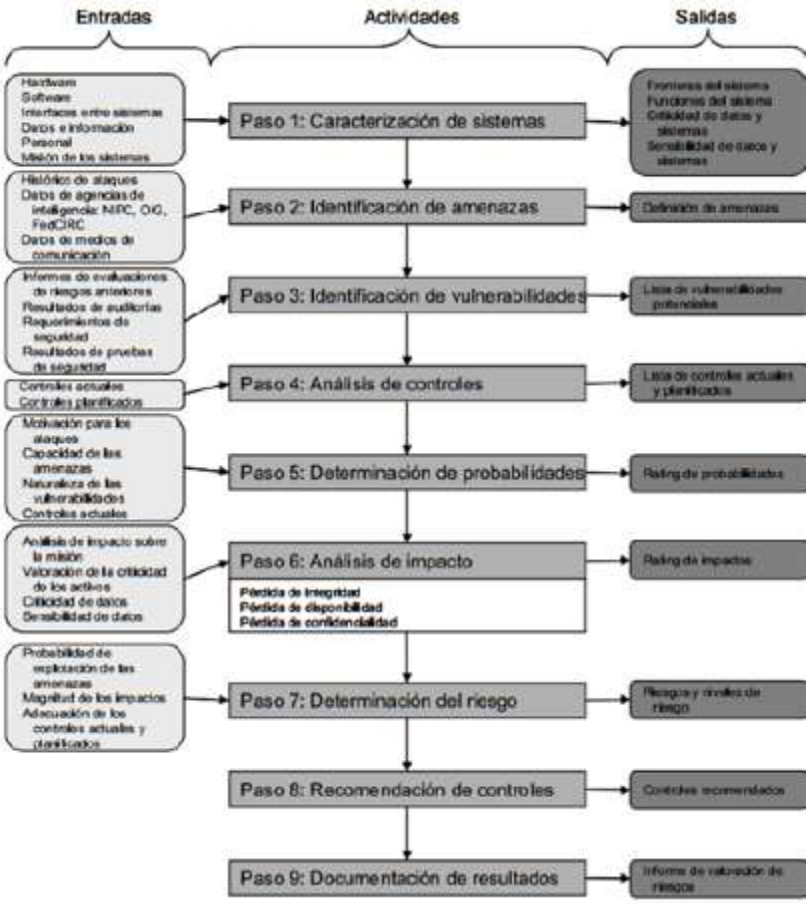

Figura 6. Descripción fases NIST 800

Fuente: NIST 800 (2006)

1.4. Formulación del problema

¿En qué medida el modelo de ciberseguridad previene de ataques cibernéticos a la oficina de seguros de la DIRIS Lima Norte 2020?.

1.5. Objetivos

1.5.1. Objetivo general

Determinar en qué medida el modelo de ciberseguridad previene de ataques cibernéticos a la oficina de seguros de la DIRIS Lima Norte 2020.

1.5.2. Objetivos específicos

Determinar en qué medida el modelo de ciberseguridad implementa políticas de control y de accesos en la oficina de seguros de la DIRIS Lima Norte 2020.

Determinar en qué medida el modelo de ciberseguridad implementa políticas de privacidad y confidencialidad en la oficina de seguros de la DIRIS Lima Norte 2020.

Determinar en qué medida el modelo de ciberseguridad implementa políticas de disponibilidad en la oficina de seguros de la DIRIS Lima Norte 2020.

1.6. Hipótesis

1.6.1. Hipótesis general

El modelo de ciberseguridad previene de ataques cibernéticos a la oficina de seguros de la DIRIS Lima Norte 2020.

1.6.2. Hipótesis específicas

El modelo de ciberseguridad implementa eficientemente políticas de control y de accesos en la oficina de seguros de la DIRIS Lima Norte 2020

El modelo de ciberseguridad implementa eficientemente políticas de privacidad y confidencialidad en la oficina de seguros de la DIRIS Lima Norte 2020.

El modelo de ciberseguridad implementa eficientemente políticas de disponibilidad en la oficina de seguros de la DIRIS Lima Norte 2020.

1.7. Variables

Prevención de ataques cibernéticos.

Medidas o controles que permiten evitar por completo los impactos negativos y los daños resultantes. Entran en vigor antes de, garantizando de antemano que no ocurra un evento adverso o se produzca un evento no deseado. (Lagos, 2019)

Acción de impulsar la implantación de la normativa sobre la protección de infraestructuras críticas y de las capacidades necesarias para la protección de los servicios esenciales. (Presidencia del Gobierno de España,2013).

Modelo de ciberseguridad.

Un marco es un diseño que tiene en cuenta los puntos comunes y las variabilidades de un dominio de aplicación específico. Proporciona la aplicación de los elementos comunes listos para su uso y localiza la variabilidad en puntos de variación abstractos predefinidos. Los marcos son más complejos y abstractos que los programas habituales, y están activos. Incorporan un flujo de control que interconecta sus elementos y llama a las partes específicas de la aplicación (que, a su vez, pueden llamarla de nuevo). Los elementos de los marcos no son reutilizables individualmente, sino como un todo, y las dependencias entre ellos pueden ser indirectas y ofuscar la arquitectura. En consecuencia, los marcos suelen ser difíciles de comprender y de reutilizar, especialmente por primera vez. (Lopes et al. 2009)

1.8. Justificación

En conclusión, la mayoría de las organizaciones no escatiman en gastos sobre los recursos adecuados para mitigar riesgos para proteger la información privada del paciente e institución. Por ello, se propone como proyecto de fin de carrera desarrollar e implementar un modelo de ciberseguridad enfocado en la seguridad de la información y basado en los controles de la ISO27001 y normas complementarias de NIST SP 800-30 y OSSTMM 3, con la finalidad de prevenir ataques cibernéticos en la oficina de seguros de la DIRIS Lima Norte 2020.

CAPÍTULO II. METODOLOGÍA

2.1. Tipo de investigación

El tipo de investigación es aplicada porque involucra el uso de computadoras, datos estadísticos y herramientas matemáticas para obtener resultados. Es concluyente en su propósito ya que trata de cuantificar el problema y entender qué tan generalizado está mediante la búsqueda de resultados proyectables a una población mayor. (Monje Alvarez, 2011)

El diseño de investigación es experimental, el tipo de diseño es preexperimental, debido a que es el procedimiento más indicado para analizar una variable.

$$G \quad O1 \quad X \quad O2$$

Ecuación 1. Fórmula Pre Experimental

Donde, según Baptista, Fernández y Hernández (2014),:

G: Oficina de Seguros DIRIS Lima Norte

X: Aplicación del modelo de ciberseguridad

O1: Cantidad de ciberataques antes de aplicar el modelo de ciberseguridad

O2: Cantidad de ciberataques después de aplicar el modelo de ciberseguridad

2.2. Población y muestra (Materiales, instrumentos y métodos)

Unidad de estudio

La unidad de estudio para la presente investigación son las operaciones realizadas por la empresa del área de TI del sector salud de la Oficina de seguros de la DIRIS Lima Norte.

Población

De acuerdo con Baptista, Fernández y Hernández (2014), "Un estudio no será mejor por tener una población más grande; la calidad de un trabajo investigativo estriba en delimitar claramente la población con base en el planteamiento del problema." (p.174).

Por este motivo, se determinó como población todas las operaciones realizadas en el 2020 en el área Dirección de Monitoreo y Gestión Sanitaria de la Oficina de seguros de la DIRIS Lima Norte, la cual cuenta con aproximadamente 100 operaciones al mes.

Muestra

Debido al tipo de investigación, se escogió el tipo de muestra probabilístico de tipo aleatorio simple, ya que según López (2004), es el método más recomendable para una investigación cuantitativa porque todos los componentes de la población tienen la misma posibilidad de ser seleccionados para la muestra.

La muestra seleccionada, es la cantidad de operaciones realizadas entre el mes de julio y diciembre en el área de Dirección de Monitoreo y Gestión Sanitaria de la Oficina de seguros de la DIRIS Lima Norte.

En el proceso de recolección de datos, se utilizará la encuesta de ciberseguridad (Anexo 1) como herramienta de recolección de datos, que se realizará en octubre de 2020.

Vara (2012) mencionó que para la investigación cuantitativa, el tamaño de la muestra se calcula mediante la siguiente fórmula estadística. (p.227).

$$n = \frac{(z)^2 * p * q * N}{(e)^2 * (N-1) + (z)^2 * p * q}$$

Ecuación 2: Fórmula para obtener la muestra

N = tamaño de la población.

z = nivel de confianza.

p = proporción.

q = porcentaje complementario (1-p).

e = margen de error.

n = tamaño de la muestra.

Para la presente investigación, se considera que un 99% como nivel de confianza, por lo que de acuerdo la siguiente tabla, el coeficiente Z será igual a 1.96.

Nivel de confianza	Z_{alfa}
99.7%	3
99%	2,58
98%	2,33
96%	2,05
95%	1,96
90%	1,645
80%	1,28
50%	0,674

Figura 7. Nivel de confianza

Fuente: Pedro Morales Vallejo (2012)

Para la proporción se tomará 50% y para el porcentaje complementario, el otro 50%

El tamaño de la población es de 100 y el margen de error se tomará como un 15%.

Aplicando la ecuación, el tamaño de la muestra es de 30 operaciones

2.3. Técnicas e instrumentos de recolección y análisis de datos

Tabla 1
Técnicas de recolección de datos

Variables	Indicadores	Instrumentos
Prevención de ataques de ciberseguridad (variable dependiente)	Número de controles de seguridad de información de control y de accesos implementadas	Ficha de observación
	Número de controles de seguridad de información de privacidad y confidencialidad implementadas	
	Número de controles de seguridad de información de disponibilidad implementadas	

Modelo de ciberseguridad (variable independiente)	Número de controles de seguridad de información implementadas	Ficha de observación

Fuente: Elaboración propia

Análisis

Según el enfoque de investigación, se utilizará el análisis estadístico, que establecerá patrones de comportamiento y probar teorías. (Hernández, Fernández y Baptista ,2006, p. 4).

Aspectos éticos

Con respecto a los aspectos éticos, la presente investigación defiende la propiedad intelectual de los autores, citándolos según el formato APA y precisando las fuentes bibliográficas; con respecto a la confidencialidad de información, la cual corresponde a la gestión de la organización, se tendrán las autorizaciones respectivas, para su exhibición o publicación en los medios digitales correspondientes, como lo es el caso del repositorio institucional académico.

Validez

Según, Hernandez Sampieri, (2014) La evidencia sobre la validez del contenido se obtiene mediante las opiniones de expertos en donde se asegura de que las dimensiones medidas por el instrumento sean representativas del universo o dominio de dimensiones de las variables de interés. (pág. 298).

Las validaciones de los 3 expertos correspondientes se encuentran en el ANEXO B.

Confiabilidad

Según, Hernandez Sampieri, (2014) indica que La confiabilidad de un instrumento de medición se refiere al grado en que su aplicación repetida al mismo individuo u objeto produce resultados iguales. (p.200).

Según Valderrama, Vallejo (2013), define que "un instrumento es confiable o fiable si produce resultados consistentes cuando se aplica en diferentes ocasiones […], se evalúa administrando el instrumento a una misma muestra de sujetos, ya sea en dos ocasiones diferentes o por dos o más observadores diferentes". (p.30).

Según Navas (2012) menciona el método Test – Pretest que el coeficiente de fiabilidad de la prueba se ha definido como la correlación de las puntuaciones de la prueba consigo mismo. Por tanto, una forma posible de obtener una estimación.

Medición de la normalidad:

Shapiro Wilk es una de las pruebas más sencillas y potentes, la cual indica si la variable presenta una distribución normal o no. La condición para realizar esta prueba es que la muestra sea igual o menor a 50 (Segnini, s.f.).

Debido a que se realizó un piloto aplicando la ficha de observación a 10 operaciones de la DIRIS Lima Norte, se realizó la prueba de normalidad de Shapiro Wilk.

Indicador 1: Número de controles de seguridad de información de control y de accesos implementadas

Tabla 2
Normalidad del indicador Número de controles de seguridad de información de control y de accesos implementadas

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
P_PreTest	,514	15	,000	,413	15	,000
P_PosTest	,514	15	,000	,413	15	,000

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia realizada con el Software SPSS.

Según la tabla N°2 el nivel de sig. Es 0.000, menor a 0.05. Se determina que la prueba no obedece a parámetros normales

Indicador 2: Número de controles de seguridad de información de privacidad y confidencialidad implementadas

Tabla 3
Normalidad del indicador Número de controles de seguridad de información de privacidad y confidencialidad implementadas

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
IC__PreTest	,535	15	,000	,284	15	,000
IC_PosTest	,535	15	,000	,284	15	,000

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia realizada con el Software SPSS.

Según la tabla N°3 el nivel de sig. Es 0.000, menor a 0.05. Se determina que la prueba no obedece a parámetros normales

Indicador 3: Número de controles de seguridad de información de disponibilidad implementadas

Tabla 4
Normalidad del indicador Número de controles de seguridad de información de disponibilidad implementadas

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PR_PreTest	,535	15	,000	,284	15	,000
PR_PosTest	,535	15	,000	,284	15	,000

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia realizada con el Software SPSS.

Según la tabla N°4 el nivel de sig. Es 0.000, menor a 0.05. Se determina que la prueba no obedece a parámetros normales

Al analizar el nivel de, se evidencia que los valores son menores a 0.05, por lo tanto se afirma que los datos tienen distribución no normal, por ende para poder medir la confiabilidad se aplica Spearman.

Medición de confiabilidad

Según Hernández, Fernández y Baptista (2017), creen que ninguna herramienta es útil sin antes evaluar y confirmar su confiabilidad. Por lo tanto, el instrumento debe presentarse antes de la medición diseñada para determinar su confiabilidad a fin de obtener los atributos de puntaje que demuestren la factibilidad de la prueba (pág.85).

Según Hernández Sampieri (2014), para poder estimar la confiabilidad de un instrumento, se requiere aplicarlo a una muestra y calcular este factor de acuerdo con los resultados. (pág.208).

Dados los resultados anteriores, para poder medir la confiabilidad en el instrumento de recolección de datos se realizó la prueba de Spearman.

Cabe resaltar que el coeficiente rho de Spearman se interpreta de la siguiente manera:

Tabla 5
Interpretación del coeficiente rho de Spearman, según rango de valores

Coeficiente	Interpretación
0	Relación nula
0 -0,2	Relación muy baja
0,2 – 0,4	Relación baja
0,4 – 0,6	Relación moderada
0,6 – 0,8	Relación alta
0,8 – 1	Relación muy alta
1	Relación perfecta

Fuente: Elaboración propia realizada con el Software SPSS.

Indicador 1: Número de controles de seguridad de información de control y de accesos implementadas.

Ilustración 6

Tabla 6
Confiabilidad del indicador Número de controles de seguridad de información de control y de accesos implementadas

.

			P_PreTest	P_PosTest
Rho de Spearman	P_PreTest	Coeficiente de correlación	1,000	1,000**
		Sig. (bilateral)	.	.
		N	15	15
	P_PosTest	Coeficiente de correlación	1,000**	1,000
		Sig. (bilateral)	.	.
		N	15	15

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia realizada con el Software SPSS.

Se visualiza que la correlación es 1.0, según la Tabla N° 5, la relación es perfecta.

Indicador 2: Número de controles de seguridad de información de privacidad y confidencialidad implementadas

Tabla 7
Confiabilidad del indicador Número de controles de seguridad de información de privacidad y confidencialidad implementadas

Correlaciones

			IC__PreTest	IC_PosTest
Rho de Spearman	IC__PreTest	Coeficiente de correlación	1,000	1,000**
		Sig. (bilateral)	.	.
		N	15	15
	IC_PosTest	Coeficiente de correlación	1,000**	1,000
		Sig. (bilateral)	.	.
		N	15	15

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia realizada con el Software SPSS.

Se visualiza que la correlación es 1.0, según la Tabla N° 5, la relación es perfecta.

Indicador 3: Número de controles de seguridad de información de disponibilidad implementadas

Tabla 8
Confiabilidad del indicador Número de controles de seguridad de información de disponibilidad implementadas

Correlaciones

			PR_PreTest	PR_PosTest
Rho de Spearman	PR_PreTest	Coeficiente de correlación	1,000	1,000**
		Sig. (bilateral)	.	.
		N	15	15
	PR_PosTest	Coeficiente de correlación	1,000**	1,000
		Sig. (bilateral)	.	.
		N	15	15

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia realizada con el Software SPSS.

Se visualiza que la correlación es 1.0, según la Tabla N° 5, la relación es perfecta.

Para la presente investigación el nivel de confiabilidad es perfecto para las tres dimensiones, la dimensión Integridad cuenta con 1.0, la dimensión Confidencialidad 1,0, finalmente Disponibilidad 1.0, contando finalmente con un alto nivel de confiabilidad.

2.4. Procedimiento

El presente proyecto se desarrolló de la siguiente manera:

Inicialmente, se determinó el modelo de ciberseguridad a implementar, tomando en cuenta que sea sencillo, completo y práctico de implementar.

Se sabe que, a nivel mundial, existen diversos marcos de ciberseguridad, estándares y normas, los cuales sirven de referencia para llevar a cabo la correcta gestión de la ciberseguridad, empleando buenas prácticas en el gobierno de tecnología de información. Estos se encuentran basado en diversas políticas y normas.

Por este motivo se hace referencia a los marcos y/o normas internacionales que guarden relación y apoyen a salvaguardar la seguridad de la información. Bajo esta premisa, se decidió enfocar el modelo de ciberseguridad en la seguridad de la información y basado en los controles de la ISO27001 y normas complementarias de NIST SP 800-30 y OSSTMM 3 Según el estudio realizado por Lara y Corella (2018), están basadas en la gestión de riesgos, orientadas a procesos, se pueden aplicar a diferentes empresas y brindan la metodología sobre cómo implementar la seguridad de la información en una organización.

Indicador	OSSTMM 3	NIST	COBIT 5	ISO 27001
Recursos y métodos para la implementación	No	Suministra documentación para desarrollar metodologías de implementación	Proporciona documentación para desarrollar metodologías de implementación	Provee metodologías de implementación
Está orientado a procesos	Se orienta en proveer procedimientos de pruebas para verificar la seguridad del sistema	Si	Si	Si
Ejecuta la seguridad que está basada en gestión de riesgos	No	El propósito principal de la norma es la seguridad	Adopta una gestión de riesgos que definen qué controles de seguridad deben aplicarse	El propósito principal de la norma es la seguridad
Se puede aplicar a diferentes empresas	Si	Está orientada a empresas de los Estados Unidos	No es un framework oficial de soluciones globales	Se emplea en cualquier tipo de empresa y de cualquier tamaño
Objetivos claramente definidos	Si	Requiere de información previa para definir los objetivos	Si	Requiere de información previa para definir los objetivos
Estructura de gestión claramente definida	No	No	Si	No
Cobertura de los controles	No	Se enfoca en la seguridad de los equipos de cómputo.	Enfoca el control en las tecnologías de la información	Tiene controles de seguridad para cada proceso de implementación
Utiliza certificados	No	Sólo en Estados Unidos	Si	Si

Figura 8. Tabla comparativa entre frameworks

Fuente: Lara y Corella (2018)

Estos tres modelos van a ayudar en el avance del Modelo de Seguridad de la Información de la DIRIS Lima Norte. ISO 27001 brindará la metodología para desarrollar el modelo, OSSPMMv3 proporcionará las directivas para hacer las pruebas que aseguren la seguridad de la red de información, y por último, NIST 800-30 va a servir de guía para el desarrollo de medidas de administración de peligros en la red de información.

Hay que tomar en cuenta que los estándares fueron creados para diferentes necesidades o propósitos, por lo que, no siempre pueden encajar el uno con el otro. El reto se encuentra en saber que partes de cada estándar o modelo se puede utilizar en determinada institución en particular, para ayudar a cumplir sus objetivos institucionales.

El modelo de ciberseguridad propuesto cuenta con la siguiente estructura:

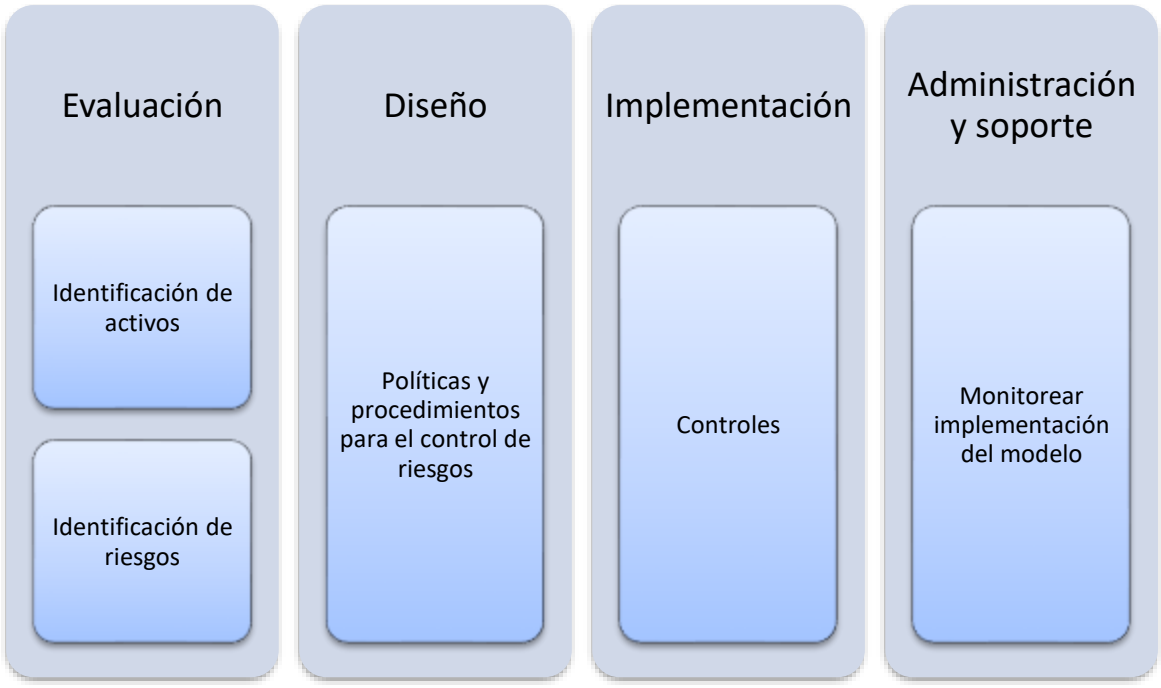

Figura 9. Estructura de modelo de ciberseguridad

Fuente: Elaboración propia

Etapa de Evaluación

Nos indica cuál es la situación actual de la institución. Deriva de la norma ISO 27001, tomándose en cuenta, además, las recomendaciones de la norma NIST 800 y del manual OSSTMM versión 3. Esta compuesta por los siguientes apartados:

- Identificación de activos

Un activo necesita protección para asegurar las correctas operaciones y continuidad de la institución. Se define como un bien con valor o utilidad para la organización, sus operaciones y continuidad. El conservar una adecuada protección de los activos de la empresa, se debe principalmente a mantener la gestión apropiada de los activos. (Peltier, 2010) Cada activo debe estar identificado y valorado apropiadamente.

- Identificación de riesgos

Las vulnerabilidades halladas mediante las hojas de observación se detallan en este apartado.

Etapa de Diseño

Deriva de la norma ISO 27001, tomándose en cuenta, además, las recomendaciones de la norma NIST 800 y del manual OSSTMM versión 3. Señala en dónde debemos estar.

Esta compuesta por los siguientes apartados:

- Organización de la seguridad de la información
- Gestión de incidentes en la seguridad de la información
- Seguridad en redes y telecomunicaciones
- Seguridad física
- Plan de contingencia y continuidad
- Control de accesos
- Seguridad del recurso humano

- Cumplimiento de regulaciones
- Protección de la información

Etapa de Implementación

Especifica cómo desde nuestra posición actual podemos llegar a donde necesitamos. Deriva de la norma ISO 27001, tomándose en cuenta, además, las recomendaciones de la norma NIST 800 y del manual OSSTMM versión 3.

Esta compuesta por los siguientes apartados:

- Controles lógicos
- Controles de red
- Controles de seguridad de aplicaciones
- Controles de seguridad física
- Controles acceso físico a los equipos
- Controles de protección contra software malicioso
- Controles de Gestión de la Seguridad de Red
- Controles en el uso de los Servicios de Red
- Controles de Seguridad de la Red Inalámbrica

Etapa de Administración y Soporte

Indica cómo nos mantenemos y mejoramos.

Para más detalle, revisar el Anexo 5.

i. Una vez realizada la selección, se planteó y determinó una guía de documentos, procesos y tareas a implementar para cumplir con dicho marco.

ii. Al mismo tiempo se realizó la elaboración del instrumento de recolección de datos. La conclusión es que cada indicador se puede evaluar a través del cuestionario (ver Anexo 5), según García (2003), este indicador es una herramienta de recolección de datos muy útil, especialmente aquellos de difícil acceso por distancia o distancia. Cabe resaltar que el instrumento fue validado por el juicio experto de los ingenieros: Miguel Lévano, Rolando Heli Moreno y Julio César Vidal Rischmoller, mediante un documento de validación de instrumento (ver Anexo nro. 6). En el cual se verifica que las variables tengan relación con sus dimensiones correspondientes.

iii. Luego de tener los datos con la situación actual de la empresa, se procedió con el análisis respectivo. Al analizar, se encontraron actividades por mejorar, procesos a optimizar, roles por asignar, y otros que influyeron en la propuesta del nuevo método de trabajo. Teniendo la propuesta de mejora, se informaron los cambios, que, según el marco de ciberseguridad, estándar o norma elegida, se debe aplicar. Se realizó un seguimiento constante al funcionamiento.

iv. Finalmente, se compararon los datos obtenidos con la estrategia inicial y con la nueva, para evaluar el impacto que se ha tenido sobre la gestión de ciberseguridad, de la misma manera se efectuaron pruebas estadísticas para validar si aceptaban las hipótesis de relación e influencia entre las variables de investigación.

CAPÍTULO III. RESULTADOS

3.1. Análisis Descriptivo

Análisis descriptivo del indicador Número de controles de seguridad de información de control y de accesos implementados.

Tabla 9
Frecuencia del indicador Número de controles de seguridad de información de control y de accesos implementados

Informe

	P_PreTest	P_PosTest
Media	3,13	,07
N	30	30
Desviación estándar	,346	,254
Mínimo	3	0
Máximo	4	1

Fuente: Elaboración propia realizada con el Software SPSS.

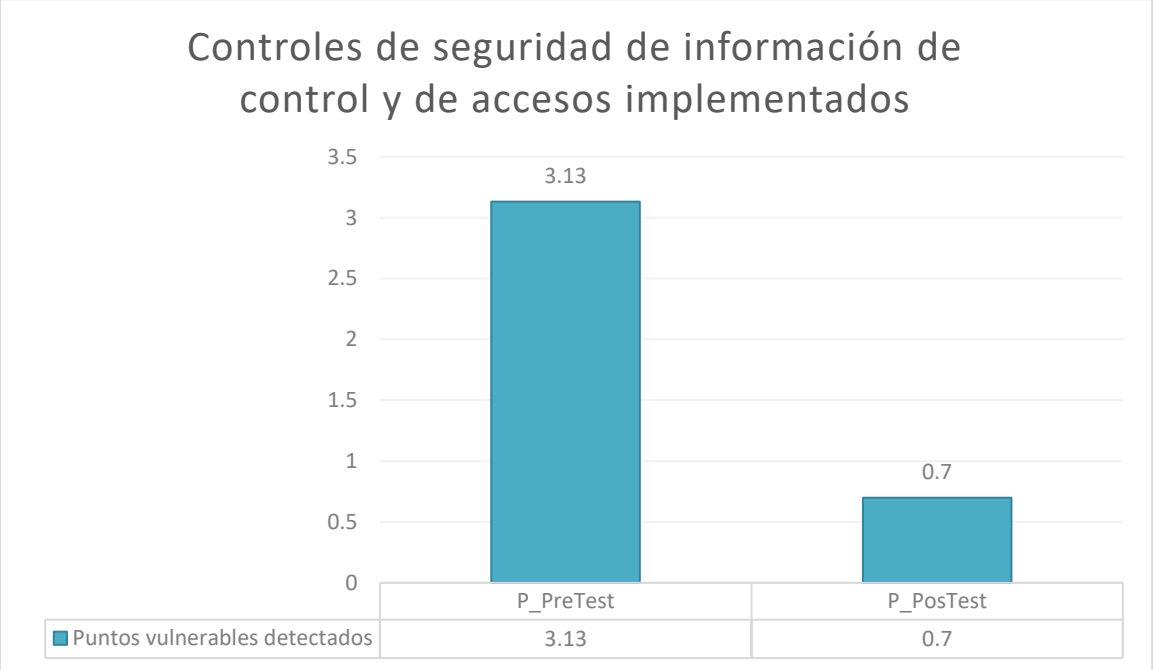

Figura 10. Histograma Pretest y Post Test del indicador Número de controles de seguridad de información de control y de accesos implementados

Fuente: Elaboración propia realizada con Word.

De acuerdo con los resultados mostrados en la tabla N° 9 y figura N° 9, para el indicador Número de puntos vulnerables detectados, en el pretest se obtuvo un valor en la media de 3.13% y para el post test fue de 0.7%. Con estos resultados se puede ver que hubo un decremento de 2.43%.

Análisis descriptivo del indicador Número de controles de seguridad de información de privacidad y confidencialidad implementados

Tabla 10
Frecuencia del indicador Número de controles de seguridad de información de privacidad y confidencialidad implementados

Informe

	IC_PreTest	IC_PosTest
Media	5,93	,33
N	30	30
Desviación estándar	,254	,479
Mínimo	5	0
Máximo	6	1

Fuente: Elaboración propia realizada con el Software SPSS.

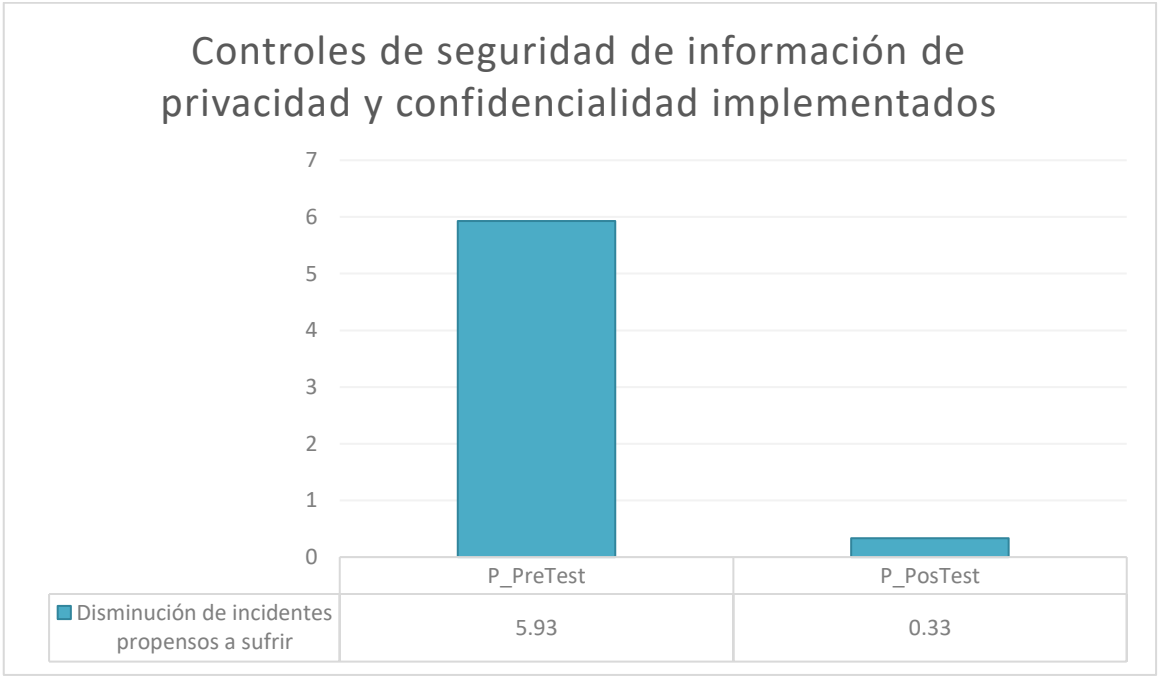

Figura 11. Histograma Pretest y Post Test del indicador Número de controles de seguridad de información de privacidad y confidencialidad implementados

Fuente: Elaboración propia realizada con el Software SPSS.

De acuerdo con los resultados mostrados en la tabla N° 10 y figura N° 12, para el indicador Número de amenazas propensos, en el pretest se obtuvo un valor en la media de 5.93% y para el post test fue de 0.33%. Con estos resultados se puede ver que hubo un decremento de 5.6%.

Análisis descriptivo del indicador Número de controles de seguridad de información de disponibilidad implementadas

Tabla 11
Frecuencia del indicador Número de controles de seguridad de información de disponibilidad implementadas

Informe

	PR_PreTest	PR_PosTest
Media	6,87	,10
N	30	30
Desviación estándar	,346	,305
Mínimo	6	0
Máximo	7	1

Fuente: Elaboración propia realizada con el Software SPSS.

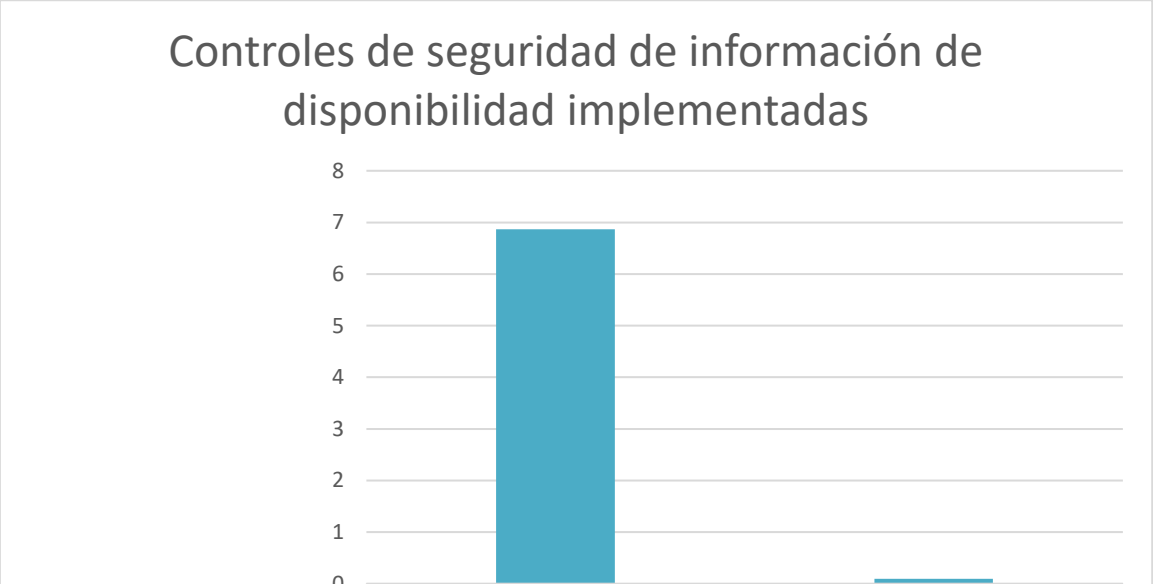

Figura 12. Histograma Pretest y Post Test del indicador Número de controles de seguridad de información de disponibilidad implementadas

Fuente: Elaboración propia realizada con el Software SPSS.

De acuerdo con los resultados mostrados en la tabla N° 11 y figura N° 13, para el indicador Número de posibles ataques cibernéticos, en el pretest se obtuvo un valor en la media de 6.87% y para el post test fue de 0.1%. Con estos resultados se puede ver que hubo un decremento de 6.77%.

3.2.Análisis Inferencial

Con la finalidad de seleccionar la prueba de hipótesis; la data fue sometida a una prueba de normalidad, para verificar si los indicadores contaban con distribución no normal.

Se cuenta con una muestra de 30 operaciones con datos de tipo escala, dicho esto, se hace uso de la prueba de Shapiro-Wilk, debido a que se presenta una muestra menor a 50. (Segnini, s.f.).

Según Herrero y Fontalvo (2012) indican que la prueba de Normalidad de Shapiro-Wilk: "Es un caso particular de contraste ajuste, donde se trata de comprobar si los datos provienen de una distribución normal. El contraste de Shapiro-Wilk mide el ajuste de una muestra a una recta el dibujarla en un papel probabilístico normal". (p.165).

Prueba de normalidad del indicador Número de controles de seguridad de información de control y de accesos implementados.

Sí:

Sig. < 0.05 acepta la distribución no normal.

Sig. ≥ 0.05 acepta la distribución normal.

Dónde:

Sig.: P-valor o nivel crítico del contraste.

H0: El indicador Número de controles de seguridad de información de control y de accesos implementados tiene una distribución normal.

H1: El indicador Número de controles de seguridad de información de control y de accesos implementados no tiene una distribución normal.

Tabla 12
Prueba de normalidad del indicador Número de controles de seguridad de información de control y de accesos implementados

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
P_PreTest	,517	30	,000	,404	30	,000
P_PosTest	,537	30	,000	,275	30	,000

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia realizada con el Software SPSS.

Como se muestra en la tabla N°12 los resultados de la prueba indican que el porcentaje del indicador Número de controles de seguridad de información de control y de accesos implementados para el pretest es de 0.000, cuyo valor es menor a 0.05, por lo que se indica tiene una distribución no normal. Los resultados de la prueba post test para el indicador integridad es de 0.000, cuyo valor es menor a 0.05, por lo que se indica que el porcentaje de crecimiento de ventas tiene una distribución no normal.

Por ende, se rechaza la H0. la variable integridad no cuenta con Distribución Normal.

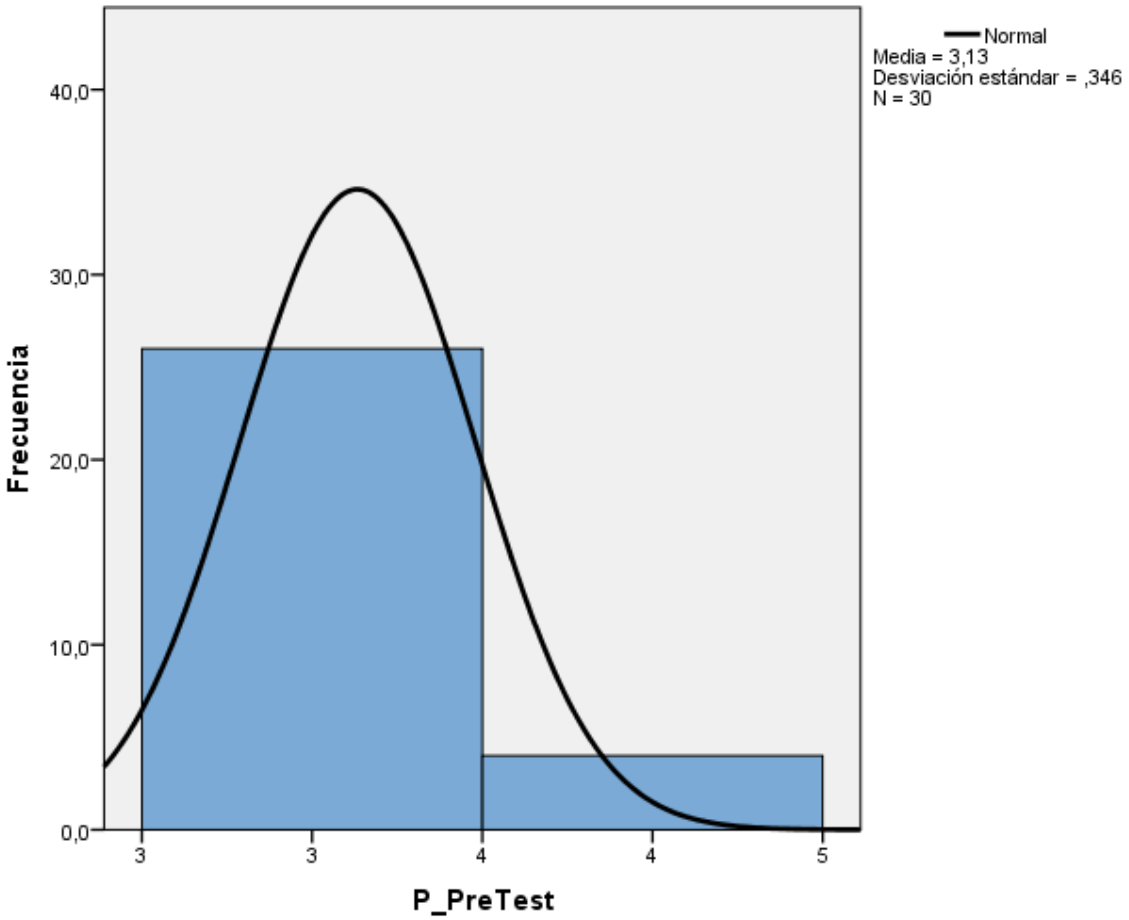

Figura 13. Prueba de normalidad del indicador Número de controles de seguridad de información de control y de accesos implementados antes de implementar el modelo de ciberseguridad

Fuente: Elaboración propia realizada con el Software SPSS.

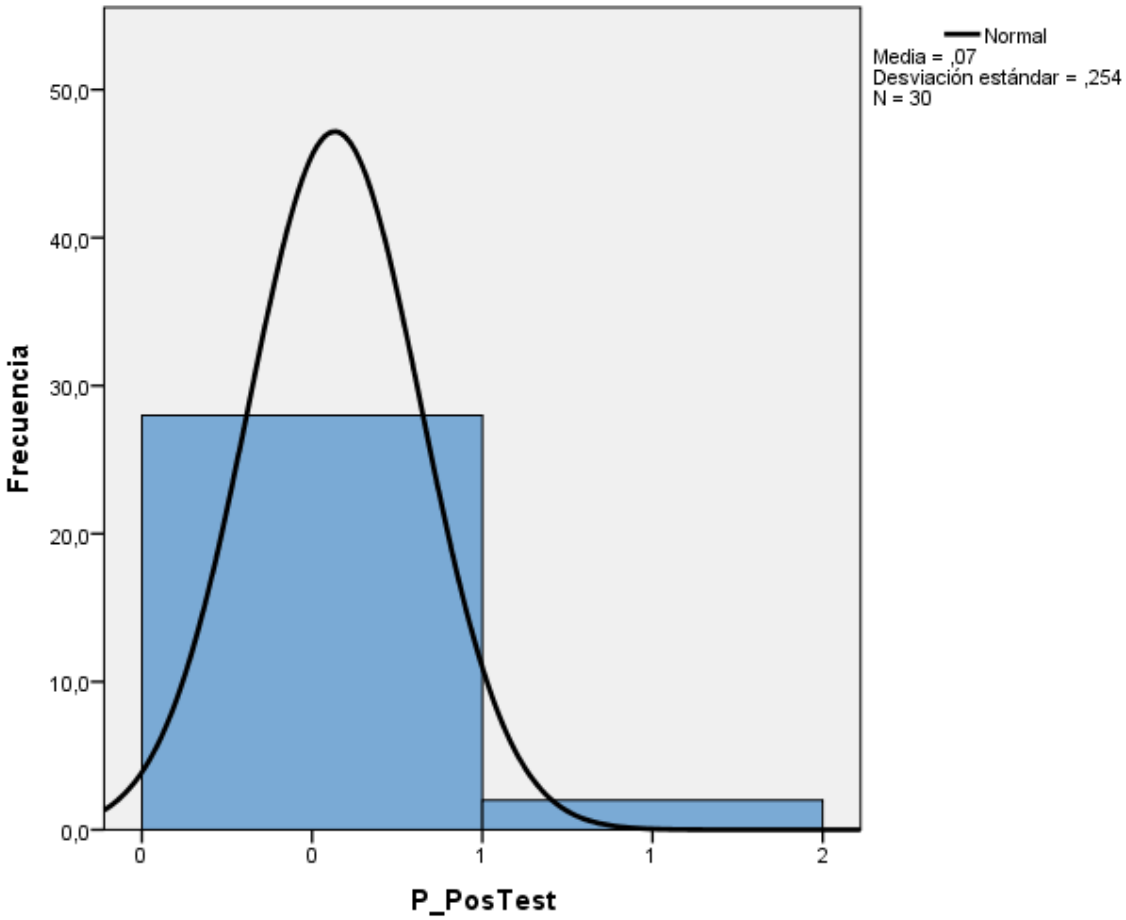

Figura 14. Prueba de normalidad del indicador Número de controles de seguridad de información de control y de accesos implementados después de implementar el modelo de ciberseguridad

Fuente: Elaboración propia realizada con el Software SPSS.

Prueba de normalidad del indicador Número de controles de seguridad de información de privacidad y confidencialidad implementados

Sí:

Sig. < 0.05 acepta la distribución no normal.

Sig. ≥ 0.05 acepta la distribución normal.

Dónde:

Sig.: P-valor o nivel crítico del contraste.

H0: El indicador Número de controles de seguridad de información de privacidad y confidencialidad implementados tiene una distribución normal.

H1: El indicador Número de controles de seguridad de información de privacidad y confidencialidad implementados no tiene una distribución normal.

Tabla 13
Prueba de normalidad del indicador Número de controles de seguridad de información de privacidad y confidencialidad implementados

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
IC_PreTest	,537	30	,000	,275	30	,000
IC_PosTest	,423	30	,000	,597	30	,000

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia realizada con el Software SPSS.

Como se muestra en la tabla N°13 los resultados de la prueba indican que el porcentaje del indicador Número de controles de seguridad de información de privacidad y confidencialidad implementados para el pretest es de 0.000, cuyo valor es menor a 0.05, por lo que se indica tiene una distribución no normal. Los resultados de la prueba

post test para el indicador confidencialidad es de 0.000, cuyo valor es menor a 0.05, por lo que se indica que el número de controles de seguridad de información de privacidad y confidencialidad implementados no tiene una distribución normal.

Por ende, se rechaza la H0. la variable confidencialidad no cuenta con Distribución Normal.

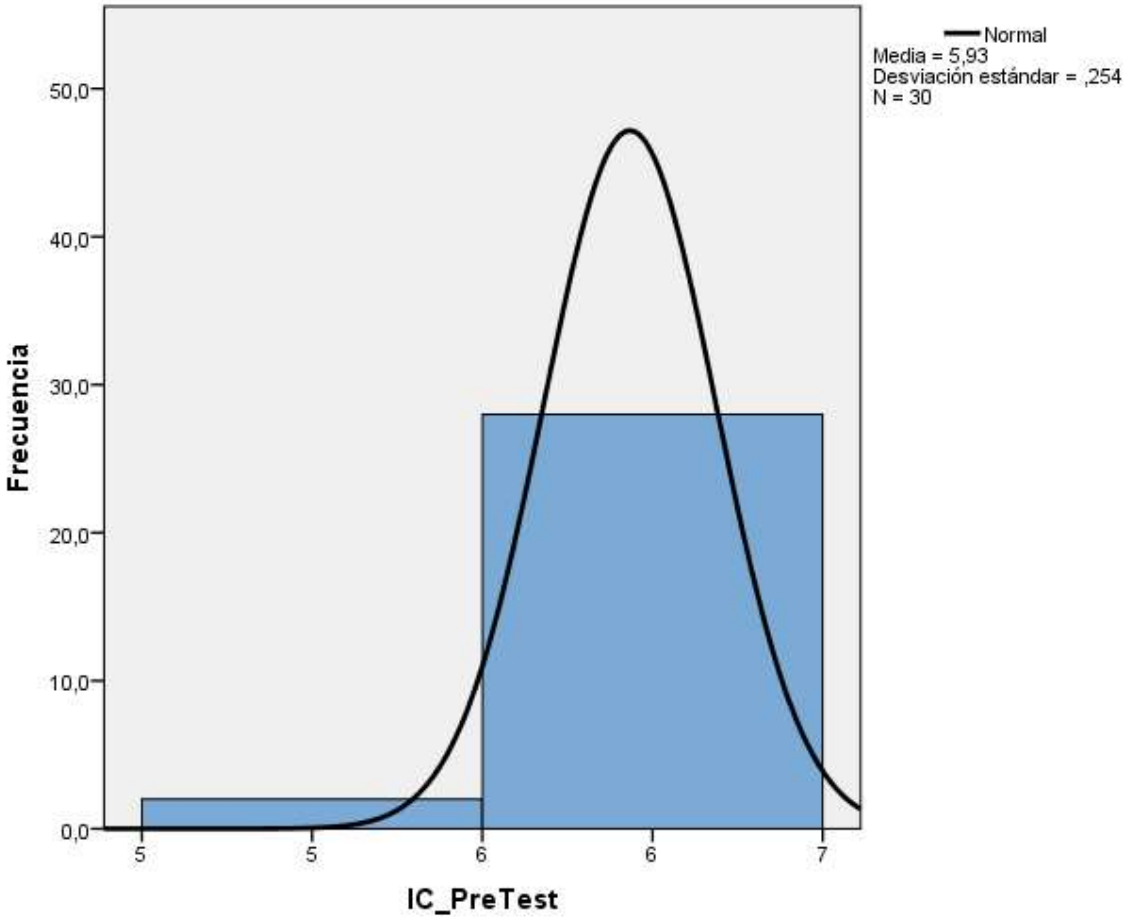

Figura 15. Prueba de normalidad del indicador Número de controles de seguridad de información de privacidad y confidencialidad implementados antes de implementar el modelo de ciberseguridad

Fuente: Elaboración propia realizada con el Software SPSS.

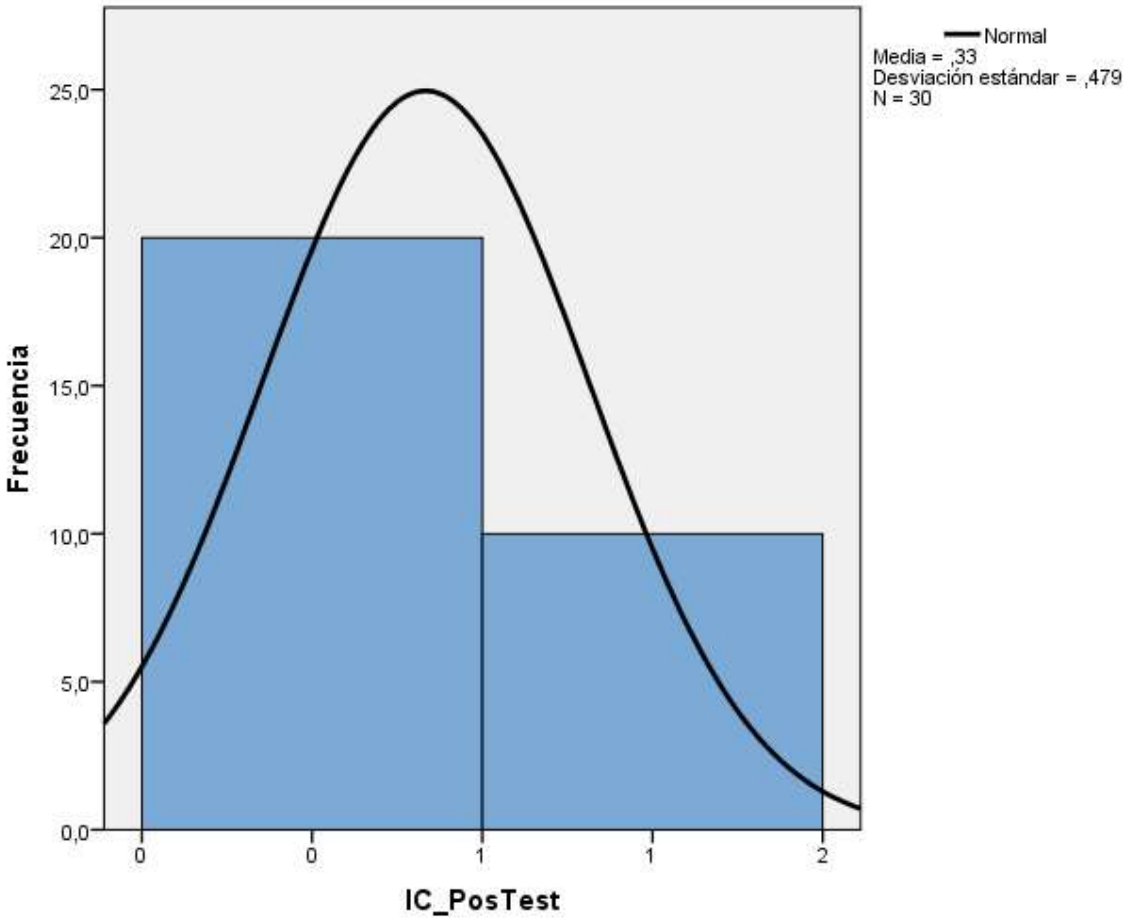

Figura 16. Prueba de normalidad del indicador Número de controles de seguridad de información de privacidad y confidencialidad implementados después de implementar el modelo de ciberseguridad

Fuente: Elaboración propia realizada con el Software SPSS.

Prueba de normalidad del indicador Número de controles de seguridad de información de disponibilidad implementadas

Sí:

Sig. < 0.05 acepta la distribución no normal.

Sig. ≥ 0.05 acepta la distribución normal.

Dónde:

Sig.: P-valor o nivel crítico del contraste.

H0: El indicador Número de controles de seguridad de información de disponibilidad implementadas tiene una distribución normal.

H1: El indicador Número de controles de seguridad de información de disponibilidad implementadas no tiene una distribución normal.

Tabla 14
Prueba de normalidad del indicador Número de controles de seguridad de información de disponibilidad implementadas

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PR_PreTest	,517	30	,000	,404	30	,000
PR_PosTest	,528	30	,000	,347	30	,000

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia realizada con el Software SPSS.

Como se muestra en la tabla N° 14 los resultados de la prueba indican que el porcentaje del indicador Número de controles de seguridad de información de disponibilidad implementadas para el pretest es de 0.000, cuyo valor es menor a 0.05, por lo que se indica tiene una distribución no normal. Los resultados de la prueba post test para el

indicador disponibilidad es de 0.000, cuyo valor es menor a 0.05, por lo que se indica que el número de controles de seguridad de información de disponibilidad implementadas no tiene una distribución normal.

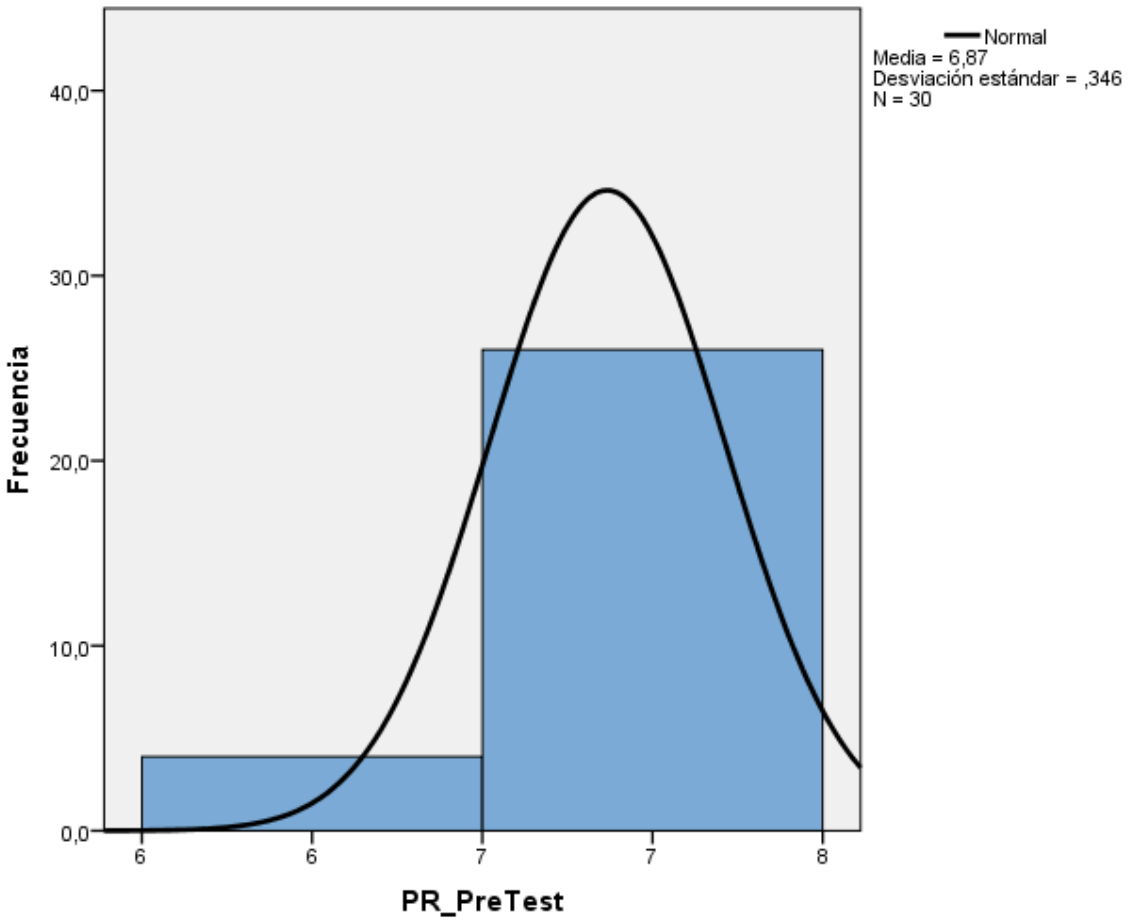

Figura 17. Prueba de normalidad del indicador Número de controles de seguridad de información de disponibilidad implementadas antes de implementar el modelo de ciberseguridad

Fuente: Elaboración propia realizada con el Software SPSS.

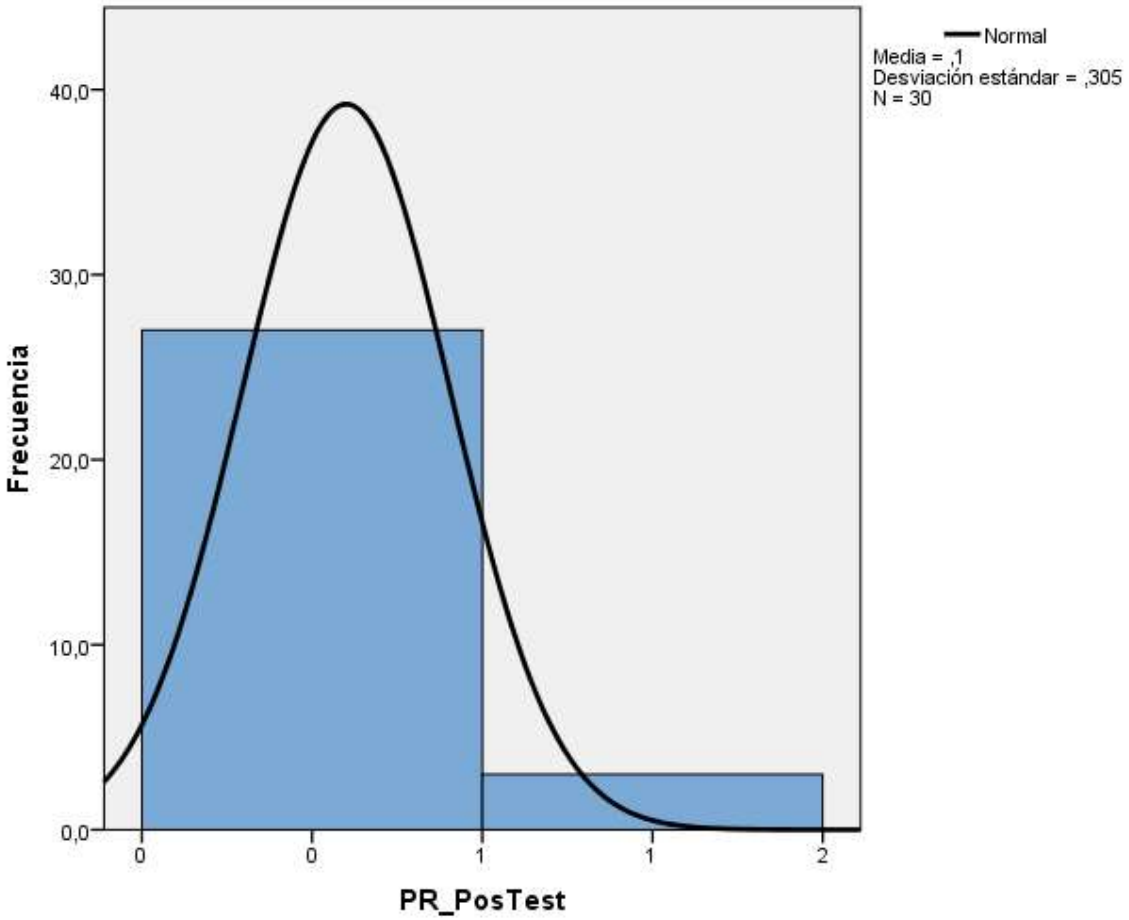

Figura 18. Prueba de normalidad del indicador Número de controles de seguridad de información de disponibilidad implementadas después de implementar el modelo de ciberseguridad

Fuente: Elaboración propia realizada con el Software SPSS.

Después de obtener estos resultados, se determinó que se cuenta con una distribución no normal, por lo tanto se rechaza la H0 y se debe aplicar la Prueba No Paramétrica Wilconson.

3.3.Contrastación de Hipótesis

Según Hernandez Sampieri, (2014), indica que "como se ha dicho, en el proceso cuantitativo las hipótesis se someten a prueba o escrutinio empírico para determinar si son apoyadas o refutadas, de acuerdo con lo que el investigador observa. De hecho,

para esto se formulan en la tradición deductiva. Ahora bien, en realidad no podemos probar que una hipótesis sea verdadera o falsa, sino argumentar que fue apoyada o no de acuerdo con ciertos datos obtenidos en una investigación particular. Las hipótesis, en el enfoque cuantitativo, se someten a prueba en la "realidad" cuando se implementa un diseño de investigación, se recolectan datos con uno o varios instrumentos de medición, y se analizan e interpretan esos mismos datos". (p. 117).

Según Hernandez Sampieri, (2014), indica que las hipótesis nulas son, en cierto modo, el reverso de las hipótesis de investigación. También constituyen proposiciones acerca de la relación entre variables, sólo que sirven para refutar o negar lo que afirma la hipótesis de investigación. (p.114).

Prueba de hipótesis

Formulación de Hipótesis específica 1

H0:

El modelo de ciberseguridad no implementa eficientemente controles de accesos y control en la oficina de seguros de la DIRIS Lima Norte 2020.

H1:

El modelo de ciberseguridad implementa eficientemente controles de accesos y control en la oficina de seguros de la DIRIS Lima Norte 2020.

Tabla 15
Rangos

Rangos

		N	Rango promedio	Suma de rangos
P_PosTest - P_PreTest	Rangos negativos	30[a]	15,50	465,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		

	Total	30

a. P_PosTest < P_PreTest

b. P_PosTest > P_PreTest

c. P_PosTest = P_PreTest

Fuente: Elaboración propia realizada con el Software SPSS.

Tabla 16

Prueba Wilconson

Estadísticos de prueba[a]

	P_PosTest - P_PreTest
Z	-5,104[b]
Sig. asintótica (bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: Elaboración propia realizada con el Software SPSS.

Como la significación estadística (p=0.00) es menos a 0.05 (α). Entonces se rechaza H0 y se acepta H1. Concluyendo que El modelo de ciberseguridad implementa eficientemente controles de accesos y control en la oficina de seguros de la DIRIS Lima Norte 2020.

Formulación de Hipótesis específica 2

H0:

El modelo de ciberseguridad no implementa eficientemente controles de privacidad y confidencialidad en la oficina de seguros de la DIRIS Lima Norte 2020.

H1:

El modelo de ciberseguridad implementa eficientemente controles de privacidad y confidencialidad en la oficina de seguros de la DIRIS Lima Norte 2020.

Tabla 17
Rangos

Rangos

		N	Rango promedio	Suma de rangos
IC_PosTest - IC_PreTest	Rangos negativos	30[a]	15,50	465,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	30		

a. IC_PosTest < IC_PreTest
b. IC_PosTest > IC_PreTest
c. IC_PosTest = IC_PreTest

Fuente: Elaboración propia realizada con el Software SPSS.

Tabla 18
Prueba Wilconson

Estadísticos de prueba[a]

	IC_PosTest - IC_PreTest
Z	-4,972[b]
Sig. asintótica (bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

Fuente: Elaboración propia realizada con el Software SPSS.

Como la significación estadística (p=0.00) es menos a 0.05 (α). Entonces se rechaza H0 y se acepta H1. Concluyendo que El modelo de ciberseguridad implementa eficientemente controles de privacidad y confidencialidad en la oficina de seguros de la DIRIS Lima Norte 2020.

Formulación de Hipótesis específica 3

H0:

El modelo de ciberseguridad no implementa eficientemente controles de disponibilidad en la oficina de seguros de la DIRIS Lima Norte 2020..

H1:

El modelo de ciberseguridad implementa eficientemente controles de disponibilidad en la oficina de seguros de la DIRIS Lima Norte 2020.

Tabla 19
Rangos

Rangos

		N	Rango promedio	Suma de rangos
PR_PosTest - PR_PreTest	Rangos negativos	30[a]	15,50	465,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	30		

a. PR_PosTest < PR_PreTest
b. PR_PosTest > PR_PreTest
c. PR_PosTest = PR_PreTest

Fuente: Elaboración propia realizada con el Software SPSS.

Tabla 20
Prueba Wilconson

Estadísticos de prueba[a]

	PR_PosTest - PR_PreTest
Z	-5,106[b]
Sig. asintótica (bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: Elaboración propia realizada con el Software SPSS.

Como la significación estadística (p=0.00) es menos a 0.05 (α). Entonces se rechaza H0 y se acepta H1. Concluyendo que El modelo de ciberseguridad implementa eficientemente controles de disponibilidad en la oficina de seguros de la DIRIS Lima Norte 2020.

CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES

4.1 Discusión

A partir de los resultados obtenidos en el presente trabajo de investigación, se observa en el análisis descriptivo del indicador Número de controles de seguridad de información de control y de accesos, en el post test se tiene una media de 3.13%; en la contrastación de hipótesis, según lo indicado por la tabla N° 9, hay implementación eficiente de controles de accesos y control, se observa en la tabla N° 16 que el nivel de significancia es igual a 0.000 es menor a 0.005 determinándose que el modelo de ciberseguridad implementa eficientemente controles de accesos y control de la oficina de seguros de la DIRIS Lima Norte 2020.

A partir de los resultados obtenidos en el presente trabajo de investigación, se observa en el análisis descriptivo del indicador Número de controles de seguridad de información de privacidad y confidencialidad implementados, en el post test se tiene una media de 0.33%; en la contrastación de hipótesis, según lo indicado por la tabla N° 10, hay una implementación eficiente de controles de privacidad y confidencialidad, se observa en la tabla N° 18 que el nivel de significancia es igual a 0.000 es menor a 0.005, determinándose que el modelo de ciberseguridad implementa controles de privacidad y confidencialidad en la oficina de seguros de la DIRIS Lima Norte 2020. Estos resultados coinciden con la investigación de Lara (2017, p. 84) en el que indica que con el modelo de ciberseguridad se logró identificar las vulnerabilidades internas de la institución, debido a que se aplicaron procesos

técnicos como el mapeo de la red, revisión de puertos que están abiertos, acceso a la red wifi sin claves, etc.

A partir de los resultados obtenidos en el presente trabajo de investigación, se observa en el análisis descriptivo del indicador Número de controles de seguridad de información de disponibilidad implementadas, en el post test se tiene una media de 0.10%; en la contrastación de hipótesis, según lo indicado por la tabla N° 11, hay una implementación eficiente de controles de disponibilidad, se observa en la tabla N° 20 que el nivel de significancia es igual a 0.000 es menor a 0.005, determinándose que modelo de ciberseguridad implementa eficientemente controles de disponibilidad en la oficina de seguros de la DIRIS Lima Norte 2020. Estos resultados coinciden con la investigación de Guillintina y Merino (2021, p.386) en donde se indica que gracias a que el modelo implementado se comprendió la importancia que representan la gestión de riesgos y los planes de contingencia (generación de backups) para el cumplimiento de los objetivos e indicadores planteados para el proyecto.

4.2 Conclusiones

En base a los resultados obtenidos en la presente investigación, se llegó a las siguientes conclusiones:

El modelo de ciberseguridad previene de ataques cibernéticos a la oficina de seguros de la DIRIS Lima Norte 2020.

Primero: Se concluye que la variable integridad es influenciada por el indicador Número de controles de seguridad de información de control y de accesos implementados; asimismo en la tabla 16 observamos que el valor P (0.000) <0.000

determinando que el modelo es estadísticamente significativo y determinando que modelo de ciberseguridad implementa eficientemente controles de accesos y control en la oficina de seguros de la DIRIS Lima Norte 2020, como los controles:

La definición del perfil de acceso, la asignación y retiro de privilegios

Control periódico de los derechos de acceso

Identificación y autenticación de usuarios en recursos informáticos

Uso personalizado de identificadores de usuario

Definir usuarios privilegiados y usuarios normales.

Conexión segura entre el tercero y la red

Restringir el acceso a los servicios de Internet.

La contraseña debe ser interactiva y cambiar periódicamente, y debe constar de letras, números y caracteres especiales.

Segundo: Se concluye que la variable confidencialidad es influenciada por el indicador Número de controles de seguridad de información de privacidad y confidencialidad implementados; asimismo en la tabla 18 observamos que el valor P (0.000) <0.000 determinando que el modelo es estadísticamente significativo y determinando que modelo de ciberseguridad implementa eficientemente controles de privacidad y confidencialidad en la oficina de seguros de la DIRIS Lima Norte 2020, como los controles:

Inventario regular (activos de la empresa).

Definir las reglas de uso de los activos de la empresa.

Asignar información responsable.

Gestión de riesgos en seguridad de la información.

Determine el nivel de confidencialidad.

Destruir la información de forma segura.

Tercero: Se concluye que la variable disponibilidad es influenciada por el indicador Número de controles de seguridad de información de disponibilidad implementadas; asimismo en la tabla 20 observamos que el valor P (0.000) <0.000 determinando que el modelo es estadísticamente significativo y determinando que modelo de ciberseguridad implementa eficientemente controles de disponibilidad en la oficina de seguros de la DIRIS Lima Norte 2020, como los controles:

La seguridad de los planes de emergencia y continuidad.

Usuarios de contingencia.

Respaldo de información crítica.

Pruebas sobre el plan de contingencia y continuidad.

REFERENCIAS

Coban, Cigdem, and Mehmet Fatih Tuysuz. 2019. "E-Health and Privacy: Risks, Opportunities and Solutions." UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering 554–59.

Coventry, Lynne, and Dawn Branley. 2018. "Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward." Maturitas 113(March):48–52.

E. Ferrero, (2006), Análisis y gestión de riesgos del servicio IMAT del sistema de información del I.C.A.I. Madrid, Universidad Pontificia Comillas, [On line]. Disponible en http://www.iit.upcomillas.es/pfc/ resumenes/44a527e27a231.pdf

H. Leteller, (2013, julio), Consultor Alfresco y J2EE en Blaunia, Seguridad de los sistemas de información, Metodología MAGERIT. [On line]. Disponible en: http:// www.belt.es/expertos/home2_experto.asp?id=5374

ISO27000. (2020). ISO27000.es. Recuperado 16 noviembre 2020, a partir de https://www.iso27000.es/iso27000.html

Izaara, Ambrose Atuheire, Richard Ssembatya, and Fred Kaggwa. 2019. "An Access Control Framework for Protecting Personal Electronic Health Records." 2018 International Conference on Intelligent and Innovative Computing Applications, ICONIC 2018 1–6.

Lopes, Sérgio F., Francisco Afonso, Adriano Tavares, and João Monteiro. 2009. "Framework Characteristics - A Starting Point for Addressing Reuse Difficulties." 4th International Conference on Software Engineering Advances, ICSEA 2009, Includes SEDES 2009: Simposio Para Estudantes de Doutoramento Em Engenharia de Software 256–64.

López, P. (2020). POBLACIÓN MUESTRA Y MUESTREO. Scielo.org.bo. Recuperado 16 noviembre 2020, a partir de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1815-02762004000100012

Monjes Alvarez, C. (2011). Guía didáctica de la metodología de la investigación (1st ed., pp. 9-50). Colombia: Universidad Surcolombiana.

Nevmerzhitskaya, Julia. 2018. "Cybersecurity Education and Training in Hospitals." 2048–52.

Normas y estándares en proyectos de TI. (2013). Wordpress. Recuperado 16 noviembre 2020, a partir de https://karron10.wordpress.com/2013/04/14/normas-y-estandares-en-proyectos-de-ti-2/

PAe - MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (2020). Administracionelectronica.gob.es. Recuperado 16 noviembre 2020, a partir de

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WKoNQlXhCUk

Tyas Tunggal, A. (2020). ¿What is a Cyber Attack?. Recuperado 29 abril 2020, a partir de https://www.upguard.com/blog/cyber-attack

Vallejo, P. (2012). Web.upcomillas.es. Recuperado 16 noviembre 2020, a partir de https://web.upcomillas.es/personal/peter/investigacion/Tama%f1oMuestra.pdf

Vera Tudela, V. (2020). Ciberseguridad para el Sector Salud en la nueva normalidad. Bdo.com.pe. Recuperado 16 noviembre 2020, a partir de https://www.bdo.com.pe/es-pe/blogs/blog-bdo-peru/septiembre-2020/ciberseguridad-para-el-sector-salud-en-la-nueva-normalidad

Lagos, J. (2012). Web.upcomillas.es. Recuperado 16 noviembre 2020, a partir de https://web.upcomillas.es/personal/peter/investigacion/Tama%f1oMuestra.pdf

Segnini, S. (s.f.). APENDICE A: Prueba de Normalidad de Shapiro Wilk. Recuperado el 29 de marzo de 2019, de INFLUENCIA DEL TAMAÑO DE VIDRIO MOLIDO EN LA RESISTENCIA A COMPRESIÓN DEL CONCRETO, TRUJILLO 2019 Br. Chávez Silva, Ana Felicitas Pág. 98 http://webdelprofesor.ula.ve/ciencias/segninis/Docencia/ANEXO_A_SahapiroWilks.pd

Jansen, W., Winograd, T. and Scarfone, K., 2021. Guidelines on Active Content and Mobile Code. [online] https://nvlpubs.nist.gov/. Available at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-28ver2.pdf> [Accessed 15 August 2021].

ANEXOS

ANEXO N°1 Matriz de consistencia

Problema	Objetivo	Hipótesis	Variable	Dimensiones	Indicadores
GENERAL	GENERAL	GENERAL	GENERAL	GENERAL	GENERAL
¿En qué medida el modelo de ciberseguridad previene de ataques cibernéticos a la oficina de seguros de la DIRIS Lima Norte 2020?	Determinar en qué medida el modelo de ciberseguridad previene de ataques cibernéticos a la oficina de seguros de la DIRIS Lima Norte 2020.	El modelo de ciberseguridad previene de ataques cibernéticos a la oficina de seguros de la DIRIS Lima Norte 2020.	Modelo de ciberseguridad	Preparación de los recursos	Número de controles de seguridad de información implementados
ESPECÍFICO	ESPECÍFICO	ESPECÍFICO	ESPECÍFICO	ESPECÍFICO	ESPECÍFICO
¿En qué medida el modelo de ciberseguridad implementa políticas de control y de accesos en la oficina de seguros de la DIRIS Lima Norte 2020?	Determinar en qué medida el modelo de ciberseguridad implementa controles de accesos y control en la oficina de seguros de la DIRIS Lima Norte 2020	El modelo de ciberseguridad implementa eficientemente controles de accesos y control en la oficina de seguros de la DIRIS Lima Norte 2020	Prevención de ataques cibernéticos	Integridad	Número de controles de seguridad de información de control y de accesos implementados
¿En qué medida el modelo de ciberseguridad implementa controles de privacidad y confidencialidad en la oficina de seguros de la DIRIS Lima Norte 2020.	Determinar en qué medida el modelo de ciberseguridad implementa controles de privacidad y confidencialidad en la oficina de seguros de la DIRIS Lima Norte 2020.	El modelo de ciberseguridad implementa eficientemente controles de privacidad y confidencialidad en la oficina de seguros de la DIRIS Lima Norte 2020.		Confidencialidad	Número de controles de seguridad de información de privacidad y confidencialidad implementados

¿En qué medida el modelo de ciberseguridad implementa controles de disponibilidad en la oficina de seguros de la DIRIS Lima Norte 2020?	Determinar en qué medida el modelo de ciberseguridad implementa controles de disponibilidad en la oficina de seguros de la DIRIS Lima Norte 2020.	El modelo de ciberseguridad implementa eficientemente controles de disponibilidad en la oficina de seguros de la DIRIS Lima Norte 2020.		Disponibilidad	Número de controles de seguridad de información de disponibilidad implementadas

ANEXO N°2 Matriz de operaciones

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN
VARIABLE DEPENDIENTE: Prevención de ataques cibernéticos	Garantizar la continuidad del negocio y prevenir o minimizar el posible daño el impacto de los incidentes. (INCIBE,2015)	Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información, por parte de la alta dirección.	Integridad	Número de controles de accesos y control implementadas	ESCALA NUMERAL
			Confidencialidad	Número de controles de privacidad y confidencialidad implementadas	
			Disponibilidad	Número de controles de disponibilidad implementadas	
VARIABLE INDEPENDIENTE: Modelo de ciberseguridad	Es un diseño que tiene en cuenta los puntos comunes y las variabilidades de un dominio de aplicación específico. Proporciona la aplicación de los elementos comunes listos para su uso y localiza la variabilidad en	Autoevaluación que identifique incluye el reconocimiento, la definición, la medición, el análisis, la mejora, el control y el mantenimiento de los asuntos de ciberseguridad	Preparación de los recursos	Número de controles de seguridad de información implementados	ESCALA

	puntos de variación abstractos predefinidos (Lopes et al. 2009)	con un enfoque en la gestión de riesgos.			

ANEXO N°3 Instrumento de recolección de datos

Ficha de observación			
Investigador			
Empresa			
Fecha			
Operación			
Número de controles de seguridad de información implementados			
Número de controles de seguridad de información de control y de accesos implementados			
Número de controles de seguridad de información de privacidad y confidencialidad implementados			
Número de controles de seguridad de información de disponibilidad implementadas			
Indicador		**Check**	**Observación**
Integridad	¿Todos los empleados, internos y externos, han firmado un acuerdo de confidencialidad?		
	Se dispone en la empresa de una política permanente de utilización de dispositivos móviles.		
	Se conceden accesos a la infraestructura de los sistemas de información solamente si son necesarios para el cumplimiento de las tareas		
	Se tiene conocimiento de todas las aplicaciones y programas, individuales y colectivos, utilizados en la organización.		
	Se ha asegurado el acceso a Internet a través de medidas de protección.		
Confidencialidad	¿Tiene la empresa una Política de Seguridad de la Información aprobada para esta operación? ¿Está esta política alineada con los estándares de la industria (ISO27001, CoBIT, etc.) ¿Con qué frecuencia se revisan las políticas, estándares, pautas y procedimientos de seguridad de la información?		
	Se han definido responsabilidades concretas para la seguridad de la información para esta operación		
	¿Todos los empleados, internos y externos, están informados sobre las medidas de seguridad de la información con respecto a esta operación?		
	¿Se revisan de forma regular las directrices de administración de los sistemas de información y los perfiles de acceso y usuario de acuerdo a la operación?		
	¿Tiene la empresa una Política de Seguridad de la Información aprobada para esta operación? ¿Está esta política alineada con los estándares de la industria (ISO27001, CoBIT, etc.) ¿Con qué frecuencia se revisan las políticas, estándares,		

	pautas y procedimientos de seguridad de la información?		
Disponibilidad	Se ha definido en la empresa el concepto de incidente de seguridad con respecto a esta operación		
	Se ha definido en la empresa una política de gestión de incidentes de seguridad que involucre esta operación		
	Se hacen copias de seguridad de los datos clave de la empresa que involucre esta operación		
	Se hacen regularmente pruebas de comprobación de los sistemas de copias de seguridad de datos de esta operación de acuerdo con un ciclo fijo preestablecido.		
	¿Se ha creado un plan de respuesta a incidentes que ataquen a esta operación, para varios escenarios que incluyen: infección de malware, violación externa y denegación de servicio?		
	¿Realiza evaluaciones de riesgo periódicas para evaluar su postura de seguridad con respecto a esta operación?		
	¿Con qué frecuencia el plan de respuesta a incidentes para esta operación se “prueba”?		

ANEXO N°4 Validación de expertos

Certificado de validez de contenido de los instrumentos

N°	DIMENSIONES / Ítems	Pertinencia[1]			Relevancia[2]			Claridad[3]			Sugerencias
	Variable independiente: Eficiencia del modelo de ciberseguridad	Si	No		Si	No		Si	No		
	Protección										
1	¿Tiene la empresa una Política de Seguridad de la Información aprobada? ¿Está esta política alineada con los estándares de la industria (ISO27001, CoBIT, etc.) ¿Con qué frecuencia se revisan las políticas, estándares, pautas y procedimientos de seguridad de la información?			X		X				X	
2	Se han definido responsabilidades concretas para la seguridad de la información			X			X			X	
3	¿Todos los empleados, internos y externos, están informados regularmente sobre las medidas de seguridad de la información?			X		X				X	
4	¿Se revisan de forma regular las directrices de administración de los sistemas de información y los perfiles de acceso y usuario de acuerdo con un ciclo periódico fijo definido previamente?			X		X				X	
	Integridad y Confidencialidad									X	
5	¿Todos los empleados, internos y externos, han firmado un acuerdo de confidencialidad?			X		X				X	
6	Se dispone en la empresa de una política permanente de utilización de dispositivos móviles.			X		X				X	
7	Se conceden accesos a la infraestructura de los sistemas de información solamente si son necesarios para el cumplimiento de las tareas			X		X				X	
8	Se tiene conocimiento de todas las aplicaciones y programas, individuales y colectivos, utilizados en la organización.			X		X				X	
9	Se ha asegurado el acceso a Internet a través de medidas de protección.			X		X				X	
10	¿Se solicita a los usuarios identificarse en el real malandrino?			X		X				X	
11	Se han definido los requisitos de seguridad necesarios para cada proyecto de externalización de tecnologías de la información.			X		X				X	
12	Se efectúa un registro aleatorio de las actividades de los usuarios con el fin de determinar acciones frecuentes, para así detectar "supuestas" colaboraciones para el hurto información			X		X				X	
	Prevención y respuesta										
13	Se ha definido en la empresa el concepto de incidente de seguridad.			X		X				X	
14	Se ha definido en la empresa una política de gestión de incidentes de seguridad.			X		X				X	
15	Se hacen copias de seguridad de los datos clave de la empresa.			X		X				X	
17	Se hacen regularmente pruebas de comprobación de los sistemas de copias de seguridad de datos de acuerdo con un ciclo fijo preestablecido.			X		X				X	
18	¿Se ha creado un plan de respuesta a incidentes para varios escenarios que incluyen: infección de malware, violación externa y denegación de servicio?			X		X				X	
19	¿Realiza evaluaciones de riesgo periódicas en los proveedores externos para evaluar su postura de seguridad?			X		X				X	
20	¿Con qué frecuencia el plan de respuesta a incidentes se "prueba"?			X		X				X	

Observaciones: _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador Dr. / Mg: **Miguel Alfredo Levano Stella** **DNI: 10306862**

Especialidad del validador: Ingeniería de sistemas

Link del CTI VITAE

http://directorio.concytec.gob.pe/appDirectorioCTI/VerDatosInvestigador.do;jsessionid=2dc44a0c1cf07c810e888eb222ed?id_investigador=88183

30 de Setiembre de 2020

[1]Pertinencia: El ítem corresponde al concepto teórico formulado.
[2]Relevancia: El ítem es apropiado para representar el componente o dimensión específica del constructo
[3]Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante.

Especialidad

Certificado de validez de contenido de los instrumentos

N°	DIMENSIONES / Items	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
	Variable independiente: Eficiencia del modelo de ciberseguridad	Si		No		Si		No		Si		No		
	Protección													
1	¿Tiene la empresa una Política de Seguridad de la Información aprobada? ¿Está esta política alineada con los estándares de la industria (ISO27001, ~~CoBIT~~, etc.) ¿Con qué frecuencia se revisan las políticas, estándares, pautas y procedimientos de seguridad de la información?			X			X					X		
2	Se han definido responsabilidades concretas para la seguridad de la información			X				X				X		
3	¿Todos los empleados, internos y externos, están informados regularmente sobre las medidas de seguridad de la información?			X			X					X		
4	¿Se revisan de forma regular las directrices de administración de los sistemas de información y los perfiles de acceso y usuario de acuerdo con un ciclo periódico fijo definido previamente?			X			X					X		
	Integridad y Confidencialidad											X		
5	¿Todos los empleados, internos y externos, han firmado un acuerdo de confidencialidad?			X			X					X		
6	Se dispone en la empresa de una política permanente de utilización de dispositivos móviles.			X			X					X		
7	Se conceden accesos a la infraestructura de los sistemas de información solamente si son necesarios para el cumplimiento de las tareas			X			X					X		
8	Se tiene conocimiento de todas las aplicaciones y programas, individuales y colectivos, utilizados en la organización.			X			X					X		
9	Se ha asegurado el acceso a Internet a través de medidas de protección.			X			X					X		
10	¿Se solicita a los usuarios identificarse en el sistema?			X			X					X		
11	Se han definido los requisitos de seguridad necesarios para cada proyecto de externalización de tecnologías de la información.			X			X					X		
12	Se efectúa un registro aleatorio de las actividades de los usuarios con el fin de determinar acciones frecuentes, para así detectar "sugestas" colaboraciones para el hurto información			X			X					X		
	Prevención y respuesta													
13	Se ha definido en la empresa el concepto de incidente de seguridad.			X			X					X		
14	Se ha definido en la empresa una política de gestión de incidentes de seguridad.			X			X					X		
15	Se hacen copias de seguridad de los datos clave de la empresa.			X			X					X		
17	Se hacen regularmente pruebas de comprobación de los sistemas de copias de seguridad de datos de acuerdo con un ciclo fijo preestablecido.			X			X					X		
18	¿Se ha creado un plan de respuesta a incidentes para varios escenarios que incluyen: infección de malware, violación externa y denegación de servicio?			X			X					X		
19	¿Realiza evaluaciones de riesgo periódicas en los proveedores externos para evaluar su postura de seguridad?			X			X					X		
20	¿Con qué frecuencia el plan de respuesta a incidentes se "prueba"?			X			X					X		

Observaciones: _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador Dr. / Mg: **Rolando Moreno Reyes** **DNI: 44687118**

Especialidad del validador: Ingeniería de sistemas

Link del CTI VITAE: https://otivitae.concytec.gob.pe/appDirectorioCTI/VerDatosInvestigador.do?id_investigador=178218

4 de Noviembre de 2020

[1]Pertinencia: El ítem corresponde al concepto teórico formulado.
[2]Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante.
Especialidad

Certificado de validez de contenido de los instrumentos

N°	DIMENSIONES / Ítems	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
	Variable independiente: Eficiencia del modelo de ciberseguridad	Si		No		Si		No		Si		No		
	Protección													
1	¿Tiene la empresa una Política de Seguridad de la Información aprobada? ¿Está esta política alineada con los estándares de la industria (ISO27001, ~~CoBIT~~, etc.) ¿Con qué frecuencia se revisan las políticas, estándares, pautas y procedimientos de seguridad de la información?			X			X					X		
2	Se han definido responsabilidades concretas para la seguridad de la información			X				X				X		
3	¿Todos los empleados, internos y externos, están informados regularmente sobre las medidas de seguridad de la información?			X			X					X		
4	¿Se revisan de forma regular las directrices de administración de los sistemas de información y los perfiles de acceso y usuario de acuerdo con un ciclo periódico fijo definido previamente?			X			X					X		
	Integridad y Confidencialidad											X		
5	¿Todos los empleados, internos y externos, han firmado un acuerdo de confidencialidad?			X			X					X		
6	Se dispone en la empresa de una política permanente de utilización de dispositivos móviles.			X			X					X		
7	Se conceden accesos a la infraestructura de los sistemas de información solamente si son necesarios para el cumplimiento de las tareas			X			X					X		
8	Se tiene conocimiento de todas las aplicaciones y programas, individuales y colectivos, utilizados en la organización.			X			X					X		
9	Se ha asegurado el acceso a Internet a través de medidas de protección.			X			X					X		
10	¿Se solicita a los usuarios identificarse en ~~el end-point/sistema~~?			X			X					X		
11	Se han definido los requisitos de seguridad necesarios para cada proyecto de externalización de tecnologías de la información.			X			X					X		
12	Se efectúa un registro aleatorio de las actividades de los usuarios con el fin de determinar acciones frecuentes, para así detectar "supuestas" colaboraciones para el hurto información			X			X					X		
	Prevención y respuesta													
13	Se ha definido en la empresa el concepto de incidente de seguridad.			X			X					X		
14	Se ha definido en la empresa una política de gestión de incidentes de seguridad.			X			X					X		
15	Se hacen copias de seguridad de los datos clave de la empresa.			X			X					X		
17	Se hacen regularmente pruebas de comprobación de los sistemas de copias de seguridad de datos de acuerdo con un ciclo fijo preestablecido.			X			X					X		
18	¿Se ha creado un plan de respuesta a incidentes para varios escenarios que incluyen: infección de malware, violación externa y denegación de servicio?			X			X					X		
19	¿Realiza evaluaciones de riesgo periódicas en los proveedores externos para evaluar su postura de seguridad?			X			X					X		
20	¿Con qué frecuencia el plan de respuesta a incidentes se "prueba"?			X			X					X		

Observaciones: _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador Dr. / Mg: **JULIO CESAR VIDAL RISCHMOLLER** **DNI: 07401072**

Especialidad del validador: Ingeniería Industrial

Link del CTI VITAE |

30 de Setiembre de 2020

[1]Pertinencia: El ítem corresponde al concepto teórico formulado.
[2]Relevancia: El ítem es apropiado para representar el componente o dimensión específica del constructo
[3]Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

ANEXO N°5 PLAN DE IMPLEMENTACIÓN DEL MODELO DE CIBERSEGURIDAD PARA LA DIRIS LIMA NORTE

1. Introducción

1.1. Contexto y justificación

Uno de los activos intangibles más valiosos de DIRIS LIMA NORTE es la información, por lo que vale la pena protegerla y la razón de sustentar y proteger su sistema informático.

Se debe enfatizar que al implementar un modelo de ciberseguridad, es necesario revisar y evaluar los controles y procesos en todas las áreas de la organización, con el fin de buscar no solo el primer acceso, sino también el uso oportuno de prácticas y eficientes. procesos, que son fáciles de mantener, la certificación se puede renovar sin gastos excesivos o esfuerzo extra.

Actualmente, no cuentan con un modelo de seguridad de red establecido, por lo que estos procesos necesitan ser desarrollados y actualizados con los últimos estándares enfocados en la seguridad de la información.

1.2. Planificación

Para el desarrollo de este trabajo se realiza el siguiente diagrama de Gantt en el cual se describen los hitos de cada PEC, las tareas a realizar en cada una de ellas, la planificación de cada tarea.

	Name	Start Date	Duration
2	Etapa 1: Evaluación	Jul 30, 2020	10 days
3	Identificación de activos	Jul 30, 2020	10 days
4	Identificación de riesgos	Oct 11, 2020	10 days
5	Etapa 2: Diseño	Oct 21, 2020	10 days
6	Definir políticas y controles del modelo	Oct 21, 2020	10 days
7	Etapa 3: Implementación	Nov 07, 2020	15 days
8	Implementación del modelo de ciberseguridad	Nov 07, 2020	15 days
9	Etapa 4: Administración y soporte	Nov 21, 2020	15 days
10	Monitorear implementación del modelo	Nov 21, 2020	15 days

1.3.**Esquema del modelo de ciberseguridad**

El modelo de ciberseguridad propuesto cuenta con la siguiente estructura:

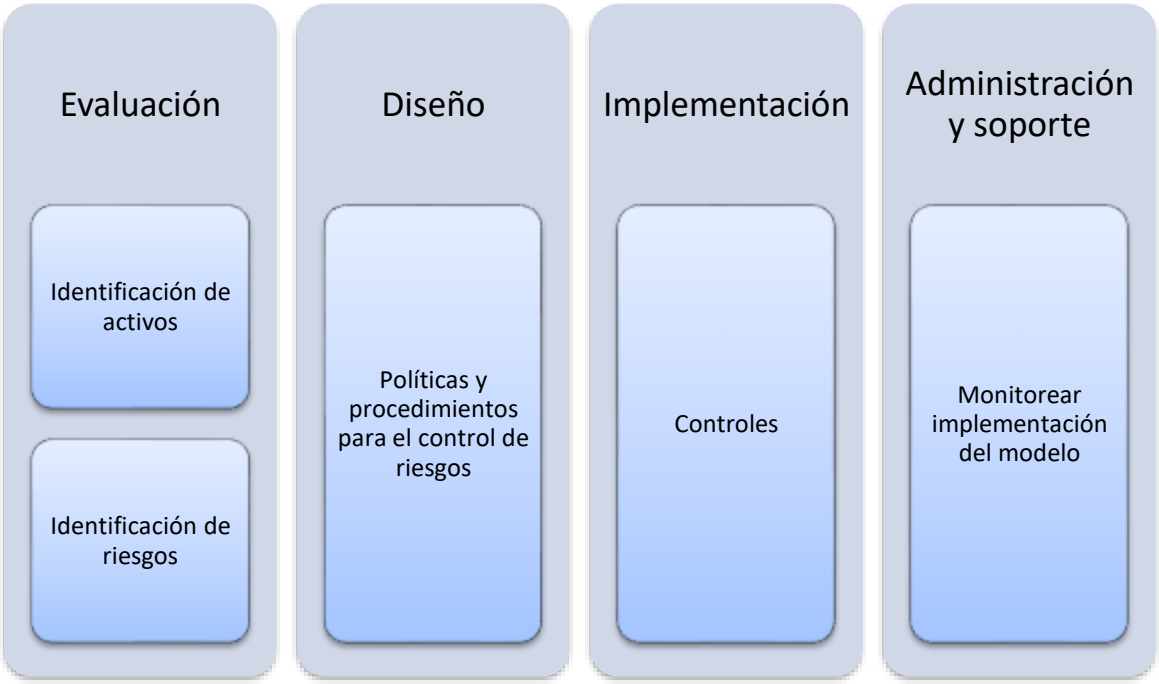

Figura 19. Estructura de modelo de ciberseguridad

Fuente: Elaboración propia

Etapa de Evaluación

Nos indica cuál es la situación actual de la institución. Deriva de la norma ISO 27001, tomándose en cuenta, además, las recomendaciones de la norma NIST 800 y del manual OSSTMM versión 3. Esta compuesta por los siguientes apartados:

- Identificación de activos

Un activo necesita protección para asegurar las correctas operaciones y continuidad de la institución. Se define como un bien con valor o utilidad para la organización, sus operaciones y continuidad. El conservar una adecuada protección de los activos de la empresa, se debe

principalmente a mantener la gestión apropiada de los activos. (Peltier, 2010) Cada activo debe estar identificado y valorado apropiadamente.

- Identificación de riesgos

Las vulnerabilidades halladas mediante las hojas de observación, se detallan en este apartado.

Etapa de Diseño

Deriva de la norma ISO 27001, tomándose en cuenta, además, las recomendaciones de la norma NIST 800 y del manual OSSTMM versión 3. Señala en dónde debemos estar.

Esta compuesta por los siguientes apartados:

- Organización de la seguridad de la información
- Gestión de incidentes en la seguridad de la información
- Seguridad en redes y telecomunicaciones
- Seguridad física
- Plan de contingencia y continuidad
- Control de accesos
- Seguridad del recurso humano
- Cumplimiento de regulaciones
- Protección de la información

Etapa de Implementación

Especifica cómo desde nuestra posición actual podemos llegar a donde necesitamos. Deriva de la norma ISO 27001, tomándose en cuenta, además, las recomendaciones de la norma NIST 800 y del manual OSSTMM versión 3.

Esta compuesta por los siguientes apartados:

- Controles lógicos
- Controles de red
- Controles de seguridad de aplicaciones
- Controles de seguridad física
- Controles acceso físico a los equipos
- Controles de protección contra software malicioso
- Controles de Gestión de la Seguridad de Red
- Controles en el uso de los Servicios de Red
- Controles de Seguridad de la Red Inalámbrica

Etapa de Auditoría de Cumplimiento

Indica cómo nos mantenemos y mejoramos. Aquí se evaluará en qué punto la institución acata las buenas prácticas del modelo de ciberseguridad.

2. **Desarrollo**

Los hallazgos detallados son el resultado del análisis de las normativas y medidas de seguridad que tiene la organización en relación a la seguridad de la información, esta verificación se centró en la revisión de los diferentes controles de las áreas del alcance. Este análisis dará a conocer el estado actual de la DIRIS Lima Norte en relación de la seguridad de la información.

2.1.**Evaluación**

2.1.1. Identificación de activos

Un activo necesita protección para asegurar las correctas operaciones y continuidad de la institución. Se define como un bien con valor o utilidad para la organización, sus operaciones y continuidad. El conservar una adecuada protección de los activos de la empresa, se debe

principalmente a mantener la gestión apropiada de los activos. (Peltier, 2010) Cada activo debe estar identificado y valorado apropiadamente. Según la ISO 17799:2005, los activos se pueden clasificar en:

i. Activos de información: bases de datos, documentación del sistema, manuales de usuario, planes de continuidad, entre otros.
ii. Documentos impresos: contratos, lineamientos, documentos de la institución.
iii. Activos de software: Software de aplicación, de sistema, herramientas de desarrollo.
iv. Activos físicos: Equipos de comunicación y computación, medios magnéticos, otros servicios técnicos.
v. Personas: Todo el personal.
vi. Servicios: Servicios de computación y comunicación, otros servicios técnicos.

Tabla 21
Activos de las oficinas DIRIS Lima Norte

Tipo de activo	Posee
Documentos físicos	FUAS
	PEDI
	POA
	Documentación del personal
	Contratos del personal
Activos de software	Windows server 2008 R2
	Windows server 2012
	Bases de datos: SQL server 2008 estándar
	Antirvirus: Mcafee
Activos físicos	Tienen una red VLAN con switch de capa 3

	Cada switch tiene 10 VLAN para un total de 120 pcs
	Máquinas de escritorio, portátiles
	Acceso a internet
Personal	9 auditores
	9 supervisores
	10 administrativos
	113 digitadores
Servicio	Correo organizacional
	Intranet
	Telefonía

Fuente: Elaboración propia

2.1.2. Identificación de riesgos

De acuerdo con los valores de las hojas de observación; se detectaron algunas vulnerabilidades en la red de datos. Las vulnerabilidades encontradas se detallan en la siguiente tabla.

Tabla 22
Riesgos de DIRIS Lima Norte

Vulnerabilidad	Amenazas	Riesgos Potenciales
Problemas de seguridad del software utilizado	Ataques de inyección de código, errores de integridad de datos, información inconsistente	Se pierde o modifica información, se roban las credenciales de acceso (nombre de usuario y contraseña)
Actualice el sistema operativo en su computadora	Actualice el sistema operativo en su computadora	Actualice el sistema operativo en su computadora
Personas de fuera del área ingresan a la oficina y al equipo de cómputo de manera indiscriminada	Personas de fuera del área ingresan a la oficina y al equipo de cómputo de manera indiscriminada	Personas de fuera del área ingresan a la oficina y al equipo de cómputo de manera indiscriminada
Control de acceso deficiente al sistema	Control de acceso deficiente al sistema	Control de acceso deficiente al sistema
Vulnerabilidad del navegador de Internet utilizado	Vulnerabilidad del navegador de Internet utilizado	Vulnerabilidad del navegador de Internet utilizado
Usuarios con una formación inadecuada	Usuarios con una formación inadecuada	Usuarios con una formación inadecuada
Ataque involuntario, ingeniería social.	Ataque involuntario, ingeniería social.	Ataque involuntario, ingeniería social.

Fuente: Elaboración propia

Una vez identificadas las vulnerabilidades y amenazas, determinaremos su impacto y probabilidad de ocurrencia de acuerdo con el estándar NIST 800 (determinación de probabilidad). Por esta razón, las amenazas se dividen en: alta (son totalmente capaces de violar el sistema y el control es inexistente o defectuoso), media (la amenaza puede violar el sistema, pero el control es efectivo) y baja (la la amenaza no puede violar el sistema y el control es efectivo). También considerando su posible impacto en el sistema de información, se establecieron las siguientes clasificaciones: leve (L), moderada (M) y catastrófica (C).

En consecuencia, las vulnerabilidades de la red de información en la Tabla 31 se compilan de acuerdo con el estándar NIST 800.

Riesgo	Probabilidad			Impacto		
	A	M	B	L	M	C
Sistema sin restricciones de acceso						
Falta de control de actualización de software						
Se utilizan pocos controles para restringir el acceso a la computadora						
Falta de seguridad en el entorno laboral						
Falta de control de acceso físico a la oficina.						
Control de acceso de usuarios deficiente						
Vulnerabilidades en los navegadores de Internet						
Utilice aplicaciones						

poco fiables para el intercambio de información.						

Construcción de la Matriz de Riesgos con flujo de calor para la DIRIS Lima Norte

Las consideraciones para la probabilidad de amenaza son las siguientes:

Intereses de personas externas.

Nivel de vulnerabilidad.

La frecuencia del incidente.

La evaluación de la probabilidad de amenaza es la siguiente:

Baja: en algunos casos, la posibilidad de ataque es muy pequeña.

Medio: en algunos casos, es poco probable que ocurra un ataque a corto plazo, pero no es suficiente para prevenir un ataque a largo plazo.

Gao: El ataque es inminente. Ninguna condición interna o externa obstaculiza el desarrollo del ataque.

Las consideraciones para evaluar el impacto son las siguientes:

¿Quiénes resultarán perjudicados?

Violación de la confidencialidad (interna y externa).

Violación de obligaciones legales (contratos, convenios).

Costos de recuperación (imagen, emoción, recursos).

La evaluación de impacto del ataque es la siguiente:

Leve: Daño aislado, no daña ninguna parte de la organización.

Moderado: provoca una parte desarticulada de la organización. A largo plazo, puede conducir a la desintegración de la organización.

Grave: estancamiento o desintegración de la organización en un corto período de tiempo.

Con base en el contenido anterior, se da un valor numérico para el rango de probabilidad y el impacto, como se muestra a continuación:

Probabilidad	**Impacto**
1 Baja	1 Leve
2 Media	2 Moderado
3 Alta	3 Severo

A continuación se construye una matriz con estos pesos, de manera que se pueda obtener el producto de probabilidad e influencia, y se pueda realizar la información cruzada de las dos variables.

	PROBABILIDAD			
IMPACTO		1 Baja	2 Media	3 Alta
	1 Leve	Leve-Baja	Leve-Media	Leve-Alta
	2 Moderado	Moderado-Baja	Moderado-Media	Moderado-Alta

	3 Severo	Severo-Baja	Severo-Media	Severo-Alta

Dado que el producto más alto es 9 (la probabilidad de combinación es alta y el impacto es grave), este valor se considera 100% de riesgo.

La ponderación de riesgo, expresada en porcentaje, se obtiene multiplicando el valor asignado de cada probabilidad por el valor asignado de cada nivel de impacto y dividiendo el producto por 9.

La generación del mapa de calor usa el color del semáforo (se usa internacionalmente, por lo que es fácil de entender), y los valores se dividen en tres categorías:

Verde (bajo riesgo) con un valor inferior al 33%.

Amarillo (riesgo medio) con un valor entre 34% y 66%.

Rojo (alto riesgo) con un valor superior al 66%

Los pesos de los parámetros utilizados para hacer la matriz de riesgo en la DIRIS Lima Norte, y los colores asignados a cada parámetro en la misma matriz, siguen los lineamientos anteriores.

No.	IDENTIFICACIÓN DEL RIESGO									ANÁLISIS DEL RIESGO							
	TIPO DE RIESGO (F=Funcional, O=Organizacional)	RIESGO	ORIGEN	Tipo		¿Qué afecta?			CONSECUENCIAS	Probabilidad			Impacto			Resultado	Categoría
				Interna	Externa	Confidencialidad	Integridad	Disponibilidad		A (3)	M (2)	B (1)	S (3)	M (2)	L (1)		
R1	F	Pérdida de Datos y/o daños en equipos de cómputo	Suministro Eléctrico	X				X	Por la forma abrupta que se va la energía se puede: 1.Dañar los dispositivos de la red, como: disco duro, memorias, servidores, entre otros. 2. Perder la información que no fue guardada			1	3			33%	BB
R2	F O	Inestabilidad en la plataforma virtual	Funcionamiento inadecuado de la plataforma virtual	X			X	X	1. Pérdida de tiempo de los estudiantes. 2. Sobrecarga de servidor y capacidad de canal. 3. Malestar entre los usuarios.		2			2		44%	MM
R3	F	Pérdida del servicio	Saturación de la capacidad del canal. Ataque de negación de servicio. Actividad ilegal en la red.	X		X	X	X	1. Los datos no están disponibles a todo momento. 2. Mala imagen para los usuarios. 3. Pérdida de información.		2		3			67%	MB
R4	F O	Alteración y/o pérdida de la información por deficiencias en los controles de acceso físicos y lógicos a los servidores.	Accesos ilegales Políticas permisivas de acceso Falta de seguridad física (guardias, acceso restringidos, entre otros)			X	X	X	1. Accesos no autorizados. 2. Accesos autorizados concurrentes. 3. Vulnerabilidad del sistema informático.	3			3			100%	AA
R5	O	Fuga de información	Procesos internos no establecidos (ejemplo: gente va a comprar un derecho y no encuentra el proceso adecuado, no se puede hacer consulta a sus notas y prefiere preguntar verbalmente a su docente)		X	X			1. Inconformidad del usuario de la red 2. Publicidad negativa		2		3			67%	MB
R6	F	Pérdidas de datos	Falta de políticas y procedimientos de respaldo de información o backup	X			X	X	1. Información desactualizada ante incidentes de seguridad 3. Alteración de la información 2. Pérdida de datos 3. Descontento de los usuarios		2			2		44%	MM

	PROBABILIDAD			
IMPACTO		B (1)	M (2)	A (3)
	L (1)	11%	22%	33%
	M (2)	22%	44%	66%
	S(3)	33%	66%	100%

L = Leve
M = Medio
S = Severo

B = Baja
M = Media
A = Alta

2.2.**Acción**

2.2.1. Políticas de seguridad de la información

De acuerdo con los resultados del análisis de vulnerabilidades, se procedió a elaborar el siguiente esquema de políticas de seguridad de la información, que se sugiere que implemente la oficina de seguros DIRIS Lima Norte

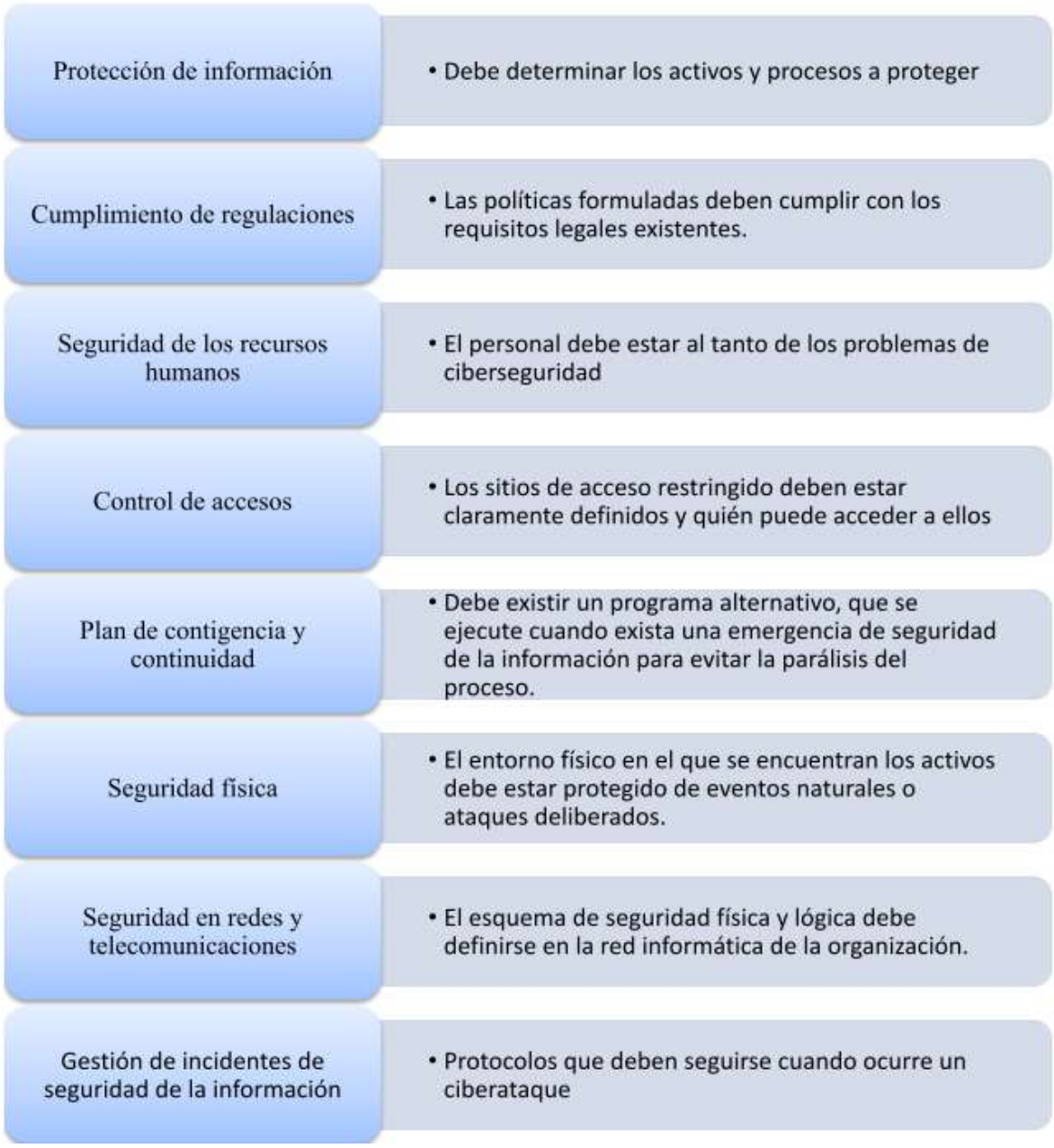

Figura 20. Esquema de las Políticas de seguridad de la información

Fuente: Elaboración propia

Una de las recomendaciones originales de la norma ISO 27001 fue establecer la política de seguridad de la información de una organización, porque estableció su objetivo de "proporcionar dirección y soporte a la gestión de seguridad de la información, de acuerdo con los requisitos del negocio, las leyes, y reglamentos pertinentes."

1. Política 1 Organización de la seguridad de la información

Basada en el anexo A.5.1.1 de la norma ISO 27001. Se establece:

1.1 Creación de un comité de seguridad de la información.

1.2 Aprobación y revisión por parte de la Dirección.

2. "Protección de la información "

Basado en el Anexo A8 "Gestión de activos" de la norma ISO 27001.

2.1 Inventario regular (activos de la empresa).

2.2 Definir las reglas de uso de los activos de la empresa.

2.3 Asignar información responsable.

2.4 Gestión de riesgos en seguridad de la información.

2.5 Determine el nivel de confidencialidad.

2.6 Destruir la información de forma segura.

3. "Cumplimiento de regulaciones "

Basado en el Anexo A.18 de la norma ISO 27001.

3.1 Cumplir con las leyes y normativas vigentes en todos los aspectos relacionados con la red de información.

3.2 Utilice software e información patentados

3.3 Restricciones al uso de datos personales

4. "Seguridad en el recurso humano"

Basada en el anexo A.7 "Seguridad en recursos humanos" de la norma ISO 27001, en el capítulo 7 del manual OSSTMM v3 y el modelo desarrollado por Lara (2019)

4.1 Capacitar y establecer una cultura de seguridad de la información.

4.2 Acuerdo de confidencialidad.

4.3 Requisitos de seguridad en contratos firmados con terceros.

5. "Control de accesos"

Basada en el anexo A.9 "Control de acceso" de la norma ISO 27001.

5.1 La definición del perfil de acceso, la asignación y retiro de privilegios

5.2 Control periódico de los derechos de acceso

5.3 Identificación y autenticación de usuarios en recursos informáticos

5.4 Uso personalizado de identificadores de usuario

5.5 Definir usuarios privilegiados y usuarios normales.

5.6 Conexión segura entre el tercero y la red

5.7 Restringir el acceso a los servicios de Internet.

5.8 La contraseña debe ser interactiva y cambiar periódicamente, y debe constar de letras, números y caracteres especiales.

6. "Plan de contingencia y continuidad"

Basada en el capítulo 7 del manual OSSTMM v3.

5.1 La seguridad de los planes de emergencia y continuidad.

6.2 "Usuarios de contingencia". (OSSTMM 7.4; 7.5)

6.3" Respaldo de información crítica". (OSSTMM 7.4; 7.5)

6.4 "Pruebas sobre el plan de contingencia y continuidad". (OSSTMM 7.6)

7. "Seguridad Física"

Basada en el anexo A.11 "Seguridad física y del entorno" de la norma ISO 27001, en el capítulo 8 del manual OSSTMM.

7.1 “Control de acceso y perímetro de las instalaciones”. (A.11.1.1 Perímetro de seguridad física)

7.2 “Gestión de amenazas ambientales.” (A.11.1.4; OSSTMM 8.2.1)

7.3 “Manejo de áreas de carga y descarga.” (A.11.1.6)

7.4 “Protección física de equipos de cómputo.” (A.11.1.3)

7.5 “Seguridad en el cableado.” (A.11.2.3)

7.6 “Protección contra fallos del suministro eléctrico”. (A.11.2.2)

8. “Seguridad en redes y telecomunicaciones”

Basada en el anexo A.13 “Seguridad en las comunicaciones” de la norma ISO 27001, en el capítulo 10 del manual OSSTMM v3.

8.1 “Segmentación de redes y control de enrutamiento en la red.” (A.13.1.3; OSSTMM 10.1.6)

8.2 “Intercambio de información con terceros.” (A.13.1.2; OSSTMM 10.2.1)

8.3 “Uso de barreras de comunicaciones.” (A.13.1.1; OSSTMM 10.2.2)

8.4 “Seguridad en el correo electrónico.” (A.13.2.3)

9. “Gestión de incidentes en la seguridad de la información”

Basada en el anexo A.16 “Gestión de incidentes de seguridad de la información” de la norma ISO 27001.

9.1 Designación de responsables del sistema de seguridad de la información. (A.16.1.1)

9.2 “Reporte de incidentes de seguridad de la información.” (A.16.1.2)

9.3 Reporte de debilidades de la seguridad de la información.” (A.16.1.3)

9.4 “Recopilación de evidencias.” (A.16.1.7)

9.5 “Valoración de impacto en incidentes de Seguridad de la información”. (A.16.1.4)

2.3.**Implementación**

2.3.1. Implementación de controles

De acuerdo con la política establecida, se han establecido las medidas de control correspondientes, de acuerdo con la normativa de Lara (2019), esta medida puede asegurar el cumplimiento de estas medidas de control.

2.3.2. Controles de seguridad Lógica

i. Identificación

Para que los usuarios puedan acceder al sistema de información, se deben establecer procedimientos formales escritos para estandarizar y requerir el ingreso de los siguientes datos:

a. El ID de usuario debe ser un valor alfanumérico único
b. La contraseña debe ser una contraseña personal y no se puede transferir
c. Nombres completos y apellido
d. El grupo de trabajo al que pertenece el usuario
e. Tiempo de vencimiento de la contraseña
f. Contador anti-fallos
g. Autorización para ingresar al área de usuarios.

El permiso asignado debe ser completamente necesario para que el usuario realice correctamente su trabajo diario en la oficina. Considere los siguientes factores, el acceso al

sistema y el uso de los recursos de la red de datos de la Oficina de Seguros de DIRIS Lima Norte deben tener horarios establecidos:

a. Fuera del horario laboral, no podrá acceder a las cuentas de usuario a menos que haya obtenido autorización previa
b. La cuenta de usuario debe desactivarse durante las vacaciones o durante el período de licencia del propietario de la cuenta.

La primera autenticación es la contraseña asociada con la identificación de usuario, que le dará acceso a la computadora y a la información en primer lugar. Cabe señalar que la contraseña debe ser secreta, personal e intransferible.

El Departamento de Recursos Humanos debe comunicar cualquier cambio en el formulario y, al recibir esta notificación, el administrador del sistema debe revocar los permisos de la cuenta o deshabilitarla

La computadora debe estar configurada con un sistema operativo y cerrar sesión después de cinco minutos de inactividad.

Los usuarios generales deben permanecer deshabilitados en todas las computadoras. Prohibir el uso de cuentas de invitado

Utilice privilegios de administrador para minimizar el acceso a los perfiles de usuario. Estos privilegios solo deben otorgarse a aquellos usuarios que son directamente responsables de la seguridad del sistema.

El uso de privilegios de administrador puede minimizar el acceso a los perfiles de usuario. Estos privilegios solo deben otorgarse a aquellos usuarios que sean directamente responsables de la seguridad del sistema.

ii. Contraseñas

De acuerdo con las buenas prácticas de seguridad, la contraseña utilizada debe reunir las siguientes características:

a. La longitud mínima es de 8 caracteres.
b. Contiene una combinación de caracteres alfanuméricos y no alfanuméricos. (Caso combinado)
c. Los sistemas y aplicaciones de las instituciones que contienen información crítica necesitan cambiar sus contraseñas al menos cada 90 días.
d. La nueva contraseña debe ser al menos diferente de las 3 últimas contraseñas utilizadas.
e. Los datos personales de cualquier usuario que falle más de tres autenticaciones consecutivas deben estar bloqueados.
f. Cada nuevo usuario debe cambiar la contraseña proporcionada por el administrador al iniciar sesión por primera vez.
g. El usuario es responsable de almacenar y administrar su contraseña.
h. Antes de la puesta en producción, se deben cambiar las contraseñas predefinidas del nuevo equipo de TI..

2.3.3. Controles para la seguridad en la red

Topología de la red

Contar con documentación detallada de todo lo relacionado con la implementación física de la red.

Si falla el método de comunicación principal, se debe implementar la redundancia en el canal de comunicación.

Red de datos

Se debe Se debe recopilar la siguiente información:

Capacidad de canal, contratada y utilizada.

Tráfico generado por la aplicación.

El estado de cada aplicación.

Intentos de intrusión.

Las actualizaciones y las nuevas instalaciones de software en los equipos de red, así como los cambios de dirección IP y la reconfiguración del equipo de enrutamiento, deben registrarse y aprobarse.

Propiedad de la información

Los sistemas de comunicación y los mensajes generados y procesados por dichos sistemas, incluidas las copias de seguridad, se considerarán propiedad de la agencia.

Uso de los sistemas de comunicación

Los recursos de la red de información institucional solo se pueden utilizar para actividades laborales. Está prohibido el uso personal de ellos.

Conexiones Externas

Filtre y controle el tráfico entrante y saliente de la red interna a través del firewall y prohíba el tráfico no autorizado.

Supervise constantemente el uso de Internet.

Configuración lógica de la red

En casos extremos, se deben considerar los siguientes elementos para conectar algunos dispositivos externos a la red:

No se identifique como usuario de la red.

No ejecute programas de monitoreo de tráfico sin la autorización explícita de la Administración General y la aprobación del administrador de la red.

Sin autorización previa, no agregue ningún equipo que amplíe la infraestructura de red.

Asegurar la confidencialidad de la dirección IP de la red de información de la organización..

Antivirus

El software antivirus seleccionado debe cumplir las siguientes condiciones:

Debe detectar y monitorear las medidas tomadas por el malware en tiempo real.

Analice periódicamente todas las unidades de almacenamiento de la estación de trabajo en busca de malware.

Actualice la base de datos diariamente.

Debe ser un producto completamente legal. (Licencia o software gratuito) A menos que sea absolutamente necesario y haya sido escaneado previamente por software antivirus, no se pueden usar dispositivos externos en las computadoras de la organización.

Firewall

La organización debe instalar un firewall y debe proporcionar una política de denegación completa de forma predeterminada. Por lo tanto, habilite solo los servicios y puertos que se utilizarán. La configuración de los firewalls y los servicios de red debe estar constantemente controlada por el administrador de mantenimiento y responsable de registrar este proceso

Ataques de red

Se deben tomar las siguientes medidas para minimizar los ataques a través de la red de información:

Toda la información transmitida a través de la red debe estar encriptada o transmitida en un formato ilegible.

Para detectar infiltraciones, la red debe estar constantemente monitoreada.

La red debe estar segmentada física o lógicamente para reducir el riesgo de rastreo.

2.3.4. Controles para la seguridad de aplicaciones

i. Software

Cualquier aplicación que desee descargar debe ser aprobada por el comité. Porque pueden contener códigos maliciosos que socavan la seguridad de la red. La instalación de software no autorizado está estrictamente prohibida, por lo tanto, la agencia debe obtener licencias para todo el software utilizado en sus actividades diarias. Si es necesario instalar software libre, el comité debe analizarlo previamente.

ii. Control de aplicaciones en las computadoras

Para mantener la seguridad de la estación de trabajo, se deben seguir las siguientes recomendaciones:

Los documentos deben generarse en la ubicación especificada según el perfil de cada usuario y las aplicaciones que se deben instalar. Y frecuencia Estas aplicaciones están actualizadas.

Copia de seguridad periódica o información del dispositivo de copia de seguridad.

Registrar el proceso de instalación, mantenimiento y reparación de todos los componentes equipo.

Notificar a los nuevos usuarios sobre las restricciones de instalación Software no autorizado por la Comisión

iii. Control de datos en las aplicaciones

Solo los administradores pueden acceder a los archivos de datos generados en el trabajo diario, y estos archivos de datos deben almacenarse en un directorio protegido estableciendo un control de acceso.

2.3.5. Controles para la seguridad física

Los recursos físicos y lógicos de la organización solo deben utilizarse en un entorno seguro, para lograr este objetivo se deben considerar los siguientes aspectos:

No modifique la configuración de hardware y software de los equipos establecidos por el comité.

Está prohibido fumar, comer o beber cualquier tipo de bebida en el puesto de trabajo.

El equipo debe estar protegido de los riesgos ambientales. (Polvo, fuego, agua)

No mueva ni mueva equipos sin permiso. Para que el equipo salga del campus, se requiere autorización por escrito.

Cualquier pérdida o robo de componentes de hardware o software debe informarse de inmediato.

Cualquier problema con la computadora o la red debe ser informado rápidamente para evitar problemas graves como pérdida de información o falta de disponibilidad de servicios.

Control de acceso físico a los equipos

Tanto las estaciones de trabajo como la red troncal deben tener derechos de acceso restringidos para minimizar el riesgo de ataques internos. Deben seguirse las siguientes recomendaciones:

Todo el personal que ingrese al área restringida debe estar debidamente identificado y autorizado en consecuencia.

Solo el administrador debe tener acceso al fondo de la red.

Control de acceso a los equipos

Los siguientes controles de seguridad deben activarse en todas las estaciones de trabajo para evitar su robo.

Configurar para usar una contraseña para proteger el teclado y la pantalla. Cuando el dispositivo ingresa al modo de ahorro de energía, debe activarse después de 5 minutos de inactividad.

Dispositivo de apoyo

La organización debe contar con el siguiente equipo de apoyo:

Aire acondicionado en la columna vertebral de la red para mantener el ambiente a una temperatura entre 19 ° C y 20 ° C.

Un extintor que cumpla con las especificaciones, preferiblemente polvo químico utilizado en equipos eléctricos e informáticos. En el centro de datos, debe haber un extintor de incendios dedicado al centro.

Alarmas de intrusión: Deben activarse fuera del horario laboral y deben permitir la activación manual durante el horario laboral..

UPS: el centro de datos debe tener al menos un UPS para brindar servicios para equipos de misión crítica y tener la capacidad de apagar el equipo de manera segura.

Luz de emergencia: debe haber una luz de emergencia, que se activará automáticamente.

Cableado estructurado

El cableado de red actual debe cumplir con el estándar de cableado estructurado, para ello:

Los canales de enrutamiento de cable existentes y los puntos de red deben registrarse en el plan.

La capacidad del canal ocupado debe medirse periódicamente. Si se excede el valor mínimo permitido, se deben tomar las medidas correctivas necesarias.

En caso de un corte de energía, como precaución, el equipo del centro de datos debe apagarse de manera segura..

2.3.6. Controles de acceso físico a los equipos

Las vulnerabilidades en la seguridad física están relacionadas con daños físicos, intrusos y problemas ambientales, lo que conduce a daños accidentales al equipo.

Perímetro de seguridad

Para establecer una zona de seguridad perimetral, que es la primera línea de defensa contra ataques informáticos, se debe implementar una arquitectura de seguridad basada en firewalls.

Control de acceso físico: Es fundamental contar con un control de acceso físico para proteger todos los activos de la organización.

Monitorear a los visitantes de la agencia y registrar la hora de entrada y salida.

Mantenimiento del equipo: el equipo informático de la organización debe recibir mantenimiento periódico. Para ello, debes considerar:

El comité debe implementar un programa de mantenimiento para el equipo y registrar la frecuencia de mantenimiento que se debe realizar y sus detalles.

Asegúrese de que solo el personal autorizado pueda mantener el equipo y realizar tareas de reparación (si es necesario).

2.3.7. Controles de Protección contra Software Malicioso

Controlar el malware

Estos controles deben considerar las siguientes acciones:

Está prohibido el uso de software no autorizado.

Instale y actualice periódicamente el software de eliminación de virus, compruebe

Medios informáticos y de almacenamiento.

Mantener el sistema operativo de la computadora con las últimas actualizaciones de seguridad disponibles.

Inspeccione con regularidad el software y el contenido de datos de la computadora que maneja las actividades clave de la organización e investigue formalmente si hay documentos no autorizados o modificaciones no autorizadas.

Antes de usar el software antivirus, escanee todos los archivos o medios de datos extraíbles recibidos a través de medios que no sean de confianza y luego use el software antivirus para escanear.

Informar a los empleados sobre los riesgos causados por virus y software malicioso y sus posibles consecuencias..

2.3.8. Controles de Gestión de la Seguridad de Red

Controles de red

El comité considerará los siguientes parámetros y definirá medidas de control para garantizar la seguridad de prevenir el acceso no autorizado a los datos:

Proteger la confidencialidad e integridad del procesamiento de datos.

Mantener la disponibilidad de los servicios de red y las computadoras conectadas.

A través de actividades de monitoreo, hay que asegurar que se apliquen controles en toda la infraestructura de procesamiento de información.

Gestión de medios removibles

Al administrar medios de computadora extraíbles, se deben considerar las siguientes medidas:

Elimine de forma segura el contenido que ya no necesita de ningún medio

Los que se pueden reutilizar deben ser retirados o reutilizados por la agencia.

Siga las instrucciones a continuación para almacenar todos los medios en un entorno seguro:

Especificaciones del fabricante o proveedor.

Intercambio de información. Mensaje electrónico

Con respecto al uso del correo electrónico, se deben establecer reglas claras:

Todos los empleados de la organización pueden solicitar y tener una cuenta de correo electrónico

Correo institucional

La persona responsable será responsable de configurar una cuenta de correo electrónico en la computadora del empleado solicitante.

La activación de las cuentas de correo electrónico institucionales debe realizarse de forma centralizada..

Para activar una cuenta de correo electrónico institucional, se deberá enviar una solicitud por escrito, misma que debe ser debidamente aprobada.

Cuando los usuarios reciben una nueva cuenta de correo electrónico institucional, deben firmar un documento que indique que conocen las políticas y procedimientos de seguridad y aceptan las responsabilidades asociadas con la cuenta.

Cuando un empleado de la organización renuncia o renuncia a la organización, se debe desactivar la cuenta de correo electrónico correspondiente, para lo cual el área administrativa debe emitir el aviso correspondiente.

Dependiendo del software de correo electrónico utilizado por la organización, los administradores pueden monitorear el contenido de los correos electrónicos enviados por los usuarios. La organización debe explicar esto claramente a los empleados y también debe informar las condiciones que deben cumplirse para monitorear la cuenta de correo electrónico de la organización.

3.9.1 Controles en el uso de los Servicios de Red

Se debe controlar el acceso a los servicios de red internos y externos. Esto es necesario para garantizar que los usuarios que pueden acceder a la red y sus servicios no comprometan su seguridad.

Solo a solicitud formal del solicitante, la persona responsable de otorgar permisos, servicios y recursos de red es el administrador de la red. Por tanto, se deben establecer procedimientos para la activación y desactivación del acceso a la red. Estos procedimientos son:

a. Determine a qué servicios de red se puede acceder.
b. Determinar reglas y procedimientos de autorización para controlar el personal y los servicios de red a los que se les otorgará acceso..

3.9.2 Controles de Seguridad de la Red Inalámbrica

Los más vulnerables a los ataques informáticos son los enlaces inalámbricos. Por tanto, se deben considerar los siguientes aspectos:

Limite el tráfico permitido en estos enlaces.

Uso obligatorio de contraseñas seguras.

Después de una investigación cuidadosa, el punto de acceso solo se puede colocar en el área especificada.

Evitar el uso de repetidores por personas ajenas a la organización.

Acceso privilegiado a redes inalámbricas registrando una dirección física en el enrutador o usando un software específico.

2.4.**Administración y Soporte**

2.4.1. Monitoreo de los Controles de Acceso

Es fundamental implementar un sistema de monitoreo de red que debe brindar información completa sobre las actividades de cada usuario conectado.

Conformidad con la política de seguridad

El oficial de seguridad designado por el comité realiza revisiones periódicas de todas las áreas de la agencia para asegurar el cumplimiento de las políticas, reglas y procedimientos de seguridad, y este período debe ser al menos una vez cada 6 meses.