UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Sistema de Gestión para la Seguridad de la Información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín,2021

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Risco Villarreal, Eduardo Giap (ORCID: 0000-0001-9681-7741)

ASESOR:

Mg. Acuña Melendez, Maria Eudelia (ORCID: 0000-0002-5188-3806)

LÍNEA DE INVESTIGACIÓN:
Auditoria de Sistemas y Seguridad de la información

LIMA - PERÚ

2021

DEDICATORIA

A Dios, por haberme dado la vida y permitirme alcanzar mi sueño de ser profesional en la carrera que amo. A mis padres Ernesto Risco & Lorena Villarreal por darme la mejor herencia que es mi profesión para poder triunfar a lado mi comprometida Jennifer & mi sobrino Leonardo quienes me acompañaron en toda mi etapa universitaria y llegar hasta acá ha sido la mayor satisfacción de la vida para formar mi familia a lado de ellos

AGRADECIMIENTO

Queremos agradecer a la Constructora Pérez & Pérez SAC por darme toda la herramienta que fueron necesarias para llevar a cabo el proceso de investigación. No hubiésemos podido arribar a estos resultados de no haber sido por su incondicional ayuda para el planteamiento de la investigación y desarrollo del estudio. A los ingenieros especialistas en Seguridad de la Información que me han ayudado en nuestra formación profesional, por compartirnos sus conocimientos, darnos ánimos para seguir adelante y nunca dejarnos rendir a cumplir nuestra meta de convertirnos en profesionales

ÍNDICE DE CONTENIDOS

Dedicatoria ..... **ii**
Agradecimiento ..... **iii**
Índice de Contenidos ..... **iv**
Índice de Tablas ..... **v**
Índice de Gráficos y Figuras ..... **vi**
Resumen ..... **vii**
Abstract ..... **viii**
I. INTRODUCCIÓN **9**
II. MARCO TEÓRICO **12**
III. METODOLOGÍA **18**
3.1. Tipo y diseño de investigación 18
3.2. Variables y operacionalización 19
3.3. Población (criterios de selección), muestra, muestreo, unidad de análisis 21
3.4. Técnicas e instrumentos de recolección de datos 22
3.5. Procedimientos 23
3.6. Método de análisis de datos 23
3.7. Aspectos éticos 24
IV. RESULTADOS **25**
V. DISCUSIÓN **33**
VI. CONCLUSIONES **36**
VII. RECOMENDACIONES **37**
REFERENCIAS **38**
ANEXOS **43**

ÍNDICE DE TABLAS

Tabla 1: Matriz de operacionalización de variables…… 20
Tabla 2: Población & Muestra ……..…… 21
Tabla 3: Técnicas e instrumentos empleados…….…… 22
Tabla 4: Estadísticos descriptivos Accesos No autorizados…… 22
Tabla 5: Estadísticos descriptivos Eliminar Borrar Manipular Datos…. …. 25
Tabla 6: Estadísticos descriptivos Virus informático……..… .25
Tabla 7: Prueba Normalidad Accesos No autorizados…… 26
Tabla 8: Prueba normalidad Eliminar Manipular Borrar Datos…….. 27
Tabla 9: Prueba normalidad Virus Informático…….. ..27
Tabla 10: Prueba de rango de Wilcoxon de ANA ……..…28
Tabla 11: Estadístico de contraste del Indicador 1 Accesos No autorizados29
Tabla 12: Prueba t Student de Manipular Borrar Eliminar Datos…… 30
Tabla 13: Prueba de rango de Wilcoxon de Virus Informático ……...… 30
Tabla 14: Estadístico de contraste de Virus Informático……31
Tabla 15 Matriz de Consistencia……43

ÍNDICE DE GRÁFICOS Y FIGURAS

Figura 1: Diseño de investigación Preexperimental……...18
Figura 2: Eset Reporte Anual 2019…….42
Figura 2: Ciclo de Deming asociado a cláusulas de norma ISO/IEC 27001….. .46
Figura 3: Cultura Organizacional y las Métricas de Seguridad…… 47

RESUMEN

La presente investigación fue ejecutada durante el año 2021, tuvo como objetivo principal determinar la influencia de un sistema de gestión para la seguridad de la información basado en la norma 270001:2013 en la Empresa Constructora Pérez & Pérez SAC, ya que presenta vulnerabilidades en todo los procesos de toda las áreas y peligra los activos de información de la organización, la metodología fue cuantitativa aplicada, se trabajó con el diseño de investigación experimental del tipo preexperimental. Además, se conformó la muestra de 20 registros en cada indicador con la finalidad de obtener un resultado favorable en las dimensiones de seguridad de la información, la confidencialidad de la información de un 68,85% de vulnerabilidad disminuyó a un 15,40% para la integridad de la información tuvo una disminución de vulnerabilidad de un 52,60% a 11,40% y por último la disponibilidad de la información se logró disminuir la vulnerabilidad de un 47,15% a 11,95% en los tres dimensiones se logró aumentar la seguridad de la información a un 80% a 90% de efectividad.

Finalmente se acierta que el sistema de gestión para la seguridad de la información basado en la norma iso27001 influye favorablemente en la constructora Pérez & Pérez SAC

Palabras claves: Sistema de gestión, seguridad de la información, norma ISO 27001:2013, confidencialidad, integridad, disponibilidad, Análisis de Riesgo.

ABSTRACT

This research was carried out during the year 2021, its main objective was to determine the influence of a management system for information security based on standard 270001: 2013 in Empresa Constructora Perez & Perez SAC, since it presents vulnerabilities in all the processes of all areas and jeopardize the organization's information assets, the methodology was applied quantitative, we worked with the experimental research design of the pre-experimental type. In addition, a sample of 20 records was made up for each indicator in order to obtain a favorable result in the dimensions of information security, the confidentiality of information from a 68.85% vulnerability decreased to 15.40% for The integrity of the information had a decrease in vulnerability from 52.60% to 11.40% and finally the availability of the information was achieved to reduce the vulnerability from 47.15% to 11.95% in the three dimensions. I managed to increase information security to 80% to 90% effectiveness.

Finally, it is correct that the information security management system based on the iso27001 standard has a favorable influence on the construction company perez & perez sac

Keywords: Management system, information security, rule 27001: 2013, confidentiality, integrity, availability.

I. INTRODUCCIÓN

En el Consejo Europeo creó un reglamento sobre la ciberseguridad que crea un esquema de certificación a escala EU y un nueva ley mejorada para la agencia de la UE con la finalidad de reemplazar en aquel entonces (ENISA) para garantizar un mercado digital transparente con miras al 2024 para salvaguardar la información, ya que la lucha con la delincuencia organizada digital están entre los 10 prioridades del periodo 2018-2021 (Consilium.europa.eu, 2021, ”Ciberseguridad: cómo la UE combate las amenazas cibernéticas”, párr.2 **),** La compañía Eset una empresa eslovaca que son expertos en la seguridad de la información, como todo los años dieron su informe anual año 2019 sobre cada continente, en esta oportunidad Latinoamérica ha reportado una tendencia baja de las variantes de diferentes Ransomware vistas en el año 2019 (**Ver Anexo A)** equiválete a un 26% (Eset Security Report ,2019 “ESET-security-report-LATAM-2019”, pág. 8); Según El Informe Técnico “Demografía Empresarial en el Perú – III TRIMESTE 2020 N° 02 – Noviembre 2020” En el mes de setiembre del 2020, Las empresas peruanas tuvieron una crecimiento de 2 millones 701 mil 66 empresas, una cifra mayor en 0,1% en comparación del informe el 2019. Según rubro registraron una alta de empresa que más resaltaron fueron explotación de minas y canteras (19,1%) y el comercio al por mayor (4,7%) (**Ver ANEXO B**) Para el sector Información y Comunicaciones que tiene una representación del %2,4.(**Ver ANEXO B**), a toda esta tabla se debe visualizar la información que lleva cada una de las empresas, aplacar las amenazas en la seguridad de la información para las PYMES del Perú; Para (Carnero, Armas & otros,2020) , solo el 10% de las empresas del Perú se encuentran monitoreando los problemas de seguridad, y el 51% de las empresas ya han resultados vulneradas.

La investigación se realizó en la Empresa Constructora Pérez & Pérez SAC, fue creada el 24 de abril del 2008 en la ciudad de Moyobamba, San Martín, en el rubro de construcción a lo largo de tu trayectoria obtuvo dos premios consecutivos de EMPRESA PERUANA DEL AÑO 2015-2016 **(ver ANEXO D),** obteniendo grandes resultados en sus obras en la región San Martín, como toda empresa va creciendo asume nuestros retos y responsabilidades lo cual implica tener más control en todos

sus procesos en cada área para que pueda tener una buena ejecución de obra. En el 2015 adquirieron 10 ordenadores nuevas distribuidos en sus diferentes áreas **(Ver ANEXO E)**, cada ordenador tiene los programas principales para su funcionamiento en la categoría de oficina, con el transcurso del tiempo cada ordenador se va almacenando información confidencial en el disco duro donde se divide en dos particiones (Disco C & Disco D) , en el Disco C se almacena toda la información de Windows & Programas de uso de oficina y en el Disco D es donde se almacena toda la información confidencial de cada área, cuando el personal de la área renuncia por motivos personales hay una alta probabilidad de que pueda sustraer la información confidencial del ordenador mediante un dispositivo USB este lo reconoce como tal y no manda ninguna alerta eso se baja al no tener unas políticas de seguridad de la información pueden insertar cualquier dispositivo externo, acceso a páginas web sin certificado SSL, descargas de aplicaciones de dudosa procedencia, no protegían los activos de la empresa, los incidentes eran mayores y su grado de complejidad se hacía más difícil encontrar la información sustraída, se registraban todo los días incidentes en toda las áreas de la organización producto del mal manejo en los procesos de las actividades de la organización como resultado cuando se deseaba buscar un documento y al visualizar su información dicho documento ya estaba manipulado, cada ordenador no tiene contraseñas seguras de accesos y los antivirus no tienen suficiente protección para salvaguardar la información confidencial. Dado las circunstancias, nace la investigación para mejorar la seguridad de la información de la constructora Pérez & Pérez, mediante el uso de la norma 27001:2013 y un sistema de gestión para salvaguardar la información su confidencialidad, disponibilidad e integridad de la forma más rápida y eficiente.

La formulación del problema nos lleva a criticar: ¿de qué manera un sistema de gestión basado en la norma ISO/ IEC 27001:2013 influye en la seguridad de la información de la empresa constructora Pérez & Pérez SAC, Moyobamba, San Martin, 2020, Teniendo en cuenta una justificación metodológica ya que vamos a utilizar la mejora continua en los procesos de la organización y una justificación practica ya que vamos emplear la normativa ISO/IEC: 27001:2013 ya que contienen elementos esenciales para tener un sistema de gestión de la seguridad de la

información , por lo tanto, se expresó el objetivo principal: determinar de qué manera un sistema de gestión basado en la norma ISO/IEC 27001:2013 influye en la seguridad de la información de la empresa constructora Pérez & Pérez SAC, Moyobamba, san martin,2020 paralelo se obtuvo como objetivos específicos: determinar de qué manera un sistema de gestión basado en la norma ISO/IEC 27001:2013 influye en la confidencialidad de la empresa Pérez & Pérez SAC, Moyobamba, San Martin,2020, teniendo como segundo objetivo : determinar de qué manera un sistema de gestión basado en la norma ISO/IEC 27001:2013 influye en la integridad de la empresa constructora Pérez & Pérez SAC, Moyobamba, San Martin,2020 y por ultimo determinar de qué manera un sistema de gestión basado en la norma ISO/IEC 27001:2013 influye en la disponibilidad de la empresa constructora Pérez & Pérez SAC, Moyobamba, San Martin,2020

Se planteó la hipótesis según los criterios recopilados en un sistema de gestión basado en la norma ISO/IEC 27001:2013 influye positivamente en la seguridad de la información de la empresa constructora Pérez & Pérez SAC, Moyobamba, San Martin,2020

II. MARCO TEÓRICO

Como base para esta investigación se defiende mediante investigaciones anteriores, Según el autor (Yáñez Cáceres,2017) cuyo objetivo fue la implementación de un SGSI teniendo en cuenta un software open source, basado en la normativa ISO27001:2013 con la finalidad de salvaguardar la información y que cumplan con los procedimientos para que las brechas de seguridad estén establecidas para mitigar los activos, ya con esta base iniciamos en el antecedente nacional cuyo autor (Ortiz Morales, 2018) el objetivo de esta investigación fue incrementar la mejora para la gestión de seguridad de la información. El tipo de investigación fue Aplicada con un método cuasiexperimental por lo tanto la conclusión fue lograr la implementación de 24 controles que sugiere la Norma ISO/IEC 27002:2013 que tuvo una mejora del 95%, de confianza en la siguiente investigación del autor (Zacarias Villafranca,2017) se pudo comprender el objetivo de esta investigación fue que tanto influye un modelo de seguridad de la información para mitigar los riesgos de los activos de información, el tipo de metodología empleada fue científica con un tipo de investigación aplicada y como resultado se obtuvo el 75% al realizar la implementación del modelo de seguridad de la información. En la siguiente investigación del autor (Pizarro Sánchez, 2018) se observó que el objetivo fue diseñar un modelo de seguridad de la información con un nivel de investigación descriptiva & Aplicada con una fusión de No-Experimental con un diseño transversal teniendo como resultado final se debe invertir en la seguridad de la información para poder demostrar que el factor humano tiene un gran conocimiento para la información. Con el siguiente autor (Huacasi Huacas, 2018)su objetivo principal fue mejorar el sistema de gestión basándose en la NTP ISO/IEC 207001 que ya cuentan en el Ejercito del Perú, con un nivel de investigación Aplicada y explicativa con un diseño preexperimental con un resultado favorable permitió identificar los activos críticos, identificación de las amenazas y vulnerabilidad dentro de la dirección del Ejercito del Perú Y por último tenemos al autor (Puma Arosquipa, 2017) nos comenta que su objetivo es reducir costos en auditorías externas, la metodología utilizada es cuantitativa y los resultados fueron que al momento de tener las herramientas necesarias lograron tener éxito en la reducción de costos siendo un 71% de gastos económicos.

Se menciona el antecedente internacional, cuyo autor (Vásquez García, 2017), en su investigación está basada en implementar políticas y controles en el servicio de Servicies Desk en la empresa SONDA, esto desplegará varias deficiencias para poder subsanar y así proteger la información confidencial, como resultado se dio a conocer que se debe realizar reuniones cada dos meses con la área de seguridad para poder dar los alcances del mismo y así pueda tener conocimientos de lo que se debería mejorar, con el siguiente autor (Torres Chango, 2020) su objetivo es la implementación de un modelo estructurado de un Sistema de Gestión de Seguridad de la Información (SGSI), modelando la norma iso27001, radica en la información de la empresa a partir de ese punto se propone políticas de seguridad muy coherentes y enmarcadas dentro de los límites de cumplimiento para tener un proceso de mejora continua, con el siguiente autor (Contreras Esguera, 2017) aplico la metodología magerit para determinar los riesgos para garantizar una buena seguridad de los activos para que al implementar el SGSI logre una identificación temprana de los diferentes eventos, al utilizar esta metodología identifica características esenciales para minimizar todos los posibles riesgos que puedan salvaguardar la información, con el penúltimo autor (Yánez Cáceres, 2017) propone utilizar 44 de los 114 objetivos de control de la norma ISO27001:2013 que prioriza las brechas de seguridad que recomienda DIPRES con la finalidad de mejorar los procesos en la organización, su metodología se concentran en la aprobación de los implementos para tener una buenas políticas y procedimientos de la seguridad de la información con el objetivo de continuar con la implementación de los 70 objetivos restantes y por ultimo (Diez Gutiérrez, 2019) nos explica que su objetivo es generar conocimientos para el sector público como se maneja de manera técnica la correcta configuración y esquema de la seguridad de la información para evitar las fallas de seguridad de un sistema informático que puedan generar grandes pérdidas económicas para las organizaciones.

Según el artículo **(**Think&Sell,2021) define que es un conjunto de reglas y principios que va de una manera ordenada para gestionar los procesos de una organización donde permitirá establecer políticas, objetivos y alcances del mismo, por otro lado según el autor**,** (Torres Alvarado 2019), la definición de un sistema de gestión transforma el ámbito empresarial en un entorno de desarrollo de los componentes

los cuales integran: estratégico, táctico, mejora anual de la operación y operacional la combinación de estos componentes es el resultado del día en los procesos de una organización, para los autores (Buenaño y Tierra, 2016) la denominan Circulo de Deming a los procesos de mejora continua en toda la organización que se desea implementar, se repite el ciclo con el fin de asegurar el mejoramiento de los procesos para reducir errores es una herramienta clásica e importante para cualquier campo de una actividad, por mientras en el artículo de (Ramos Davidson, 2021**)** da como resultado que gracias a las mejoras del ciclo Deming, los procesos de las organizaciones tienen una alta tasa de resultados calificándolo como buena y excelente gestión transformando su filosofía empresarial. Para el autor (Miladinovic Vitomir, 2020) resalta que para tener un buen desarrollo y funcionamiento de un sistema de gestión que sea eficaz y eficiente se basa a las condiciones previas para reducir riesgos en la seguridad de la información al tener en cuenta estas condiciones definimos los requisitos que debe cumplir el sistema para que sea capaz salvaguardar los datos de la organización, para (Youngin You ,Junhyoung Oh & Otros, 2018) un sistema de gestión debe tener características físicas necesarias para lograr una seguridad de la información para la organización, actualmente se verifica y se diagnostica la madurez de seguridad por niveles para ello debe tener un enfoque y cobertura diferentes para poder definir y medir con precisión la madurez. Según (Frayssinet Maurice, 2017) el circulo de Deming tiene como herramienta principal lograr la mejora continua en los procesos de las organizaciones reflejando un sistema de gestión, se denomina ciclo PHVA **(ver anexo F)** a los siguientes términos:

Plan: (Quiñones Seguil, 2019) Se debe definir como está actualmente la organización dentro de sus procesos y problemas, al tener una buena planificación de fechas, actividades & responsables el resultado será satisfactorio para la organización al cumplir con la actividad.

Hacer: (Túquerres Yuxara,2021), En etapa, una vez definido la planificación de los procesos, es hacer que las actividades definidas se pongan a la práctica empleando las mejoras que se acomoden al cambio de los procesos

Verificar: Para (Carla Carvalho, Eduardo Marques, 2018) en esta etapa se refiere a verificar la implementación que se está realizando en el SGSI mediante los indicadores desempeño de cada control dando un análisis crítico a las políticas de seguridad

Actuar: Para (Sartor, Marco & Orzes. Guido ,2019) este último paso es el resultado de la adaptación de los procesos adecuados para la mejora continua, con esto se realiza la estandarización del proceso existe dentro de la organización

Los beneficios de tener un SGSI con la norma ISO 27001 para (Calder, Alan,2016) tiene como principales pilares:

- Acelere la implementación de su sistema de gestión, ahorrándole tiempo y dinero.
- Proporcione a sus partes interesadas pruebas de que los riesgos se han abordado adecuadamente
. • Asegúrese de que no quede nada fuera de la documentación de su SGSI.
- Optimice el cumplimiento de la norma ISO 27001: 2013, haciéndolo más fácil y sencillo para usted y su equipo.
- Reduzca el margen de error y pérdida de tiempo al desarrollar sus propias plantillas.
- Bloquee los posibles callejones sin salida del proyecto.
- Integre fácilmente la documentación de su SGSI con sus procesos comerciales.

Mientras para la seguridad de la información, según el Autor (Cano, Jeimy), las buenas métricas de seguridad de la información **(Ver Anexo G)** son aquellas que tienen como resultado la toma decisiones en los procesos de la organización, dentro de las métricas, tenemos los elementos a evaluar que en este caso Confidencialidad, integridad y disponibilidad ya que es un modelo operativo para cualquier organización que desea implementar

Según (Solano Gilberto 2020) **,** en la dimensión disponibilidad es muy importante

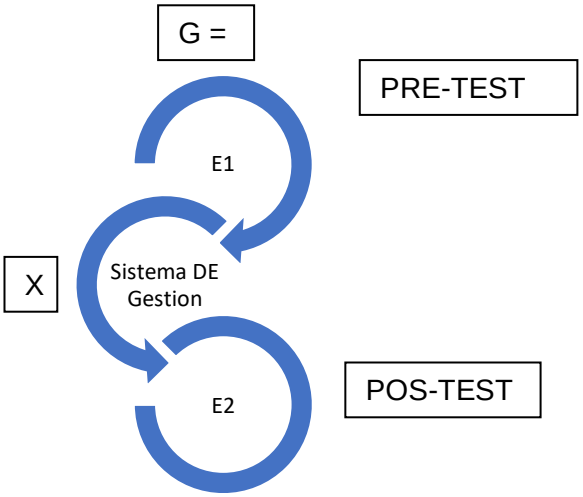
ya que no debe tener restricciones para los usuarios externos e internos que desean información de una empresa con tal solo una autorización previa para su uso adecuado, un ataque cibernético puede interrumpir los servicios que afectan los procesos del mismo, en la dimensión de confidencialidad según el mismo autor, es de carácter prioritario que las organizaciones autorizadas puedan tener el acceso a la información, ya que al tener un mal uso de la información puede ser publicada y ocasionar problemas legales por el uso no autorizado del mismo, por lo que explica que es importante tener medidas para resguardar el acceso a usuarios no autorizados y por último el autor señala que la dimensión de la integridad se encarga de no alterar la información de ninguna forma cuando el usuario final tiene acceso con autorización y deben ser auténticos para poder definir la información segura. Llegando a un análisis minucioso en toda las investigaciones presentadas estas son dirigidas a un SGSI en el cual se fundamenta la prioridad de la confidencialidad, disponibilidad e integridad de la información, estos tres dimensiones son pilares de la estructura de la seguridad de la información donde se busca que la confidencialidad no se encuentre disponible para el sector público sino a un sector segmentado de acuerdo a la organización, la integridad tenga una precisión y totalidad en la información de sus procesos y la disponibilidad es un conjunto de procesos de la información para el acceso de acuerdo a las políticas de la organización cuando las soliciten, en cuanto a la seguridad de la información, la autora (Jara Omar,2019**)**,Menciona que en una organización carece de políticas y controles eficientes en cuanto a la protección de los activos de la información los procesos, las tecnologías de información incluido el hardware y el software y las instalaciones, teniendo este beneficio da como resultado el uso de un sistema de gestión de la seguridad de la información basándose en la normativa 27001, para el autor (Cuervo Álvarez, 2017)**,** la norma ISO 27001 los pilares es confidencialidad, disponibilidad e integridad de los activos de la información en una organización, para identificar un peligro de información es importante resaltar los riegos y definir los parámetros para mitigar el peligro. Para (Death Darrem 2017), la seguridad de la información ha cambiado en los últimos años, la incorporación a nivel ejecutivo de las organizaciones se ha convertido en contribuyentes al éxito de las organizaciones comerciales, la disciplina consiste en asegurar las configuraciones de IT y las marchas de las herramientas de seguridad, para el (Grupo ACMS

Consultores, 2017) indica que la Norma 27001tiene dos fases , la primera fase es planificar e implementar las políticas del objetivo de los procesos de la organización después medir el rendimiento para la segunda fase se analizará los resultados de la primera fase para luego medirlas y mejorarlas con acciones correctivas para que tenga un buen progreso para prevenir cualquier fuga de información para tener una buena auditoria. por eso Talavera (2015,)27 indica que es un Estándar de carácter Internacional desarrollado con fundamentos para el análisis, implementación, control y mantenimiento, a través del establecimiento de un grupo de requisitos, como es de conocimiento menciona que tiene un enfoque orientado a los procesos de la organización dentro de los activos de información que puedan tener.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Según **(** Espinoza Ciro,2014 **)** su propósito es la aplicación de los conocimientos científicos para brindar alternativas positivas en los problemas en la sociedad, ya que se va a utilizar periféricos para tener un sistema de gestión viable, dentro de esta investigación aplicativa según el mismo autor en mención se basa en innovación con el propósito de dar resultados positivos a la investigación experimental del tipo preexperimental para crear tecnologías de aplicación para las soluciones que sea eficientes y productivas, ya que evaluaremos que tan eficiente es la seguridad de la información antes de aplicar el sistema de gestión y después de implementarla junto con los periféricos dando una comparación en ambos escenarios.



Dónde: G = Grupo experimental.

E1 = Variable dependiente Pretest (Seguridad de la información)

X = Variable independiente (Sistema de Gestión)

E2 = Variable dependiente Post-test (Seguridad de la información)

3.2. Variables y operacionalización

Variable independiente: Sistema de Gestión.

Variable dependiente: Seguridad de la información.

DVARIABLES	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICION
DE SISTEMA GESTION	La estructura de los sistemas de gestión debe ser tal que sea factible realizar una coordinación y un control ordenado y permanente sobre la totalidad de las actividades que se realizan (Virginia, azcurram, Cavallaro & Otros, 2014)	Es una combinación de roles y responsabilidades que va implementado en los procesos de infraestructura, personal, operaciones y aplicaciones que se llevará periódicamente una auditoria donde se accionará medidas preventivas como correctivas para el buen uso de la información			
SEGURIDAD DE LA INFORMACION	Es una disciplina que debe ser mencionada en toda la empresa para la gestión de TIC, su función principal es que todo el nivel sea aceptable para determinar el riesgo de la información y de los dispositivos tecnológicos que permiten sus procesos para la recopilación de información que correspondan. (Valencia & Orozco, 2017**)**	Se trata de un estado donde relaciona todo los procesos y sistemas destinados a reducir número de incidentes de robo de información mediante un virus informático o accesos no autorizados de factor humano.	CONFIDELIDAD	***Accesos no autorizados*** $$\mathbf{ANA} = \frac{\boldsymbol{RANA}}{\boldsymbol{TAD}} \times \mathbf{100}$$ Donde: **ANA**: Accesos No Autorizados **TAD**: Total de Accesos del Dia **RANA**: Reporte de Accesos No Autorizados	DE RAZON
			INTEGRIDAD	**Virus informático** $$\mathbf{VI} = \frac{\boldsymbol{VINE}}{\mathbf{VID}} \times \mathbf{100}$$ Donde: **VI:** Virus Informático **VINE**: Virus Informático No Eliminado **VID**: Virus Informático del día	
			DISPONIBILIDAD	***Eliminar, borrar manipular datos** $$\mathbf{EBMD} = \frac{\mathrm{EMBDNR}}{\mathrm{TMDD}} \times \mathbf{100}$$ Donde: **EBMD:** Manipulación de Datos TMDD: Total de Manipulación de datos del día EMBDNR: Eliminar, Manipular, Borrar Datos No reconocidos	

Tabla 1: Matriz de Operacionalización de Variables

3.3. Población (criterios de selección), muestra, muestreo, unidad de análisis

Según (Ñaupas, Paitán, Ramírez & Otros, 2014**)** un muestreo es definir con mucha claridad la población o universo que representa con un conjunto de personas o registros que son motivo de investigación.

INDICADOR	CANTIDAD DE POBLACION
accesos no autorizados	253 reporte de accesos no autorizados
virus informático	240 reportes de manipulación de datos
eliminar, borrar manipular datos	87 reportes de virus informático

Tabla 2: Población

(Elaboración Propia)

Según (Ñaupas, Paitán, Ramírez & Otros, 2014 **)** El resultado de la muestra es una selección por diferentes métodos diversos con la finalidad de no alterar la población.

Reporte de Acceso No Autorizados

$$n = \frac{253 * 1.96^2 * 0.5 * 0.5}{0.05^2(253 - 1) + 1.96^2 * 0.5 * 0.5} = 153$$

Reporte de Virus Informático

$$n = \frac{240 * 1.96^2 * 0.5 * 0.5}{0.05^2(240 - 1) + 1.96^2 * 0.5 * 0.5} = 148$$

Reporte de Manipulación de Datos

$$n = \frac{87 * 1.96^2 * 0.5 * 0.5}{0.05^2(87 - 1) + 1.96^2 * 0.5 * 0.5} = 71$$

Según **(**Ñaupas, Paitán, Ramírez & Otros, 2014) Tras obtener el resultado de las muestras representativas estas generan confianzas para tener una investigación clara. Para este estudio el muestreo asignado es de tipo probabilístico, tienen más ventajas que los no probabilísticos ya que la muestra todos los individuos tienen la misma probabilidad de ser seleccionados lo que más determina el nivel de confianza y el error del muestro realizado Como se puede apreciar nuestra muestra tiene diferentes resultados en los tres indicadores por lo tanto quedo confirmada en 20 fichas de registro, ya que el muestreo es probabilístico por conveniencia.

3.4. Técnicas e instrumentos de recolección de datos

TÉCNICA	INSTRUMENTO	FUENTE	INFORMANTE
Observación	Guía de observación de campo	Documentación del área de IT	EDUARDO RISCO – ENCARGADO DE IT

Tabla 3: Técnicas e instrumentos empleados

Elaboración Propia

Técnica:

***Observación:**

Para (Tenorio & Rivas,2017) la técnica de observación se aplica para observar todas las áreas de una organización para evaluar sus planes de trabajo y así determinar los procesos de la organización.

Instrumento de recolección de datos:

***Guía de Observación de Campo:**

Para (Campos & Lule, 2012) La guía de observación es el instrumento que permite al observador situarse de manera sistemática en aquello que realmente es objeto de estudio para la investigación; también es el medio que conduce la recolección y obtención de datos e información de un hecho o fenómeno.

Validez del instrumento de investigación

- **Validez de contenido:**

Para (Espinoza Ciro,2014) Se medirán los Items que se medirán y seran

evaluados mediante el juicio de expertos.

- **Validez de criterio:**

Para (Espinoza Ciro,2014) Se realiza una comparación entre los ítems validadas y un criterio que se asemeje a la realidad.

- **Validez de constructo**:

Para (Espinoza Ciro,2014) Se realiza un proceso de resultados analíticos mediante un programa SPSS o minitab.

3.5. Procedimientos

Los datos obtenidos de la empresa Constructora Perez & Perez SAC fueron gestionados mediante una carta de presentación hacia el gerente general dando a conocer que estaré realizando una investigación para darle una solución a su problemática, autorizando el uso de su información para poder llevarlo a cabo con éxito. **(VER ANEXO H)**

A lo largo de los meses del 2021, se realizó un registro en Excel mencionando los incidentes que presentaron en las distintas áreas de la empresa, se realizó una evaluación minuciosa a través del juicio de expertos usando el procedimiento test y pro test dando una confianza de datos plasmándole al IBM SPSS Statistics Ver. 26 para su análisis correspondiente,

Además, esta investigación fue desarrollada con metodología de la norma ISO/IEC 27001:2013, para poder identificar los objetivos que menciona la normativa ISO/IEC 27001:2013 se requiere organizar la seguridad de la empresa y efectuar la implementación de acuerdo al ciclo Deming para mejorar cada proceso y así pueda cumplir con las políticas establecidas por la norma, Por último, se realizó la discusión de resultados, conclusiones y recomendaciones para la investigación

3.6. Método de análisis de datos

En esta investigación de acuerdo a los resultaros arrojados en el pretest y después de la implementación del sistema de gestión para la seguridad de la información con los resultados pos-test realizaremos la comparación de las

hipótesis y dialogar si es aprobada o desaprobada para ello se logró efectuar la (autor) Prueba T de Student para muestras menores a 30 & y la prueba Z para muestras mayores a 30, ya que para estos cálculos estadísticos, se realizó el apoyo del programa SPSS V26 para determinar el pretest y postest ya que nos dará el resultado en instantes, como resultado final nos dirigimos al test de normalidad y con los resultados en las muestras utilizaremos Kolmogorov – Smirnov para muestras grandes mayores a 50, ya que según el autor (Thomas Viehmann, 2021) , comenta que la prueba en mención viene hacer una prueba estadística muy importante para detectar las muestras mayores de la misma distribución y la shapiro Wilk para muestras pequeñas ya que los autores(Flores, Muñoz Escobar & Sánchez Ac, 2019) nos comenta que en esta prueba su funciona es estimar mediante un proceso de simulación la potencia de las muestras en distintas fases y así resulte una probabilidad de rechazar la hipótesis nula cuando esta arroje un resultado falso, considerando una muestra menos de 50 para el uso correspondiente

3.7. Aspectos éticos

Es de carácter importante la responsabilidad de lleva el investigador al honrar la originalidad del estudio que se está realizando, así mismo de la confianza de los datos incorporados por parte de la empresa Constructora Perez & Perez SAC, salvaguardar la información obtenida para no perjudicar a las personas que me brindaron los datos como también honrar la confianza depositada al investigador para poder darle solución a su problemática

IV. RESULTADOS

Los resultados de los análisis obtenidos en este estudio tienen como importancia que tanto contribuye un sistema de gestión basado en la Norma ISO/IEC 27001:2013 en la parte fundamental de la organización que resalta la parte operativa en temas de seguridad de la información, determinará si influye favorablemente o no dentro de las políticas de seguridad para salvaguardar la confidencialidad, integridad & disponibilidad.

La presente investigación efectuó el pretest de la situación actual de la empresa constructora Perez & Perez Sac (**Ver anexo I**) y el postest luego de ejecutar el sistema de gestión (**Ver anexo I)** para identificar las hipótesis propuestas en el estudio de esta presenta investigación:

Análisis Descriptivo:

Los hallazgos conseguidos para la investigación se puedes observar en las tablas 4 y 5 y 6 de los tres indicadores que están se presentan en esta investigación:

Indicador 1: Accesos no autorizados:

Los resultados de este indicador son los siguientes:

Tabla 4: Estadísticos Descriptivos Accesos No autorizados

	N	MÍNIMO	MÁXIMO	MEDIA	DESVIACIÓN ESTÁNDAR	VARIANZA
Pretest_ANA	20	45	83	68,85	12,991	168,766
Postest_ANA	20	0	30	15,40	8,165	66,674
N valido (Por lista)	*20*					

Elaboración: SPSS V26

En la Tabla 4 podemos visualizar que para la mediana el nivel de Accesos No Autorizados entabla un 68,85% en el pretest y para el postest es de un 15,40% para nuestra muestra, al realizar la comparación de las medias conseguidas, se

puede apreciar una disminución del 53% dando como resultado que al implementar el sistema de gestión para la seguridad de la información se logró disminuir los accesos no autorizados.

Indicador 2: Eliminar, Manipular, Borrar Datos

Los resultados descriptivos para el segundo indicador se pueden apreciar en lo siguiente:

Tabla 5: Estadísticos descriptivos Eliminar Borrar Manipular Datos

	N	MINIMO	MAXIMO	MEDIA	DESVIACION ESTÁNDAR	VARIANZA
Pretest_EMBD	20	0	70	52,60	8,708	75,832
Postest_EMBD	20	40	22	11,40	7,287	53,095
N valido (Por lista)	*20*					

Elaboración: SPSS V26

En la tabla 5, se puso medir que la media de la tasa de promedio de Eliminar, Manipular y Borrar datos alcanzó un valor del 52,60% mientras que en el post test obtuvo un valor de 11.40% para la muestra, por lo tanto, al efectuar la similitud entre las medias encontramos se logo una reducción del 41.20%, logrando que la manipulación de datos tenga diferencia y mayor control en todas las áreas dentro del sistema de gestión para la seguridad de la información

Indicador 3: Virus informático

Los resultados descriptivos para el segundo indicador se pueden apreciar en el siguiente cuadro

Tabla 6: Estadísticos descriptivos Virus Informático

	N	MINIMO	MAXIMO	MEDIA	DESVIACION ESTÁNDAR	VARIANZA
Pretest_VI	20	30	75	47,15	12,419	154,239
Postest_VI	20	0	29	11,95	9,795	95,945
N valido (Por lista)	*20*					

Elaboración: SPSS V26

En la tabla 6 se pudo medir que la media de la tasa promedio de Virus Informático alcanzo un valor del 47.15% mientras que en el post test obtuvo un valor del 11.95% para la muestra correspondiente, por lo tanto, al efectuar la similitud entre las medias encontramos una reducción del 35.20% logrando que el virus informático sea eliminado de acuerdo al sistema de gestión de la seguridad de la información

Análisis Inferencial

En esta oportunidad se utilizará el método Kolmogorov- Smirnov ya que su métrica depende de los detalles proporcionados en el uso de distribución estándar en los tamaños de muestra que son mayores a 50 muestras (Renato Fabbri Renato & Gularte De Leon, 2017). si el valor es mayor a 0.05 se mide que la información admita una distribución normal, caso contrario si es menor a 0.05 resulta que es una distribución atípica. La prueba se ejecutó con el programa estadísticos SPSS v26, logrando los siguientes resultados

Indicador 1: Accesos no autorizados

La prueba de normalidad para el primer indicador es efectuada en el pretest y postre obtuvieron los siguientes resultados estadísticos

Tabla 7: Prueba de Normalidad de Accesos No Autorizados

	KOLMOGOROV – SMIRNOV		
	Estadístico	Gl	Sig.
PRETEST_ANA	,254	20	.002
POSTEST_ANA	,213	20	.018
Corrección de significación de Lilliefors			

Elaboración: SPSS V26

En la Tabla 8, los resultados de la prueba indican que el Sig de la muestra generada antes fue de 0.002 cuyo valor es menor que el 0.05(Nivel de significancia), con este resultado se rechaza la hipótesis nula, de igual manera, en el post de la prueba indica el Sig. es de 0.018 cuyo valor es menor, por tanto, aplicaremos Wilcoxon ya que ambos tienes una distribución atípica.

Indicador 2: Eliminar, Manipular Eliminar Datos

La prueba de normalidad para el segundo indicador es efectuada en el pretest y postre obtuvieron los siguientes resultados estadísticos

Tabla 8: Prueba de Normalidad Accesos No Autorizados

	KOLMOGOROV – SMIRNOV		
	Estadístico	Gl	Sig.
PRETEST_ANA	,167	20	.144
POSTEST_ANA	,102	20	.200
Corrección de significación de Lilliefors			

Elaboración: SPSS V26

En la tabla 8, se estimó que el resultado procede a una distribución normal, ya que el valor de significancia del pretest es de 0.114 y el pos-test es de 0.200, ambos valores cumplen su función que es superior al margen de error ($\alpha = 0,05$)

Indicador 3: Virus Informático

La prueba de normalidad para el tercer indicador es efectuada en el pretest y postre obtuvieron los siguientes resultados estadísticos

Tabla 9: Prueba de Normalidad de Virus Informático

	KOLMOGOROV – SMIRNOV		
	Estadístico	Gl	Sig.
PRETEST_ANA	,268	20	.001
POSTEST_ANA	,189	20	.060
Corrección de significación de Lilliefors			

Elaboración: SPSS V26

En la tabla 9, se estimó que el resultado procede que tiene una distribución no normal, ya que el significante del pre test tiene 0.001 y el poste test es de 0.060, en este caso utilizaremos Wilcoxon ya que en el pretest es inferior al margen de error (α = 0,05)

.

Prueba de hipótesis

En esta investigación se utilizó el T-Student y Wilcoxon. Según (Caycho Carlos, Castillo Carlos, Merino Víctor, 2020) los datos experimentales o muestras obtenidas para la hipótesis debe cumplir con la condición de normalidad teniendo datos no paramétricos en el resultado de la hipótesis

Hipótesis de investigación 1:

Hipótesis H0: El sistema de gestión no incrementa los accesos no autorizados para la seguridad de la información en la empresa constructora Pérez & Pérez sac

H0= ANA ≥ ANA

Hipótesis Ha: El sistema de gestión incrementa los accesos no autorizados para la seguridad de la información en la empresa constructora Pérez & Pérez sac

Ha = ANA < ANA

Para la contratación de la hipótesis de la investigación 1, se explicó la prueba de Wilcoxon, en vista que la información adoptó una distribución no normal, en la tabla 10, se apreció que existe un valor de 0.000 menor a 0.05 lo que significa

que hay una diferencia en el % de accesos no autorizados antes y después del sistema de gestión para la seguridad de la información

Tabla 10: Prueba de rango de Wilcoxon de ANA

		N	Rango promedio	Suma de rangos
Pretest_ANA & Postest_ANA	Rangos negativos	20a	10,50	210,00
	Rangos positivos	0b	,00	,00
	Empates	0c		
	Total	20		
a. **Postest_ANA** < **Pretest_ANA**				
b. **Postest_ANA** > **Pretest_ANA**				
c. **Postest_ANA** = **Pretest_ANA**				

Elaboración: SPSS V26

Tabla 11: Estadístico de contraste del Indicador 1 Accesos No Autorizados

	Pretest_ANA & Postest_ANA
Z	-3,922b
Sig. asintótica(bilateral)	,000
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos positivos.	

Elaboración: SPSS V26

Una de las maneras de validar la hipótesis es por medio de la aproximación normal (Z), ya que este obtuvo el valor de (-3,922) < α (0,05) empleado a nivel de significancia. En conclusión, se determinar lo anteriormente descrito, la Hipótesis alterna es la que se admite.

Hipótesis de investigación 2:

Hipótesis H_0: El sistema de gestión no incrementa la manipulación, borrar y eliminar datos para la seguridad de la información en la empresa constructora Pérez & Pérez sac

$$\mathbf{H_0 = EMBD_a \geq EMBD_d}$$

Hipótesis H_a: El sistema de gestión incrementa la manipulación, borrar y eliminar datos para la seguridad de la información en la empresa constructora Pérez & Pérez sac

$$\mathbf{H_0 = EMBD_a < EMBD_d}$$

Para la contratación de la hipótesis de investigación 2, se empleó la prueba t Student, en vista de que la información adoptó una distribución normal. En la Tabla 12, se aprecia que existe una diferencia significativa entre las medias antes y después del procedimiento porque el valor de t (17,588) < α (0,05).

Tabla 12: Prueba t Student de Manipular Borrar Eliminar Datos

	Media	t	gl	Sig. (bilateral)
Pretest_EMDB	52,60	17,588	19	,000
Postest_EMDB	11,40			

Elaboración: SPSS V26

Hipótesis de investigación 3:

Hipótesis H0: El sistema de gestión no incrementa el virus informático para la seguridad de la información en la empresa constructora Pérez & Pérez sac

$$\mathbf{H0 = VIE \geq VIE}$$

Hipótesis Ha: El sistema de gestión incrementa el virus informático para la seguridad de la información en la empresa constructora Pérez & Pérez sac

Ha = VIE < VIE

Para la contratación de la hipótesis de la investigación 3, se explicó la prueba de Wilcoxon, en vista que la información adoptó una distribución no normal, en la tabla 10, se apreció que existe un valor de 0.000 menor a 0.05 lo que significa que hay una diferencia en el % de accesos no autorizados antes y después del sistema de gestión para la seguridad de la información

Tabla 13: Prueba de rango de Wilcoxon de VI

		N	Rango promedio	Suma de rangos
Pretest_VIE & Postest_VIE	Rangos negativos	20a	10,50	210,00
	Rangos positivos	0b	,00	,00
	Empates	0c		
	Total	20		
a. **Postest_VIE** < **Pretest_VIE**				
b. **Postest_VIE** > **Pretest_VIE**				
c. **Postest_VIE** = **Pretest_VIE**				

Elaboración: SPSS V26

Tabla 14: Estadístico de contraste de VIE

	POStest_VIE & Pretest_VIE
Z	-3,921b
Sig. asintótica(bilateral)	,000
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos positivos.	

Elaboración: SPSS V26

Una de las maneras de validar la hipótesis es por medio de la aproximación normal (Z), ya que este obtuvo el valor de (-3,921) < α (0,05) empleado a nivel de significancia. En conclusión, se determinar lo anteriormente descrito, la Hipótesis alterna es la que se admite.

V. DISCUSIÓN

La presente investigación se efectuó en la empresa constructora Perez & Perez Sac que se encuentra en la ciudad de Moyobamba, provincia de san Martin, Con los resultados obtenidos en la presenta investigación se analizó y se comparó los indicadores de “Accesos No autorizados”, “Manipular, Eliminar y Borrar Datos” y por último “Virus Informático” antes y después de la implementación de un sistema de gestión para la seguridad de la información basado en la norma 27001.

Después de haber implementado el sistema de gestión, se realizó un postest para recolectar nuevamente la información de los mismos indicadores lo cual provienen del pretest, para llegar a una conclusión en los resultados, se utilizó el programa IBM SPSS26, los cuales indican que el sistema de gestión mejora la seguridad de la información basado en la normativa 27001 en la empresa constructora Pérez & Pérez sac.

Se detalla los resultados realizados para obtener la comparación de resultados de los indicadores, para el primer indicador “Accesos No Autorizados” se obtuvo un valor 68,85% de accesos sin autorización antes de implementar el sistema de gestión y un valor de 15,40% después de la implementación y como resultado que este indicador hubo una disminución del 53,45%, quiere decir que la seguridad de la información de este indicador tiene una aceptación del 84,6%, para el segundo indicador “Eliminar, Manipular y Borrar Datos” se obtuvo los siguientes valores 52,60% antes de la implementación y 11,40% después de la implementación y como resultado de este indicador que disminuyó un 41,20% quiere decir que 88,60% tiene una aceptación favorable en la seguridad de la información y para ultimo indicador “Virus Informático” antes de realizar la implementación se obtuvo un 47,15% y después de la implementación del sistema se obtuvo una reducción del 11,95% como resultado el 88.05% cumple la función de la seguridad de la información , como podemos observar el sistema de gestión ayudo a mejorar la seguridad de la información aplicando la normativa 27001 para la empresa constructora Pérez & Pérez sac y disminuir los riesgos para salvaguardar la información de la empresa.

Para poder comparar esta investigación, vamos analizar con los antecedentes

previamente citados, en este caso el autor (Ortiz Morales, 2018) según los resultados que dicta esta investigación antes de la implementación los controles estratégicos tenía una medición del 12% y para los controles operativos el nivel inicial era de 16%, después de la implementación basándose en la normativa 27002:2013 aumento significativamente a un 14% y el 20% dando como un promedio general de 28% a 34% al nivel de seguridad de la información de su organización,

.

Por otro (Zacarias Villafranca,2017) en la Central de Operaciones Policiales de la Región Policial Junín los resultados obtenidos a raíz de la mitigación de riesgos antes de la implementación fue de 1,22% que representa al global un 24% y post implementación fue de 4,96% que representa un 99% con el balance general lo que significa un aumento del 3,74% que representa un 75% del nivel de concientización y percepción sobre la mitigación de riesgos de los activos de información, teniendo estos resultado el autor refleja que se ha incrementado un 75% , para la mitigación de las amenazas representaba un 26% y al implementar tuvo un resultado del 99%, para el autor representa un aumento de nivel de mitigación equivalente al 75% y por último en la mitigación de las vulnerabilidades representa un 30% y después de la implementación representa un 100% con esto el autor resalta un 70% en el nivel de amenazas de los activos de información.

Para el autor (Pizarro Sánchez, 2018) en donde realiza su investigación para un modelo de gestión de seguridad de la información con el factor humano como principal protagonista en la institución Icpna de la región centro obtuvo los siguientes resultados arrojaron que los entrevistados un 57% no tienen conocimiento sobre temas de seguridad de la información, mientras que un 34% solo tienen conocimiento básico, con esta resultado nos evidencia que la institución no invierte en capacitación sobre las herramientas de it para la seguridad de la información .

Así mismo en la investigación del autor (Huacasi Icono, 2018) resalta en sus resultados que la implementación del sistema de gestión de la seguridad de la

información aplicando la NTP ISO/IEC 27001, permite a la organización tener un análisis adecuado en los activos para que sea claros y precisos, dentro de la implementación del sistema de gestión se evalúa, analiza y valora los riesgos permitidos para identificarlos y medir el grado de impacto que puede ocasionar dentro de la organización

Para (Contreras Esguera, 2017) aplico un diseño de un sistema de gestión de seguridad de la información para su organización se apoyó de varios métodos para la recolección de información para este proceso se utilizó la entrevista verbal, encuestas, análisis de red con toda esta información pudo identificar los activos y recursos a proteger y las posibles vulnerabilidades de cada proceso, una vez identificado los riesgos se evalúa las acciones más seguras apoyándose del estándar iso 27001,

(Yánez Cáceres, 2017) ejecutó la implementación de un SGSI compuesto en 5 sistemas basados en un software open source para la mejora continua de los procesos de seguridad de la información en la organización, desarrollando un aprendizaje y la creación de equipos de trabajos orientados a las políticas para los ciclos de aprobación, donde se cumplieron 44 objetivos del control, es fundamental resaltar que su objetivo principal es la implementación de los 144 objetivos para que la organización salvaguarde sus activos de información.

(Vásquez García, 2017), una propuesta de Gestión de seguridad de la información donde lleva a cabo Análisis de riesgo que permitirá conocer los riesgos, amenazas, vulnerabilidad de cada activos de la organización, el resultado es disminuir el mínimo del riesgo aplicando la normativa iso 27001:2013 para cual debido al crecimiento que tiene la organización debe configurar sus políticas de seguridad constantemente y así poder identificar las nuevas amenazas para que puedan analistas y mitigar el riesgo, no existe una seguridad al 100% por lo tanto la organización debe cubrir requerimientos y buenas prácticas que establece dicha norma para una mejora continua .

VI. CONCLUSIONES

Finalmente, en este estudio se obtuvieron los siguientes hallazgos para determinar el resultado:

Se ha comprobado que el porcentaje de Accesos no Autorizados utilizando el sistema de gestión para la seguridad de la información de la empresa constructora Pérez & Pérez sac disminuyo favorablemente de 68,85% a un 15,40%, dando un resultado favorable 84,6

Se ha comprobado que el porcentaje de Manipulación, Borrar y Eliminar Datos utilizando el sistema de gestión para la seguridad de la información de la empresa constructora Pérez & Pérez sac disminuyo favorablemente de un 52,60% a un 11,40% como resultado favorable asciende un 88,60%

Se ha comprado que el porcentaje de Virus informático utilizando el sistema de gestión para la seguridad de la información de la empresa constructora Pérez & Pérez sac disminuyo favorablemente de un 52,60% a 11,40% dando como resultado a 88,05%

Se ha comprado que al implementar el sistema de gestión basado en la normativa 27001 se pudo configurar políticas de seguridad para todos los activos de la organización

VII. RECOMENDACIONES

Mis recomendaciones para final para futuros trabajos de la tesis son:

Se sugiere utilizar todas las políticas de la normativa iso 27001 de acuerdo a la estructura de la organización y que áreas desean tocar

Se sugiere realizar la compra de tecnologías it para salvaguardar la información de la organización

Se sugiere implementar la norma ISO/EIC 27001:2013 en toda la organización con el fin de proyectarse a lograr una certificación internacional y generar confianza a todos sus clientes

Se debe invertir en la seguridad de la información de la organización ya que es una empresa escalable por lo tanto necesitará más políticas a medida que van creciendo en el rubro

Se recomienda tener en planos toda la estructura de la empresa para el cableado estructurado con el fin de conectarse con todas las tecnologías it para salvaguardar la información

REFERENCIAS

Buenaño Lliguin, Y. M., & Tierra Satán, J. P. (2017). Efectos de la aplicación del ciclo de Deming/pdca (planificar, hacer, verificar y actuar) de la organización de los ii juegos deportivos nacionales estudiantiles Universitarios y Politécnico. Recuperado en : http://dspace.unach.edu.ec/handle/51000/3773

Campos y Covarruubias, Guillermo & Lule Martinez, Nallely Emma(2012): "LA OBSERVACIÓN, UN MÉTODO PARA EL ESTUDIO DE LA REALIDAD" Recuperado en : https://dialnet.unirioja.es/servlet/articulo?codigo=3979972

Calder, A. (2016). Nine Steps to Success : An ISO27001:2013 Implementation Overview: Vol. Third edition. ITGP. Recuperado en : http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1232541&lang=es&site=eds-live&ebv=EB&ppid=pp_108

Caycho, C., Castillo, C., & Merino, V. (2019). *Manual de estadística no paramétrica aplicada a los negocios*. Alianza Editorial. Recuperado en : https://hdl.handle.net/20.500.12724/9349

Cano, Jeimy, Métricas en Seguridad Informatica: Una Revision Academica. Recuperado en https://acis.org.co/portal/sites/all/themes/argo/assets/img/Pagina/07-MetricasSeguridadInformaticaUnaRevisionAcademica.pdf

Carvalho, C., & Marques, E. (2019). Adapting ISO 27001 to a Public Institution. CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings, 1–6. Recuperado en : http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=1&sid=a7602241-4688-46bf-8a8f-3d05d0b54aba%40sdc-v-sessmgr02

ESPINOZA MONTES, CIRO,2014, Metodologia de investigación tecnológica "Pensando en Sistemas", Recuperado en : https://ciroespinoza.files.wordpress.com/2012/01/metodologc3ada-de-investigacic3b3n-tecnolc3b3gica.pdf

Consilium.europa.eu. 2021. Ciberseguridad: cómo la UE combate las amenazas cibernéticas. [online] Recuperado en: <https://www.consilium.europa.eu/es/policies/cybersecurity/>

CONTRERAS ESGUERA 2017, diseño de un sistema de gestión de seguridad de la información basado en la norma iso/iec 27001 para la direccion de sistemas de la gobernación de boyacá, recuperado en: https://repository.unad.edu.co/bitstream/handle/10596/11895/33367604.pdf

Cuervo Alvarez, Sara. 2017. Implementación ISO 27001. 2017 Recuperado en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64827/8/scuervoTFM0617memoria.pdf

Carnero Garay, D. F., Armas-Aguirre, J., Antonio, M., Ramos, C., & Madrid Molina, J. M. (2020). Modelo de gestión de riesgos de seguridad de información para mitigar el impacto en las PYMEs en Perú. CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings, 1–6 Recuperado en. http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=147256080&lang=es&site=eds-live

Death, D. (2017). Information Security Handbook. Van Haren Publishing.Recuperado en : http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=1655557&lang=es&site=ehost-live&ebv=EB&ppid=pp_Cover

DIEZ GUTIERREZ 2019, implementacion de una solucion tecnologica enfocada a fortalecer los pilares de la seguridad de la informacion de un sistema web, mediante la aplicación de herramientas de codigo abierto, recuperado en http://132.248.9.195/ptd2019/octubre/0796817/0796817.pdf

Espinoza Montes, C. (2017, 13 enero). Metodología de Investigación Tecnológica Pensando en Sistemas. Recuperado en http://repositorio.uncp.edu.pe/handle/UNCP/1148.

Fabbri Renato , Gularte De Leon Fernando, 2017: A statistical distance derived from the kolmogorov-smirnov test: specification, reference measures (benchmarks) and example uses, recuperado en : https://arxiv.org/pdf/1711.00761.pdf

Frayssinet Maurice, 2017: Taller de Implementación de la norma ISO 27001, Recuperado en : https://www.pecert.gob.pe/images/publicaciones/4.pdf

Flores Muñoz Pablo, Muñoz Escobar Laura , Sánchez Acalo Tania 2019: estudio de potencia de pruebas de normalidad usando distribuciones desconocidas con distintos niveles de no normalidad: recuperado en : http://dspace.espoch.edu.ec/bitstream/123456789/11192/1/per_n21_v1_05.pdf

Grupo ACMS Consultores (2017). *UNE-ISO/IEC 27001- Protección ante Riesgos de la Seguridad de la Información.* (En línea). Recuperado en: https://www.grupoacms.com/blog/une-isoiec-27001-proteccion-riesgos-seguridad-informacion/

HUACASI HUACASI, 2018: implementación de un sistema de gestión de seguridad de la información aplicando la ntp iso/iec 27001 para mejorar el proceso de seguridad de información en el ejército del perú, recuperado en https://repositorio.utelesup.edu.pe/handle/utelesup/781

Jara, Omar. (2019, 11 abril). Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018. Https://Repositorio.Ucv.Edu.Pe/Handle/20.500.12692/31209.

Instituto Nacional de Estadistica e Informatica,2020. "Demografia

Empresarial en el Perú III trimestre 2020 N°02-Noviembre 2020 Recuperado en: <http://m.inei.gob.pe/media/MenuRecursivo/boletines/boletin-demografia_empresarial.pdf>

Miladinović, V. T. (2020). development of awareness and competences of employees in the processes of information security management system - guidelines for practical application -. journal of information technology & applications, 10(2), 87–95 recuperado en : http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=1&sid=e5fda9c1-baf2-4f0f-b47f-efe2eb5a1acc%40sessionmgr4008

Ñaupas, H., Paitán, H. Ñ., Ramírez, E. N., Mejía, E. M., & Paucar, A. V. (2014). *metodología de la investigación*. ediciones de la u. recuperado en : https://corladancash.com/wp-content/uploads/2019/03/metodologia-de-la-investigacion-naupas-humberto.pdf

ORTIZ MORALES (2018). Controles de seguridad según la norma ISO/IEC 27002:2013 para el mejoramiento de la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva (Tesis de titulación) Recuperado en : . http://repositorio.unas.edu.pe/handle/UNAS/1710

PIZARRO SÁNCHEZ 2018: Diseño de un modelo de gestión de seguridad de la información con un enfoque en el factor humano para el ICPNA Región Centro en el año 2017, recuperado en https://hdl.handle.net/20.500.12394/4902

PUMA AROSQUIPA 2017: IMPLANTACIÓN DE UN PROCESO DE AUDITORÍA DE SEGURIDAD DE INFORMACIÓN BAJO LA NORMA ISO/IEC 27002 EN UNA ENTIDAD FINANCIERA DE PUNO – 2016, recuperado en http://repositorio.unap.edu.pe/bitstream/handle/UNAP/6629/Puma_Arosquipa_Max_Yonel.pdf?sequence=1&isAllowed=y

Quiñones Seguil, C. G. (2019, 19 agosto). *Aplicación del ciclo PHVA para mejorar la productividad en la fabricación de pernos en Industrias Mendoza S.R.L, Callao - 2019*. Recuperado en : https://repositorio.ucv.edu.pe/handle/20.500.12692/45588

Ramos, D. (2021, 1 marzo). *Gurús de la calidad: William Edwards Deming - Blog de la Calidad % %*. Blog de la Calidad. Recuperado en : https://blogdelacalidad.com/gurus-de-la-calidad-william-edwards-deming/

Sartor, Marco & Orzes. Guido (2019). *Quality Management : Tools, Methods and Standards: Vol. First edition*. Emerald Publishing Limited. Recuperado en : http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1949715&lang=es&site=eds-live&ebv=EB&ppid=pp_122

Solano Méndez, G. E. (2020). Propuesta mediante la normativa ISO 27001 para la gestión de la seguridad de la información en la empresa Udersol en Costa Rica. [Proyecto de Graduación de Licenciatura, Universidad Latina de Costa Rica]. Repositorio Institucional de la Universidad Latina de Costa Rica.Recuperado en: https://hdl.handle.net/20.500.12411/293

Tenorio Arque, Abraham Marcos, Rivas Minaya, Jose Alberto, 2017: sistema de gestión de seguridad de información para la municipalidad provincial de huaral recuperado en: http://repositorio.unjfsc.edu.pe/handle/unjfsc/2317

Túquerres Martínez, Y. S. (2021, 13 abril). Repositorio Universidad Técnica de Ambato: Gestión de la calidad con énfasis en el servicio del sector hotelero de la Ciudad de Puyo. Recuperado en : https://repositorio.uta.edu.ec/jspui/handle/123456789/32803.

Think& Sell,2021: sistemas de gestión normalizados
recuperado en :
https://thinkandsell.com/servicios/consultoria/software-y-sistemas/sistemas-de-gestion-normalizados/#:~:text=un%20sistema%20de%20gesti%c3%b3n%20es,objetivos%20y%20alcanzar%20dichos%20objetivos.

TORRES CHANGO 2020: plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada megaprofer s.a." recuperado en: https://repositorio.uta.edu.ec/jspui/bitstream/123456789/30690/3/tesis_t1657si.pdf

Torres Alvarado, I. D. (2019). El Sistema de Gestión y sus componentes: estratégico, táctico y operacional. Compendium, 22(42), 1–6. Recuperado en : https://revistas.uclave.org/index.php/Compendium/article/view/2555/1547

VASQUEZ GARCIA 2017: Propuesta de gestión de seguridad de la información de mesas de servicio de la empresa sonda México s.a de c.v., recuperado en : http://hdl.handle.net/20.500.11799/80295

Valencia-Duque Francisco Javier , Orozco-Alzate Mauricio,2017: Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000, recuperado en : http://www.scielo.mec.pt/pdf/rist/n22/n22a06.pdf

Virginia Acoria – Juan Azcurra – Vito Cavallaro Ezequiel Ferraro – Silvina Gatti – Paola Tropea 2014: KENKA: SISTEMA INTEGRAL DE GESTION DE CALIDAD recuperado en: https://core.ac.uk/download/pdf/290469489.pdf

Thomas Viehmann , 2021_ Numerically more stable computation of the p-values for the two-sample Kolmogorov-Smirnov test recuperado en : https://arxiv.org/pdf/2102.08037.pdf

Welivesecurity.com. 2019 ESET SECURITY REPORT Latinoamérica 2019 Recuperado en**: https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf**

YAÑEZ CACERES 2017: sistema de gestión de seguridad de la información para la subsecretaria de economía y empresas de menor tamaño, recuperado

en http://repositorio.uchile.cl/bitstream/handle/2250/147976/sistema-de-gestion-de-seguridad-de-la-informacion-para-la-subsecretaria-de-economia-y-empresas.pdf?sequence=1&isallowed=y

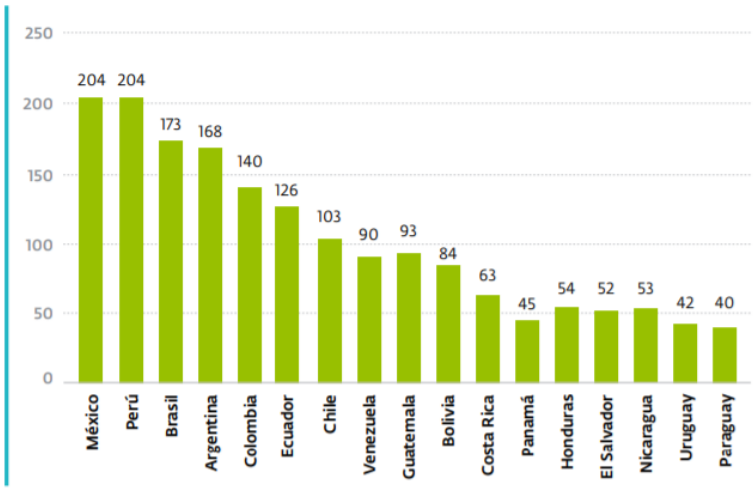
Youngin You , Junhyoung Oh, Sooheon Kim and Kyungho Lee, 2018 Advanced approach to information security management system utilizing maturity models in critical infrastructure. (2018, octubre). https://www.koreascience.or.kr/article/JAKO201835372300442.pdf

ZACARIAS VILLAFRANCA(2017): modelo de seguridad de la información basado en la iso/iec 27001:2013 para mitigar los riesgos de los activos de información en la central de operaciones policiales de la región policial junín, recuperado de https://hdl.handle.net/20.500.12394/4105

ANEXOS

Anexo A: Cantidad de variantes diferentes de Ransomware vistas en países de Latinoamerica durante 2019

GRÁFICO 3 | Cantidad de variantes diferentes de Ransomware vistas en países de Latinoamérica durante 2019



Fuente: Eset Reporte Anual 2019

ANEXO B : Cuadro de Tablas de Altas & Bajas de empresas según actividad económicas

CUADRO N°2
PERÚ: STOCK, ALTAS Y BAJAS DE LAS EMPRESAS, SEGÚN ACTIVIDAD ECONÓMICA, III TRIMESTRE 2020

Actividad económica	Stock	Altas 1/	Bajas 2/	Tasa de altas (%) 3/	Tasa de bajas (%) 4/
Total	**2 701 066**	**78 258**	**5 835**	**2,9**	**0,2**
Agricultura, ganadería, silvicultura y pesca	41 009	1 587	64	3,9	0,2
Explotación de minas y canteras	25 236	4 824	48	19,1	0,2
Industrias manufactureras	205 378	4 939	366	2,4	0,2
Construcción	83 183	3 104	60	3,7	0,1
Venta y reparación de vehículos	75 730	2 237	138	3,0	0,2
Comercio al por mayor	260 971	12 267	934	4,7	0,4
Comercio al por menor	849 367	23 987	2 032	2,8	0,2
Transporte y almacenamiento	162 758	4 654	509	2,9	0,3
Actividades de alojamiento	27 795	290	77	1,0	0,3
Actividades de servicio de comidas y bebidas	218 963	3 686	453	1,7	0,2
Información y comunicaciones	55 101	1 305	66	2,4	0,1
Servicios prestados a empresas	259 543	6 811	304	2,6	0,1
Salones de belleza	40 815	859	99	2,1	0,2
Otros servicios 5/	395 217	7 708	685	2,0	0,2

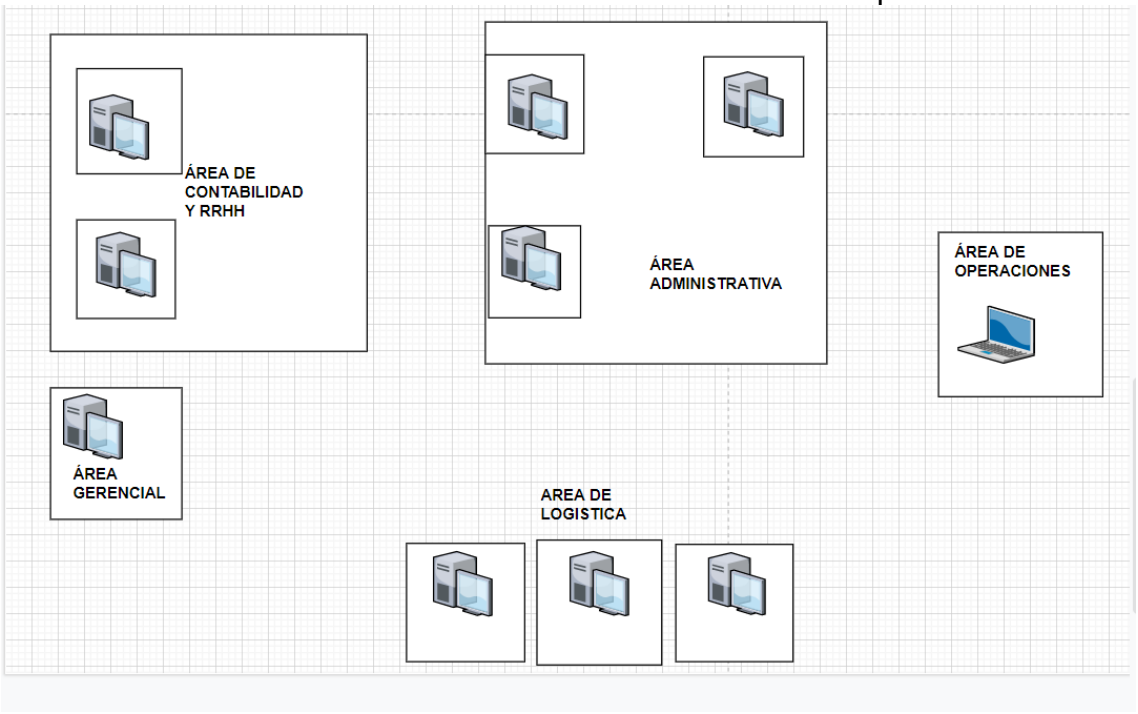
ANEXO C : Matriz de Consistencia

TITULO	PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLE	DIMENSIONES	INDICADORES	TECNICA	INSTRUMENTO	ESCALA	MÉTODO
SISTEMA DE GESTION PARA LA SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA 27001:2013 EN LA CONSTRUCTORA PEREZ & PEREZ SAC, SAN MARTIN,2021	Problema General	Objetivo General	Hipotesis General	Variable Independiente: Sistema de Gestión						**Enfoque de la Investigación:** Cuantitativa **Tipo de Estudio:** Aplicada **Diseño de la Investigación:** Pre-Experimental
	¿de que manera un sistema de gestión basado en la norma iso/iec27001 influye en la seguridad de la informació de la empresa constructora Pérez & Pérez sac, Moyobamba, san martin, 2021?	un sistema de gestión basado en la norma iso/iec27001 influye positivamente en la seguridad de la informació de la empresa constructora Pérez & Pérez sac, Moyobamba, san martin,2021	determinar de qué manera un sistema de gestión basado en la norma iso/iec27001 influye en la seguridad de la información de la empresa constructora Pérez & Pérez sac, Moyobamba, san martin,2021							
	Problema Específicos	Objetivos Específicos	Hipótesis Especificas							
	p1: ¿de qué manera un sistema de gestión basado en la norma iso/iec27001 influye en la confidencialidad de la empresa constructora Pérez & Pérez sac, Moyobamba, san martin,2021?	h1: un sistema de gestión basado en la norma iso/iec27001 influye positivamente en la confidencialidad de la empresa constructora Pérez & Pérez sac, Moyobamba, san martin,2021	o1: determinar de qué manera un sistema de gestión basado en la norma iso/iec27001 influye en la confidencialidad de la empresa constructora Pérez & Pérez sac, Moyobamba, san martin,2021	Variable Dependiente: Seguridad de la Información	CONFIDENCIALIDAD (J. cano)	Accesos no autorizados Muestra: 253 Muestreo: 153 $\mathbf{ANA} = \frac{\boldsymbol{RANA}}{\boldsymbol{TAD}} \times \mathbf{100}$ Donde: **ANA**: Accesos No Autorizados **TAD**: Total de Accesos del Dia **RANA**: Reporte de Accesos No Autorizados	Observación / Ficha de registro Escala de razón			

	p2 ¿de qué manera un sistema de gestión basado en la norma iso/iec27001 influye en la integridad de la empresa constructora Pérez & Pérez sac, Moyobamba, san martin,2021¿	h2: un sistema de gestión basado en la norma iso/iec27001 influye positivamente en la integridad de la empresa constructora Pérez & Pérez sac, Moyobamba, san martin,2021	o2: determinar de qué manera un sistema de gestión basado en la norma iso/iec27001 influye en la integridad de la empresa constructora Pérez & Pérez sac, Moyobamba, san martin,2021		INTEGRIDAD (J. cano)	Virus informático Muestra: 87 Muestreo 148 $\mathbf{VI} = \frac{\boldsymbol{VINE}}{\mathbf{VID}} \times \mathbf{100}$ Donde: **VI:** Virus Informático **VINE**: Virus Informático No Eliminado **VID**: Virus Informático del día		
	p3: ¿de qué manera un sistema de gestión basado en la norma iso/iec27001 influye en la disponibilidad de la empresa constructora Pérez & Pérez sac, Moyobamba, san martin,2021?	h3 un sistema de gestión basado en la norma iso/iec27001 influye positivamente en la disponibilidad de la empresa constructora Pérez & Pérez sac, Moyobamba, san martin,2021	o3: determinar de qué manera un sistema de gestión basado en la norma iso/iec27001 influye en la disponibilidad de la empresa constructora Pérez & Pérez sac, Moyobamba, san martin2021		DISPONIBILIDAD (J. cano)	*eliminar, borrar manipular datos Muestra: 240 Muestreo: 71 $\mathbf{EBMD} = \frac{\mathrm{EMBDNR}}{\mathrm{TMDD}} \times \mathbf{100}$ Donde: **EBMD:** Manipulación de Datos TMDD: Total de Manipulación de datos del día EMBDNR: Eliminar, Manipular, Borrar Datos No reconocidos		

ANEXO D: Logos Autorizados “Premio Empresa Peruana del Año”

ANEXO E: Distribución de Áreas de la Empresa



ANEXO F

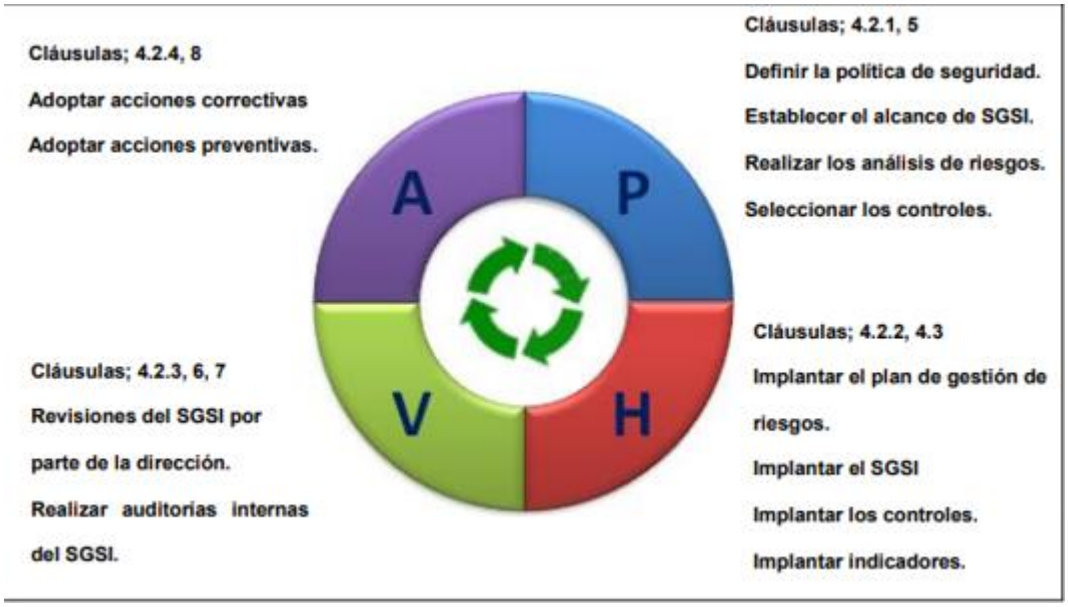
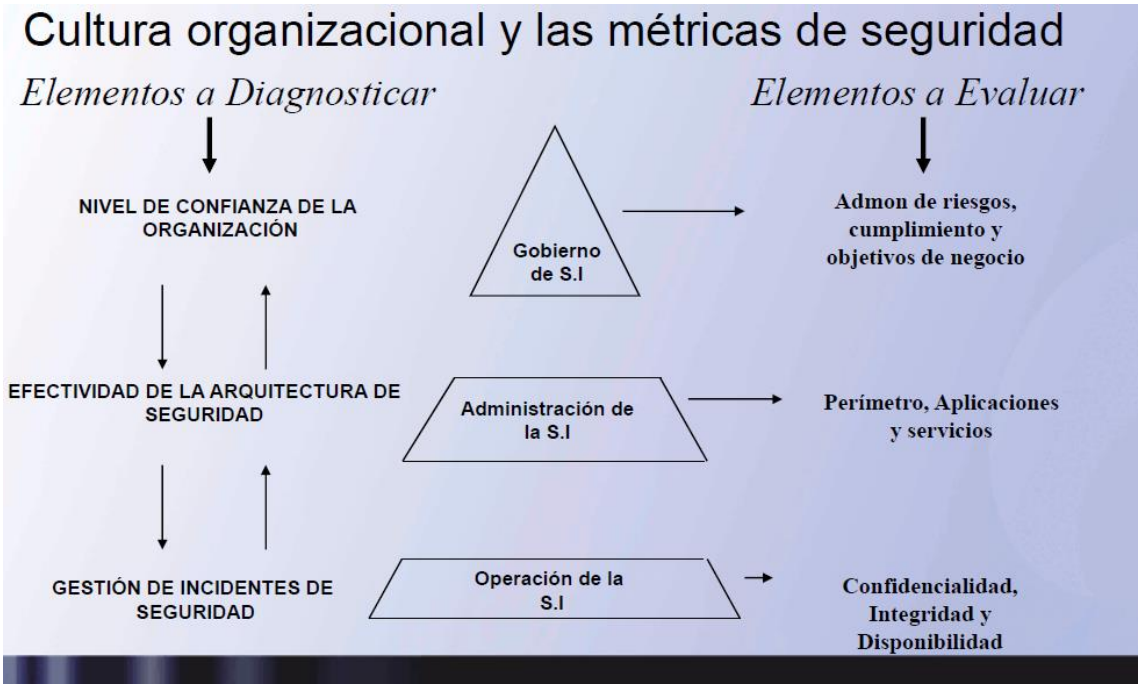


Figura 2.1 Ciclo de Deming asociado a cláusulas de norma ISO/IEC 27001 (3)
Fuente: ISO 27001, adaptación modelo PDCA.

ANEXO G



(Fuente: Métricas en Seguridad Informática: Una revisión académica, Jeimy Cano)

ANEXO H: Carta de Autorización

PREMIO EMPRESA PERUANA DEL AÑO 2016

PEREZ&PEREZ S.A.C. CONSTRUCTORA

AÑO DE LA UNIVERSALIZACIÓN DE LA SALUD

Moyobamba 04 de agosto de 2020

CARTA N° 070-2020-CONSPEPESAC/GG

Señor. -
EDUARDO GIAP RISCO VILLARREAL
Ciudad.
Callo.

Asunto: **AUTORIZACIÓN PARA EJECUTAR PLAN DE TESIS "SISTEMA DE GESTION PARA LA SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA ISO/IEC 27001:2013 CONSTRUCTORA PEREZ & PEREZ SAC.**

Ref.-
Solicitud de autorización para ejecutar el plan de tesis "Sistema informático para la seguridad de la información en la constructora Perez & Perez Sac

De mi mayor consideración:

Autorizo la facilidad de acceso a la información de nuestros procesos y documentos de gestión que llevará a cabo el tesista en implementar un sistema informático para la seguridad de la información en nuestra empresa que lo requerimos con mucha urgencia.

Atentamente,

CONSTRUCTORA PEREZ & PEREZ SAC.
Pedro Perez Rivera
GERENTE GENERAL

Jr. San Martin N° 122 - Celular: 942436483 - Teléfono: 042-56243 - Moyobamba – San Martin

ANEXO I: Instrumentos y Población aplicados en el test, pretest y post-test del presente año 2021

INVESTIGADOR	RISCO VILLARREAL EDUARDO GIAP
EMPRESA	CONSTRUCTORA PEREZ & PEREZ SAC
DIRRECION	JIRON SAN MARTIN 130 – MOYOBAMBA – SAN MARTIN
FECHA DE INICIO	01/01/2020
FECHA DE TERMINACION	31/01/2020
VARIABLE	FORMULA

REPORTES		$\mathbf{ANA} = \frac{\boldsymbol{RANA}}{\boldsymbol{TAD}} \times \mathbf{100}$
INDICADOR	MEDIDA	
ACCESOS NO AUTORIZADOS **(TEST)**	PORCENTAJE	Donde: **ANA**: Accesos No Autorizados **TAD**: Total de Accesos del Dia **RANA**: Reporte de Accesos No Autorizados

ITEM	FECHA	RANA	TAD	ANA (%)
1	04/01/2021	13	20	65
2	05/01/2021	10	18	56
3	06/01/2021	15	20	75
4	07/01/2021	10	19	53
5	08/01/2021	13	18	72
6	09/01/2021	15	17	88
7	11/01/2021	10	20	50
8	12/01/2021	11	18	61
9	13/01/2021	15	19	79
10	14/01/2021	13	20	65
11	15/01/2021	10	17	59
12	16/01/2021	16	18	89
13	18/01/2021	13	19	68
14	19/01/2021	10	20	50
15	20/01/2021	15	22	68
16	21/01/2021	10	17	59
17	22/01/2021	10	18	56
18	23/01/2021	15	17	88
19	25/01/2021	13	17	76
20	26/01/2021	16	17	94
	TOTAL	**253**	**371**	
	PROMEDIO			**68**

INVESTIGADOR	RISCO VILLARREAL EDUARDO GIAP
EMPRESA	CONSTRUCTORA PEREZ & PEREZ SAC
DIRRECION	JIRON SAN MARTIN 130 – MOYOBAMBA – SAN MARTIN
FECHA DE INICIO	01/02/2020
FECHA DE TERMINACION	28/02/2020
VARIABLE	FORMULA

REPORTES		$\text{ANA} = \frac{RANA}{TAD} \times 100$
INDICADOR	MEDIDA	
ACCESOS NO AUTORIZADOS **(RE-TEST)**	PORCENTAJE	Donde: **ANA**: Accesos No Autorizados **TAD**: Total de Accesos del Dia **RANA**: Reporte de Accesos No Autorizados

ITEM	FECHA	RANA	TAD	ANA (%)
1	01/02/2021	15	20	75
2	02/02/2021	14	18	78
3	03/02/2021	13	20	65
4	04/02/2021	14	19	74
5	05/02/2021	10	18	56
6	06/02/2021	13	17	76
7	08/02/2021	10	20	50
8	09/02/2021	15	18	83
9	10/02/2021	14	19	74
10	11/02/2021	10	20	50
11	12/02/2021	14	17	82
12	13/02/2021	13	18	72
13	15/02/2021	10	19	53
14	16/02/2021	10	20	50
15	17/02/2021	10	22	45
16	18/02/2021	14	17	82
17	19/02/2021	14	18	78
18	20/02/2021	13	17	76
19	22/02/2021	13	17	76
20	23/02/2021	14	17	82
		253	**371**	

	PROMEDIO	**68**

INVESTIGADOR	RISCO VILLARREAL EDUARDO GIAP
EMPRESA	CONSTRUCTORA PEREZ & PEREZ SAC
DIRRECION	JIRON SAN MARTIN 130 – MOYOBAMBA – SAN MARTIN
FECHA DE INICIO	01/01/2020
FECHA DE TERMINACION	31/02/2020
VARIABLE	FORMULA

REPORTES

INDICADOR	MEDIDA
ELIMINAR, MANIPILAR BORRAR, DATOS **(TEST**)	PORCENTAJE

$$\mathbf{EBMD} = \frac{\text{EMBDNR}}{\text{TMDD}} \times \mathbf{100}$$

Donde:

EBMD: Manipulación de Datos

TMDD: Total de Manipulación de datos del día

EMBDNR: Eliminar, Manipular, Borrar Datos No reconocidos

ITEM	FECHA	EMBDNR	TMDD	EBMD%
1	04/01/2021	10	20	50
2	05/01/2021	10	25	40
3	06/01/2021	15	20	75
4	07/01/2021	10	22	45
5	08/01/2021	13	23	57
6	09/01/2021	10	24	42
7	11/01/2021	10	25	40
8	12/01/2021	11	20	55
9	13/01/2021	15	22	68
10	14/01/2021	20	25	80
11	15/01/2021	10	20	50
12	16/01/2021	10	25	40
13	18/01/2021	13	20	65
14	19/01/2021	10	20	50
15	20/01/2021	15	22	68

16	21/01/2021	10	23	43
17	22/01/2021	10	24	42
18	23/01/2021	15	25	60
19	25/01/2021	13	22	59
20	26/01/2021	10	23	43
		240	**450**	
	PROMEDIO DEL SPSS			**53**

INVESTIGADOR	RISCO VILLARREAL EDUARDO GIAP
EMPRESA	CONSTRUCTORA PEREZ & PEREZ SAC
DIRRECION	JIRON SAN MARTIN 130 – MOYOBAMBA – SAN MARTIN
FECHA DE INICIO	01/02/2020
FECHA DE TERMINACION	28/02/2020
VARIABLE	FORMULA

REPORTES

INDICADOR	MEDIDA
ELIMINAR, MANIPILAR BORRAR, DATOS **(RE-TEST)**	PORCENTAJE

$$\mathbf{EBMD} = \frac{\text{EMBDNR}}{\text{TMDD}} \times \mathbf{100}$$

Donde:
EBMD: Manipulación de Datos
TMDD: Total de Manipulación de datos del día
EMBDNR: Eliminar, Manipular, Borrar Datos No reconocidos

ITEM	FECHA	EMBDNR	TMDD	EBMD%
1	01/02/2021	15	22	68
2	02/02/2021	10	23	43
3	03/02/2021	14	24	58
4	04/02/2021	10	22	45
5	05/02/2021	10	20	50
6	06/02/2021	10	25	40

7	08/02/2021	14	20	70
8	09/02/2021	15	24	63
9	10/02/2021	10	20	50
10	11/02/2021	10	22	45
11	12/02/2021	10	23	43
12	13/02/2021	14	24	58
13	15/02/2021	10	20	50
14	16/02/2021	10	22	45
15	17/02/2021	15	27	56
16	18/02/2021	14	25	56
17	19/02/2021	10	20	50
18	20/02/2021	14	26	54
19	22/02/2021	10	22	45
20	23/02/2021	15	24	63
	TOTAL	**240**	**455**	
	PROMEDIO DEL SPSS			53

.

INVESTIGADOR	RISCO VILLARREAL EDUARDO GIAP
EMPRESA	CONSTRUCTORA PEREZ & PEREZ SAC
DIRRECION	JIRON SAN MARTIN 130 – MOYOBAMBA – SAN MARTIN
FECHA DE INICIO	01/02/2020
FECHA DE TERMINACION	28/02/2020
VARIABLE	FORMULA

REPORTES		
INDICADOR	MEDIDA	$$\mathbf{VI} = \frac{\boldsymbol{VINE}}{\mathbf{VID}} \times \mathbf{100}$$
VIRUS INFORMATICO **(TEST**)	PORCENTAJE	Donde: **VI:** Virus Informático **VINE**: Virus Informático No Eliminado **VID**: Virus Informático del día

ITEM	FECHA	TEBMDS	EBMDR	EBMD%
1	04/01/2021	3	10	30
2	05/01/2021	5	10	50
3	06/01/2021	4	8	50
4	07/01/2021	3	9	33
5	08/01/2021	5	10	50
6	09/01/2021	4	8	50
7	11/01/2021	5	7	71
8	12/01/2021	4	9	44
9	13/01/2021	5	8	63
10	14/01/2021	5	7	71
11	15/01/2021	4	9	44
12	16/01/2021	5	9	56
13	18/01/2021	5	7	71
14	19/01/2021	4	9	44
15	20/01/2021	5	9	56
16	21/01/2021	5	10	50
17	22/01/2021	3	8	38
18	23/01/2021	5	7	71
19	25/01/2021	4	10	40
20	26/01/2021	4	8	50
		87	**172**	
	PROMEDIO DEL SPSS			**51**

INVESTIGADOR	RISCO VILLARREAL EDUARDO GIAP
EMPRESA	CONSTRUCTORA PEREZ & PEREZ SAC
DIRRECION	JIRON SAN MARTIN 130 – MOYOBAMBA – SAN MARTIN
FECHA DE INICIO	01/01/2020
FECHA DE TERMINACION	31/01/2020
VARIABLE	FORMULA

REPORTES		$$VI = \frac{VINE}{VID} \times 100$$
INDICADOR	MEDIDA	Donde: **VI:** Virus Informático **VINE**: Virus Informático No Eliminado **VID**: Virus Informático del día
VIRUS INFORMATICO **(RE TEST**)	PORCENTAJE	

ITEM	FECHA	AAS	TANA	ANA (%)
1	01/02/2021	6	8	75
2	02/02/2021	4	10	40
3	03/02/2021	6	9	67
4	04/02/2021	5	10	50
5	05/02/2021	4	10	40
6	06/02/2021	3	9	33
7	08/02/2021	4	10	40
8	09/02/2021	4	10	40
9	10/02/2021	5	8	63
10	11/02/2021	4	10	40
11	12/02/2021	4	9	44
12	13/02/2021	4	10	40
13	15/02/2021	4	10	40
14	16/02/2021	3	8	38
15	17/02/2021	6	10	60
16	18/02/2021	4	9	44
17	19/02/2021	3	10	30
18	20/02/2021	5	8	63

19	22/02/2021	4	10	40
20	23/02/2021	5	9	56
	TOTAL	**87**	**187**	
	PROMEDIO DEL SPSS			47

INVESTIGADOR	RISCO VILLARREAL EDUARDO GIAP			
EMPRESA	CONSTRUCTORA PEREZ & PEREZ SAC			
DIRRECION	JIRON SAN MARTIN 130 – MOYOBAMBA – SAN MARTIN			
FECHA DE INICIO	01/03/2020			
FECHA DE TERMINACION	31/03/2020			
VARIABLE	FORMULA			
REPORTES		$\mathbf{ANA} = \frac{\boldsymbol{RANA}}{\boldsymbol{TAD}} \times \mathbf{100}$		
INDICADOR	MEDIDA			
ACCESOS NO AUTORIZADOS **(POSTEST)**	PORCENTAJE	Donde: **ANA**: Accesos No Autorizados **TAD**: Total de Accesos del Dia **RANA**: Reporte de Accesos No Autorizados		
ITEM	FECHA	RANA	TAD	ANA (%)
1	01/03/2021	3	15	20
2	02/03/2021	4	14	29
3	03/03/2021	3	10	30
4	04/03/2021	0	15	0
5	05/03/2021	3	15	20
6	06/03/2021	3	15	20
7	07/03/2021	3	15	20
8	08/03/2021	2	14	14
9	09/03/2021	1	15	7
10	10/03/2021	1	15	7
11	11/03/2021	0	10	0
12	12/03/2021	2	14	14

13	13/03/2021	2	15	13
14	14/03/2021	1	10	10
15	15/03/2021	2	15	13
16	16/03/2021	3	15	20
17	17/03/2021	3	14	21
18	18/03/2021	2	10	20
19	19/03/2021	3	15	20
20	20/03/2021	1	10	10
	TOTAL	**42**	**271**	
	PROMEDIO DEL SPSS			**15**

INVESTIGADOR	RISCO VILLARREAL EDUARDO GIAP
EMPRESA	CONSTRUCTORA PEREZ & PEREZ SAC
DIRRECION	JIRON SAN MARTIN 130 – MOYOBAMBA – SAN MARTIN
FECHA DE INICIO	01/03/2020
FECHA DE TERMINACION	31/03/2020
VARIABLE	FORMULA

REPORTES

INDICADOR	MEDIDA
ELIMINAR, MANIPILAR BORRAR, DATOS **(POSTEST**)	PORCENTAJE

$$\mathbf{EBMD} = \frac{\text{EMBDNR}}{\text{TMDD}} \times \mathbf{100}$$

Donde:

EBMD: Manipulación de Datos

TMDD: Total de Manipulación de datos del día

EMBDNR: Eliminar, Manipular, Borrar Datos No reconocidos

ITEM	FECHA	TEBMDS	EBMDR	EBMD%
1	01/03/2021	3	22	14
2	02/03/2021	5	23	22
3	03/03/2021	4	24	17
4	04/03/2021	1	22	5
5	05/03/2021	0	20	0
6	06/03/2021	2	25	8

7	07/03/2021	4	20	20
8	08/03/2021	2	24	8
9	09/03/2021	3	20	15
10	10/03/2021	1	22	5
11	11/03/2021	5	23	22
12	12/03/2021	0	24	0
13	13/03/2021	2	20	10
14	14/03/2021	2	22	9
15	15/03/2021	3	27	11
16	16/03/2021	5	25	20
17	17/03/2021	3	20	15
18	18/03/2021	5	26	19
19	19/03/2021	0	22	0
20	20/03/2021	2	24	8
	TOTAL	**52**	**455**	
	PROMEDIO DEL SPSS			**11**

INVESTIGADOR	RISCO VILLARREAL EDUARDO GIAP			
EMPRESA	CONSTRUCTORA PEREZ & PEREZ SAC			
DIRRECION	JIRON SAN MARTIN 130 – MOYOBAMBA – SAN MARTIN			
FECHA DE INICIO	01/03/2020			
FECHA DE TERMINACION	31/03/2020			
VARIABLE	FORMULA			
REPORTES		$\text{VI} = \frac{VINE}{\text{VID}} \times 100$		
INDICADOR	MEDIDA	Donde:		
VIRUS INFORMATICO **(POSTTEST**)	PORCENTAJE	**VI:** Virus Informático **VINE**: Virus Informático No Eliminado **VID**: Virus Informático del día		
ITEM	FECHA	TEBMDS	EBMDR	EBMD%

1	01/03/2021	1	8	13
2	02/03/2021	2	9	22
3	03/03/2021	1	9	11
4	04/03/2021	1	7	14
5	05/03/2021	1	9	11
6	06/03/2021	0	8	0
7	07/03/2021	0	7	0
8	08/03/2021	0	8	0
9	09/03/2021	0	7	0
10	10/03/2021	1	8	13
11	11/03/2021	1	8	13
12	12/03/2021	1	8	13
13	13/03/2021	1	9	11
14	14/03/2021	2	7	29
15	15/03/2021	0	8	0
16	16/03/2021	0	8	0
17	17/03/2021	2	7	29
18	18/03/2021	2	8	25
19	19/03/2021	2	9	22
20	20/03/2021	1	8	13
		19	**160**	
	PROMEDIO DEL SPSS			**12**

Anexo H: Ficha de Juicio de Expertos

TABLA DE EVALUACIÓN DE EXPERTOS - INDICADOR 1: ACCESOS NO AUTORIZADOS
Apellidos y nombres del experto: Estrada Aro Marcelino Título y/o grado Académico: Ing. de Sistemas Doctor () Magister (x) Ingeniero () Otro () Universidad que labora: Universidad Cesar Vallejo Fecha: 07/04/2021
TÍTULO DE PROYECTO
"**SISTEMA DE GESTIÓN** PARA LA **SEGURIDAD DE LA INFORMACIÓN** basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020." AUTOR: EDUARDO GIAP RISCO VILLARREAL

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)
Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con un lenguaje apropiado				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y la tecnología				80%	
ORGANIZACIÓN	Existe una organización lógica				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
SUFICIENCIA	Está basado en aspectos teóricos y científicos				80%	
CONSISTENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de la investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación				80%	
TOTAL PROMEDIO					80%	

(x) El instrumento puede ser aplicado, tal como está elaborado
( ) El instrumento debe ser mejorado antes de ser aplicado

_____
Firma Experto

TABLA DE EVALUACIÓN DE EXPERTOS - INDICADOR 2:
Eliminar, borrar manipular datos

Apellidos y nombres del experto: Estrada Aro Marcelino
Título y/o grado Académico: Ing. de Sistemas
Doctor () Magister (x) Ingeniero () Otro ()
Universidad que labora: Universidad Cesar Vallejo
Fecha: 07/04/2021

TÍTULO DE PROYECTO

"**SISTEMA DE GESTIÓN** PARA LA **SEGURIDAD DE LA INFORMACIÓN** basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020."
AUTOR: EDUARDO GIAP RISCO VILLARREAL Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%) Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con un lenguaje apropiado				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y la tecnología				80%	
ORGANIZACIÓN	Existe una organización lógica.				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
SUFICIENCIA	Está basado en aspectos teóricos y científicos				80%	
CONSISTENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de la investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80%	
TOTAL PROMEDIO					80%	

(x) El instrumento puede ser aplicado, tal como está elaborado
() El instrumento debe ser mejorado antes de ser aplicado

_____
Firma Experto

TABLA DE EVALUACIÓN DE EXPERTOS - INDICADOR 3: VIRUS INFORMATICO
Apellidos y nombres del experto: Estrada Aro Marcelino Título y/o grado Académico: Ing. de Sistemas Doctor () Magister (x) Ingeniero () Otro () Universidad que labora: Universidad Cesar Vallejo Fecha: 07/04/2021

TÍTULO DE PROYECTO

"**SISTEMA DE GESTIÓN** PARA LA **SEGURIDAD DE LA INFORMACIÓN** basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020."

AUTOR: EDUARDO GIAP RISCO VILLARREAL

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con un lenguaje apropiado				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y la tecnología				80%	
ORGANIZACIÓN	Existe una organización lógica				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
SUFICIENCIA	Está basado en aspectos teóricos y científicos				80%	
CONSISTENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de la investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de				80%	
TOTAL PROMEDIO					80%	

(x) El instrumento puede ser aplicado, tal como está elaborado

() El instrumento debe ser mejorado antes de ser aplicado

_____

Firma Experto

EVALUACIÓN DE METODOLOGÍA DE DESARROLLO DE SOFTWARE

TABLA DE EVALUACION DE EXPERTOS

Apellidos y nombres del experto: Estrada Aro Marcelino

Título y/o Grado: Ing. de Sistemas

Fecha: 07/04/2021

SISTEMA DE GESTIÓN PARA LA **SEGURIDAD DE LA INFORMACIÓN**

basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020.”
EVALUACIÓN DE METODOLOGÍA DE SOFTWARE Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante unas series de criterios con puntuaciones especificadas al final de la tabla. Así mismo le exhortamos en la correcta determinación de la metodología para desarrollar un SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020.”

ITEM	CRITERIOS	METODOLOGÍAS		
		COBIT	MARGERIT	ISO 27001
1	Permite un desarrollo iterativo	1	3	2
2	Los resultados son más rápidos	1	3	2
3	Requiere de comunicación con el cliente	1	3	2
4	Requiere de entregas constantes	1	3	2
5	Se adecua para tiempos cortos de entrega	1	3	2
6	Los resultados son más rápidos	1	3	2
7	Adaptable y flexible a cambios	1	3	2
8	Implementa las necesidades del sistema	1	3	2
	Total	8	24	16

La escala a evaluar es de 1**: Malo, 2: Regular y 3: Bueno**
Sugerencias: La metodología es aplicable

_____
Firma Experto

TABLA DE EVALUACIÓN DE EXPERTOS - INDICADOR 1: ACCESOS NO AUTORIZADOS

Apellidos y nombres del experto: Vásquez Valecia Yesenia
Título y/o grado Académico: Ing. de Sistemas
Doctor (x) Magister ( ) Ingeniero ( ) Otro ( )
Universidad que labora: Universidad Cesar Vallejo
Fecha: 07/04/2021

TÍTULO DE PROYECTO
"**SISTEMA DE GESTIÓN** PARA LA **SEGURIDAD DE LA INFORMACIÓN** basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020."

AUTOR: EDUARDO GIAP RISCO VILLARREAL
Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)
Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con un lenguaje apropiado				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y la tecnología				80%	
ORGANIZACIÓN	Existe una organización lógica				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
SUFICIENCIA	Está basado en aspectos teóricos y científicos				80%	
CONSISTENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de la investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de				80%	
TOTAL PROMEDIO					80%	

(x) El instrumento puede ser aplicado, tal como está elaborado
( ) El instrumento debe ser mejorado antes de ser aplicado

_____
Firma Experto

TABLA DE EVALUACIÓN DE EXPERTOS - INDICADOR 2: Eliminar, borrar manipular datos
Apellidos y nombres del experto: Vásquez Valecia Yesenia Título y/o grado Académico: Ing. de Sistemas Doctor (x) Magister () Ingeniero ( ) Otro ( ) Universidad que labora: Universidad Cesar Vallejo Fecha: 07/04/2021
TÍTULO DE PROYECTO "**SISTEMA DE GESTIÓN** PARA LA **SEGURIDAD DE LA INFORMACIÓN** basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020." AUTOR: EDUARDO GIAP RISCO VILLARREAL
Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%) Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con un lenguaje apropiado				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y la tecnología				80%	
ORGANIZACIÓN	Existe una organización lógica				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
SUFICIENCIA	Está basado en aspectos teóricos y científicos				80%	
CONSISTENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de la investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80%	
TOTAL PROMEDIO					80%	

(x) El instrumento puede ser aplicado, tal como está elaborado
( ) El instrumento debe ser mejorado antes de ser aplicado

_____

Firma Experto

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS - INDICADOR 3: VIRUS INFORMATICO

Apellidos y nombres del experto: Vásquez Valecia Yesenia
Título y/o grado Académico: Ing. de Sistemas
Doctor (x) Magister ( ) Ingeniero ( ) Otro ( )
Universidad que labora: Universidad Cesar Vallejo
Fecha: 07/04/2021

TÍTULO DE PROYECTO

"**SISTEMA DE GESTIÓN** PARA LA **SEGURIDAD DE LA INFORMACIÓN** basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020."

AUTOR: EDUARDO GIAP RISCO VILLARREAL

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con un lenguaje apropiado				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y la tecnología.				80%	
ORGANIZACIÓN	Existe una organización lógica				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
SUFICIENCIA	Está basado en aspectos teóricos y científicos				80%	
CONSISTENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de la investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de				80%	
TOTAL PROMEDIO					80%	

(x) El instrumento puede ser aplicado, tal como está elaborado
( ) El instrumento debe ser mejorado antes de ser aplicado

firma Experto

EVALUACIÓN DE METODOLOGÍA DE DESARROLLO DE SOFTWARE
TABLA DE EVALUACION DE EXPERTOS Apellidos y nombres del experto: Vásquez Valencia Yesenia Título y/o Grado: Ing. de Sistemas Fecha: 07/04/2021
EVALUACIÓN DE METODOLOGÍA DE SOFTWARE Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante unas series de criterios con puntuaciones especificadas al final de la tabla. Así mismo le exhortamos en la correcta determinación de la metodología para desarrollar un SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020.”

ITEM	CRITERIOS	METODOLOGÍAS		
		COBIT	MARGERIT	ISO 27001
1	Permite un desarrollo iterativo	1	3	2
2	Los resultados son más rápidos	1	3	2
3	Requiere de comunicación con el cliente	1	3	2
4	Requiere de entregas constantes	1	3	2
5	Se adecua para tiempos cortos de entrega	1	3	2
6	Los resultados son más rápidos	1	3	2
7	Adaptable y flexible a cambios	1	3	2
8	Implementa las necesidades del sistema	1	3	2
	Total	8	24	16

La escala a evaluar es de 1**: Malo, 2: Regular y 3: Bueno**
Sugerencias: La metodología es aplicable

_____
Firma Experto

TABLA DE EVALUACIÓN DE EXPERTOS - INDICADOR 1: ACCESOS NO AUTORIZADOS

Apellidos y nombres del experto: Rivera Crisostomo Renne
Título y/o grado Académico: Ing. de Sistemas
Doctor ( ) Magister (x) Ingeniero ( ) Otro ( )
Universidad que labora: Universidad Cesar Vallejo
Fecha: 07/04/2021

TÍTULO DE PROYECTO
"**SISTEMA DE GESTIÓN** PARA LA **SEGURIDAD DE LA INFORMACIÓN** basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020."
AUTOR: EDUARDO GIAP RISCO VILLARREAL

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)
Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con un lenguaje apropiado				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y la tecnología				80%	
ORGANIZACIÓN	Existe una organización lógica				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
SUFICIENCIA	Está basado en aspectos teóricos y científicos				80%	
CONSISTENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de la investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de				80%	
TOTAL PROMEDIO					80%	

(x) El instrumento puede ser aplicado, tal como está elaborado
( ) El instrumento debe ser mejorado antes de ser aplicado

_____
Firma Experto

TABLA DE EVALUACIÓN DE EXPERTOS - INDICADOR 2: Elminiar, borrar manipular datos
Apellidos y nombres del experto: Rivera Crisostomo Renne Título y/o grado Académico: Ing. de Sistemas Doctor ( ) Magister (x) Ingeniero ( ) Otro ( ) Universidad que labora: Universidad Cesar Vallejo Fecha: 07/04/2021
TÍTULO DE PROYECTO "**SISTEMA DE GESTIÓN** PARA LA **SEGURIDAD DE LA INFORMACIÓN** basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020."
AUTOR: EDUARDO GIAP RISCO VILLARREAL Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%) Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con un lenguaje apropiado				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y la tecnología				80%	
ORGANIZACIÓN	Existe una organización lógica				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
SUFICIENCIA	Está basado en aspectos teóricos y científicos				80%	
CONSISTENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de la investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80%	
TOTAL PROMEDIO					80%	

(x) El instrumento puede ser aplicado, tal como está elaborado
( ) El instrumento debe ser mejorado antes de ser aplicado

_____
Firma Experto

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS - INDICADOR 3: VIRUS INFORMATICO

Apellidos y nombres del experto: Rivera Crisostomo Renne
Título y/o grado Académico: Ing. de Sistemas
Doctor ( ) Magister (x) Ingeniero ( ) Otro ( )
Universidad que labora: Universidad Cesar Vallejo
Fecha: 07/04/2021

TÍTULO DE PROYECTO

"**SISTEMA DE GESTIÓN** PARA LA **SEGURIDAD DE LA INFORMACIÓN** basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020."

AUTOR: EDUARDO GIAP RISCO VILLARREAL

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con un lenguaje apropiado				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y la tecnología				80%	
ORGANIZACIÓN	Existe una organización lógica				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
SUFICIENCIA	Está basado en aspectos teóricos y científicos				80%	
CONSISTENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de la investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de				80%	
TOTAL PROMEDIO					80%	

(x) El instrumento puede ser aplicado, tal como está elaborado
( ) El instrumento debe ser mejorado antes de ser aplicado

_____
Firma Experto

EVALUACIÓN DE METODOLOGÍA DE DESARROLLO DE SOFTWARE
TABLA DE EVALUACION DE EXPERTOS Apellidos y nombres del experto:Rivera Crisostomo Renee Título y/o Grado: Ing. de Sistemas Fecha: 07/04/2021 TÍTULO TESIS
SISTEMA DE GESTIÓN PARA LA **SEGURIDAD DE LA INFORMACIÓN** basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020."
EVALUACIÓN DE METODOLOGÍA DE SOFTWARE Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante unas series de criterios con puntuaciones especificadas al final de la tabla. Así mismo le exhortamos en la correcta determinación de la metodología para desarrollar un SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN basado en la Norma ISO/IEC27001 DE LA EMPRESA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN,2020."

ITEM	CRITERIOS	METODOLOGÍAS		
		COBIT	MARGERIT	ISO 27001
1	Permite un desarrollo iterativo	1	3	2
2	Los resultados son más rápidos	1	3	2
3	Requiere de comunicación con el cliente	1	3	2
4	Requiere de entregas constantes	1	3	2
5	Se adecua para tiempos cortos de entrega	1	3	2
6	Los resultados son más rápidos	1	3	2
7	Adaptable y flexible a cambios	1	3	2
8	Implementa las necesidades del sistema	1	3	2
	Total	8	24	16

La escala a evaluar es de 1**: Malo, 2: Regular y 3: Bueno**
Sugerencias: La metodología es aplicable

_____
Firma Experto

.

ANEXO J: SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA CONSTRUCTORA PEREZ & PEREZ SAC, MOYOBAMBA, SAN MARTIN

Un Sistema de Gestión para la seguridad de la información su función es salvaguardar la protección de la información de la organización, teniendo como base principal en un SGSI al estar alineada a la normativa ISO 27001:2013 obteniendo como resultado pequeñas diferencias, entre el enfoque, metodologías y zonas de concentración lo cual nos referimos a la confidencialidad, integridad y disponibilidad de la información y los activos de la organización, al tener en cuenta estas 3 dimensiones vamos más allá de tecnología, abarcamos más aspectos operativos, normativos para la organización.

Para establecer y mantener salvaguardado la información es necesario tener controles y políticas de seguridad para salvaguardar las 3 dimensiones mencionadas con esto tendremos un enfoque de mejora continúa aplicando el ciclo Deming para cada proceso de la organización, esta estructura viene con 114 controladores, 35 objetivos de control y 14 dominios según los parámetros de la normativa 27001 son suficientes para mitigar las amenazas

***Objetivo**

Seleccionar controles de la ISO/IEC 27001:2013 para aplicar a la Constructora Perez & Perez SAC de acuerdo a los procesos que se necesiten

Establecer políticas en todas las áreas de la Empresa Constructora Perez & Perez SAC para salvaguardar los activos de información.

***Alcance**

La propuesta presentada se define para la protección de los activos físicos, lógicos y de información que están expuestas en todas las áreas de la organización ya que se identificaron vulnerabilidad y amenazas que se pueden ser gestionadas por la norma iso 27001:2013

***Documentos de referencia**

ISO/IEC 27001: 2013

NTP/ISO 27001:2014

Ley de protección de datos personales

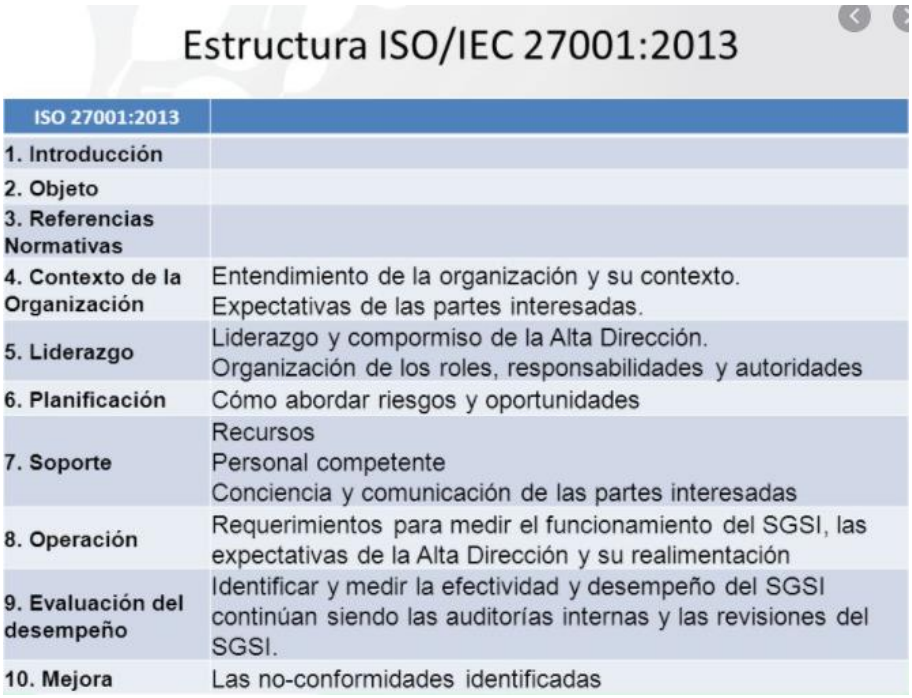


Figura 4: Estructura de la ISO/IEC 27001:2013

***Situación Actual de la Empresa:**

Actualmente en la Constructora Perez & Perez SAC desde enero desde enero del 2014 hasta la fecha 2021 se determinaron lo siguiente:

Unidades de Análisis	**Cantidad**
Activos de información	34
Políticas de Seguridad de la Información	3
Controles de seguridad de la información	6
Roles y Responsabilidades asignadas	1

***Activos de Información**

Los activos de información, se dividen en categorías de acuerdo a la valoración tanto de las amenazas como de las vulnerabilidades.

ID ACTIVO	Nombre del Activo	Descripción
A001	PC GERENTE	hp all in one 22-c1xx
A002	PC Gerente Administrativo	hp all in one 22-c1xx
A003	PC Residente de Obra	hp all in one 22-c1xx
A004	PC Jefe de Almacén	hp all in one 22-c1xx
A005	PC Auxiliar de Presupuesto & Finanzas	hp all in one 22-c1xx
A006	PC de contabilidad	hp all in one 22-c1xx
A007	PC de Recursos Humanos	hp all in one 22-c1xx
A008	PC de Encargado de Compras	hp all in one 22-c1xx
A009	PC De Asistente Logístico	hp all in one 22-c1xx
A010	PC de Sistemas IT	hp all in one 22-c1xx
A011	Copias de respaldo	Backup de información en caso de perdida
A012	Control de Asistencia	Software
A013	Fotografías de eventos	Fotos Confidenciales de las Obras ejecutadas
A014	Microsoft office	Software
A015	Windows	Arquitectura
A016	Access Point	Dlink
A017	Switch	Dlink
A018	UPS Area de Administrativa	FORZA
A019	UPS Area de Operaciones	FORZA
A020	UPS Area de Logística	Forza
A021	Disco Duro Externo 1	Wester Digital
A022	Disco Duro Externo 2	Wester Digital
A023	Disco Duro Externo 3	Wester Digital
A024	Disco Duro Externo 4	Wester Digital
A025	DVR CCTV	Hikvision
A026	Servidor HP	Servidor HP ProLiant ML110 Gen9, Intel Xeon E5-2603v4, 1.70GHz,

		8GB DDR4, 2TB SATA.
A027	Equipo de Control de Acceso Biométrico	Zkteco Biometrico Facial Obra
A028	Equipo de Control de Acceso Biométrico	Equipo de Control de Acceso Biométrico Oficina
A029	Impresora	Epson L850
A030	Impresora	Epson L850
A031	Impresora	Epson L850
A032	Sistema ERP	Sistema Web
A033	Sistema SUNAT	Sistema Web
A034	Internet	Operador Movistar

1. Las políticas de Seguridad

Las políticas de seguridad de la información que se van a implementar son

N°	Política
01	Políticas de Seguridad
02	Seguridad Física y Ambiental
03	Seguridad en la Operativa

1.1 Políticas de Seguridad

En lo que representa esta política de seguridad la Empresa debe organizar en afrontar toma de decisiones que implique afrontar riesgos, así mismo que todo el personal este informado y sean responsables de la seguridad de la información de cada área para que puedan tener una gestión operativa de los controles que mantenga este conjunto para su proceso de implementación.

1.2 Seguridad Física Y Ambiental

En lo que representa esta política es minimizar los riesgos que puede presentar en la Empresa, para establecer bien esta política se debe realizar un análisis de su entorno y verificar las áreas protegidas para que faciliten la implementación de los controles para la protección contra accesos físicos no autorizados, daño e interferencia.

1.3 Seguridad en la Operativa

En lo que representa esta política es controlar los procesos operativos, desarrollo y mantenimiento de los activos, se debe evaluar constantemente el impacto operativo de los cambios para verificar los sistemas y equipamiento para el

monitoreo de las necesidades de los sistema en operación y por último se debe definir y documentar los controles para la detección y prevención de los accesos no autorizados, deberían definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la empresa.

2. Controles de Seguridad de la Información

2.1 Conjunto de políticas para la seguridad de la información.

A vista que son 6 áreas que mantienen la empresa es importante definir el conjunto de políticas que van hacer implementadas en cada una de ellas para luego estar conectadas entre si

2.2 Revisión de las políticas para la seguridad de la información.

Al tener claro ya el conjunto seleccionado, se realiza una revisión de las políticas y sus controles con el fin de realizar una buena implementación para la organización y así poder tener la mejora continúa aplicando el ciclo de Deming en cada proceso

2.3 Perímetro de seguridad física:

Se define como control a proveer protección contra accesos no autorizados con el fin de determinaren un análisis o evaluación de riesgos para ello de debe tener en cuenta los niveles de protección que se necesite para proteger a la información (Muros, alarmas, cerraduras, etc.),

2.4 Mantenimiento de los Equipos:

Se trata de controles para garantizar el funcionamiento adecuado de los Equipos con el fin de salvaguardar la información y que no se deterioren y siempre estén activos para el uso del personal en la empresa y solo puede hacerse cargo del personal autorizado para mantener un registro de cada mantenimiento de cada Equipo en la Empresa

2.5 Copias de seguridad de la información:

Para este control se trata de alcanzar el grado de protección contra la perdida de datos para prevenir esto se debe realizar pruebas regulares de las copias de seguridad de la información, algún software como imágenes relacionadas a la política de seguridad, en la empresa hay varios discos duros externos como copias de seguridad.

2.6 Proteccion del registro de información.

Para los eventos registrados en la Empresa deben tener un nivel de protección para evitar pérdidas, corrupción o cambios no autorizados de la información que ellos protegen, las actividades que se deben realizar deben tener privilegios para poder definir los parámetros de seguridad y las copias de seguridad deberán ser guardadas con el fin de ser administradas por los administradores de red de la empresa

3. Brechas:

En los activos de información se determinó las siguientes amenazas de los activos, de los cuales están los 3 indicadores como principales en esta investigación

TIPO DE AMENAZAS	**FRECUENCIA**
Accesos No autorizados	**ALTO**
Virus Informático	**ALTO**
Eliminar, Manipular y Borrar Datos	**ALTO**
Revelación de información	**ALTO**
Revelación de información confidencial	**ALTO**
Mal funcionamiento de los Equipos	**INTERMEDIO**
Sustracción de información de la empresa	**ALTO**
Perdida de documentación	**ALTO**
Accesos al servidor de personas no identificadas	**INTERMEDIO**

Instalación de software que vulneren la información	**INTERMEDIO**

En cuanto a las vulnerabilidades se resalta las siguientes:

TIPO DE AMENAZAS	**FRECUENCIA**
Contraseñas Débiles	**ALTO**
Falta de documentación interna	**ALTO**
Falta de políticas de accesos remoto	**ALTO**
Falta de capacitación al personal sobre seguridad de la información	**ALTO**
Sensibilidades del equipo a la humedad en el biométrico	**ALTO**
Cableado Estructurado inadecuado	**INTERMEDIO**
Copia de controlada de la información	**ALTO**

Al aplicar los controles según la normatividad ISO27001, se determinó que, en la Empresa Constructora Perez & Perez SAC, existe evidencia en las áreas que no están estandarizadas por un auditor en seguridad información, lo cual revisado a continuación los check list que están aplicando a la empresa segunda la norma 270001

CONTROLES APLICADOS SEGÚN LA NORMATIVA			
Sección 27001:2013	**Controles**	**SI**	**NO**
A.5	Políticas de seguridad de la información		
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información	X	
A.5.1.1	Políticas para la seguridad de la información	X	
A.5.1.2	Revisión de las políticas para la seguridad de la información	X	
A.6	Organización de la seguridad de la información		
A.6.1	Organización interna		
A.6.1.1	Roles y responsabilidades para la seguridad de la información		X
A.6.1.2	Separación de deberes		X
A.6.1.3	Contacto con las autoridades	X	
A.6.1.4	Contactos con grupos de interés especial		X
A.6.1.5	Seguridad de la información en la gestión de proyectos		X
A.6.2	Dispositivos móviles y teletrabajo		
A.6.2.1	Política para dispositivos móviles		X
A.6.2.2	Teletrabajo		X
A.7	Seguridad de los recursos humanos		
A.7.1	Antes de asumir el empleo		
A.7.1.1	Selección	X	
A.7.1.2	Términos y condiciones del empleo	X	
A.7.2	Durante la ejecución del empleo		
A.7.2.1	Responsabilidades de la dirección	X	

A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	X	
A.7.2.3	Proceso disciplinario	X	
A.7.3	Terminación y cambio de empleo		
A.7.3.1	Terminación o cambio de responsabilidades de empleo		X
A.8	Gestión de activos		
A.8.1	Responsabilidad por los activos		
A.8.1.1	Inventario de activos	X	
A.8.1.2	Propiedad de los activos	X	
A.8.1.3	Uso aceptable de los activos	X	
A.8.1.4	Devolución de activos	X	
A.8.2	Clasificación de la información		
A.8.2.1	Clasificación de la información		X
A.8.2.2	Etiquetado de la información	X	
A.8.2.3	Manejo de activos	X	
A.8.3	Manejo de medios		
A.8.3.1	Gestión de medios removibles		X
A.8.3.2	Disposición de los medios	X	
A.8.3.3	Transferencia de medios físicos		X
A.9	Control de acceso		
A.9.1	Requisitos del negocio para control de acceso		
A.9.1.1	Política de control de acceso		X
A.9.1.2	Acceso a redes y a servicios en red	X	
A.9.2	Gestión de acceso de usuarios		
A.9.2.1	Registro y cancelación del registro de usuarios	X	
A.9.2.2	Suministro de acceso de usuarios	X	
A.9.2.3	Gestión de derechos de acceso privilegiado	X	
A.9.2.4	Gestión de información de autenticación secreta de usuarios	X	
A.9.2.5	Revisión de los derechos de acceso de los usuarios	X	
A.9.2.6	Retiro o ajuste de los derechos de acceso	X	
A.9.3	Responsabilidades de los usuarios		
A.9.3.1	Uso de información de autenticación secreta	X	
A.9.4	Control de acceso a sistemas y aplicaciones		
A.9.4.1	Restricción de acceso a la información	X	
A.9.4.2	Procedimiento de ingreso seguro	X	
A.9.4.3	Sistema de gestión de contraseñas	X	
A.9.4.4	Uso de programas utilitarios privilegiados		X
A.9.4.5	Control de acceso a códigos fuente de programas		X
A.10	Criptografía		
A.10.1	Controles criptográficos		

A.10.1.1	Política sobre el uso de controles criptográficos		X
A.10.1.2	Gestión de llaves	X	
A.11	Seguridad física y del entorno		
A.11.1	Áreas seguras		
A.11.1.1	Perímetro de seguridad física	X	
A.11.1.2	Controles de acceso físico	X	
A.11.1.3	Seguridad de oficinas, recintos e instalaciones		X
A.11.1.4	Protección contra amenazas externas y ambientales	X	
A.11.1.5	Trabajo en áreas seguras	X	
A.11.1.6	Áreas de despacho y carga	X	
A.11.2	Equipos		
A.11.2.1	Ubicación y protección de los equipos	X	
A.11.2.2	Servicios de suministro	X	
A.11.2.3	Seguridad del cableado	X	
A.11.2.4	Mantenimiento de equipos	X	
A.11.2.5	Retiro de activos	X	
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	X	
A.11.2.7	Disposición segura o reutilización de equipos	X	
A.11.2.8	Equipos de usuarios desatendidos		X
A.11.2.9	Política de escritorio limpio y pantalla limpia	X	
A.12	Seguridad de las operaciones		
A.12.1	Procedimientos operacionales y responsabilidades		
A.12.1.1	Procedimientos de operación documentados	X	
A.12.1.2	Gestión de cambios		X
A.12.1.3	Gestión de capacidad		X
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	X	
A.12.2	Protección contra códigos maliciosos		
A.12.2.1	Controles contra códigos maliciosos	X	
A.12.3	Copias de respaldo		
A.12.3.1	Respaldo de la información	X	
A.12.4	Registro y seguimiento		
A.12.4.1	Registro de eventos	X	
A.12.4.2	Protección de la información de registro	X	
A.12.4.3	Registros del administrador y del operador	X	
A.12.4.4	Sincronización de relojes		X
A.12.5	Control de software operacional		
A.12.5.1	Instalación de software en sistemas operativos	X	
A.12.6	Gestión de la vulnerabilidad técnica		
A.12.6.1	Gestión de las vulnerabilidades técnicas	X	

A.12.6.2	Restricciones sobre la instalación de software	X	
A.12.7	Consideraciones sobre auditorias de sistemas de información		
A.12.7.1	Controles de auditoria de sistemas de información	X	
A.13	Seguridad de las comunicaciones		
A.13.1	Gestión de la seguridad de las redes		
A.13.1.1	Controles de redes	X	
A.13.1.2	Seguridad de los servicios de red	X	
A.13.1.3	Separación en las redes		X
A.13.2	Transferencia de información		
A.13.2.1	Políticas y procedimientos de transferencia de información		X
A.13.2.2	Acuerdos sobre transferencia de información		X
A.13.2.3	Mensajería electrónica	X	
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	X	
A.14	Adquisición, desarrollo y mantenimiento de sistemas		
A.14.1	Requisitos de seguridad de los sistemas de información		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	X	
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	X	
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones		X
A.14.2	Seguridad en los procesos de desarrollo y soporte		
A.14.2.1	Política de desarrollo seguro		X
A.14.2.2	Procedimientos de control de cambios en sistemas		X
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	X	
A.14.2.4	Restricciones en los cambios a los paquetes de software		X
A.14.2.5	Principios de construcción de los sistemas seguros	X	
A.14.2.6	Ambiente de desarrollo seguro		X
A.14.2.7	Desarrollo contratado externamente		X
A.14.2.8	Pruebas de seguridad de sistemas	X	
A.14.2.9	Prueba de aceptación de sistemas	X	
A.14.3	Datos de prueba		
A.14.3.1	Protección de datos de prueba	X	
A.15	Relaciones con los proveedores		
A.15.1	Seguridad de la información en las relaciones con los proveedores		
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	X	
A.15.1.2	Tratamiento de seguridad dentro de los acuerdos con proveedores	X	
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	X	

A.15.2	Gestión de la prestación de servicios de proveedores		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores		X
A.15.2.2	Gestión de cambios en los servicios de los proveedores		X
A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información		
A.16.1.1	Responsabilidades y procedimientos		X
A.16.1.2	Reporte de eventos de seguridad de la información		X
A.16.1.3	Reporte de debilidades de seguridad de la información		X
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	X	
A.16.1.5	Respuesta a incidentes de seguridad de la información	X	
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	X	
A.16.1.7	Recolección de evidencia	X	
A.17	Aspectos de seguridad de la información de la gestión de continuidad del negocio		
A.17.1	Continuidad de seguridad de la información		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	X	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	X	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	X	
A.17.2	Redundancias		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	X	
A.18	Cumplimiento		
A.18.1	Cumplimiento de requisitos legales y contractuales		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	X	
A.18.1.2	Derechos de propiedad intelectual		X
A.18.1.3	Protección de registros	X	
A.18.1.4	Privacidad y protección de información de datos personales	X	
A.18.1.5	Reglamentación de controles criptográficos		X
A.18.2	Revisiones de seguridad de la información		
A.18.2.1	Revisión independiente de seguridad de la información		X
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	X	
A.18.2.3	Revisión del cumplimiento técnico		X

4. Identificaron de Vulnerabilidades

4.1 Metodología Margerit:

En este cuadro representa el semáforo de riesgo & impacto con las siguientes representaciones:

MB: MUY ALTO
A: ALTO
M: MEDIO
B: BAJO
MB: MUY BAJO

RIESGO		Probabilidad				
IMPACTO		MB	B	N	A	MA
	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

ESCALA			
IMPACTO0	PROBABILIDAD	RIESGO	VALORES
MA	MA	MA	5
A	A	A	4
M	M	M	3
B	B	B	2
MB	MB	MB	1

IMPACTO		Degradacion		
		1%	10%	100%
VALOR	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

4.2Evaluación de riesgos

En la empresa se ah recopilado los activos de información para su análisis de riesgo, las mismas que serán observadas a continuación en las siguientes imágenes de acuerdo a los niveles de la Metodología Margerit

Evaluación de riesgos

N°	Riesgo	Valor de impacto			TV	Nivel de riesgo	Acciones correctivas
		D	C	I			
1	Acceso no autorizado	5	5	5	5	MA	Mitigar
2	Eliminar Borrar y Manipular Datos	5	5	5	5	MA	Mitigar
3	Virus Informático	5	5	5	5	MA	Mitigar
4	Configuración por Defecto	5	3	5	4	M	Mitigar
5	Suplantación de IP	5	4	4	4	MA	Mitigar
6	Monitoreos no autorizados	3	4	3	3	A	Mitigar
7	Contraseñas Débiles	4	4	4	4	M	Mitigar
8	Negación de Servicio	4	3	5	4	A	Mitigar
9	Inundación de Paquetes	3	5	4	4	A	Mitigar
10	Aseguramiento de los equipos	4	4	5	4	M	Mitigar
11	Copias de Respaldo	4	4	4	4	M	Mitigar
12	Defectos Identificados en el Sotfware	3	4	3	3	M	Mitigar
13	Efectividad del antivirus	3	3	3	3	M	Mitigar
14	Efectividad de Antispam	3	3	3	3	M	Mitigar

4.3 Plan de tratamiento de riesgos

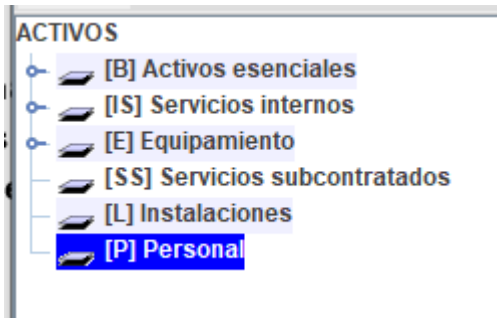
En el plan de tratamiento de riesgos se implementaran los controles de la norma ISO/IEC 27001:2013 para poder mitigar los riesgos que se están generando en la Empresa

N°	Nombre del riesgo	Nivel del riesgo	Controles según ISO 27001	Encargado
1	Acceso no autorizado	MA	Política de control de accesos.	Jefe de soporte
2	Eliminar Borrar y Manipular Datos	MA	Etiquetado y manipulado de la información.	Jefe de soporte
3	Virus Informático	MA	Controles contra el código malicioso.	Jefe de soporte
4	Configuración por Defecto	M	Gestión de cambios.	Jefe de soporte r
5	Suplantación de IP	MA	Gestión de las vulnerabilidades técnicas	Auxiliar de Soporte
6	Monitoreos no autorizados	A	Emplazamiento y protección de equipos.	Jefe de soporte
7	Contraseñas Débiles	M	Gestión de claves.	Jefe de soporte
8	Negación de Servicio	A	Controles de auditoría de los sistemas de información.	Jefe de soporte
9	Inundación de Paquetes	A	Registro y gestión de eventos de actividad	Auxiliar de Soporte
10	Aseguramiento de los equipos	M	Mantenimiento de los equipos.	Auxiliar de Soporte
11	Copias de Respaldo	M	Copias de seguridad de la información.	Jefe de soporte
12	Defectos Identificados en el Sotfware	M	Procedimientos de control de cambios en los sistemas.	Auxiliar de Soporte
13	Efectividad del antivirus	M	Uso de principios de ingeniería en protección de sistemas.	Jefe de soporte
14	Efectividad de Antispam	M	Protección de los datos utilizados en pruebas.	Auxiliar de Soporte

ANEXO L : DESARROLLO DEL PROYECTO PROPUESTO UTILIZANDO PILAR versión 7.4.8 (22.4.2021)

1. Identificación de los Activos de información de la Empresa

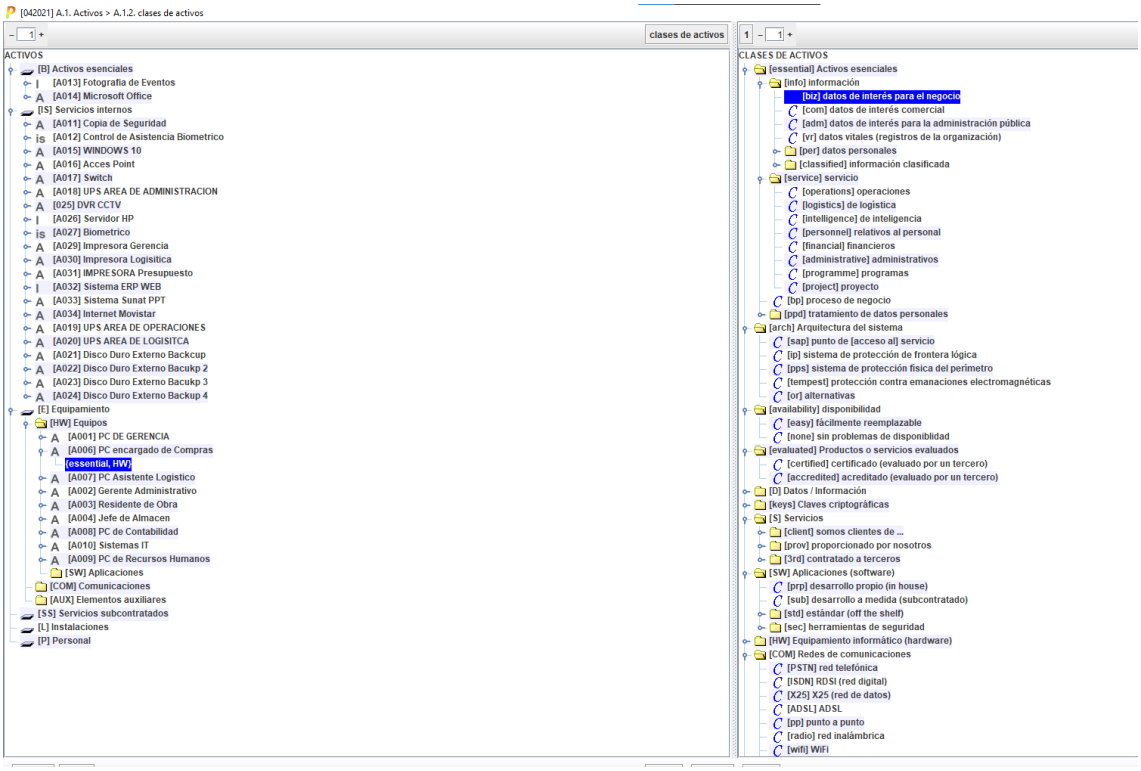
Una vez creado el proyecto, de acuerdo a la instrucción del software Pilar, debemos elegir los activos de información con un código y nombre, su calificación es de manera automática que se resaltará en el siguiente grafico



2. Activos de la informacion con sus categorías representativas.

3. Dependencia de los activos de información de la empresa

Una vez definido ya los activos de información tenemos que enlazarlo con la dependencia que nos resalta como defensa perimetral basado en el Sotfware Pilar


[042021] A.1. Activos > A.1.2. clases de activos
clases de activos
ACTIVOS
[B] Activos esenciales
[A013] Fotografia de Eventos
[A014] Microsoft Office
[S] Servicios internos
[A011] Copia de Seguridad
[A012] Control de Asistencia Biometrico
[A015] WINDOWS 10
[A016] Acces Point
[A017] Switch
[A018] UPS AREA DE ADMINISTRACION
[025] DVR CCTV
[A026] Servidor HP
[A027] Biometrico
[A029] Impresora Gerencia
[A030] Impresora Logisitica
[A031] IMPRESORA Presupuesto
[A032] Sistema ERP WEB
[A033] Sistema Sunat PPT
[A034] Internet Movistar
[A019] UPS AREA DE OPERACIONES
[A020] UPS AREA DE LOGISITCA
[A021] Disco Duro Externo Backcup
[A022] Disco Duro Externo Bacukp 2
[A023] Disco Duro Externo Bacukp 3
[A024] Disco Duro Externo Backup 4
[E] Equipamiento
[HW] Equipos
[A001] PC DE GERENCIA
[A006] PC encargado de Compras
[essential, HW]
[A007] PC Asistente Logistico
[A002] Gerente Administrativo
[A003] Residente de Obra
[A004] Jefe de Almacen
[A008] PC de Contabilidad
[A010] Sistemas IT
[A009] PC de Recursos Humanos
[SW] Aplicaciones
[COM] Comunicaciones
[AUX] Elementos auxiliares
[SS] Servicios subcontratados
[L] Instalaciones
[P] Personal
CLASES DE ACTIVOS
[essential] Activos esenciales
[info] información
[biz] datos de interés para el negocio
[com] datos de interés comercial
[adm] datos de interés para la administración pública
[vr] datos vitales (registros de la organización)
[per] datos personales
[classified] información clasificada
[service] servicio
[operations] operaciones
[logistics] de logistica
[intelligence] de inteligencia
[personnel] relativos al personal
[financial] financieros
[administrative] administrativos
[programme] programas
[project] proyecto
[bp] proceso de negocio
[ppd] tratamiento de datos personales
[arch] Arquitectura del sistema
[sap] punto de [acceso al] servicio
[ip] sistema de protección de frontera lógica
[pps] sistema de protección física del perimetro
[tempest] protección contra emanaciones electromagnéticas
[or] alternativas
[availability] disponibilidad
[easy] fácilmente reemplazable
[none] sin problemas de disponiblidad
[evaluated] Productos o servicios evaluados
[certified] certificado (evaluado por un tercero)
[accredited] acreditado (evaluado por un tercero)
[D] Datos / Información
[keys] Claves criptográficas
[S] Servicios
[client] somos clientes de ...
[prov] proporcionado por nosotros
[3rd] contratado a terceros
[SW] Aplicaciones (software)
[prp] desarrollo propio (in house)
[sub] desarrollo a medida (subcontratado)
[std] estándar (off the shelf)
[sec] herramientas de seguridad
[HW] Equipamiento informático (hardware)
[COM] Redes de comunicaciones
[PSTN] red telefónica
[ISDN] RDSI (red digital)
[X25] X25 (red de datos)
[ADSL] ADSL
[pp] punto a punto
[radio] red inalámbrica
[wifi] WiFi

4. Valorización de los Activos

Se realiza la evaluación de los activos de acuerdo a las dimensiones que hemos utilizado (Confidencialidad, integridad y disponibilidad) nos da como resultado que las variaciones podría ver si se expone a las amenazas del entorno provocando la perdida de información o daños en los activos de información, esta evaluación lo mediremos con la metodología Margerit con los siguientes valores: 5 (Muy alto), 4 (alto), 3 (medio), 2 (bajo) y 1 (muy bajo).

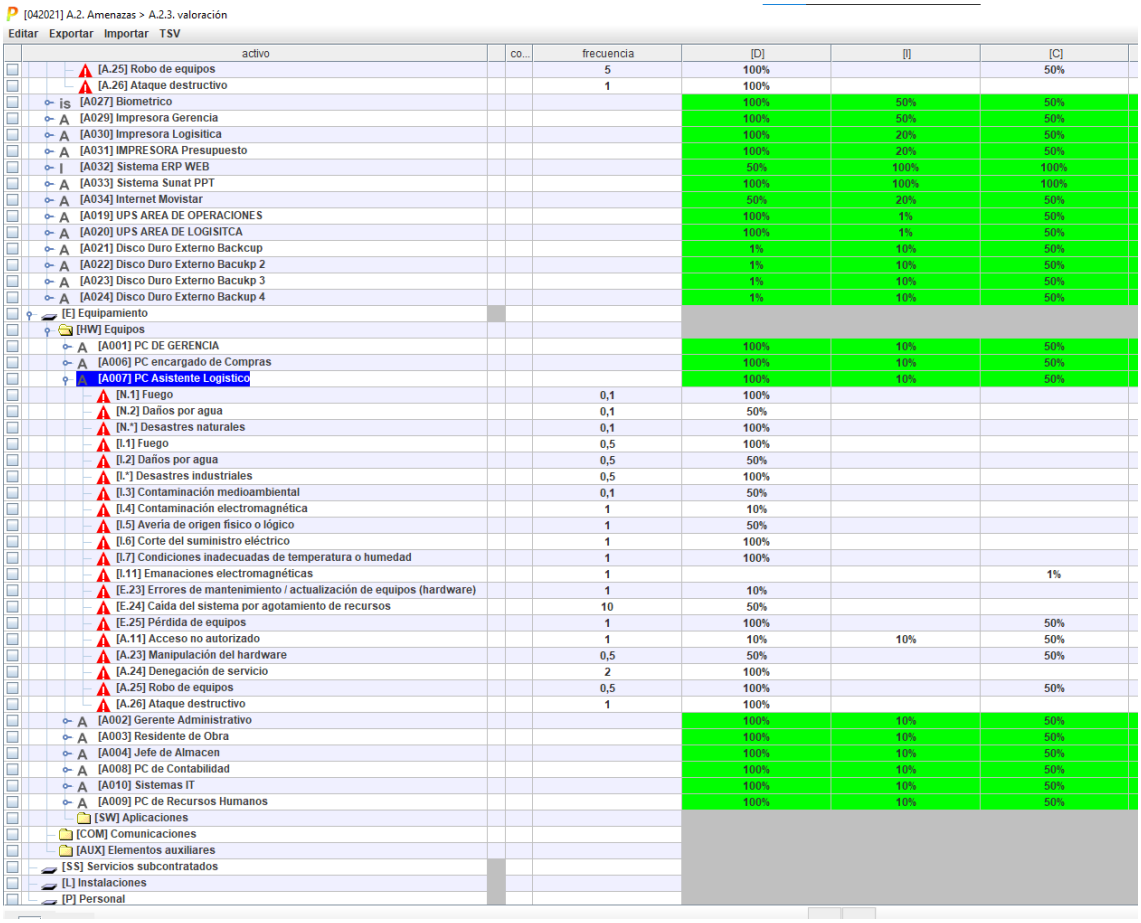
[042021] A.1. Activos > A.1.4. valoración de los activos

Editar Exportar Importar

activo	[D]	[I]	[C]
ACTIVOS			
[B] Activos esenciales			
[A013] Fotografía de Eventos	[5]	[4]	[5]
[A014] Microsoft Office			
[IS] Servicios internos			
[A011] Copia de Seguridad	[5]	[5]	[5]
[A012] Control de Asistencia Biometrico	[4]	[3]	[4]
[A015] WINDOWS 10			
[A016] Acces Point			
[A017] Switch			
[A018] UPS AREA DE ADMINISTRACION			
[025] DVR CCTV	[3]	[4]	[4]
[A026] Servidor HP	[5]	[3]	[3]
[A027] Biometrico			
[A029] Impresora Gerencia			
[A030] Impresora Logisitica			
[A031] IMPRESORA Presupuesto			
[A032] Sistema ERP WEB	[5]	[3]	[3]
[A033] Sistema Sunat PPT	[5]	[3]	[3]
[A034] Internet Movistar	[5]	[4]	[4]
[A019] UPS AREA DE OPERACIONES			
[A020] UPS AREA DE LOGISITCA			
[A021] Disco Duro Externo Backcup	[4]	[3]	[3]
[A022] Disco Duro Externo Bacukp 2	[4]	[3]	[3]
[A023] Disco Duro Externo Bacukp 3			
[A024] Disco Duro Externo Backup 4			
[E] Equipamiento			
[HW] Equipos			
[A001] PC DE GERENCIA	[5]	[3]	[5]
[A006] PC encargado de Compras	[5]	[3]	[3]
[A007] PC Asistente Logistico	[5]	[4]	[4]
[A002] Gerente Administrativo	[5]	[3]	[3]
[A003] Residente de Obra	[5]	[3]	[3]
[A004] Jefe de Almacen	[5]	[5]	[4]
[A008] PC de Contabilidad	[5]	[5]	[5]
[A010] Sistemas IT	[5]	[5]	[5]
[A009] PC de Recursos Humanos	[5]	[5]	[5]
[SW] Aplicaciones			
[COM] Comunicaciones			
[AUX] Elementos auxiliares			
[SS] Servicios subcontratados			
[L] Instalaciones			
[P] Personal			

5. Identificación y valoración de amenazas

Dentro del software se logró identificar las amenazas que más daño producen para identificar el nivel de riesgo que puede llevar esto al no tomar acción con las medidas correctivas, su valorización es automática ya el Software Pilar realiza una evaluación de su frecuencia con el impacto que puede causar



[042021] A.2. Amenazas > A.2.3. valoración

Editar Exportar Importar TSV

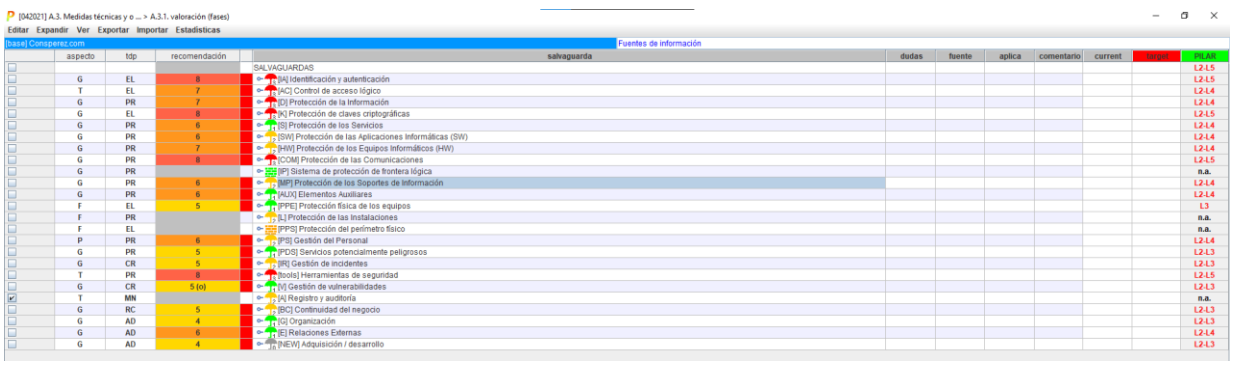
activo	co...	frecuencia	[D]	[I]	[C]
[A.25] Robo de equipos		5	100%		50%
[A.26] Ataque destructivo		1	100%		
[A027] Biometrico			100%	50%	50%
[A029] Impresora Gerencia			100%	50%	50%
[A030] Impresora Logisitica			100%	20%	50%
[A031] IMPRESORA Presupuesto			100%	20%	50%
[A032] Sistema ERP WEB			50%	100%	100%
[A033] Sistema Sunat PPT			100%	100%	100%
[A034] Internet Movistar			50%	20%	50%
[A019] UPS AREA DE OPERACIONES			100%	1%	50%
[A020] UPS AREA DE LOGISITCA			100%	1%	50%
[A021] Disco Duro Externo Backcup			1%	10%	50%
[A022] Disco Duro Externo Bacukp 2			1%	10%	50%
[A023] Disco Duro Externo Bacukp 3			1%	10%	50%
[A024] Disco Duro Externo Backup 4			1%	10%	50%
[E] Equipamiento					
[HW] Equipos					
[A001] PC DE GERENCIA			100%	10%	50%
[A006] PC encargado de Compras			100%	10%	50%
[A007] PC Asistente Logistico			100%	10%	50%
[N.1] Fuego		0,1	100%		
[N.2] Daños por agua		0,1	50%		
[N.*] Desastres naturales		0,1	100%		
[I.1] Fuego		0,5	100%		
[I.2] Daños por agua		0,5	50%		
[I.*] Desastres industriales		0,5	100%		
[I.3] Contaminación medioambiental		0,1	50%		
[I.4] Contaminación electromagnética		1	10%		
[I.5] Avería de origen físico o lógico		1	50%		
[I.6] Corte del suministro eléctrico		1	100%		
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%		
[I.11] Emanaciones electromagnéticas		1			1%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%		
[E.24] Caida del sistema por agotamiento de recursos		10	50%		
[E.25] Pérdida de equipos		1	100%		50%
[A.11] Acceso no autorizado		1	10%	10%	50%
[A.23] Manipulación del hardware		0,5	50%		50%
[A.24] Denegación de servicio		2	100%		
[A.25] Robo de equipos		0,5	100%		50%
[A.26] Ataque destructivo		1	100%		
[A002] Gerente Administrativo			100%	10%	50%
[A003] Residente de Obra			100%	10%	50%
[A004] Jefe de Almacen			100%	10%	50%
[A008] PC de Contabilidad			100%	10%	50%
[A010] Sistemas IT			100%	10%	50%
[A009] PC de Recursos Humanos			100%	10%	50%
[SW] Aplicaciones					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

6. **Evaluación de Salvaguardas:**

Se realizo este análisis a base de las 3 políticas que hemos clasificado que son:

Políticas de Seguridad
Seguridad Física y Ambiental
Seguridad en la Operativa

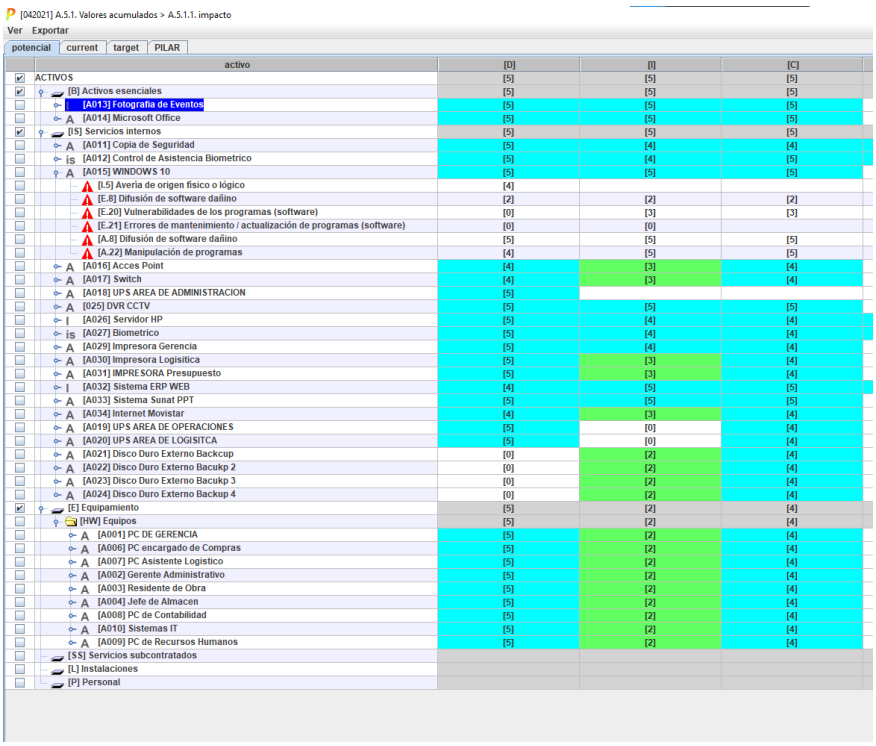
Dentro de la figura podemos apreciar el tipo de activo a base de la situación actual de la empresa con la base recomendada de Pilar para el análisis de Riesgo, teniendo las escalas de semáforo para poder evaluar el nivel de seguridad a tratar



7. **Impacto:**

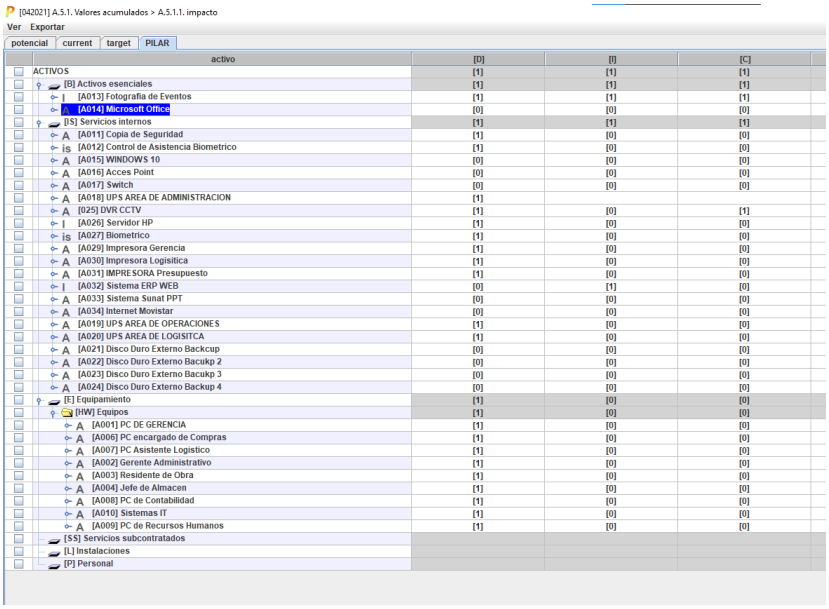
Después de haber realizado las configuraciones de los perímetros en cada activo de la informacion de la empresa, el software realiza de manera automática el nivel del impacto de cada categoría de acuerdo a los niveles de la metodología Magerit

7.1 En esta parte de “Potencial” verificamos el nivel que se encuentra nuestra organización los activos de la informacion antes de la aplicación de la normativa ISO/EIC 27001:2013



activo	[D]	[I]	[C]
ACTIVOS	[5]	[5]	[5]
[B] Activos esenciales	[5]	[5]	[5]
[A013] Fotografia de Eventos	[5]	[5]	[5]
[A014] Microsoft Office	[5]	[5]	[5]
[IS] Servicios internos	[5]	[5]	[5]
[A011] Copia de Seguridad	[5]	[4]	[4]
[A012] Control de Asistencia Biometrico	[5]	[4]	[5]
[A015] WINDOWS 10	[5]	[5]	[5]
[I.5] Avería de origen físico o lógico	[4]		
[E.8] Difusión de software dañino	[2]	[2]	[2]
[E.20] Vulnerabilidades de los programas (software)	[0]	[3]	[3]
[E.21] Errores de mantenimiento / actualización de programas (software)	[0]	[0]	
[A.8] Difusión de software dañino	[5]	[5]	[5]
[A.22] Manipulación de programas	[4]	[5]	[5]
[A016] Acces Point	[4]	[3]	[4]
[A017] Switch	[4]	[3]	[4]
[A018] UPS AREA DE ADMINISTRACION	[5]		
[025] DVR CCTV	[5]	[5]	[5]
[A026] Servidor HP	[5]	[4]	[4]
[A027] Biometrico	[5]	[4]	[4]
[A029] Impresora Gerencia	[5]	[4]	[4]
[A030] Impresora Logisitica	[5]	[3]	[4]
[A031] IMPRESORA Presupuesto	[5]	[3]	[4]
[A032] Sistema ERP WEB	[4]	[5]	[5]
[A033] Sistema Sunat PPT	[5]	[5]	[5]
[A034] Internet Movistar	[4]	[3]	[4]
[A019] UPS AREA DE OPERACIONES	[5]	[0]	[4]
[A020] UPS AREA DE LOGISITCA	[5]	[0]	[4]
[A021] Disco Duro Externo Backcup	[0]	[2]	[4]
[A022] Disco Duro Externo Bacukp 2	[0]	[2]	[4]
[A023] Disco Duro Externo Bacukp 3	[0]	[2]	[4]
[A024] Disco Duro Externo Backup 4	[0]	[2]	[4]
[E] Equipamiento	[5]	[2]	[4]
[HW] Equipos	[5]	[2]	[4]
[A001] PC DE GERENCIA	[5]	[2]	[4]
[A006] PC encargado de Compras	[5]	[2]	[4]
[A007] PC Asistente Logistico	[5]	[2]	[4]
[A002] Gerente Administrativo	[5]	[2]	[4]
[A003] Residente de Obra	[5]	[2]	[4]
[A004] Jefe de Almacen	[5]	[2]	[4]
[A008] PC de Contabilidad	[5]	[2]	[4]
[A010] Sistemas IT	[5]	[2]	[4]
[A009] PC de Recursos Humanos	[5]	[2]	[4]
[SS] Servicios subcontratados			
[L] Instalaciones			
[P] Personal			

7.2 En esta parte “Pilar” se visualiza las recomendaciones que el software nos recomienda para mitigar por completo las dimensiones mencionadas de Confidencialidad, Integridad & Disponibilidad


[042021] A.5.1. Valores acumulados > A.5.1.1. impacto

Ver Exportar

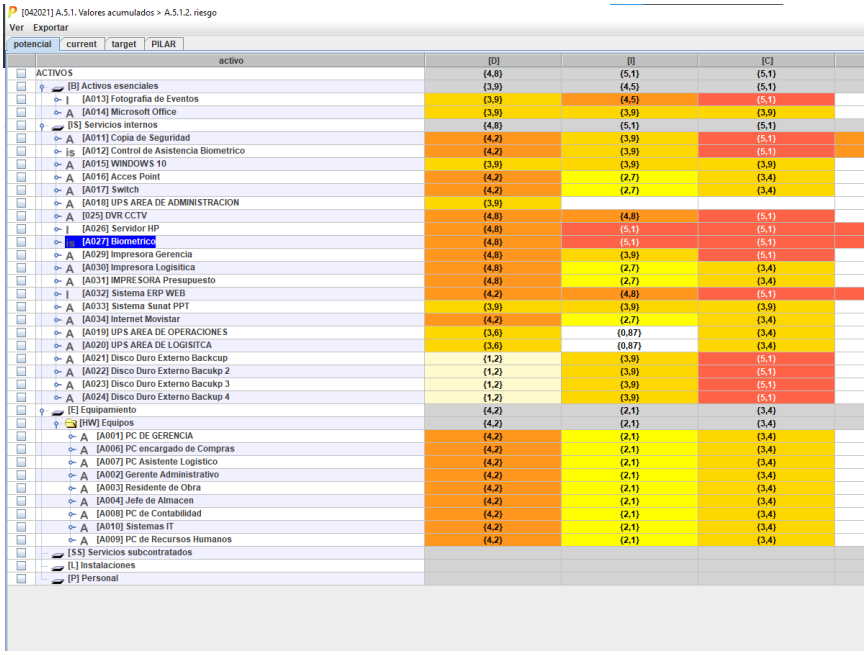
potencial | current | target | PILAR

activo	[D]	[I]	[C]
ACTIVOS	[1]	[1]	[1]
[B] Activos esenciales	[1]	[1]	[1]
[A013] Fotografia de Eventos	[1]	[1]	[1]
[A014] Microsoft Office	[0]	[0]	[0]
[S] Servicios internos	[1]	[1]	[1]
[A011] Copia de Seguridad	[1]	[0]	[0]
[A012] Control de Asistencia Biometrico	[1]	[0]	[0]
[A015] WINDOWS 10	[0]	[0]	[0]
[A016] Acces Point	[0]	[0]	[0]
[A017] Switch	[0]	[0]	[0]
[A018] UPS AREA DE ADMINISTRACION	[1]		
[025] DVR CCTV	[1]	[0]	[1]
[A026] Servidor HP	[1]	[0]	[0]
[A027] Biometrico	[1]	[0]	[0]
[A029] Impresora Gerencia	[1]	[0]	[0]
[A030] Impresora Logisitica	[1]	[0]	[0]
[A031] IMPRESORA Presupuesto	[1]	[0]	[0]
[A032] Sistema ERP WEB	[0]	[1]	[0]
[A033] Sistema Sunat PPT	[0]	[0]	[0]
[A034] Internet Movistar	[0]	[0]	[0]
[A019] UPS AREA DE OPERACIONES	[1]	[0]	[0]
[A020] UPS AREA DE LOGISITCA	[1]	[0]	[0]
[A021] Disco Duro Externo Backcup	[0]	[0]	[0]
[A022] Disco Duro Externo Bacukp 2	[0]	[0]	[0]
[A023] Disco Duro Externo Bacukp 3	[0]	[0]	[0]
[A024] Disco Duro Externo Backup 4	[0]	[0]	[0]
[E] Equipamiento	[1]	[0]	[0]
[HW] Equipos	[1]	[0]	[0]
[A001] PC DE GERENCIA	[1]	[0]	[0]
[A006] PC encargado de Compras	[1]	[0]	[0]
[A007] PC Asistente Logistico	[1]	[0]	[0]
[A002] Gerente Administrativo	[1]	[0]	[0]
[A003] Residente de Obra	[1]	[0]	[0]
[A004] Jefe de Almacen	[1]	[0]	[0]
[A008] PC de Contabilidad	[1]	[0]	[0]
[A010] Sistemas IT	[1]	[0]	[0]
[A009] PC de Recursos Humanos	[1]	[0]	[0]
[SS] Servicios subcontratados			
[L] Instalaciones			
[P] Personal			

8. Riesgo de los Activos de la informacion

8.1 En esta parte “Potencial” es donde actualmente se encuentra las valorizaciones de nuestros activos y nos da como resultado que los niveles son altos ya que no se esta aplicando la norma ISO/IEC 27001:2013

8.2


[042021] A.5.1. Valores acumulados > A.5.1.2. riesgo

Ver Exportar

potencial | current | target | PILAR

activo	[D]	[I]	[C]
ACTIVOS	{4,8}	{5,1}	{5,1}
[B] Activos esenciales	{3,9}	{4,5}	{5,1}
[A013] Fotografia de Eventos	{3,9}	{4,5}	{5,1}
[A014] Microsoft Office	{3,9}	{3,9}	{3,9}
[IS] Servicios internos	{4,8}	{5,1}	{5,1}
[A011] Copia de Seguridad	{4,2}	{3,9}	{5,1}
[A012] Control de Asistencia Biometrico	{4,2}	{3,9}	{5,1}
[A015] WINDOWS 10	{3,9}	{3,9}	{3,9}
[A016] Acces Point	{4,2}	{2,7}	{3,4}
[A017] Switch	{4,2}	{2,7}	{3,4}
[A018] UPS AREA DE ADMINISTRACION	{3,9}		
[025] DVR CCTV	{4,8}	{4,8}	{5,1}
[A026] Servidor HP	{4,8}	{5,1}	{5,1}
[A027] Biometrico	{4,8}	{5,1}	{5,1}
[A029] Impresora Gerencia	{4,8}	{3,9}	{5,1}
[A030] Impresora Logisitica	{4,8}	{2,7}	{3,4}
[A031] IMPRESORA Presupuesto	{4,8}	{2,7}	{3,4}
[A032] Sistema ERP WEB	{4,2}	{4,8}	{5,1}
[A033] Sistema Sunat PPT	{3,9}	{3,9}	{3,9}
[A034] Internet Movistar	{4,2}	{2,7}	{3,4}
[A019] UPS AREA DE OPERACIONES	{3,6}	{0,87}	{3,4}
[A020] UPS AREA DE LOGISITCA	{3,6}	{0,87}	{3,4}
[A021] Disco Duro Externo Backcup	{1,2}	{3,9}	{5,1}
[A022] Disco Duro Externo Bacukp 2	{1,2}	{3,9}	{5,1}
[A023] Disco Duro Externo Bacukp 3	{1,2}	{3,9}	{5,1}
[A024] Disco Duro Externo Backup 4	{1,2}	{3,9}	{5,1}
[E] Equipamiento	{4,2}	{2,1}	{3,4}
[HW] Equipos	{4,2}	{2,1}	{3,4}
[A001] PC DE GERENCIA	{4,2}	{2,1}	{3,4}
[A006] PC encargado de Compras	{4,2}	{2,1}	{3,4}
[A007] PC Asistente Logistico	{4,2}	{2,1}	{3,4}
[A002] Gerente Administrativo	{4,2}	{2,1}	{3,4}
[A003] Residente de Obra	{4,2}	{2,1}	{3,4}
[A004] Jefe de Almacen	{4,2}	{2,1}	{3,4}
[A008] PC de Contabilidad	{4,2}	{2,1}	{3,4}
[A010] Sistemas IT	{4,2}	{2,1}	{3,4}
[A009] PC de Recursos Humanos	{4,2}	{2,1}	{3,4}
[SS] Servicios subcontratados			
[L] Instalaciones			
[P] Personal			

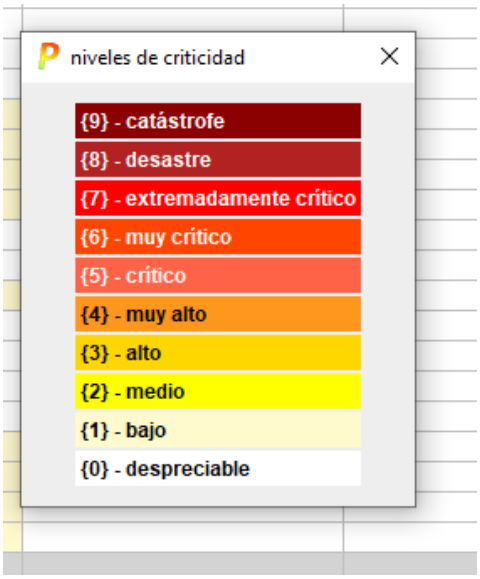
8.2 En la parte “Pilar” al aplicar la normativa ISO/IEC 27001:2013 nos recomienda que su valorización disminuye los riesgos para la seguridad de la informacion de la empresa por lo tanto se realiza un resultado favorable para la organización

[042021] A.5.1. Valores acumulados > A.5.1.2. riesgo

Ver Exportar

potencial | current | target | PILAR

activo	[D]	[I]	[C]
ACTIVOS	{0,99}	{1,2}	{1,3}
[B] Activos esenciales	{0,84}	{0,92}	{1,2}
[A013] Fotografia de Eventos	{0,84}	{0,92}	{1,2}
[A014] Microsoft Office	{0,71}	{0,73}	{0,75}
[IS] Servicios internos	{0,99}	{1,2}	{1,3}
[A011] Copia de Seguridad	{0,86}	{0,76}	{1,0}
[A012] Control de Asistencia Biometrico	{0,83}	{0,74}	{0,98}
[A015] WINDOWS 10	{0,71}	{0,73}	{0,75}
[A016] Acces Point	{0,88}	{0,56}	{0,70}
[A017] Switch	{0,89}	{0,56}	{0,72}
[A018] UPS AREA DE ADMINISTRACION	{0,82}		
[025] DVR CCTV	{0,99}	{0,96}	{1,2}
[A026] Servidor HP	{0,98}	{1,2}	{1,1}
[A027] Biometrico	{0,98}	{1,1}	{1,1}
[A029] Impresora Gerencia	{0,97}	{0,78}	{1,1}
[A030] Impresora Logisitica	{0,96}	{0,54}	{0,69}
[A031] IMPRESORA Presupuesto	{0,96}	{0,54}	{0,69}
[A032] Sistema ERP WEB	{0,88}	{0,97}	{1,2}
[A033] Sistema Sunat PPT	{0,71}	{0,73}	{0,75}
[A034] Internet Movistar	{0,89}	{0,56}	{0,72}
[A019] UPS AREA DE OPERACIONES	{0,77}	{0,09}	{0,70}
[A020] UPS AREA DE LOGISITCA	{0,77}	{0,09}	{0,70}
[A021] Disco Duro Externo Backcup	{0,28}	{0,82}	{1,3}
[A022] Disco Duro Externo Bacukp 2	{0,28}	{0,82}	{1,3}
[A023] Disco Duro Externo Bacukp 3	{0,28}	{0,82}	{1,3}
[A024] Disco Duro Externo Backup 4	{0,28}	{0,82}	{1,3}
[E] Equipamiento	{0,84}	{0,41}	{0,67}
[HW] Equipos	{0,84}	{0,41}	{0,67}
[A001] PC DE GERENCIA	{0,84}	{0,41}	{0,67}
[A006] PC encargado de Compras	{0,84}	{0,41}	{0,67}
[A007] PC Asistente Logistico	{0,84}	{0,41}	{0,67}
[A002] Gerente Administrativo	{0,84}	{0,41}	{0,67}
[A003] Residente de Obra	{0,84}	{0,41}	{0,67}
[A004] Jefe de Almacen	{0,84}	{0,41}	{0,67}
[A008] PC de Contabilidad	{0,84}	{0,41}	{0,67}
[A010] Sistemas IT	{0,84}	{0,41}	{0,67}
[A009] PC de Recursos Humanos	{0,84}	{0,41}	{0,67}
[SS] Servicios subcontratados			
[L] Instalaciones			
[P] Personal			



Niveles de Criticidad del Software Pilar

ANEXO: M

Análisis de riesgos

proyecto: [042021] PEREZ & PEREZ

Datos del proyecto

042021	PEREZ & PEREZ
Organización	Constructora
Descripción	Constructora de Obra Publicas
Responsable del Sistema	Eduardo Risco Villarreal
Responsable de la Seguridad de la Información	Eduardo Risco Villarreal
biblioteca	[std] Biblioteca INFOSEC (8.10.2019)

Licencia

[edu] Eduardo Risco
Escuela Profesional de Ingeniería de Sistemas
Universidad César Vallejo - Lima
[... 1.8.2021]

Dimensiones

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos
- [V] Valor (ej. vidas humanas, patromonio corporativo, etc.)
- [DP] Datos personales

Dominios de seguridad

- [base] Consperez.com

valoración de los activos

dominio: [base] Consperez.com

capa: [B] Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[A013] Fotografia de Eventos	[5]	[4]	[5]				

capa: [IS] Servicios internos

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[A011] Copia de Seguridad	[5]	[5]	[5]				
[A012] Control de Asistencia Biometrico	[4]	[3]	[4]				
[025] DVR CCTV	[3]	[4]	[4]				
[A026] Servidor HP	[5]	[3]	[3]				
[A032] Sistema ERP WEB	[5]	[3]	[3]				
[A033] Sistema Sunat PPT	[5]	[3]	[3]				
[A034] Internet Movistar	[5]	[4]	[4]				
[A021] Disco Duro Externo Backcup	[4]	[3]	[3]				
[A022] Disco Duro Externo Bacukp 2	[4]	[3]	[3]				

capa: [E] Equipamiento

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[A001] PC DE GERENCIA	[5]	[3]	[5]				
[A006] PC encargado de Compras	[5]	[3]	[3]				
[A007] PC Asistente Logistico	[5]	[4]	[4]				
[A002] Gerente Administrativo	[5]	[3]	[3]				
[A003] Residente de Obra	[5]	[3]	[3]				
[A004] Jefe de Almacen	[5]	[5]	[4]				
[A008] PC de Contabilidad	[5]	[5]	[5]				
[A010] Sistemas IT	[5]	[5]	[5]				
[A009] PC de Recursos Humanos	[5]	[5]	[5]				

valoración de los dominios

dominio de seguridad	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[base] Consperez.com	[5]	[5]	[5]				

Riesgo acumulado
Fase: [potencial]
Dominio: [base] Consperez.com

amenaza	dimensión	impacto	probabilidad	riesgo
[A.11] Acceso no autorizado	C, A	[5]	100	{5,7}

Fase: [current] situación actual
Dominio: [base] Consperez.com

amenaza	dimensión	impacto	probabilidad	riesgo
[A.11] Acceso no autorizado	C, A	[5]	100	{5,7}

Fase: [target] situación objetivo
Dominio: [base] Consperez.com

amenaza	dimensión	impacto	probabilidad	riesgo
[A.11] Acceso no autorizado	C, A	[5]	100	{5,7}

Fase: [PILAR] recomendación
Dominio: [base] Consperez.com

amenaza	dimensión	impacto	probabilidad	riesgo
[A.11] Acceso no autorizado	C, A	[1]	3,6	{1,8}

Riesgo repercutido
Fase: [potencial]
Dominio: [base] Consperez.com

activo	amenaza	dimensión	impacto	probabilidad	riesgo
[A013] Fotografia de Eventos	[A.11] Acceso no autorizado	C	[5]	100	{5,7}
[A011] Copia de Seguridad	[A.11] Acceso no autorizado	I, C	[5]	100	{5,7}
[HW.A001] PC DE GERENCIA	[A.11] Acceso no autorizado	C	[5]	100	{5,7}

Fase: [current] situación actual
Dominio: [base] Consperez.com

activo	amenaza	dimensión	impacto	probabilidad	riesgo
[A013] Fotografia de Eventos	[A.11] Acceso no autorizado	C	[5]	100	{5,7}
[A011] Copia de	[A.11] Acceso	I, C	[5]	100	{5,7}

Seguridad	no autorizado				
[HW.A001] PC DE GERENCIA	[A.11] Acceso no autorizado	C	[5]	100	{5,7}

Fase: [target] situación objetivo
Dominio: [base] Consperez.com

activo	amenaza	dimensión	impacto	probabilidad	riesgo
[A013] Fotografia de Eventos	[A.11] Acceso no autorizado	C	[5]	100	{5,7}
[A011] Copia de Seguridad	[A.11] Acceso no autorizado	I, C	[5]	100	{5,7}
[HW.A001] PC DE GERENCIA	[A.11] Acceso no autorizado	C	[5]	100	{5,7}

Fase: [PILAR] recomendación
Dominio: [base] Consperez.com

activo	amenaza	dimensión	impacto	probabilidad	riesgo
[A013] Fotografia de Eventos	[A.11] Acceso no autorizado	C	[1]	3,6	{1,8}
[A011] Copia de Seguridad	[A.11] Acceso no autorizado	I, C	[1]	3,6	{1,8}
[HW.A001] PC DE GERENCIA	[A.11] Acceso no autorizado	C	[1]	3,6	{1,8}
[HW.A004] Jefe de Almacen	[A.11] Acceso no autorizado	I	[1]	3,6	{1,8}
[HW.A008] PC de Contabilidad	[A.11] Acceso no autorizado	I, C	[1]	3,6	{1,8}
[HW.A010] Sistemas IT	[A.11] Acceso no autorizado	I, C	[1]	3,6	{1,8}
[HW.A009] PC de Recursos Humanos	[A.11] Acceso no autorizado	I	[1]	3,6	{1,8}

Activos
Dominio: [base] Consperez.com
Capa: [B] Activos esenciales
- [A013] Fotografia de Eventos
- [A014] Microsoft Office

Capa: [IS] Servicios internos
- [A011] Copia de Seguridad
- [A012] Control de Asistencia Biometrico
- [A015] WINDOWS 10
- [A016] Acces Point
- [A017] Switch
- [A018] UPS AREA DE ADMINISTRACION
- [025] DVR CCTV

[A026] Servidor HP
[A027] Biometrico
[A029] Impresora Gerencia
[A030] Impresora Logisitica
[A031] IMPRESORA Presupuesto
[A032] Sistema ERP WEB
[A033] Sistema Sunat PPT
[A034] Internet Movistar
[A019] UPS AREA DE OPERACIONES
[A020] UPS AREA DE LOGISITCA
[A021] Disco Duro Externo Backcup
[A022] Disco Duro Externo Bacukp 2
[A023] Disco Duro Externo Bacukp 3
[A024] Disco Duro Externo Backup 4

Capa: [E] Equipamiento

[HW] Equipos

[A001] PC DE GERENCIA
[A006] PC encargado de Compras
[A007] PC Asistente Logistico
[A002] Gerente Administrativo
[A003] Residente de Obra
[A004] Jefe de Almacen
[A008] PC de Contabilidad
[A010] Sistemas IT
[A009] PC de Recursos Humanos

ANEXO N:

Declaración de Aplicabilidad - ISO/IEC 27002:2013

[042021] PEREZ & PEREZ

18.5.2021

Introducción
Código: 042021
Nombre: PEREZ & PEREZ

Descripción:
Datos administrativos:

- Organización: Constructora
- Descripción: Constructora de Obra Publicas
- responsable del Sistema: Eduardo Risco Villarreal
- Responsable de la Seguridad de la Información: Eduardo Risco Villarreal

Dominios de seguridad
[base] Consperez.com

Valoración de los activos
capa: [B] Activos esenciales

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[A013] Fotografia de Eventos	[5]	[4]	[5]				

capa: [IS] Servicios internos

Activos esenciales

activo	[D]	[I]	[C]
[A011] Copia de Seguridad	[5]	[5]	[5]
[A012] Control de Asistencia Biometrico	[4]	[3]	[4]
[025] DVR CCTV	[3]	[4]	[4]
[A026] Servidor HP	[5]	[3]	[3]
[A032] Sistema ERP WEB	[5]	[3]	[3]
[A033] Sistema Sunat PPT	[5]	[3]	[3]
[A034] Internet Movistar	[5]	[4]	[4]
[A021] Disco Duro Externo Backcup	[4]	[3]	[3]
[A022] Disco Duro Externo Bacukp 2	[4]	[3]	[3]

capa: [E] Equipamiento

Activos esenciales

activo	[D]	[I]	[C]
[A001] PC DE GERENCIA	[5]	[3]	[5]
[A006] PC encargado de Compras	[5]	[3]	[3]
[A007] PC Asistente Logistico	[5]	[4]	[4]
[A002] Gerente Administrativo	[5]	[3]	[3]
[A003] Residente de Obra	[5]	[3]	[3]
[A004] Jefe de Almacen	[5]	[5]	[4]
[A008] PC de Contabilidad	[5]	[5]	[5]
[A010] Sistemas IT	[5]	[5]	[5]
[A009] PC de Recursos Humanos	[5]	[5]	[5]

Controles
[5] Políticas de seguridad
dominio: [base] Consperez.com

control	aplica
[5] Políticas de seguridad de la información	sí
[5.1] Directrices de gestión de la seguridad de la información	sí
[5.1.1] Políticas para la seguridad de la información	sí
[5.1.2] Revisión de las políticas para la seguridad de la información	sí

[6] Organización de la seguridad de la información
dominio: [base] Consperez.com

control	aplica
[6] Organización de la seguridad de la información	sí
[6.1] Organización interna	sí
[6.1.1] Roles y responsabilidades en seguridad de la información	sí
[6.1.2] Separación de tareas	sí
[6.1.3] Contacto con las autoridades	sí
[6.1.4] Contacto con grupos de interés especial	sí
[6.1.5] Seguridad de la información en la gestión de proyectos	sí
[6.2] Los dispositivos móviles y el teletrabajo	sí
[6.2.1] Política de dispositivos móviles	sí
[6.2.2] Teletrabajo	sí

[7] Seguridad relativa a los recursos humanos
dominio: [base] Consperez.com

control	**aplica**
[7] Seguridad relativa a los recursos humanos	sí
[7.1] Antes del empleo	sí
[7.1.1] Investigación de antecedentes	sí
[7.1.2] Términos y condiciones del empleo	sí
[7.2] Durante el empleo	sí
[7.2.1] Responsabilidades de gestión	sí
[7.2.2] Concienciación, educación y capacitación en seguridad de la información	sí
[7.2.3] Proceso disciplinario	sí
[7.3] Finalización del empleo o cambio en el puesto de trabajo	sí
[7.3.1] Responsabilidades ante la finalización o cambio	sí

[8] Gestión de activos
dominio: [base] Consperez.com

control	**aplica**
[8] Gestión de activos	sí
[8.1] Responsabilidad sobre los activos	sí
[8.1.1] Inventario de activos	sí
[8.1.2] Propiedad de los activos	sí
[8.1.3] Uso aceptable de los activos	sí
[8.1.4] Devolución de activos	sí
[8.2] Clasificación de la información	sí
[8.2.1] Clasificación de la información	sí
[8.2.2] Etiquetado de la información	sí
[8.2.3] Manipulado de la información	sí
[8.3] Manipulación de los soportes	sí
[8.3.1] Gestión de soportes extraíbles	sí
[8.3.2] Eliminación de soportes	sí
[8.3.3] Soportes físicos en tránsito	sí

[9] Control de acceso
dominio: [base] Consperez.com

control	**aplica**
[9] Control de acceso	sí
[9.1] Requisitos de negocio para el control de acceso	sí

[9.1.1] Política de control de acceso	sí
[9.1.2] Acceso a las redes y a los servicios de red	sí
[9.2] Gestión de acceso de usuario	sí
[9.2.1] Registro y baja de usuario	sí
[9.2.2] Provision de acceso de usuario	sí
[9.2.3] Gestión de privilegios de acceso	sí
[9.2.4] Gestión de la información secreta de autenticación de los usuarios	sí
[9.2.5] Revisión de los derechos de acceso de usuario	sí
[9.2.6] Retirada o reasignación de los derechos de acceso	sí
[9.3] Responsabilidades del usuario	sí
[9.3.1] Uso de la información secreta de autenticación	sí
[9.4] Control de acceso a sistemas y aplicaciones	sí
[9.4.1] Restricción del acceso a la información	sí
[9.4.2] Procedimientos seguros de inicio de sesión	sí
[9.4.3] Sistema de gestión de contraseñas	sí
[9.4.4] Uso de utilidades con privilegios del sistema	sí
[9.4.5] Control de acceso al código fuente de los programas	sí

[10] Criptografía
dominio: [base] Consperez.com

control	**aplica**
[10] Criptografía	sí
[10.1] Controles criptográficos	sí
[10.1.1] Política de uso de los controles criptográficos	sí
[10.1.2] Gestión de claves	sí

[11] Seguridad física y del entorno
dominio: [base] Consperez.com

control	**aplica**
[11] Seguridad física y del entorno	sí
[11.1] Áreas seguras	sí
[11.1.1] Perímetro de seguridad física	sí
[11.1.2] Controles físicos de entrada	sí
[11.1.3] Seguridad de oficinas, despachos y recursos	sí
[11.1.4] Protección contra las amenazas externas y ambientales	sí
[11.1.5] El trabajo en áreas seguras	sí
[11.1.6] Áreas de carga y descarga	sí
[11.2] Seguridad de los equipos	sí

[11.2.1] Emplazamiento y protección de equipos	sí
[11.2.2] Instalaciones de suministro	sí
[11.2.3] Seguridad del cableado	sí
[11.2.4] Mantenimiento de los equipos	sí
[11.2.5] Retirada de materiales propiedad de la empresa	sí
[11.2.6] Seguridad de los equipos fuera de las instalaciones	sí
[11.2.7] Reutilización o eliminación segura de equipos	sí
[11.2.8] Equipo de usuario desatendido	sí
[11.2.9] Política de puesto de trabajo despejado y pantalla limpia	sí

[12] Seguridad de las operaciones
dominio: [base] Consperez.com

control	**aplica**
[12] Seguridad de las operaciones	sí
[12.1] Procedimientos y responsabilidades operacionales	sí
[12.1.1] Documentación de los procedimientos de operación	sí
[12.1.2] Gestión de cambios	sí
[12.1.3] Gestión de capacidades	sí
[12.1.4] Separación de los recursos de desarrollo, prueba y operación	sí
[12.2] Protección contra el software malicioso (malware)	sí
[12.2.1] Controles contra el código malicioso	sí
[12.3] Copias de seguridad	sí
[12.3.1] Copias de seguridad de la información	sí
[12.4] Registros y supervisión	sí
[12.4.1] Registro de eventos	sí
[12.4.2] Protección de la información de registro	sí
[12.4.3] Registros de administración y operación	sí
[12.4.4] Sincronización del reloj	sí
[12.5] Control del software en explotación	sí
[12.5.1] Instalación del software en explotación	sí
[12.6] Gestión de la vulnerabilidad técnica	sí
[12.6.1] Gestión de las vulnerabilidades técnicas	sí
[12.6.2] Restricción en la instalación de software	sí
[12.7] Consideraciones sore la auditoría de sistemas de información	sí
[12.7.1] Controles de auditoría de sistemas de información	sí

[13] Seguridad de las comunicaciones
dominio: [base] Consperez.com

control	**aplica**
[13] Seguridad de las comunicaciones	sí
[13.1] Gestión de la seguridad de redes	sí
[13.1.1] Controles de red	sí
[13.1.2] Seguridad de los servicios de red	sí
[13.1.3] Segregación en redes	sí
[13.2] Intercambio de información	sí
[13.2.1] Políticas y procedimientos de intercambio de información	sí
[13.2.2] Acuerdos de intercambio de información	sí
[13.2.3] Mensajería electrónica	sí
[13.2.4] Acuerdos de confidencialidad o no revelación	sí

[14] Adquisición, desarrollo y mantenimiento de sistemas de información
dominio: [base] Consperez.com

control	**aplica**
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información	sí
[14.1] Requisitos de seguridad en sistemas de información	sí
[14.1.1] Análisis de requisitos y especificaciones de seguridad de la información	sí
[14.1.2] Asegurar los servicios de aplicaciones en redes públicas	sí
[14.1.3] Protección de las transacciones de servicios de aplicaciones	sí
[14.2] Seguridad en el desarrollo y en los procesos de soporte	sí
[14.2.1] Política de desarrollo seguro	sí
[14.2.2] Procedimiento de control de cambios en sistemas	sí
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	sí
[14.2.4] Restricciones a los cambios en los paquetes de software	sí
[14.2.5] Principios de ingeniería de sistemas seguros	sí
[14.2.6] Entorno de desarrollo seguro	sí
[14.2.7] Externalización del desarrollo de software	sí
[14.2.8] Pruebas funcionales de seguridad de sistemas	sí
[14.2.9] Pruebas de aceptación de sistemas	sí
[14.3] Datos de prueba	sí
[14.3.1] Protección de los datos de prueba	sí

[15] Relación con proveedores
dominio: [base] Consperez.com

control	aplica
[15] Relación con proveedores	sí
[15.1] Seguridad en las relaciones con proveedores	sí
[15.1.1] Política de seguridad de la información en las relaciones con los proveedores	sí
[15.1.2] Requisitos de seguridad en contratos con terceros	sí
[15.1.3] Cadena de suministro de tecnología de la información y de las comunicaciones	sí
[15.2] Gestión de la provisión de servicios del proveedor	sí
[15.2.1] Control y revisión de la provisión de servicios del proveedor	sí
[15.2.2] Gestión de cambios en la provisión del servicio del proveedor	sí

[16] Gestión de incidentes de seguridad de la información
dominio: [base] Consperez.com

control	aplica
[16] Gestión de incidentes de seguridad de la información	sí
[16.1] Gestión de incidentes de seguridad de la información y mejoras	sí
[16.1.1] Responsabilidades y procedimientos	sí
[16.1.2] Notificación de eventos de seguridad de la información	sí
[16.1.3] Notificación de puntos débiles de la seguridad	sí
[16.1.4] Evaluación y decisión sobre los eventos de seguridad de información	sí
[16.1.5] Respuesta a incidentes de seguridad de la información	sí
[16.1.6] Aprendizaje de los incidentes de seguridad de la información	sí
[16.1.7] Recopilación de evidencias	sí

[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio
dominio: [base] Consperez.com

control	aplica
[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio	sí
[17.1] Continuidad de la seguridad de la información	sí
[17.1.1] Planificación de la continuidad de la seguridad de la información	sí
[17.1.2] Implementar la continuidad de la seguridad de la información	sí
[17.1.3] Verificación, revisión y evaluación de la continuidad de la	sí

seguridad de la información	
[17.2] Redundancia	sí
[17.2.1] Disponibilidad de los recursos de tratamiento de la información	sí

[18] Cumplimiento
dominio: [base] Consperez.com

control	**aplica**
[18] Cumplimiento	sí
[18.1] Cumplimiento de los requisitos legales y contractuales	sí
[18.1.1] Identificación de la legislación aplicable y de los requisitos contractuales	sí
[18.1.2] Derechos de propiedad intelectual (DPI)	sí
[18.1.3] Protección de los registros de la organización	sí
[18.1.4] Protección y privacidad de la información de carácter personal	sí
[18.1.5] Regulación de los controles criptográficos	sí
[18.2] Revisiones de la seguridad de la información	sí
[18.2.1] Revisión independiente de la seguridad de la información	sí
[18.2.2] Cumplimiento de las políticas y normas de seguridad	sí
[18.2.3] Comprobación del cumplimiento técnico	sí

ANEXO Ñ: PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA LA CONSTRUCTORA PEREZ & PEREZ SAC

1. Introducción

El presente plan de seguridad de la información tiene como objetivo principal establecer las políticas de seguridad para la organización

El plan de seguridad se constituye en dos partes, la primera parte como presentación, objetivos y el alcance y con la segunda parte se describe los objetivos:

- **Elaborar políticas de seguridad de la información**
- **Mejorar la seguridad física**
- **Mejorar la seguridad lógica**
- **Mejorar la seguridad de redes**
- **Implementar estrategias de continuidad**
- **Revisar el cumplimiento de las políticas de seguridad de la información**

***Primera Parte**

***Presentación**

El plan de seguridad de la información para la constructora Perez & Perez sac responde a los siguientes principios que definen la seguridad informática.

♣ Confidencialidad: A los usuarios autorizados tendrá accesos a la información.

♣ Integridad: En la empresa tomar decisiones sobre la manipulación de datos antes & durante & después de los procesos.

♣ Disponibilidad: Sirve para utilizar los servicios informáticos siempre y cuando sea necesario.

***Objetivo General**

El objetivo del plan de Seguridad de la Información es salvaguardar la información de la empresa constructora Perez & Perez SAC

***Alcance**

Este documento se aplicará a las 6 áreas de la constructora perez & perez sac

***Resumen de Resultados del Análisis de Riesgo**

Se utilizará la plataforma PILAR para los resultados correspondientes.

***Segunda Parte**

Para el desarrollo del Plan de Seguridad de la Información se ha establecido 6 objetivos, donde cada objetivo será implementado en cada mes comenzando desde Junio.

Objetivo N°1 - Elaborar Políticas de Seguridad Informática

Tareas

a. Se analiza & se identifica los riesgos de la organización siguiendo una metodología de riesgo.

b. Se debe seguir las tareas de la metodología Magerit:

   Caracterización de los Activos.
   Caracterización de las Amenazas.
   Caracterización de las Salvaguardas.
   Estimación del estado de riesgo.

c. Se desarrolla la documentación de la política, alineada con los objetivos generales de la empresa y basada en modelos de tecnología de la información.

d. Se capacita a todo el personal en materia de seguridad y en la política.

e. Se implementa la política

Responsables
Eduardo Risco – Encargado del Area del IT
Fecha de Realización
Mes de Junio

Objetivo N°2- Mejorar la Seguridad Física

Tareas

a. Mejorar el sistema biométrico de registro de acceso del personal para obra como para oficina.

b. Se comprarán cámaras de seguridad con temperatura térmica para prevenir el COVID19 tanto para oficina como para obra.

c. Se llevará registros del mantenimiento preventivo y correctivo que se realice a los equipos de computación.

d. Se capacitará al personal en las medidas de seguridad física. Responsable directo el Encargado del Area de IT, el Jefe de almacén será el responsable de realizar las descarga de las grabaciones del CCTV

Responsables
Eduardo Risco – Encargado del Área del IT
Fecha de Realización
Mes de Julio

Objetivo N° 3- Mejorar la Seguridad Lógica

Tareas

a. Establecer que el tiempo de conexión de la red se limite al horario normal de oficina con conexión a los encargados de Obra

b. Llevar una bitácora de eventos que incluya:

-El identificador del usuario de ordenador

-Fecha, hora de conexión y desconexión.

-Registro de los intentos aceptados y rechazados de acceso al sistema, datos y otros recursos.

c. Responsable directo es el encargado del Área de IT y su auxiliar de soporte técnico

Responsables
Eduardo Risco – Encargado del Area del IT
Fecha de Realización
Mes de Agosto

Objetivo N°4- Mejorar la Seguridad en Redes

Tareas

a. Comprar licencias Endpoint Eset Nod 32 para todos los ordenadores y realizar las políticas

b. Realizar periódicamente escaneos de virus a los equipos.

c. Actualizar el antivirus en los computadores ya

sea como control preventivo o como rutina básica de seguridad.

d. Configurar los Access point para el firewall para la prevención de fuga de datos

Responsables
Eduardo Risco – Encargado del Área del IT
Fecha de Realización
Mes de Setiembre

Objetivo N° 5-Implementar Estrategias de Continuidad

Tareas

Se dará mantenimiento a las fuentes de poder interrumpidas y mejorar su voltaje (UPS).

a. Seleccionar un centro alternativo y almacenamiento externo.

b. Se realizarán respaldos diarios de la información de la Base de Datos.

Responsables
Eduardo Risco – Encargado del Área del IT
Fecha de Realización
Mes de Octubre

Objetivo N°6 Revisar el Cumplimiento de las Políticas de seguridad de Información Tareas

a. Los sistemas de información serán revisados para la conformidad con los estándares de la normativa ISO 27001:2013

b. Los jefes de Área se asegurarán de que se cumplen correctamente los procedimientos de seguridad dentro de su área de responsabilidad.

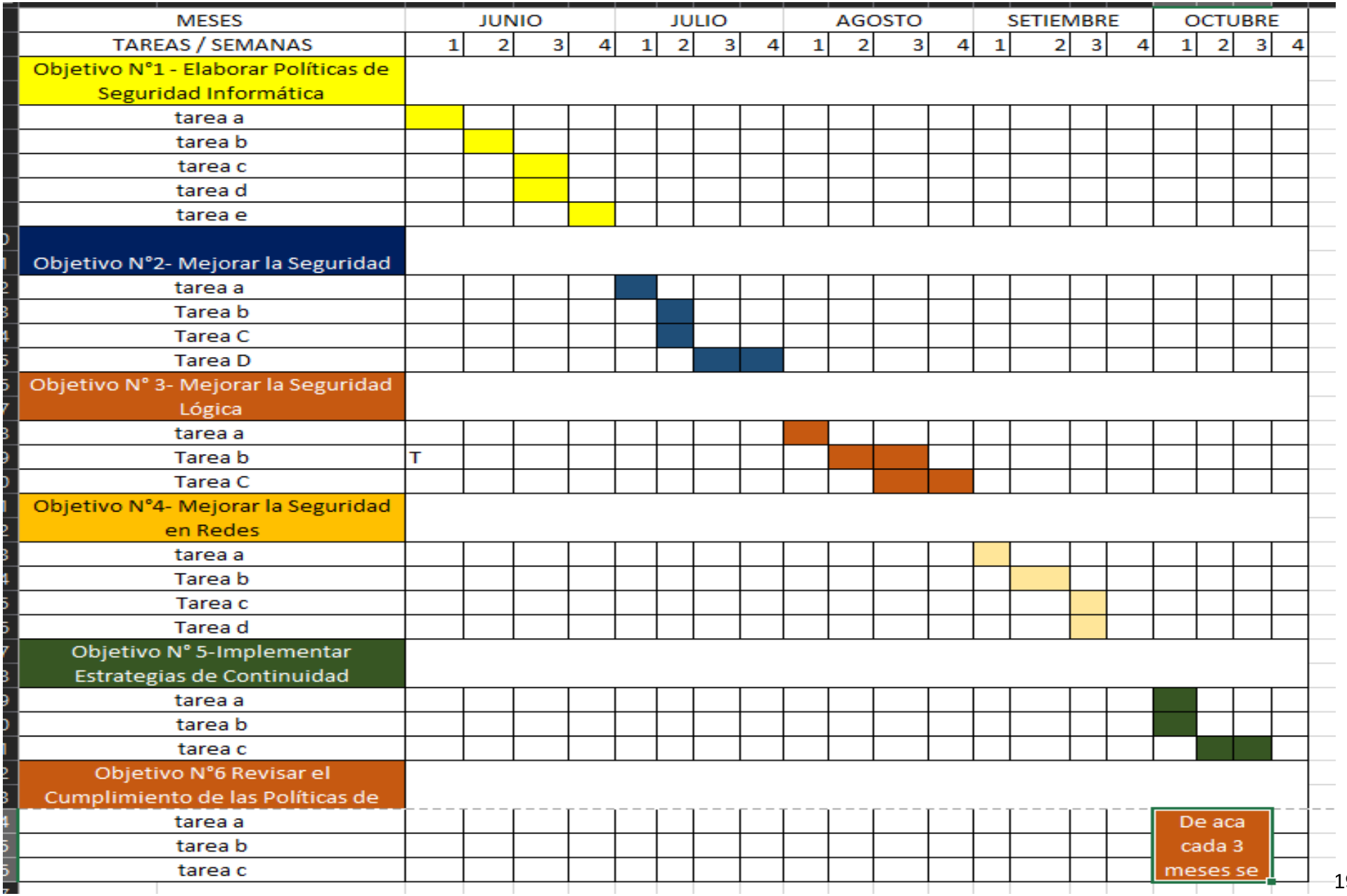
c. Toda las áreas deben estar en constante mejora continua cumpliendo los estándares

Responsables

Eduardo Risco – Encargado del Area del IT

Fecha de Realización

Cada tres meses a partir del inicio de la ejecución de este plan.


MESES
JUNIO
JULIO
AGOSTO
SETIEMBRE
OCTUBRE
TAREAS / SEMANAS
1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4
Objetivo N°1 - Elaborar Políticas de Seguridad Informática
tarea a
tarea b
tarea c
tarea d
tarea e
Objetivo N°2- Mejorar la Seguridad
tarea a
Tarea b
Tarea C
Tarea D
Objetivo N° 3- Mejorar la Seguridad Lógica
tarea a
Tarea b
T
Tarea C
Objetivo N°4- Mejorar la Seguridad en Redes
tarea a
Tarea b
Tarea c
Tarea d
Objetivo N° 5-Implementar Estrategias de Continuidad
tarea a
tarea b
tarea c
Objetivo N°6 Revisar el Cumplimiento de las Políticas de
tarea a
tarea b
tarea c
De aca cada 3 meses se

Financiamiento					
Mecanismo de Seguridad	**Características**	**Descripción**	**Cantidad**	**Costo Unitario**	**Costo Total**
Sistema Biométrico	Reconocer los rasgos combinados tanto de huella como facial para controlar el ingreso de personas autorizadas a la oficina como de obra	OBRA: Instalado en la puerta principal para ingresar a obra OFICINA: Instalado al costado del área de RR.HH , actualizar los sistemas	2	S/ 1,500.00 soles	S/. 3,000 soles
Sistema de Videovigilancia	OBRA : Cuentan con un CCTV 360 grados OFICINA: Cuentan con 4 cámaras en las distintas áreas	Obra: Esta situada en las áreas de construcción. Oficina: Esta situada en las areas de oficina	5	Paquete CCTV Obra S/. 3,800.00 Paquete CCTV Oficina: S/. 2,500.00	S/ 6.300 soles
Endpoint Eset Nod32	Permite detectar software malicioso, filtros antipishing para detectar intentos de suplantación de páginas, etc.	Antivirus EndPoint, que permitirá instalar el antivirus a cada cliente, actualizándolo automáticamente. Se encontrará en toda la red	10	S/ 150.00	S/ 1,500.00
Firewall	Ayuda a detectar actividad sospechosa o evasiva dentro de la red de la institución	FortiGate Next Generation Firewall	1	S/. 18,532.00	S/. 18,532.00
Backup HP	Ayuda a hacer una copia de los datos originales con el fin de disponer de un medio para recuperarlos en caso de su perdid	Almacenamiento de 30 Tb en la nube, toda la red	1	S/ 4,500.00	S/ 4,500.00
UPS (Fuentes de poder interrumpibles)	Permitirá dar energía por un tiempo prudente para que el	UPS para Servidor (Biblioteca central). UPS para Data Center	3	S/. 6,000.00	S/. 6,000.00

	trabajador tenga el tiempo necesario para guardar archivos de importancia y apagar el ordenador de forma correcta en caso de un corte de luz o un problema eléctrico	UPS para oficina de administrativos			
Sistema de Deteccion de Humo en Obra	Para la detección y previsión de siniestros a causa del fuego	Para obra como para Oficina	2	S/ 2,200.00	S/. 4,400.00
					S/. 44,232.00