UNIVERSIDAD NACIONAL “HERMILIO VALDIZAN”

FACULTAD DE INGENIERÍA INDUSTRIAL Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

CARRERA PROFESIONAL DE INGENIERIA DE SISTEMAS

IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT V3 PARA MEJORAR LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y PROPUESTA DE POLITICAS DE SEGURIDAD BASADAS EN NORMA TECNICA PERUANA ISO/IEC 27001:2014 EN LA DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO DE HUÁNUCO - 2021.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS

TESISTAS:

BACH. RIVERA ANASTACIO DANIEL KEVIN

BACH. VALDIVIA ESCOBAR JHONATHAN HAROLD

ASESOR:

MG. FLORES VIDAL JIMMY GROVER

HUÁNUCO – PERÚ

2021

DEDICATORIA

A mi familia, compañeros. Dedico este estudio especialmente a mi progenitora, por su apoyo y dedicación, que me ha ayudado a alcanzar uno de mis objetivos.

Bachiller. Jhonathan Harold Valdivia Escobar

DEDICATORIA

Primeramente, agradecer a Dios por permitirme llegar hasta este punto en mi vida, a mi padre por apoyarme en cada decisión de mi carrera, y mi familia por su apoyo incondicional y a mis amigos por los ánimos y confianza en mí.

Daniel Kevin Rivera Anastacio

AGRADECIMIENTO

El presente proyecto de tesis agradece a:

Al ingeniero Jimmy Flores Vidal, por su asesoría y paciencia en el transcurso para poder culminar con este proyecto de tesis.

Al ingeniero Luis Meza Ordoñes, por su sacrificio de tiempo y transferencia de conocimientos.

A la ingeniera Ines Jesus Tolentino, por su constancia, paciencia y apoyo significativo en cada momento.

A la ingeniera Velsy Rivera Vidal, por su apoyo como experta del tema y poder llegar al objetivo deseado con este proyecto.

RESUMEN

El propósito esencial del estudio fue implementar la metodología Magerit V3 y la norma técnica peruana ISO 27001-2014 mediante la propuesta de una política de privacidad para mejorar la gestión de riesgos de seguridad de la información a la Dirección Regional para la Promoción de la Seguridad de la Información Empleo, las técnicas empleadas para el recojo de data fueron observacionales a través de formatos controlados, entrevistas, el alcance del estudio fue descriptivo, correlacional, el tipo utilizado y el diseño del estudio fueron cuasi – experimental. La muestra estuvo compuesta por 54 activos, se emplearon tablas de frecuencias para las dimensiones de las variables independiente y dependiente, para la prueba de contrastación de hipótesis se empleó el Test de Wilcoxon, ya que estamos trabajando con datos no paramétricos, lo cual demostramos mediante las pruebas de normalidad de Kolmogorov – Smimov, ya que nuestra muestra es superior a 50.

Los resultados relacionados a los equipos tecnológicos arrojan que existe una reducción del estado de riesgos de la categoría “Intolerable” del 28% a 2%, así como la categoría “tolerable” disminuyo de 61% a 57%, de igual manera se vio una reducción de la probabilidad de amenaza en el 59 % al 35 % de los activos informáticos en la categoría Probabilidad de la categoría Amenaza probable, y se han observado reducciones generales. El estado de riesgo de los activos informáticos disminuye con el tiempo, aspectos de la seguridad de la información, como la confidencialidad, la integridad y la disponibilidad, para comprender mejor el contexto en el que se protege la información para que estas amenazas puedan abordarse adecuadamente a través de recomendaciones de política de privacidad.

De acuerdo a las validaciones de las hipótesis en el SPSS se llega a la conclusión general de que la implementación de la metodología Magerit v3 y la Norma Técnica Peruana ISO 27001-2014 mejora la gestión de riesgos de la seguridad de la información, esto debido a que el valor P obtenido es: 0,000 < 0,05, esto nos posibilitó admitir la hipótesis alterna (Ha), a un nivel de 95% de confiabilidad.

Palabras clave

Metodología Magerit v3, seguridad de la información, riesgos, amenazas, salvaguardas, confidencialidad, disponibilidad, integridad, políticas de seguridad.

ABSTRACT

The essential purpose of the study was to implement the Magerit V3 methodology and the Peruvian technical standard ISO 27001-2014 through the proposal of a privacy policy to improve the management of information security risks to the Regional Directorate for the Promotion of Data Security. Employment Information, the techniques used for data collection were observational through controlled formats, interviews, the scope of the study was descriptive, correlational, the type used and the design of the study were quasi-experimental. The sample consisted of 54 assets, frequency tables were used for the dimensions of the independent and dependent variables, for the hypothesis contrast test the Wilcoxon Test was used, since we are working with non-parametric data, which we demonstrate by Kolmogorov-Smimov normality tests, since our sample is greater than 50.

The results related to technological equipment show that there is a reduction in the risk status of the "Intolerable" category from 28% to 2%, as well as the "tolerable" category decreased from 61% to 57%, in the same way there was a reduction in threat probability from 59% to 35% of IT assets in the Likelihood category of the Likely Threat category, and overall reductions have been observed. The risk status of IT assets decreases over time, aspects of information security, such as confidentiality, integrity, and availability, to better understand the context in which information is protected so that these threats can be appropriately addressed through privacy policy recommendations.

According to the validations of the hypotheses in the SPSS, the general conclusion is reached that the implementation of the Magerit v3 methodology and the Peruvian Technical Standard ISO 27001-2014 improves information security risk management, this due to that the P value obtained is: 0.000 < 0.05, this allowed us to admit the alternative hypothesis (Ha), at a level of 95% reliability.

Keywords

Magerit v3 methodology, information security, risks, threats, safeguards, confidentiality, availability, integrity, security policies.

TABLAS

GRÁFICOS

CONTENIDO

INTRODUCCION

La firmeza de la información es uno de los aspectos más primordiales que debe gestionar hoy en día toda organización que quiera amparar y asegurar la continuidad del negocio. Para proteger la información de la agencia, se deben garantizar los siguientes aspectos de la seguridad de la información: confidencialidad, integridad y disponibilidad, por lo que se han desarrollado varios estándares internacionales como ISO 27001 como marco de referencia para las agencias para permitir los requisitos de desarrollo de políticas de seguridad.

Para entender los riesgos a los que está expuesto una determinada institución es necesaria la implementación de una metodología que permita determinar el estado del riesgo a la cual se expone la data que procesa, en este estudio utilizaremos el método Magerit v3, donde determina un marco de antecedente para la examinación de riesgos, permitiendo establecer el nivel de riesgo al que están sujetos los activos de la empresa. La gestión, que aborda el funcionamiento de protecciones a través de políticas de seguridad que nos ayuda a disminuir la condición de riesgo a una manejable.

Se observa en la entidad que existen falencias de seguridad descubiertas que son tales como la de **Divulgación no Autorizada debido a que** existen tramites o expedientes que en determinados casos se filtran esto principalmente se da porque la gran mayoría de las computadoras no tienen la autenticación por usuario y contraseña, lo cual es muy preocupante, y pone en grave riesgo la información de la entidad. La otra falencia encontrada es sobre un **uso inapropiado de los equipos informáticos** (computadoras de escritorio, Laptops, Tablet's), ya que no existe restricción al momento de ingresar al internet, una parte de los trabajadores de la entidad la usan para entrar a redes sociales, como a la descarga de series y música, lo que, al no haber ningún programa de antivirus, el equipo se infecta y daña la información almacenada, que en muchas ocasiones el encargado de informática tiene que formatear el equipo informático para solucionar el problema. Se resalta que la entidad no existe charlas o capacitaciones a los empleados sobre la seguridad de la data que emplean, ya que no hay una política de privacidad definida para estas situaciones.

Este estudio se elabora con el objetivo de perfeccionar la capacidad de administración de peligros de seguridad de la data dentro de la Dirección Regional de Trabajo y Promoción del Empleo (DRTPE). DRTPE se ubica en una situación de vulnerabilidad, por la ausencia de controles de gestión de la data, por lo que esta indagación tiene como objetivos: examinar y administrar peligros, reconocer y escoger elementos para la implementación y desarrollo de propuestas de políticas de privacidad utilizando la Norma Técnica Peruana NTPISO 27001: 2014

La DRTPE, no cuenta con un área de Informática, y es manejado por el Gobierno Regional (GRHCO), por tanto, el manejo de los activos como cualquier información relativa a la Metodología Magerit v3, está a cargo del área informática del GRHCO.

Habiendo llevado a cabo las entrevistas pertinentes para el inicio del proyecto, se identificó que la DRTPE no cuenta con una metodología, normas o reglas que ayude la seguridad de la información, así como la adecuada gestión de la información, para asegurar un adecuado sistema de administración de peligros y procesos en tomar una decisión.

Debido a estas problemáticas nace nuestra idea preguntándonos, ¿En qué medida la implementación de la metodología Magerit V3 y la Norma Técnica Peruana ISO/IEC 27001-2014 **mejorará** de la gestión de riesgos de la seguridad de la información en la Dirección Regional de Trabajo y Promoción del empleo, Huánuco?

La primera parte del proyecto trata del planteamiento del problema, y la identificación de objetivos trazados por los tesistas, tanto como el marco teórico y metodológico. En esta etapa se desarrollará la descripción detallada de que es la metodología Magerit y que es lo que se plantea en el proyecto.

La segunda parte del proyecto trata del análisis de situaciones en las que DRTPE se considera relevante para la seguridad de la información, se realizarán entrevistas e investigaciones para ayudar a establecer el grado de peligro que DRTPE se percibe a sí mismo, de esta manera se podrá definir el plan a tomar en cuenta para reducir y tener la aceptabilidad de los riesgos.

La tercera parte del proyecto es la implementación de la Metodología Magerit, en esta etapa involucraremos el apoyo del director de la DRTPE, para poder incentivar a los trabajadores en colaborar en la implementación, de esta manera lograr un cambio en vinculación a la seguridad de la información.

La cuarta parte del proyecto es la toma de datos final, para identificar el resultado obtenido posterior a la implementación de la Metodología, para lo cual se desarrollará encuestas y entrevistas.

La quinta parte del proyecto es realización de la contrastación de hipótesis, de acuerdo a las validaciones de las hipótesis en el SPSS se llega a la conclusión general de que la implementación de la metodología Magerit v3 y la Norma Técnica Peruana ISO 27001-2014 mejora la administración de peligros de la seguridad de la información, esto debido a que el valor P obtenido es: 0,000 < 0,05, esto nos facilitó admitir la hipótesis alterna (Ha), a un nivel de 95% de confiabilidad

I. PLANTEAMIENTO DEL PROBLEMA

1.1 Antecedentes y Fundamentación del problema

En la actualidad, el estudio de las amenazas a la seguridad de la información forma parte del proceso de toda organización, tanto pública como privada, debido a que el uso de las tecnologías de la información y la comunicación ha sido ampliamente adoptado, incluso en este caso particular, debido al Covid-19. La crisis sanitaria que estamos viviendo, expone a las organizaciones a todo tipo de amenazas y vulnerabilidades de seguridad que atentan contra la seguridad de la información en sus aspectos relevantes. Para controlar las amenazas a la seguridad de la información, es necesario desarrollar medidas de control de seguridad de acuerdo con los requerimientos de cada sujeto.

Para entender los riesgos a los que está expuesto una determinada institución es necesaria la implementación de una metodología que permita determinar el estado del riesgo a la cual la información que maneja es pública y en este artículo utilizaremos la metodología Magerit v3 enfocándonos en tres pasos: planificación, análisis de riesgos y tratamiento de riesgos. con ello se logra obtener una idea clara de los riesgos y se define las salvaguardas para ser utilizadas en caso de presentarse uno de ellos.

El estado peruano ha definido lineamientos para una Política de Ciberseguridad que tiene por objetivo principal “Proteger la infraestructura de información, los datos e información del Estado y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.” (Digital, 2017), de esta manera se define el alcance de la presente política en todas las entidades de la administración pública por lo que se tomara en cuenta para Dirección Regional de Trabajo y Promoción del Empleo, en esos lineamientos se establece el uso obligatorio de la NTP-ISO/IEC 27001:2014

La Dirección Regional de Trabajo y Promoción del Empleo no realiza una administraciòn de riesgos en vinculaciòn con las fuentes de información (depende de una evaluación precisa del riesgo), lo que no permite la disponibilidad, confidencialidad, integridad, trazabilidad y autenticidad de la información, teniendo así información sobre los recursos de grado insuficiente de seguridad, haciéndolo muy vulnerable a ataques informáticos (como malware, ciberataques, etc.) y filtrar mucha información de sujetos dentro o fuera de la organización.

“Las organizaciones con información necesitan estar protegidas contra peligros y amenazas para poder funcionar correctamente. El tipo de información que es relevante para una empresa se conoce como activo de información y puede ser un servicio (proceso comercial de la organización), datos/información (procesada dentro de la organización y, a menudo, el núcleo de una organización), sistemas y otros activos que las soportan, aplicativos(software), hardware informático, redes de comunicación, etc.” (COTERA B. G., 2016)

En la actualidad la Dirección Regional de Trabajo y promoción del Empleo presenta fallas de conexión a la red, no cuenta con normas de seguridad, no tiene lista de activos actualizada y posee vulnerabilidades al descubierto por los trabajadores de la entidad.

Una cultura de mala administración del riesgo de los activos de información mantiene a las agencias como las oficinas regionales de empleo y promoción inconscientes de la verdadera importancia de sus activos de información, lo que les impide identificar las vulnerabilidades pueden ser explotadas por diversas amenazas que podrían afectar la continuidad de los procesos comerciales. Lo mencionado tiene un importante incidencia e impacto en las políticas de seguridad de la información.

A medida que se desarrolle este estudio, se enfocará en brindar información útil a los directores de área de la unidad y demás empleados para saber exactamente qué ambientes son más propicios para una mejor seguridad. La información que permite que el mecanismo de protección seleccionado sea proporcional a un determinado riesgo y valor del elemento a asegurar.

Implementar el método de Magerit v3, a través de la examinación y gestión de riesgos, nos permitirá evaluar la seguridad de nuestros sistemas, identificando un modelo de valor que nos permita estimar el valor de los activos, así como los factores que dependen y tienen en cuenta la seguridad (autenticación, confidencialidad, integridad, disponibilidad, trazabilidad y no repudio), para obtener un mapa de riesgos (lista de amenazas a la divulgación de activos) que muestre si un activo existente está protegido para reducir los riesgos asociados con él, identificando las vulnerabilidades del sistema por donde las amenazas podrían materializarse, una vez teniendo claro este escenario se podrá realizar una adecuada implementación de salvaguardas mediante un plan de seguridad, que servirá para el tratamiento de los riesgos hasta un punto aceptable por la Dirección Regional de Trabajo y Promoción del empleo.

1.2. Formulación del Problema

1.2.1. Problema general:

- "¿En qué medida la implementación de la metodología Magerit V3 y la Norma Técnica Peruana ISO/IEC 27001-2014 **mejorará** de la gestión de riesgos de la seguridad de la información en la Dirección Regional de Trabajo y Promoción del empleo, Huánuco?"

1.2.2. Problemas Específicos:

- "¿De qué forma la identificación y valoración de los activos de información según las **dimensiones de seguridad** ayudan a **mejorar** el conocimiento actual de la información en la DRTPE-Hco 2021?"

- "¿De qué manera la identificación de **amenazas** a los que están expuestos los activos de información permite **estimar** el alcance del daño de la seguridad de la información en la DRTPE-Hco 2021?"

- "¿Permitirá la verificación del nivel de cumplimiento de salvaguardas **reducir** el nivel de **impacto** en los activos informáticos en la DRTPE-Hco 2021?"

- "¿Influye la propuesta de **políticas de seguridad** en la **reducción** del estado de riesgos a los que están expuestos los activos en la DRTPE-Hco 2021?"

1.3. Objetivos

1.3.1. Objetivo General

- “Implementar la metodología Magerit V3 y la Norma Técnica Peruana ISO 27001-2014 para mejorar la gestión de riesgos de la seguridad de la información en la DRTPE-Hco – 2021".

1.3.2. Objetivos Específicos

- “Identificar y valorar los activos de información según las dimensiones de seguridad para **mejorar** el conocimiento actual de la información en la DRTPE-Hco 2021”.

- “Identificar de las amenazas a los que están expuestos los activos de información, para **estimar** el alcance del daño de la seguridad de la información en la DRTPE-Hco 2021”.

- “Verificar el nivel de cumplimiento de las salvaguardas para **reducir** el nivel de **impacto** de los activos informáticos en la DRTPE-Hco 2021”.

- “Proponer de políticas de seguridad para **reducir** el estado de riesgos en las dimensiones de seguridad de información de la información en la DRTPE-Hco – 2021”.

1.4. Hipótesis General y Específicas

1.4.1. Hipótesis general

- H1: “La implementación de la metodología Magerit v3 y la Norma Técnica Peruana ISO 27001-2014 **mejora** la gestión de riesgos de seguridad de la información de la DRTPE-Hco 2021”.

- H0: “La implementación de la metodología Magerit v3 y la Norma Técnica Peruana ISO 27001-2014 **no mejora** la gestión de riesgos de seguridad de la información de la DRTPE-Hco 2021”.

1.4.2. Hipótesis específicas

- “La identificación y valoración de los activos según las dimensiones de seguridad **mejora** el conocimiento actual de la información en la DRTPE-Hco 2021”.

- “La identificación de las amenazas a los que están expuestos los activos de información **permite** estimar el alcance del daño de la seguridad de la información en la DRTPE-Hco 2021”.

- “La verificación del nivel de cumplimiento de las salvaguardas **reduce** el nivel de **impacto** de los activos informáticos en la DRTPE-Hco 2021”.

- “La propuesta de políticas de seguridad **reduce** el estado de riesgos en las dimensiones de seguridad de información de la información en la DRTPE-Hco – 2021”.

1.5. Variables, Dimensiones e Indicadores

Variables:

Variable independiente: Metodología Magerit v3

Variable dependiente: Seguridad de la información

Variable interviniente: Norma Técnica Peruana ISO/IEC 27001:2014

Dimensiones

V1: Mapa de valor, Amenazas, impacto, Riesgos y Salvaguardas

V2:

V2.1: Disponibilidad, Integridad, Confidencialidad, autenticidad y No repudio.

V2.2: Políticas de seguridad

Indicadores

Tabla 1, Indicadores - variable independiente

V1:

Mapa de valor:	Caracterización del valor que representan los activos para la Entidad
Amenazas:	Probabilidad de ocurrencia de la Amenaza
Impacto	Nivel de impacto
Riesgo	Estimación del Riesgo
Salvaguardas	Mecanismos de salvaguarda implantados actualmente
	Nivel de Madurez del paquete de salvaguardas

Fuente: "Elaboración Propia"

Tabla 2, Indicadores – variable dependiente

V2:

V2.1:

Disponibilidad	% Riesgo en la Disponibilidad de los Activos Informáticos
Integridad	% Riesgo en la Integridad de los Activos Informáticos
Confidencialidad	% Riesgo en la Confidencialidad de los Activos Informáticos
Autenticidad	% Riesgo en la Autenticidad de los Activos Informáticos
No repudio	% Riesgo en el No repudio de los activos Informáticos

Fuente: "Elaboración Propia"

V2.2:

Políticas de Seguridad	(no medible)

Fuente: "Elaboración Propia"

1.6. Operacionalización de Variables

Tabla 3, Operacionalización de variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADOR	ESCALA
VI=V1: Metodología Magerit v3	Implementar procedimientos de gestión de riesgos dentro del organismo regulador para tomar decisiones que considere los riesgos que plantea el uso de la tecnología de la información.	Es el nivel de influencia en la toma de decisiones de acuerdo al riesgo de los activos en la DRTPE.	Mapa de valor	% Caracterización del valor que representan los activos para la Entidad	1= Si se evidencia 0 = No se evidencia
			Amenazas	% Probabilidad de ocurrencia de la Amenaza	1 = muy raro 2 = Improbable 3 = Posible 4 = Probable 5 = Prácticamente Segura
			Impacto	% Nivel de Impacto	0 – 1 = Despreciable 2 – 3 = Bajo 4 - 6 = Medio 7 – 8 = Alto 9 - 10 = Muy Alto
			Riesgo	% Estimación de Riesgo	0 – 1 = Controlable 2 – 5 = Aceptable 6 – 16 = Tolerable 17 – 30 = Intolerable 31 – 50 = Extremo
			Salvaguarda	Mecanismos de salvaguarda implantados actualmente Nivel de Madurez del paquete de salvaguardas	1= Si se evidencia 0 = No se evidencia Inexistente – 0 =0% Inicial – 1 = 10% Repetible – 2 = 30% Definido – 3 = 50% Administrado – 4= 75% Optimizado – 5 = 90%

VD=V2: Seguridad de la información	Esto incluye amparar la integridad, disponibilidad y confidencialidad de los sistemas comprendidos en su tratamiento.	Este es el impacto de la mejora de la seguridad del sistema de información en DRTPE.	¿Qué tan efectivas son las políticas de seguridad de información? Disponibilidad Integridad Confidencialidad Autenticidad No repudio	% de reducción de los riesgos en las dimensiones de seguridad de la información % Riesgo en la Autenticidad de los Activos Informáticos % Riesgo en la Integridad de los Activos Informáticos % Riesgo en la Disponibilidad de los Activos Informáticos % Riesgo en la Confidencialidad de los Activos Informáticos % Riesgo en el No Repudio de los Activos Informáticos.	0 – 1 = Controlable 2 – 5 = Aceptable 6 – 16 = Tolerable 17 – 30 = Intolerable 31 – 50 = Extremo
			Políticas de Seguridad	Establecimiento de Políticas	1= Si se evidencia 0 = No se evidencia

Fuente: Elaboración Propia

1.7. Justificación e Importancia

En todo el mundo, las organizaciones privadas y nacionales utilizan las TIC para desarrollar sus operaciones diarias, negocios y más. Esta dependencia se ha incrementado rápidamente debido a las circunstancias especiales que estamos viviendo por la crisis sanitaria provocada por el Covid-19, pero desde entonces son demasiado dependientes de las tecnologías de la información y la comunicación, lo que nos lleva a ciertas amenazas en el ámbito de la seguridad de la información (para mantener la confidencialidad, disponibilidad, integridad) ya que enfrentan muchas amenazas.

Las entidades deben estar preparadas para esto, y muchos autores argumentan que el enfoque para desarrollar una estrategia y hoja de ruta de seguridad de la información es evaluar la vulnerabilidad de la organización a los ataques, por lo que es legítimo por las siguientes razones:

- La Dirección Regional de Trabajo y Promoción del Empleo responsable de funciones específicas de empleo y promoción laboral, actualmente no cuenta con la suficiente gestión de riesgos, lo cual es un activo necesario para definir el nivel de seguridad de la información, por lo que se deben tomar medidas para reducir el riesgo de exposición a las fuentes de información para mejorar la seguridad.

- En esta organización la información manejada y los servicios que se brindan, representan información básica y esencial para la DRTPE, estos se alojan y es operado por hardware de cómputo, redes de comunicación y personas, considerados los activos más valiosos que necesitan ser protegidos y asegurados contra los peligros de ataques y amenazas, por lo tanto, es importante que DRTPE evalúe y actúe sobre sus activos de seguridad.

- La importancia de contar con la Metodología Magerit v3 en la Dirección es para conocer el estado de los activos y salvaguardar los mismos, evitando pérdidas y/o robos de información.

- Las políticas de seguridad ayudan a proteger y dirigir los recursos hacia las finalidades de seguridad de la información, por lo que su disponibilidad en DRTPE es fundamental.

El objetivo de este estudio fue implantar el enfoque Magerit v3 en la Dirección Regional para el Trabajo y el Empleo, permitiendo la gestión de las amenazas actuales a los activos, posibilitando la toma de medidas como controles de seguridad para limitar la información necesaria. El estado de riesgo del recurso, es decir, el establecimiento de medidas de seguridad adecuadas (Política de Seguridad Recomendada basada en la NTP ISO/IEC 27001:2014), se desarrolla de manera similar a esta tesis tiene una justificación económica, porque se pretende ayudar de cierta manera a la entidad mediante el establecimiento de un Plan de Mitigación (Además de charlas en el tema) de riesgos, orientadas a mejorar la realidad existente en la entidad.

1.8. Limitaciones

- El tiempo es un factor limitante debido a que la información a recolectar para el desarrollo del proyecto se encuentra limitada, ya que no cuentan con un área de informática en la dirección. Por tanto, nunca se hizo un trabajo similar anteriormente.

- El personal de la DRTPE desconoce de las normas de uso de información y de las tecnologías que ayudan a perfeccionar la seguridad de la información, por lo que hace que la manipulación de ésta sea irregular, haciéndolo vulnerable.

- La recolección de datos parala ejecución de Políticas de Seguridad y Salvaguardas es conlleva restricciones debido a la emergencia sanitaria en la que nos encontramos en la actualidad.

- En la actualidad parte de la información que se maneja en la Dirección es manipulada desde los hogares del personal, ya que no pueden trabajar de manera presencial en la Dirección.

- La Dirección no cuenta con una lista de los activos tanto tangibles como intangibles que disponen en la misma.

- En gran mayoría los trabajadores dentro de la DRTPE son personas mayores y se les hace difícil tomar en cuenta normas y reglas para el bienestar de los activos, de la misma manera el acceso a la información es complicada debido al poco interés del personal de la DRTPE.

II. MARCO TEÓRICO

2.1. Revisión de estudios realizados

2.1.1. Antecedentes Internacionales

(González, 2018), En su trabajo de fin de grado “Análisis de recursos de información en un sistema de información de misión basado en metodología Magerit v3 y norma ISO 27001:2013”, el objetivo de la investigación es ”Examinar los recursos de información para identificar y gestionar unidades estudio de caso de los riesgos que pueden presentarse en el sistema de información de misión ", para la aplicación del método Magerit v3 y la norma ISO 27001:2014, encontraron que, los esquemas de manejo de información en el caso de estudio presentaban falencias y estaban expuestas a amenazas, y por consiguiente el riesgo de los activos era alto, siendo el más crítico la Base de datos de la institución , las conclusiones a que llega es:

- Como parte final del análisis de riesgoss, se prpresesenta elel informe de resultados para que la entidad pueda desarrollar un plan de tratamiento de riesgoss y,, enn base a ello,llo, desasarrrolllar políticas, mecanismoss o procedimiencedimientoss para proteger la integridad, integridad, confidencialidad, integridad, disponibilidad y autenticidad del estudio de ccaso.so.
- De igual manera, se proporciona una matriz en la que se detectan riesgos, ameidentificando la situación de seguridad de los recursos escaneados y algunas recomendaciones de seguridad para corregir vulnerabilidades.

De la investigación se resalta la importancia de que las instituciones cuenten con una matriz de riesgos, de forma actualizada para de esta forma plantear o proponer un plan de tratamiento de riesgos para garantizar la seguridad de la información es gestionado por la institución.

(Guamán, 2019), En su proyecto de tesis,” Aplicación de la Evaluación de la Seguridad de la Información en el Sistema de Evaluación de Docentes de la Universidad Tecnológica del Norte”, su objetivo fue” Evaluar el Sistema de Evaluación de la Seguridad de la Información del Sistema de Evaluación de Docentes de la Universidad Tecnológica del Norte, de acuerdo con ISO 27002:2017 y el enfoque Magerit v3 "muestra que la organización cuenta con salvaguardas, pero estas medidas están desactualizadas y no están ampliamente disponibles entre los docentes que las utilizan. Emplean un sistema de puntuación, lo que lleva a varias deficiencias de seguridad de la información que los estudiosos señalaron de manera similar a verificar que la matriz de riesgo de activos de información de una entidad está desactualizada,

cabe aclarar que el autor lo constata mediante encuestas a los usuarios finales, las conclusiones a la que llega son:

• La metodología utilizada para este estudio es MAGERIT, que permite analizar en profundidad los riesgos, valorando cada activo a través de los 5 aspectos de seguridad como: confidencialidad, disponibilidad, integridad, trazabilidad y autenticidad.

• ISO 27002:2017 jugó un papel clave en este estudio, ayudando a verificar el cumplimiento de los controles de seguridad de la información en el Sistema de Evaluación de Enseñanza de la Universidad Tecnológica del Norte.

El estudio destaca la importancia de las organizaciones en general en la planificación de una formación adecuada sobre los controles de seguridad a su disposición para que los sujetos no alteren la confidencialidad, e integridad. Disponibilidad de datas en los sistemas informáticos y actualización periódica de las políticas de seguridad de la información y los procedimientos.

2.1.2 Antecedentes nacionales

(Carlos Barrantes P., 2012), En su trabajo de Investigación “Diseñar e implementar un sistema de gestión de seguridad de la información en los procesos técnicos” para “reducir y minimizar los riesgos a los activos de información de los procesos bajo la dirección técnica de Card Perú S.A. Las amenazas a los recursos, servicios y continuidad de los procesos de ingeniería”, se llegó a las siguientes conclusiones:

● Implementación de una política de privacidad, comunicar y acordar a los empleados sobre ello, lo cual es útil cuando se desea implementar un sistema de gestión en su organización, ya que les brinda una comprensión clara de cómo se realiza su trabajo diario. Su día a día puede ayudar a mantener y mejorar la gestión de la empresa, de acuerdo, a un sistema de gestión.
● Inclusive con un buen sistema de gestión de seguridad de la información, en el futuro habrá más recursos de información, más amenazas de seguridad, con más riesgos. Esta situación es inevitable y por lo tanto se concluye que es necesario estar preparado para acciones inmediatas ante nuevas vulnerabilidades descubiertas.
● El componente humano es necesario para la implementación de cualquier sistema de gestión organizacional, por lo que la capacitación y el conocimiento de este sistema es crucial para una implementación exitosa.

(CHUMAN, 2015), En el trabajo “Aplicación del método Magerit para el análisis y gestión de riesgos en el servidor del Sistema de Gestión Académica de la Universidad Nacional Pedro Ruiz Gallo”, el objetivo del proyecto es presentar un plan de reducción de riesgos basado en las medidas de seguridad desplegadas, utilizando el Magerit v3, el Análisis de Riesgos y el Enfoque de

Gestión de Tecnologías de la Información, que consta de dos procesos con la siguiente estructura:
Métodos de análisis de riesgo (identificar, depender y evaluar activos; identificar y evaluar amenazas; identificar y evaluar seguridad existente; estimar impactos y riesgos). El Proceso de Gestión de Riesgos (Plan de Decisión y Mitigación), que “identifica amenazas en los servidores del Sistema de Gestión Académica de la Universidad Nacional Pedro Ruiz Gallo, aplica el enfoque MAGERIT para el análisis y gestión de riesgos”, recomendando medidas para controlar estas amenazas; sacando las siguientes conclusiones:

- Los servidores del Sistema de Gestión Académica cuentan con medidas de seguridad, pero no están instruidos, no documentados y subutilizados, por lo que esta investigación sería beneficiosa para mitigar o eliminar el riesgo.
- Debido al uso del método Magerit y el motor Pilar, se encuentra que el servidor está en riesgo de amenazas graves, tales como: falla del sistema por agotamiento de recursos, falla física o lógica, corte de energía, temperatura o humedad inadecuada condiciones, robo del dispositivo, pérdida del dispositivo, error del administrador del sistema / seguridad, desastre natural, independientemente de las medidas tomadas por la gerencia de la gerencia del sector de telecomunicaciones aplicable. Esto apoya el problema expuesto y la importancia del desarrollo del tema. El servidor habilita la funcionalidad y creación de servicios de gestión del aprendizaje.
- Las consideraciones de seguridad se tienen en cuenta al desarrollar planes de mitigación, y la importancia de la seguridad de los servidores y los recursos para los sistemas de gestión académica es un tema de investigación importante.

De este estudio podemos concluir que la aplicación de la metodología Magerit v3 ayuda a obtener una matriz de riesgos actualizada que ayuda a establecer controles para mejorar la seguridad de los activos a través de una adecuada gestión de riesgos.

(**Ramiro, 2020**), en el trabajo “Impacto del Método Magerit v3 en la seguridad de la información en Deco Interiors SAC”, el objetivo fue “Establecer el impacto del método Magerit V3 en la seguridad de la información”, se extrajeron las siguientes conclusiones:

- Hay una correlación lineal positiva significativa del 78 % entre la metodología Magerit V3 y la seguridad de la información, con una significación inferior a 0,05 establecida en el estudio, con un impacto del 70,6 % del tratado del método Magerit V3 sobre seguridad de la información

  ● La entidad Deco Interiors SAC introdujo medidas de seguridad en las primeras etapas, las cuales fueron implementadas según el criterio de cada personal de TI, resultando que estas medidas no estén

debidamente documentadas y guiadas, por lo que no se aplican correctamente.

● Se constata la falta de formación del personal de Deco Interiors SAC, en seguridad y protección de la información.

● El método MAGERIT es útil en el análisis de riesgos, empezamos por caracterizar el activo, caracterización de amenazas, caracterización de protecciones existentes y nos ayuda a implementar salvaguardas en el futuro para controlar y reducir los riesgos encontrados.

● Entendemos la necesidad de implementar planes de gestión y tratamiento de riesgos para mitigar los riesgos y desarrollar estrategias para mitigar las vulnerabilidades y amenazas a los activos de información.

Lo más resaltante en esta investigación es la correlación entre las variables que son la Metodología Magerit V3 y la Seguridad de la información, que va directamente relacionada al proyecto que estamos trabajando.

2.1.3. Antecedentes Regionales

(Bach. Pedro PAJUELO GODOY, 2019), en la tesis “Método Magerit v3 y su impacto en la seguridad de la información del distrito de Pillco marzo 2019”, el propósito principal es determinar la frecuencia de uso del método Magerit V3 en la seguridad de la información del distrito de Pillco marzo 2019. Se extraen las siguientes conclusiones generales:

- En cuanto a la meta general: “Determinar el índice de uso del método Magerit V3 en seguridad comunitaria en el distrito y comuna de Pillco Marca en el año 2019”, el índice de uso del método Magerit V3 en seguridad comunitaria, al verificar supuestos generales, según prueba de Wilcoxon , es significativo con un valor característico de: 0.00 < 0.05, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, es decir, el método Magerit V3 tiene un impacto significativo en la seguridad de la información del Distrito Pillco Marca, y el nivel de confianza fue del 95%.

Los siguientes estudios refuerzan nuestro tema de investigación al mostrar el impacto del enfoque de Magerit en la seguridad de la información.

Enzo Crespo Revilla. (2010) En su indagación "Diagnóstico del estado de la seguridad e implementación de las recomendaciones gubernamentales de política de seguridad de la información en la región de Huánuco", el objetivo fue "Evaluar el estado actual y el rendimiento de los sistemas informáticos y la seguridad de las redes de comunicación para establecer los controles

necesarios para garantizar la confiabilidad de la información y un alto nivel de seguridad", y menciona las siguientes conclusiones:

- Se logró la elaboración de la propuesta de las políticas de seguridad de la información.
- Se logró determinar el incumplimiento y la no existencia de destino objetivos de control e hitos de control que sugiere la norma COBIT 4.1 y se elaboraron sus respectivas recomendaciones.
- Tener una política de privacidad es transcendental, pero debemos comprender cuán importante es que se convierta en parte de nuestro entorno de trabajo diario. La comunicación con los usuarios del sistema es clave para crear políticas efectivas y crear una "cultura de seguridad".
- Se logró determinar los activos que son más susceptibles a amenazas y cuáles son las medidas de seguridad que se debe considerar para aminorar sus vulnerabilidades.

En el proyecto de proyección social **"Propuesta de Políticas de seguridad de la información para la subgerencia de Desarrollo Institucional y Sistemas del Gobierno Regional Huánuco mediante la aplicación de MAGERIT**" realizado por los alumnos Carrión Ventura, Alfredo; Falcón Ascencio, Lorenzo Abel; Huayanay Casimiro, Linn Kerry; Timoteo Cori, Juan Antonio; Tucto Calzada, Jerson Wilmer; en este proyecto el Gobierno Regional de Huánuco no cuenta con sistemas de seguridad de la información para administrar vulnerabilidades, riesgos y amenazas donde la información normalmente estaría expuesta en cualquier proceso interno y se tenía como objetivos considerar todos los riesgos de los activos identificados a través de MAGERIT en la Sub Gerencia de Desarrollo Institucional y Sistemas del Gobierno Regional Huánuco, determinar la estructura para el planteamiento de políticas de seguridad de la Sub Gerencia de Desarrollo Institucional y Sistemas del Gobierno Regional Huánuco, clasificar de la normativa referente lo referente a la administración de la seguridad de la información de la Sub Gerencia de Desarrollo Institucional y Sistemas del Gobierno Regional Huánuco.

(ARGÜEZO RAMIREZ, 2019), En su trabajo de suficiencia profesional, "Propuesta de Sistema de Gestión de Seguridad de la Información para proteger los recursos en el sector de información de la provincia de Huánuco basado en la norma ISO 27001", tiene como principal objetivo "Proponer un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO 27001 para la protección de los activos de información", de acuerdo al autor para la identificación y evaluación de riesgos de seguridad se usó la metodología Magerit v3, para que luego se definan los controles necesarios de acuerdo a la norma ISO 27001, las conclusiones a la que llega es:

• Las políticas de seguridad desarrolladas son muy útiles, para proteger los activos de información, y los colaboradores deben tener el conocimiento para administrar y utilizar bien los activos.

• Durante una investigación se puede identificar y evaluar el riesgo al que están expuestos los activos de información, mediante lo cual se establece una matriz de amenaza de activos, con base en la probabilidad de ocurrencia de cada activo.

2.2. Leyes fundamentales, Principios, Definiciones y Conceptos fundamentales

A continuación, se detalla conceptos básicos sobre la Metodología Magerit v3, que es necesaria para el análisis y gestión de riesgos, así como también conceptos sobre Seguridad de la Información, así como sus correspondientes dimensiones.

2.2.1. Metodologías para análisis y gestión de riesgos

Existen varias metodologías en el medio para la gestión de riesgos, entre ellas se tiene COBIT, ITIL y MAGERIT; en sus diferentes versiones que ofrecen apoyo, orientación y monitoreo para el seguimiento de las actividades relacionadas a los sistemas de información.

A continuación, se hará una breve diferencia:

Metodologías	COBIT	ITIL	MARGERIT	ISO 31000
Descripción	"Son un conjunto de herramientas orientadas a garantizar el control y seguimiento de gobernabilidad de Sistemas de Información a largo plazo a través de auditorías. CO, compila mejores prácticas levantadas por expertos en TI provenientes de diversos sectores como industria y servicios." (gbadvisors, 2018)	Es una colección de mejores prácticas para la administración efectiva de los Sistemas de Información.	Se trata de un método de análisis de sistemas de información y gestión de riesgos desarrollado por el Consejo Superior de Administración Electrónica (CSAE)	Los riesgos son diversos y complejos, por lo que esta Norma Internacional, desarrollada por ISO (international Organization for Standardization), no está destinada a un sistema de gestión específico, sino que proporciona una guía sobre las buenas prácticas en la acción de gestión de riesgos.
Funciones	Mapeo de procesos IT	Mapeo de la gestión del nivel de servicio de IT	Examinar la impresión de una brecha de seguridad en la empresa	Creación y protección de valor de los activos.
Objetivos	Comparte las mejores prácticas entre dominios y procesos, y presenta las actividades de manera manejable y optimizada.	Proporcione a los administradores de TI las mejores herramientas y documentación para ayudarlos a mejorar la calidad de sus servicios	Sensibilizar a los responsables de los sistemas de información sobre las amenazas y la necesidad de combatirlas.	Integre sus procedimientos de gestión de riesgos.

¿Para qué se Implementa?	Control del sistema informatico	Gestión de niveles de servicio.	Implantar las medidas de control más adecuadas para reducir el riesgo.	Estandarizar normas que regularicen la seguridad.
Negativa	Requiere un tiempo prudencial para adaptarlos. Pronuncia el abismo entre gerencia y operaciones.	Puede fomentar la burocracia y entorpecer los objetivos	Haciendo uso de la V1 y V2, el tiempo y disponibilidad de los activos hace complicada su implementación y adaptación	Solo son estándares

Tabla 4, Comparativa, de las Metodologías,

Fuente: Elaboración Propia

Los cuatro métodos están diseñados para garantizar la seguridad de la información, pero Magerit proporciona un proceso sistemático de análisis y gestión de riesgos.

El método también describe varias técnicas comúnmente empleadas en el análisis de riesgos. Incluye ejemplos de análisis tabular, algoritmos, árboles de ataque, análisis de costo-beneficio, técnicas de gráficos y mejores prácticas para realizar sesiones de análisis de riesgos.

En cuanto a DRTPE, al no tener un método de gestión de riesgos, es la mejor opción, ya que le permite enfocarse en los riesgos que pueden causar un mayor daño a la entidad, es decir, los riesgos asociados con el sistema de TI.

2.2.2. Metodología MAGERIT V3.0

MAGERIT es un método de gestión de sistemas de información y análisis de riesgos desarrollado por el Consejo Superior de Gestión Electrónica (CSAE) del Ministerio de Hacienda y Administraciones Públicas del Gobierno de España para implementar su mandato en dar respuesta a la creciente dependencia de los ciudadanos de los servicios públicos administraciones y tecnologías de la información.

MAGERIT, cuando se habla de esta metodología se suele pensar siempre en tecnologías de información, ya tiene que ver directamente con el proceso en este tema, si bien esto tiene beneficios obvios para el público, es importante saber que también tiene riesgos que deben mitigarse mediante medidas de seguridad que faciliten el acceso a la información.
MAGERIT, metodología conocida por las entidades tanto públicas como privadas, tanto las que trabajen con información digital como los que no; si esta información o los servicios que brinda tienen valor, MAGERIT les notificará el valor en riesgo y los ayudará a proteger esa información. Comprender los riesgos de sus elementos de trabajo es fundamental para su capacidad de gestionarlos. Gracias a MAGERIT, la información puede analizarse y procesarse de forma metódica, sin dejar lugar a la espontaneidad ni a la dependencia del criterio del analista.
En la terminología de la norma ISO 31000, MAGERIT cumple con el llamado "Proceso de Gestión de Riesgos" capítulo 4.4 ("Implementación de la Gestión de Riesgos") en el Marco de Gestión de Riesgos. En otras palabras, MAGERIT implementa procesos de gestión de riesgos en cualquier entidad y sus procesos para asistirlos en la toma de decisiones que tengan en cuenta los riesgos que presenta el uso de la información causada.

Ilustración 1. ISO 31000 - Marco de trabajo para la gestión de riesgos

Gráfico 1, Marco de trabajo para la gestión de riesgo

Fuente: (Escuela Nacional de Seguridad, 2012)

2.2.2.1. MAGERIT permite:

Investigar los riesgos que conlleva un sistema de información y su entorno asociado. MAGERIT indica realizar un análisis de riesgos que incluya evaluar el impacto de un hito de seguridad en la organización o entidad; señalar las amenazas existentes, identificar las amenazas a los sistemas de información y determinar la vulnerabilidad de los sistemas para combatir estas amenazas y obtener resultados.

Al realizar la evaluación del Magerit, los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas adecuadas que se deben poner en marcha para conocer, bloquear, prevenir, reducir o controlar los riesgos identificados y así reducir su potencial, sus posibles efectos o daños.

Es importante de evaluación realizar una identificación y evaluación de los activos que se encuentran y son parte de una organización, esto nos ayudará a posteriormente valorar cada activo.

El desarrollo de la metodología ayuda a clasificar los activos identificados en las dimensiones de seguridad detalladas por MAGERIT y los reune según una consideración principal de jerarquía organizativa y según otras posibles consideraciones:

- Subastados de seguridad (Autenticación, Confidencialidad, Integridad, Disponibilidad, referenciados brevemente cómo A-C-I-D-No repudio).
- Amenazas posibles.
- Salvaguardas de protección.

La operación reúne activos articulando en grupos detallados por el objetivo común de realizar un tipo de función determinada (lo cual es una parte esencial para el desarrollo). La agrupación más indicada para el Analisis de Riesgo son 5 capas o niveles para una mejor articulación de los activos son los siguientes:

1. Entorno
2. Sistema de información
3. Información
4. Funcionalidades de la Organización
5. Otros activos

2.2.2.2. Fases de la Metodología Magerit v3

La metodología Magerit, proporciona un proceso sistemático, el cual se inicia desde:

- **Identificación de activos informáticos:** Realizar un Test de conteo e identificación de los activos informáticos existentes.
- **Catálogos de amenazas:** En este punto las amenazas ya vienen descritas y estas amenazas están agrupadas según el origen industrial, errores, fallos, problemas y ataques intencionados y no intencionados.
- **Caracterización:** En este paso lo que se deberá de realizar es una categorización de las amenazar para conocer los niveles que tenga cada uno sobre los activos identificados anteriormente, y de esta manera conocer el daño que puedan ocasionar.

Las dimensiones son valoradas por cada amenaza que contiene dichos activos.

- **Impacto:** Para obtener el impacto de cada dimensión y para cada activo de TI, se realiza una operación que deriva de los valores de dimensión que se realizó la operación al definir el activo con los valores de dimensión disponibles en la descripción de caracterización.
- **Mapa de riesgos:** Lista de las amenazas a que están expuestos los activos de TI.
- **Salvaguardas:** En esta etapa las salvaguardas están equipadas en tipos de protección para lograr efectividad.

La metodología se compone de cuatro fases:

1. Planificación de proyectos de riesgo; proporciona las primeras estimaciones de los riesgos que pueden afectar a los sistemas de información.

2. Análisis de riesgos; Durante esta etapa se estima el impacto que tendrán los riesgos en la organización.

El análisis de riesgo considera lo siguiente:

Activos, que son elementos del sistema de información (o estrechamente vinculados a los sistemas de información) que apoyan la misión de la organización

Amenazas, son las situaciones en las que los activos pueden causar daño a la organización

3. gestión de riesgo: de tal manera que se determinen las posibles soluciones para cada riesgo.

Mecanismos de protección (o contra medidas / salvaguardas), que son medidas de protección desplegadas para que aquellas amenazas no causen daño.

Selección de mecanismos de protección; se eligen los mecanismos que implementarán las soluciones de la fase anterior.

2.2.2.3. Objetivos del Magerit:

Directos:

1. Sensibilizar a los responsables de la organización de la información sobre la existencia de riesgos y la necesidad de controlarlos.

2. proponer un método de análisis sistemático de los riesgos asociados al uso de las tecnologías de la información y la comunicación (TIC).

3. ayudar a detectar y planificar el tratamiento a tiempo para controlar los riesgos.

Indirectos:

1. preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

2.2.2.4. Clases de Riesgo

Los riesgos deben de estar en un nivel anteriormente identificado como considerable, y para que ello sea estable se describen niveles o tipos de riesgos los cuales ayudará a la entidad para la toma de decisiones. se definen las siguientes clases de riesgo:

- **Riesgo calculado:** es un riesgo estable y/o aceptable que está determinado por la política de seguridad de la entidad.

- **Riesgo residual:** es cuando el riesgo es menor al riesgo calculado, lo cual indica que la toma de decisiones fue efectiva.

- **Riesgo asumido:** es cuando el riesgo es mayor al calculado, por lo cual se debe de hacer llegar el informe correspondiente a la directiva para una toma de decisiones que implica una mejora en el riesgo de dicha información.

"Es importante en toda organización realizar análisis y gestión de riesgos, lo que les permite conocer el estado de su red, las vulnerabilidades y riesgos que enfrenta la organización. Y debido a que la organización tiene claro los riesgos a los que se enfrenta, podrá establecer políticas que le permitan tomar medidas preventivas y correctivas para garantizar el más alto nivel de seguridad". (CHÁVEZ, 2019)

Cuando el impacto es severo siempre se maximiza el riesgo, a la inversa, si el impacto es Bajo o Muy bajo, se toma en cuenta el riesgo donde los valores más bajos de vulnerabilidad son mínimos o incluso inexistentes. - existe. Siguiendo las recomendaciones de MAGERIT, encontramos que la magnitud del impacto influyó en la evaluación final del riesgo más que la vulnerabilidad.

		Vulnerabilidad						
		Muy Baja	Baja	Media-Baja	Media	Media-Alta	Alta	Muy Alta
Impacto	Muy Bajo	-	-	-	Mínimo	Mínimo	Mínimo	Mínimo
	Bajo	-	Mínimo	Bajo	Bajo	Bajo	Medio	Medio
	Medio	Mínimo	Bajo	Medio	Medio	Medio	Alto	Alto
	Alto	Medio	Medio	Medio	Alto	Alto	Alto	Alto
	Muy Alto	Alto	Alto	Alto	Muy Alto	Muy Alto	Máximo	Máximo
	Crítico	Máximo	Máximo	Máximo	Máximo	Máximo	Máximo	Máximo

Gráfico 2: Impacto vs Vulnerabilidad

Fuente: (Firma-e, 2013)

2.2.3. Análisis y Gestión de Riesgos

El análisis y la gestión de riesgos ayudan a verificar la seguridad existente en la organización, identificar las causas de las vulnerabilidades y recomendar soluciones de control para mitigarlas.

Se trata de un proceso sistemático que propone actividades clave para proteger la información y los sistemas que la manejan. Le permite seleccionar y configurar las medidas de seguridad adecuadas que controlarán o eliminarán los riesgos identificados en los sistemas de TI.

Se debe verificar la efectividad de las medidas o soluciones resultantes después de los riesgos a los que pueden estar expuestos los activos de información, además, se debe realizar un seguimiento de los riesgos periódicamente para poder ser controlados con precisión.

En general y simplificando desde Margerit, las fases del análisis de riesgos se pueden resumir en:

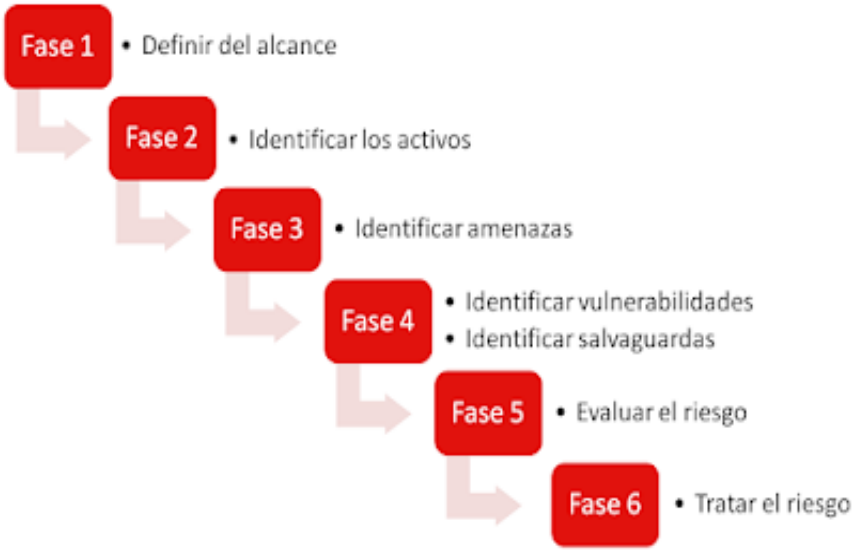


Gráfico 3, Análisis y Gestión de Riesgos.

***Fuente**: (SB, 2017)*

La gestión de riesgos se puede clasificar en las siguientes fases:

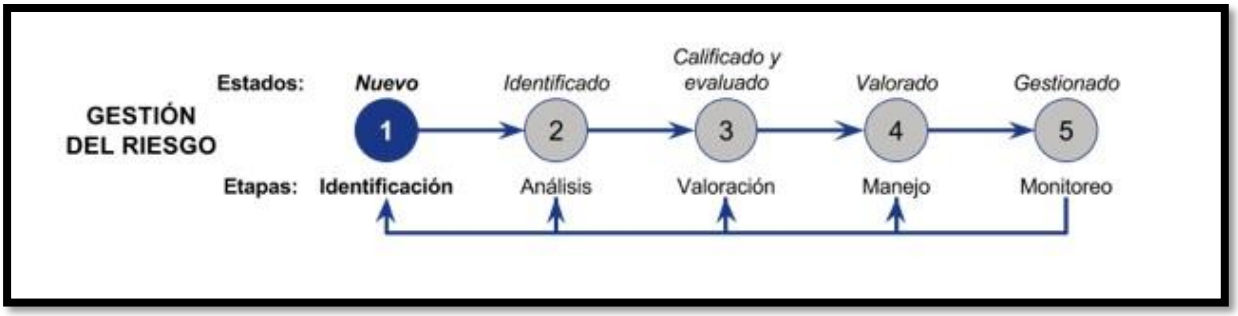


Gráfico 4, Fases de la Gestión de riesgos

Fuente: (Hernandez, 2018)

Fase 1: DEFINIR EL ALCANCE: Se debe realizar un análisis de la entidad o empresa a la que se aplicará la metodología, para ver en qué medida se puede mejorar la metodología y cómo se implementará.

Fase 2: IDENTIFICAR LOS ACTIVOS: Se debe realizar un conteo de los activos físicos y la identificación de los activos intangibles debe hacerse con cuidado, teniendo en cuenta su importancia y los riesgos a los que pueden estar expuestos en función del uso que se les dé.

Fase 3: IDENTIFICACIÓN DE AMENAZAS: Durante esta fase, necesitamos realizar análisis para identificar amenazas a la seguridad de la información.

Fase 4: IDENTIFICACIÓN DE VULNERABILIDADES Y SALVAGURADAS: Desarrollar la identificación de vulnerabilidades potenciales en los servicios de información existentes, además de identificar vulnerabilidades potenciales, ayuda a controlar las vulnerabilidades potenciales.

Fase 5: EVALUAR EL RIESGO: Una vez identificadas las amenazas y vulnerabilidades a la seguridad, es necesario evaluar el riesgo que representan, clasificando el riesgo por impacto para que se pueda prevenir por importancia.

Fase 6: TRATAR EL RIESGO: debemos implementar salvaguardas y controles para reducir el riesgo.

Magerit permite desarrollar la evaluación de riesgos a través de:

Identificación de riesgos: Documenta los activos, las relaciones entre ellos, la valoración de la entidad en estudio, identifica amenazas y evalúa riesgos. El conocimiento proviene del entorno del sistema, los informes y los documentos están disponibles en DRTPE, la disponibilidad de datos se ilustra mejor mediante la representación en información cuantitativa.
Recolección de datos, para análisis cualitativo, incluyendo la identificación de situaciones en las que los activos están en riesgo, así como sus costos, para representarlos en medidas aproximadas. Los datos que se tienen en cuenta para la evaluación son la confidencialidad, la integridad, la disponibilidad, la autenticidad y el no repudio.
Análisis de riesgos: Según (Ramiro, 2020), lo define como: “Calcula impacto y riesgo,valores posibles, y demás. Cuantificación y calidad, acumulación y sesgo. Realizar análisis de riesgo fundamental. La definición de riesgo se basa en tres parámetros: escenario de amenaza, probabilidad y consistencia (multidimensional, a menudo medible mediante escalas de categorías).”, Nos permite identificar los riesgos que tiene la organización y estimar el impacto probable, en caso de que el riesgo se materialice.

El gráfico siguiente muestra el proceso de la Metodología Magerit y los elementos del análisis de riesgos potenciales:

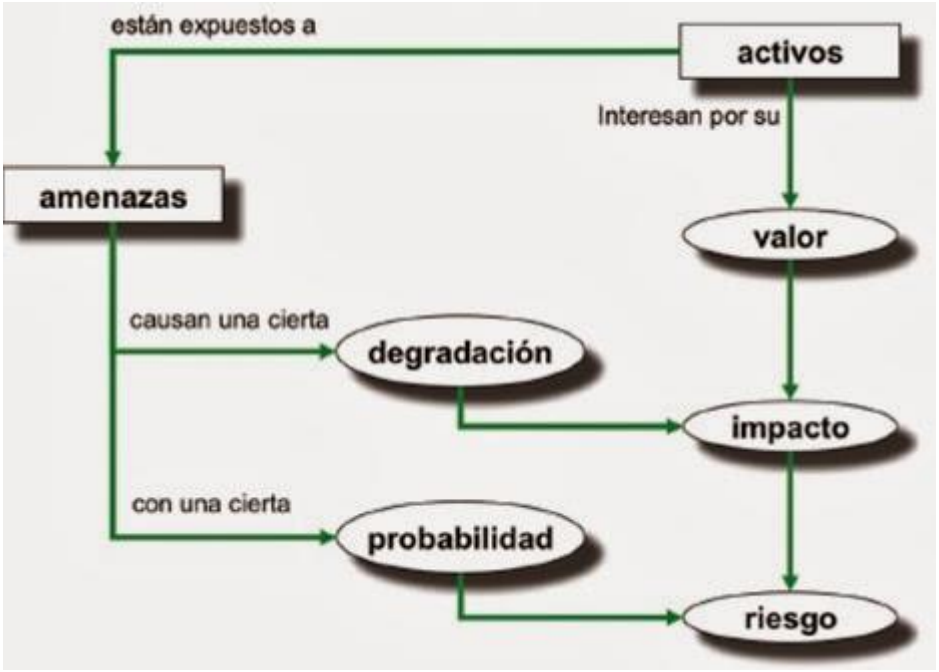


Gráfico 5, proceso de la Metodología Magerit y los elementos del análisis de riesgos potenciales,

***Fuente**:* (TecnoBlog, 2014)

Evaluación del riesgo: Según (Ramiro, 2020), lo define como “Priorizar los resultados y presentarlos a los administradores para la evaluación del desempeño. El método básico de análisis de riesgos se basa en el desarrollo de escenarios (de hecho, "basados en los hechos") y en la evaluación de las consecuencias y probabilidades (frecuencia) asociadas con los guiones. Las escalas de consecuencia a menudo se clasifican.

En resumen, el método Magerit ayuda a identificar, analizar y evaluar las alternativas ofrecidas según el grado de reducción alcanzado (o riesgo residual). El riesgo se establece en base a las vulnerabilidades identificadas, asociadas con la probabilidad, las amenazas reveladas, así como el impacto negativo que ocasiona en las operaciones comerciales.

Según (Ramiro, 2020), “Los resultados del análisis de riesgo brindan valores de modelo de las dependencias entre diferentes componentes y el número de amenazas a las que están expuestos esos elementos”, como evaluar la efectividad de las medidas existentes. Finalmente, clasifica sus métricas de riesgo. Plan de seguridad El número total de programas de seguridad que toman decisiones de gestión de riesgos.

Según (katerina, 2016), “El método Magerit es una metodología general que permite el análisis cualitativo y cuantitativo. La evaluación de impacto se basa

en activos críticos, la evaluación de riesgos tiene en cuenta la probabilidad, la vulnerabilidad (activo crítico) y el impacto (amenaza, activo) "

Gestión de Riesgos: Este método de gestión se caracteriza por ser una norma existente para manejar diversos riesgos no especulativos, los cuales simbolizan esos riesgos de los cuales se desprende una pérdida para la empresa Igualmente, la gestión de riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo, tenemos a los siguientes parámetros a continuación:

a. **Análisis del Riesgo:** Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo (CAMPOS, 2019)

b. **Clasificación:** Determina si los riesgos encontrados y los riesgos restantes son aceptables. (CAMPOS, 2019)

c. **Reducción:** Define e implementa las medidas de protección. Además, sensibiliza y capacita los usuarios conforme a las medidas. (CAMPOS, 2019)

d. **Control:** Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sancionar el incumplimiento. (CAMPOS, 2019)

Para desarrollar una buena gestión de riesgos, es fundamental tener en cuenta tanto la cultura y estructura de la organización, la misión y los objetivos comerciales establecidos, la definición de los procesos organizativos y el conocimiento de los buenos ejecutivos. práctica. generalmente aceptado, que no sean empleados de la misma organización.

En todo el mundo, tanto las organizaciones públicas como las privadas dependen de las TIC para desarrollar sus operaciones diarias, operaciones comerciales, etc. Pero la dependencia excesiva de la tecnología nos expone a ciertos riesgos que, como organización, debemos estar preparados para proteger su activo más valioso, que es la información, que se considera importante. Es fundamental cómo lograr eso, primero realizando un análisis de riesgo que nos permite ver el estado de los activos que tiene la organización, y luego idear la gestión de esos riesgos, pues nos permite reducir la intensidad del riesgo a niveles aceptables para la organización, todo en el marco de la seguridad de la información

2.2.4. NTP-ISO/IEC 17799

En nuestra revisión bibliográfica, encontramos que la norma técnica peruana NTPISO / IEC 17799 brinda todas las recomendaciones necesarias para poder administrar un sistema de seguridad de la información (ISS), así como la norma internacional ISO 27001, establece los requisitos necesarios para tomar encargado del área específica que puede iniciar, implementar, mantener y mejorar la seguridad en las organizaciones.

Según (Excellence, 2015), “la norma técnica peruana ISO / IEC 17799 es una guía práctica destinada a desarrollar estándares de seguridad organizacional y crear prácticas efectivas en la gestión de la seguridad de la información. Además, aumenta la confianza a la hora de establecer relaciones entre diferentes organizaciones. "

Entonces se puede inferir que esta Norma Internacional proporciona una base común para establecer estándares de seguridad de la información en organizaciones, tanto públicas como privadas, logrando así prácticas efectivas de gestión de la seguridad. Todas las recomendaciones en el mismo deberán ser utilizadas de acuerdo con la ley que las prescribe como instituciones, y tomando en cuenta el caso particular del desarrollo del proyecto de tesis, se llevará a cabo en una institución pública que determine el estado del Perú. directriz de política de ciberseguridad con el objetivo principal de "Proteger la infraestructura de TI, los datos y la información del estado, y la tecnología utilizada para manejarlos, contra amenazas internas o externas" externa, intencional o accidentalmente, para asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información (Digital, 2017), se debe implementar una adecuada gestión de riesgos en varios aspectos de la seguridad de la información.

La información es el activo más valioso para las organizaciones, debe estar completamente protegida, cada organización debe garantizar un nivel adecuado de seguridad de la información que maneja, hoy la información está mucho más expuesta, más que nunca debido al creciente número de amenazas en Internet, lo que puede dar lugar a agujeros de seguridad más importantes.

De acuerdo a (Excellence, 2015), “La información se transmite de muchas formas diferentes. Se puede encontrar en papel, almacenado electrónicamente, enviado por correo electrónico, en formato de video o mediante una conversación oral personal. Por todo ello, la información debe estar debidamente protegida, independientemente del formato en el que no se encuentre la información. Un sistema de seguridad de la información (ISS) ayuda a proteger la información contra una amplia gama de amenazas para garantizar la continuidad del negocio, reducir los daños incurridos dentro de la organización y maximizar el retorno de la inversión, las inversiones y las oportunidades comerciales. "

De acuerdo con NTPISO / IEC 27005, el proceso de gestión de riesgos de seguridad de la información incluye establecer el contexto, evaluar el riesgo, abordar el riesgo, aceptar el riesgo, comunicar el riesgo y monitorear y revisar el riesgo.

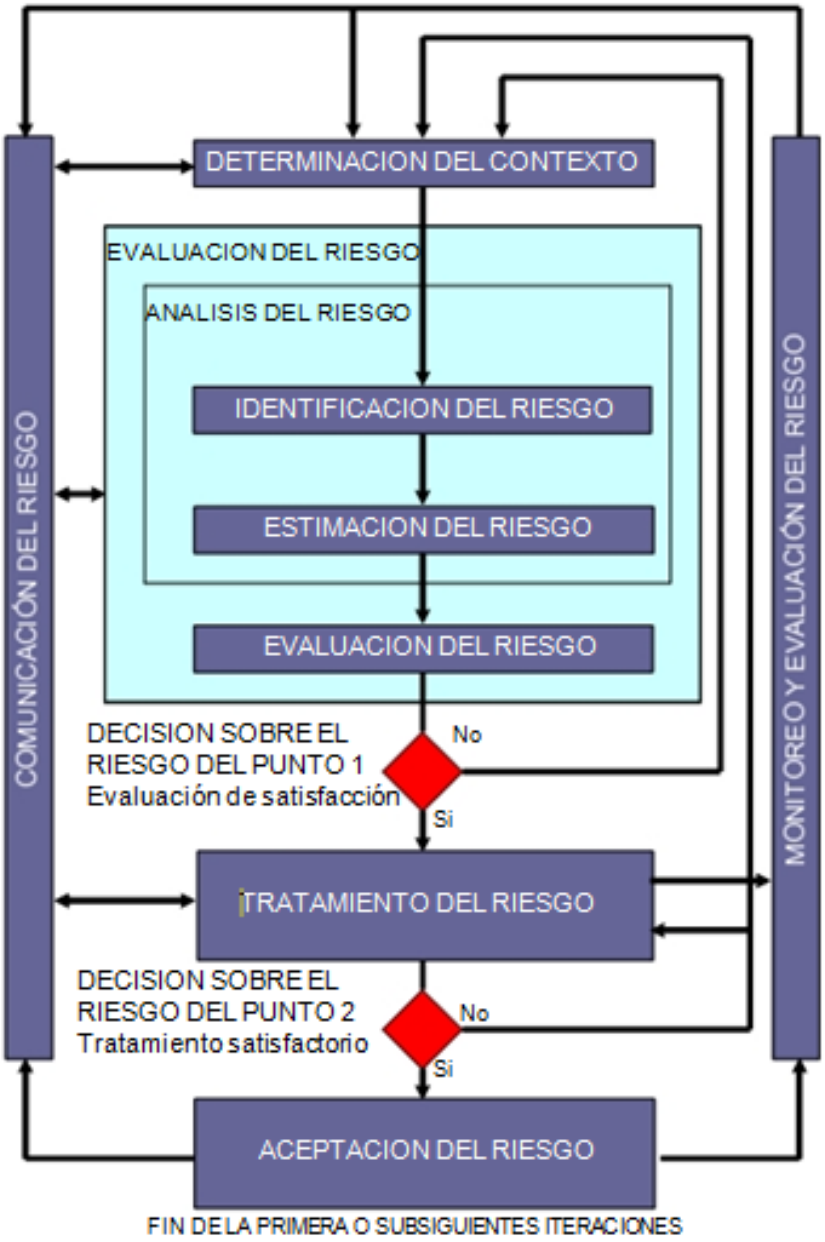


Gráfico 6. Proceso de gestión del riesgo según la ISO 31000

Fuente: (Escuela Nacional de Seguridad, 2012)

2.2.4.1. Ataques

Se dice que se ha producido un ataque accidental o intencionado al sistema cuando una amenaza es real.

Dependiendo del impacto infligido a los activos afectados, los ataques se clasifican en:

Activos. Si modifican, corrompen, eliminan o agregan información, bloquean o saturan los canales de comunicación. Las responsabilidades deben pagarse. Solo acceden a los datos contenidos en el sistema sin permiso. Estos son los más difíciles de detectar.

Un ataque puede ser directo o indirecto, si ocurre directamente del atacante al elemento “víctima”, través de recursos o intermediarios.

2.2.4.2. Amenaza

Cosa o persona que constituye una causa potencial de un incidente, el puede indicar un riesgo a la información.

Tipos de Amenaza

- Virus informáticos o código malicioso
- Uso no autorizado de Sistemas Informáticos
- Robo de Información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de Servicios (DoS)
- Ataques de Fuerza Bruta
- Alteración de la Información
- Divulgación de Información
- Desastres Naturales
- Sabotaje, vandalismo
- Espionaje

Se detallan algunas de las principales amenazas:

- **Spam:** Recibo mensajes no solicitados, principalmente vía e-mail, cuya finalidad es distribuir gran cantidad de mensajes comerciales o propagandísticos. Ha habido casos de envío a sistemas de telefonía móvil: mensajes de texto o sistemas de fax.
- **Phishing:** Se trata de un ataque de tipo ingeniería social, cuyo principal objetivo es obtener de forma fraudulenta datos confidenciales de un usuario, es decir, datos financieros, aprovechando su confianza en los servicios tecnológicos de los usuarios, desconociendo sus operaciones y prestando servicios en algunos casos con malas medidas de seguridad.

- **Troyanos, virus y gusanos:** Estos son programas maliciosos, que de diversas formas se almacenan en una computadora con el propósito de permitir que un atacante obtenga acceso no autorizado o permitir el control remoto del sistema. Además, el objetivo principal de los virus es destruir, dañar información de la máquina o crear un consumo de recursos descontrolado para bloquear o denegar el servicio.

- **Software desactualizado**: El software que no recibe el soporte y mantenimiento adecuados es vulnerable porque no tiene las actualizaciones necesarias para que funcione correctamente.

- **Desastres Naturales:** Accidente natural como terremoto, inundación, etc. En estas situaciones, el sistema de información es la víctima pasiva, pero en todos los casos, tendremos en cuenta lo que pueda suceder.

2.2.4.3. Vulnerabilidad

Se define como oportunidad ante una amenaza. Por ejemplo, la disponibilidad de cierta información para cualquier usuario o el acceso desde cualquier dispositivo en la computadora.

Estime la eficacia de un activo frente a una amenaza. (MAGERIT - v2: 2005)

La debilidad de seguridad del sistema lo hace vulnerable a ser explotado por una amenaza (CCN - STIC - 00: 2006)

Por lo tanto, de acuerdo con estas referencias, podemos decir que la vulnerabilidad de seguridad en cuestión es la debilidad del activo ante cualquier amenaza potencial.

Estas vulnerabilidades pueden afectar a los sistemas, así como a los recursos e incluso al personal que trabaja dentro de la unidad.

Criterios de vulnerabilidad

Los siguientes criterios de vulnerabilidad se aplican a todas las redes identificadas y elementos de red en el ámbito de la valoración:

1. La vulnerabilidad es alta. La vulnerabilidad existe, se puede aprovechar, es difícil de detectar y muy costosa de solucionar.

2. Vulnerabilidad moderada. Puede haber vulnerabilidades, explotables, detectables y la reparación puede ser costosa.

3. La vulnerabilidad es baja. La vulnerabilidad existe, se puede explotar, se puede descubrir y el costo de la reparación es mínimo.

4. Vulnerabilidad mínima. Existen vulnerabilidades, la posibilidad de que los costos de explotación, detección y remediación sean mínimos.

2.2.4.4. Salvaguardas

Las salvaguardas o contramedidas se definen como mecanismos, estrategias o procedimientos que nos permiten asegurar la viabilidad operativa de un activo de acuerdo con sus diversos criterios de seguridad, hasta que alcanza su vida útil.

Selección de Salvaguardas

La selección de una posible salvaguarda depende de los activos que como organización se quieran proteger

Según Margerit, se debe tener en cuenta los siguientes aspectos:

1. tipo de activos a proteger, pues cada tipo se protege de una forma específica

2. dimensión o dimensiones de seguridad que requieren protección

3. amenazas de las que necesitamos protegernos

4. sí existen salvaguardas alternativas

Como organización es necesario establecer prioridades, teniendo en cuenta

1. Mayor o menor valor individual o acumulativo de los activos, enfocándose en lo más valioso e ignorando lo irrelevante.

2. Mayor o menor probabilidad de amenaza, centrándose en los riesgos más importantes (ver áreas de riesgo).

3. La cobertura se proporciona mediante garantías alternativas.

Esto nos da un contexto claro de nuestra situación, para determinar qué respaldo estamos analizando, de la misma manera que Margerit nos brinda dos tipos de declaraciones para la mayoría excluir uno. Calificación:

- **no aplica:** decimos cuando no se aplica ningún respaldo porque técnicamente no es adecuado para la clase de activo a proteger, no protege el tamaño requerido o no protege de la amenaza percibida como consideración.
- **no se justifica:** decimos cuando la medida de protección está en su lugar, pero es no acorde con el riesgo que tenemos para proteger la protección afecta el cálculo del riesgo

las salvaguardas pueden tener 2 efectos, según Margerit:

- **Reduciendo la probabilidad de las amenazas.** Estos se denominan garantías preventivas. Los ideales van tan lejos como para evitar por completo que la amenaza se convierta en realidad.
- **Limitando el daño causado**. Hay salvaguardas que limitan directamente la posible degradación, mientras que otras permiten la detección inmediata de ataques para evitar la progresión de la degradación. Algunas copias de seguridad incluso se limitan a permitir una restauración rápida del sistema cuando una amenaza lo destruye.

En ambas versiones, la amenaza se materializa; pero las consecuencias son limitadas.

Representación de los Elementos del análisis del riesgo residual

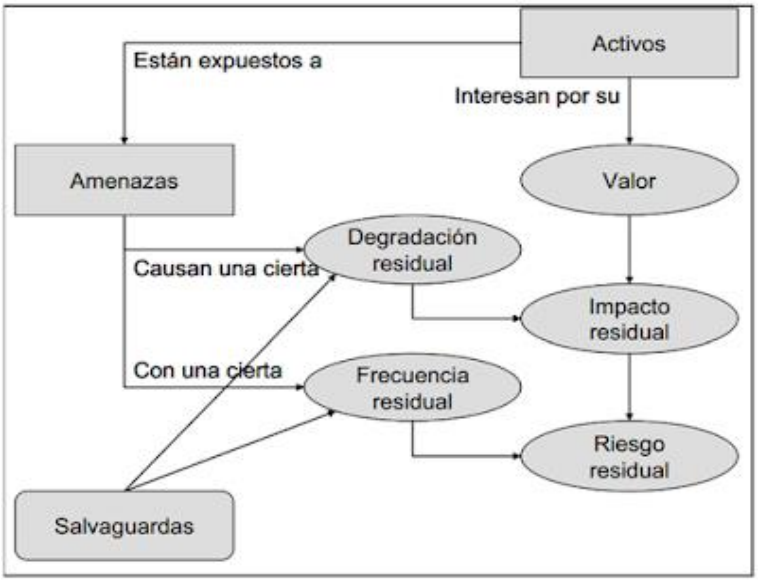


Gráfico 7, Elementos del análisis de riesgo

Fuente: Imagen Sacada de (SB, 2017)

2.2.4.5. Tipo de Protección

Los tipos de protección considerados según el método Margerit se tendrán en cuenta en el Libro de métodos, instrucciones:

"Este enfoque a veces se simplifica un poco demasiado, porque a menudo se habla de los diferentes tipos de protección que brindan las copias de seguridad:

- **[PR] prevención:** Diríamos que una copia de seguridad es preventiva ya que reduce las posibilidades de que algo salga mal. Si la copia de seguridad falla y se produce el problema, el daño es el mismo. Por ejemplo: reautorización de usuarios, gestión de privilegios, planificación de capacidad, metodología de desarrollo de software seguro, pruebas de preproducción, segregación de funciones, ...

- **[DR] disuasión:** Diríamos que la protección es inadecuada cuando tiene tal impacto en los atacantes que no se atreven ni dudan antes de atacar. Son salvaguardas que actúan antes de que ocurra un incidente, reduciendo las posibilidades de que ocurra; pero no afectan el daño causado si el atacante realmente se atreve. Por ejemplo, vallas levantadas, guardias de seguridad, avisos relacionados con el enjuiciamiento penal o persecución de los infractores.

- **[EL] eliminación:** Diríamos que una copia de seguridad elimina un problema cuando evita que suceda. Estas son garantías de acción antes de que ocurran problemas. Por ejemplo, eliminar cuentas estándar, cuentas sin contraseña, servicios innecesarios, ...; en general todo lo relacionado con fortificaciones o fortalezas, ..., cifrado de información, ..., cámaras de fuego, ...

- **[IM] minimización del impacto / limitación del impacto:** Se dice que una reserva minimiza o limita el impacto cuando limita las consecuencias de un incidente. Ejemplos: desconexión de la red o del dispositivo en caso de un ataque, cierre del servicio en caso de un ataque, cobertura, cumplimiento de las leyes aplicables.

- **[CR] corrección:** Diremos que una salvaguarda es reparable cuando, después de causar un daño, la reparará. Se trata de medidas de protección que actúan después de ocurrido el incidente y así reducen los daños. Por ejemplo, gestión de incidentes, líneas de comunicación alternativas, energía de respaldo, etc.

- **[MN] monitorización:** Son las salvaguardas que funcionan al realizar un seguimiento de lo que está sucediendo o ha sucedido. Si se detecta algo en tiempo real, podemos responder deteniendo el incidente para limitar el impacto; Si se descubre algo más tarde, podemos aprender del incidente y mejorar las medidas de protección en el futuro. Ejemplos: registros de actividad, registro de descargas de Internet, ...

- **[DC] detección** Diremos que una salvaguarda funciona detectando un ataque cuando indica que el ataque está en curso. Si bien no previene el ataque, permite que otras medidas surtan efecto para detener el progreso del ataque, minimizando así el daño. Por ejemplo: antivirus, IDS, detector de incendios.

- **[AW] concienciación:** Las actividades formativas de las personas que están adscritas al sistema pueden afectarlo. La formación reduce los errores del usuario, tiene un efecto preventivo. También mejora la garantía de todo tipo ya que quienes las extraen lo hacen de manera muy eficiente y rápida, potenciando así su efecto. Ejemplo: curso de sensibilización, curso de formación.

- **[AD] administración:** Se trata de garantías relativas a los componentes de seguridad del sistema. Una buena gestión evita no saber qué hay y así evita tener puertas desconocidas por las que un ataque pueda tener éxito. En general, se pueden considerar medidas preventivas. Por ejemplo, inventario de activos, análisis de riesgos, planificación de continuidad". (Gobierno español, 2018)

La siguiente tabla vincula cada una de estas protecciones al modelo anterior de disminución y reducción de probabilidad *Tabla 5, Tipos de Salvaguarda*

Efecto	Tipo
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente: *MAGERIT- versión 3.0. Libro 1: Método. Gobierno de España - Ministerio De Hacienda Y Relaciones Públicas. 2012*

2.2.4.6. Eficacia de la protección

Las salvaguardas se caracterizan por su eficacia frente al riesgo que se pretende evitar. La salvaguarda ideal es 100% eficaz, una actuación donde la combina 2 elementos:

Desde un punto de vista técnico

• Es técnicamente apto para afrontar riesgos, protege el

• Siempre se usa uso

Desde el punto de vista de las operaciones de la salvaguarda

• Está completamente desplegado, configurado y mantenido

• Tiene procedimientos claros para uso normal y en caso de falla

• Los usuarios están capacitados y reciben Fórmula

• Hay chequeos que advierten de posibles problemas

Entre el 0% de eficiencia para los que tienen deficiencia y el 100% para los que son adecuados y los que tienen implantes perfectos, el efecto real se estimará caso por caso. Para medir aspectos de una organización, se puede utilizar una escala de madurez para recopilar, como modificador, la confianza de que el proceso de gestión de la salvaguarda:

Tabla 6, Nivel de eficacia de protección

Factor	nivel	Significado

0%	**L0**	Inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	**L5**	Optimizado

Fuente: *MAGERIT- versión 3.0. Libro 1: Método. Gobierno de España Ministerio De Hacienda Y Relaciones Públicas. 2012*

2.2.4.7. Tratamiento de Riesgos

Incluye la organización del plan de defensa tanto para abordar los medios de prevención como para los riesgos observados tras la fase de análisis, considerando factores como: la gravedad del impacto y / o el riesgo. En consecuencia, el plan de defensa contribuirá a mitigar el riesgo a los valores que la Organización puede asumir.

Según Margerit, la calificación de cada riesgo debe clasificarse por:

1. Es importante en el sentido de que necesita atención urgente.
2. Es grave en el sentido de que requiere atención.
3. En el sentido de que puede estudiarse para su tratamiento.
4. Aceptable en el sentido de que no se tomó ninguna medida para corregirlo.

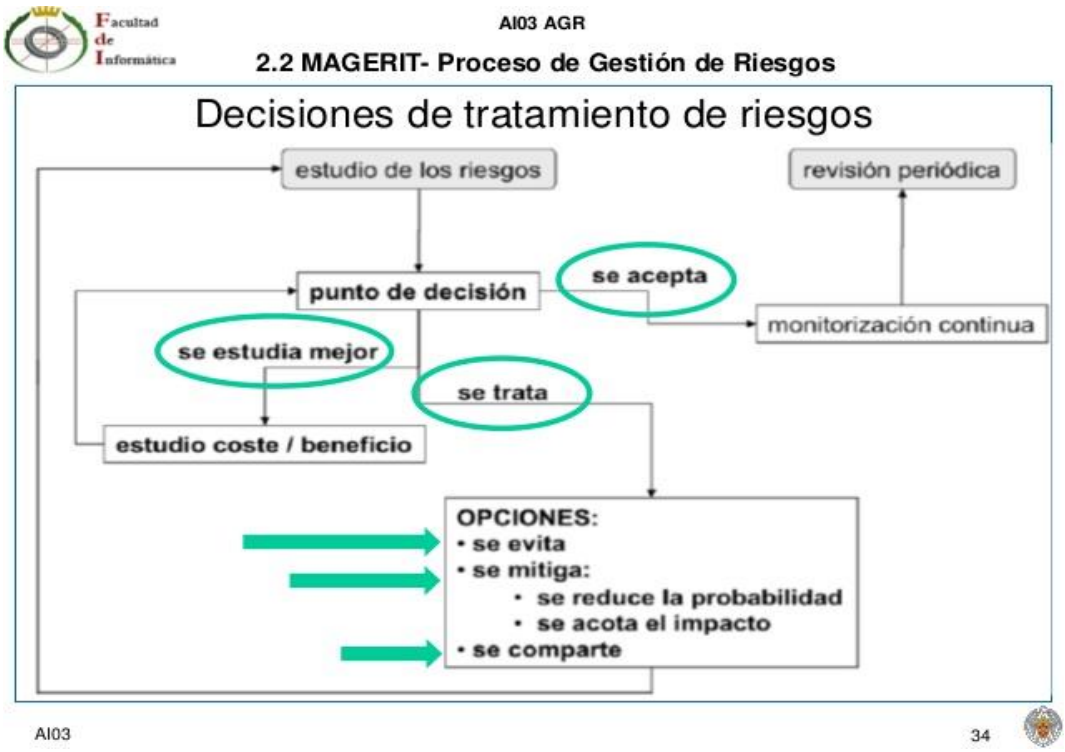


Gráfico 8, Tratamiento de riesgo

Fuente: *Imagen sacada de (Pedro García Repetto, 2014)*

La Dirección puede decidir aplicar un tratamiento a los sistemas de seguridad implementados para proteger los sistemas de información. Hay dos opciones principales:

- Reducir el riesgo residual (aceptar un riesgo menor).
- Mayor riesgo residual (mayor tolerancia al riesgo).

Al tomar tal o cual decisión, los riesgos que plantean los sistemas de información son parte de un contexto más amplio que incluye muchas consideraciones, algunas de las cuales pueden repetirse sin necesidad de declarar como completas:

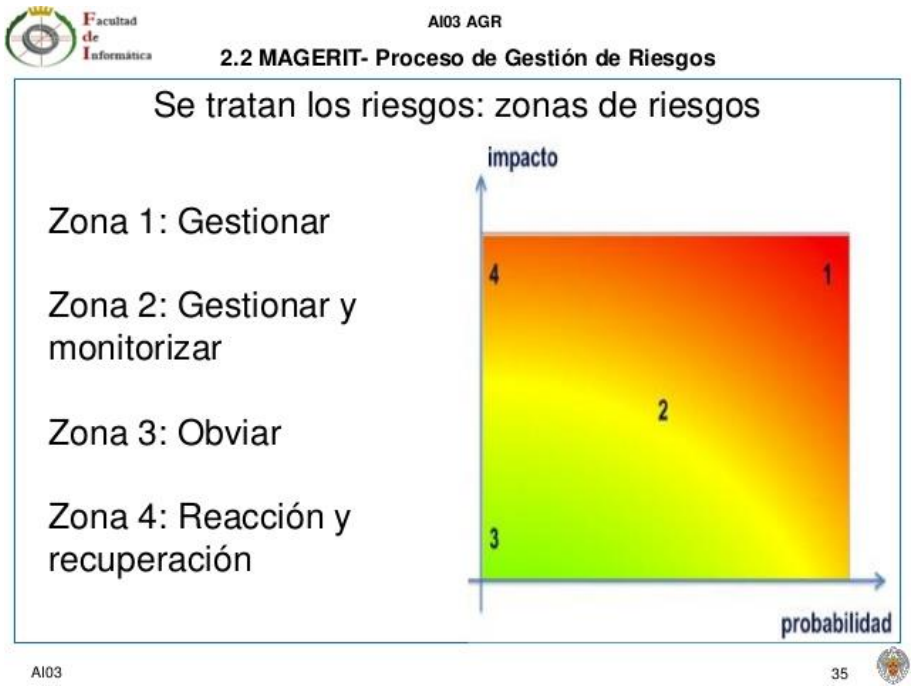


Gráfico 9, Mapeo de Gestión de riesgos

Fuente: *Imagen sacada de (Pedro García Repetto, 2014)*

2.2.4.8. Opciones para el tratamiento de Riesgos

La metodología Margerit ofrece las siguientes opciones

Eliminar el riesgo

Se logra eliminando una actividad, procedimiento o proceso que pudo haber causado el problema o modificándolo para eliminar el riesgo.

El uso de computadoras portátiles fuera de las instalaciones de una organización es un ejemplo. Prohibir esta práctica elimina la posibilidad de múltiples incidentes, creando un alto riesgo de impacto. (© 2021, 2017)

Mitigación

La mitigación del riesgo se refiere a una de dos opciones:

- Reducir la degradación causada por la amenaza (a veces se usa el término “impacto limitado”)
- Reducir la probabilidad de que una amenaza se manifieste en actualización. En cualquier caso, lo que hay que hacer es ampliar o mejorar el conjunto de garantías. En cuanto al tiempo de madurez de las protecciones: subir de nivel.

En cualquier caso, lo que hay que hacer es ampliar o mejorar el conjunto de garantías. En cuanto al tiempo de madurez de las protecciones: subir de nivel.

Compartir

En todos los casos, se trata de medidas que no previenen la ocurrencia de un incidente, ya que solo se transfiere el riesgo, pero pueden ser efectivas si se utilizan junto con una o más opciones de mitigación durante el tratamiento del riesgo. (© 2021, 2017).

Financiación

Cuando se acepta el riesgo, la Organización tendrá un buen desempeño en la constitución del fondo en caso de que se produzca el riesgo y tendrá que asumir las consecuencias. A veces se denomina "fondo de contingencia" y también puede formar parte de contratos de suscripción. Por lo general, esta opción no cambia nada en el sistema y el análisis de riesgo disponible vale la pena.

Plan de seguridad

El plan de seguridad constituye el documento que establece los principios y las políticas relacionadas a la Seguridad de los activos de información, que se consideren imprescindibles para el correcto funcionamiento de la organización, definiendo las responsabilidades por cada dimensión de la seguridad de la información.

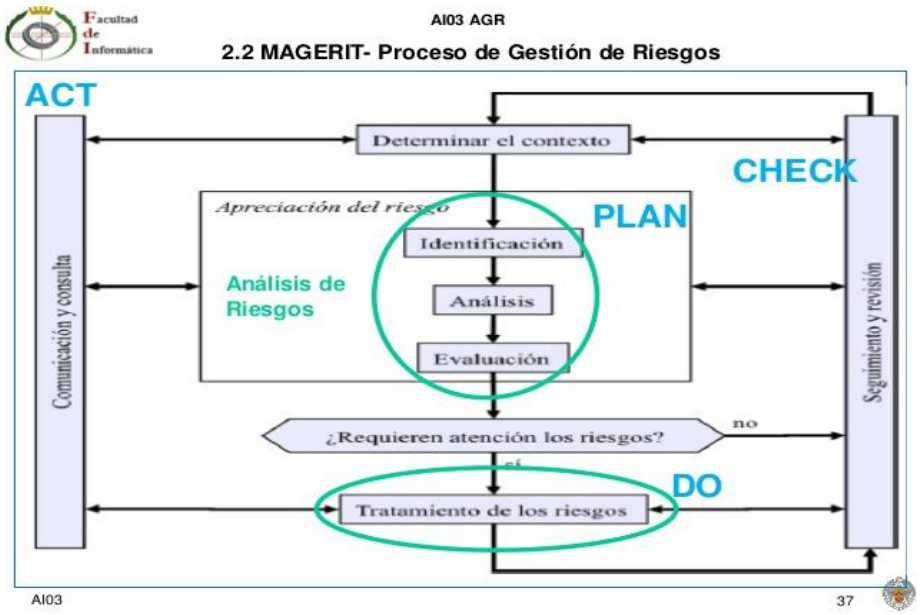


Gráfico 10, Proceso de Gestión de riesgos

Fuente: Imagen sacada de (Pedro Garcia Repetto, 2014)

2.2.5. El análisis y el tratamiento de los riesgos en su contexto

Resumiendo, la importancia de una organización en analizar y abordar continuamente el riesgo para lograr una gestión de seguridad adecuada

Según (Escuela Nacional de Seguridad, 2012), “El análisis de riesgo proporciona un sistema de modelos de activos, amenazas y protecciones, y es la base del control de todas las operaciones de la plataforma. La fase de procesamiento estructura las acciones tomadas desde una perspectiva de seguridad para satisfacer las necesidades descubiertas por el análisis. "

El modelo de trabajo debe ser iterativo, ya que los sistemas de información experimentan cambios con frecuencia, aunque tienen un alcance mayor en el nivel inicial que en una organización, como adquirir (implementar) nuevos activos, así como tener en cuenta el alcance de donde el entorno evoluciona como resultado de las nuevas formas de combatir los sistemas de información que se desarrollan a diario.

Esta estructura está sujeta bajo los fundamentos de la ISO 27001, que define las fases de un Sistema de Gestión de Seguridad de la Información.

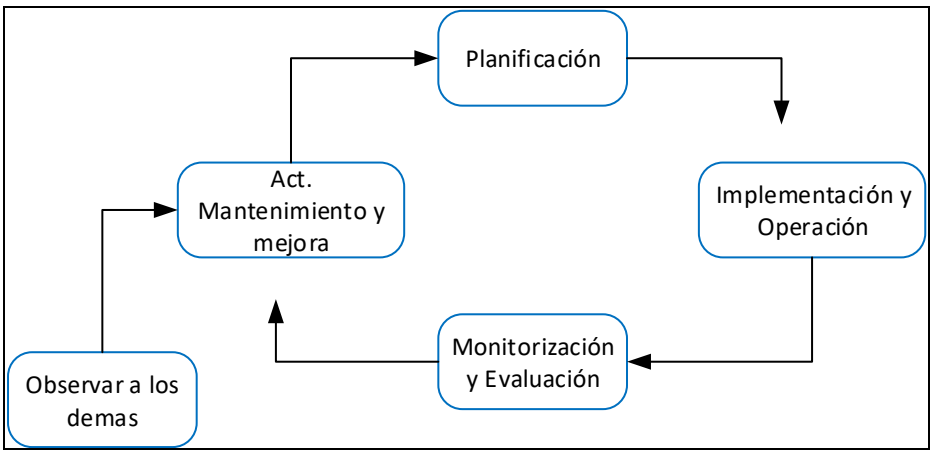


Tabla 7, Ciclo PDCA

Fuente: *(Escuela Nacional de Seguridad, 2012)*

2.2.6. Sistema de Gestión de Seguridad de la información

Un sistema de gestión de seguridad de la información (SGSI) es un conjunto de políticas de gestión de la información. ISO / IEC 27001 especifica los requisitos necesarios para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI) de acuerdo con el famoso "ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Plan, Do, Verificar, Actuar), este es un proceso de mejora continua. (Firmae, 2013), como estándar, el SGSI se sustenta en cuatro pilares de interacción, que son:

- Plan: Esta es la fase de diseño del SGSI para evaluar los riesgos de seguridad de la información y seleccionar los controles apropiados (Definición del alcance del SGSI, Definición de la política de seguridad, Metodología de evaluación de riesgos, Inventario de activos, Identificar amenazas y vulnerabilidades de seguridad, Determinar impacto, Analizar y evaluar riesgos, seleccionar y controlar).
- Do: Esta es una fase que involucra la implementación y operación de los controles (Definición del Plan de Tratamiento de Riesgos, Implementación del Plan de Tratamiento de Riesgos, Implementación de Controles, Capacitación y Sensibilización).
- Check: Esta es una fase que tiene como objetivo revisar y evaluar el funcionamiento (efectividad y efectividad) del SGSI, a través de los riesgos remanentes de los activos de información.
- Act: Durante esta fase, se realizan las modificaciones necesarias para que el SGSI vuelva a su máximo rendimiento (Implementar mejoras, Acciones correctivas, Verificar la efectividad de las acciones).

El corazón del SGSI es diseñar, implementar y mantener un conjunto de procesos para gestionar eficazmente el acceso a la información, buscando asegurar la confidencialidad, integridad y disponibilidad de la información de los activos, minimizando los riesgos de seguridad de la información, con el fin de lograr este objetivo. Los objetivos del SGSI deben ser efectivos y adaptables a los cambios internos dentro de la organización, ya que los factores externos pueden afectarla.

2.2.7. Seguridad de la información

La seguridad de la información son las medidas que se toman para proteger la información de una organización o empresa, la mayoría de estas medidas son generalmente preventivas, evitando que alguien manipule los datos, esto puede resultar en pérdida o robo de información.

“La seguridad de la información incluye un conjunto de técnicas y medidas para controlar todos los datos procesados dentro de una organización y para asegurar que los datos no salgan de los sistemas establecidos por la empresa. Este tipo de sistemas se basan principalmente en nuevas tecnologías. Por lo tanto, la seguridad de la información protege los datos disponibles en el

sistema a los que solo los usuarios autorizados tienen acceso. Sin embargo, no es posible cambiar la información a menos que esté en manos del usuario con los permisos correspondientes" (Pérez, 2021).

2.2.7.1. Objetivo de la Seguridad

El propósito principal de la seguridad de la información es proteger los datos de la empresa. Pero el concepto es genérico porque el sistema proporciona aspectos básicos como confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad.
"Para llevar a cabo estas acciones se deberán establecer estrategias donde se redacten las políticas de actuación para cada uno de estos casos. También habrá que establecer el uso de las tecnologías, incluir controles de seguridad y todos los procesos que se van a llevar a cabo para detectar los riesgos a los que se puede ver expuesto el sistema" (Pérez, 2021).

- **Confidencialidad**: Como resultado, la seguridad de la información garantiza que los datos almacenados en el sistema no se divulguen a otras entidades o personas no autorizadas para acceder a esta información.
- **Integridad**: Para que el sistema sea verdadero, los datos no deben manipularse. Esto asegura que la información recopilada sea precisa e inalterada, en otras palabras, mantiene nuestros datos precisos.
- **Disponibilidad**: La información que tenemos disponible está disponible para aquellos dentro de la organización que la necesiten.
- **Autenticidad**: Se refiere a cuando una persona, entidad o fuente de donde provienen los datos es veraz y real, el robo de identidad es un factor importante que pone en riesgo la autenticidad.
- **Trazabilidad**: La finalidad de esta función es permitirle determinar en todo momento quién hizo qué y cuándo, para poder conocer todas las incidencias y así poder analizarlas.
- **Riesgo**: Muestra lo que puede suceder con los activos si no están adecuadamente protegidos.

Es importante conocer las interesantes características de cada inmueble. Además de saber lo peligrosas que son estas características. es decir, análisis del sistema.

- **Análisis de riesgos:** Un proceso sistemático para estimular la escala de riesgo que enfrenta una organización.
- **Tratamiento de los riesgos:** Hay muchas formas de afrontar el riesgo: evitar las circunstancias que lo provocan, reducir la probabilidad de que ocurra, limitar sus consecuencias, compartirlo con otra organización (normalmente contratando servicios o seguros), o finalmente, aceptarlo como posible y proporcionar los recursos para actuar si es necesario.
- **No repudio:** Según la metodología de Margerit, este principio asegura la participación de las partes en la comunicación. En cualquier

comunicación existen remitentes y receptores, por lo que podemos distinguir dos tipos de no repudio:

No repudio en origen: asegura que el remitente del mensaje no puede negar que es el remitente, ya que el receptor tendrá prueba de entrega.

No repudio en destino: El receptor no puede negar la recepción del mensaje porque el remitente tiene un certificado. Este servicio es muy importante en las transacciones comerciales en Internet, ya que aumenta la confianza entre las partes en la comunicación.

PCM

Según (ONGEI, 2016), el presidente del Consejo de ministros - PCM, es el órgano rector del sistema nacional de TI, responsable de implementar la política nacional de e-gobierno, a través de ONGEI.

Según PCM, e-gobierno, (ONGEI, 2016), es el uso de las TIC por parte del Estado para mejorar los servicios e información que se brinda a las personas, y para incrementar la eficiencia y efectividad de la administración pública. Y aumentar significativamente el sector público transparencia y participación ciudadana.

ONGEI

Se trata de un organismo especializado subordinado a la jerarquía del presidente del Consejo de ministros, encargado de dirigir y gestionar el Sistema Nacional de Información e implementar la Política Nacional de Gobierno Electrónico y Tecnologías de la Información. -gobierno, infraestructura de datos espaciales, marco estratégico para el desarrollo de la sociedad de la información, uso de TI- TT en 'Estado, etc. (andréapazalejandro, 2017)

Entre sus actividades permanentes se encuentran:

- Normativa informática.
- Seguridad de la información.
- Desarrollo de proyectos punteros en el campo de las tecnologías de la información y las comunicaciones (TIC).
- Brindar asesoría técnica y de TI a las organizaciones públicas.
- Capacitación y difusión en temas de gobierno electrónico.
- Modernización y descentralización del Estado.
- Desarrollo de la sociedad de la información en Perú.

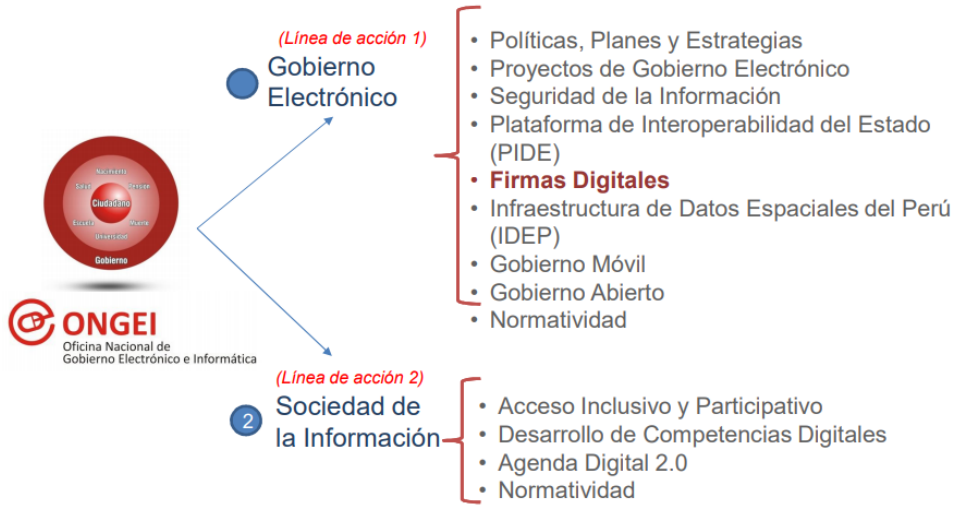


Gráfico 11, ONGEI,

Fuente: (ONGEI, 2016)

2.2.8. Norma ISO/IEC 27000

La serie de normas ISO / IEC 27000, conocida como la serie de normas ISO 27000, fue desarrollada y publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) para proporcionar un marco para el marco reconocido mundialmente para la seguridad de la información. Prácticas de manejo. (ISOTools, 2018).

Según (Briceño Huaygua, 2019), esta normativa estipula claramente los parámetros de seguridad de la información, para el desarrollo, implementación y mantenimiento de sistemas de gestión de seguridad de la información, entre ellos:

- Norma ISO/IEC 27001: Definir los requisitos para la implementación del SGSI (Sistema de Gestión de Seguridad de la Información).
- Norma ISO/IEC 27002: (anteriormente ISO 17799). Es una guía de buenas prácticas que describe los controles a seguir en el contexto de la seguridad de la información; enmarcado en 11 áreas, 39 objetivos de control y 133 controles.

- Norma ISO/IEC 27003: Proporciona, ayuda y asesoramiento sobre la implementación del SGSI, incluido un enfoque PDCA (Planificar, Hacer, Verificar y Actuar) para la evaluación y mejora continua.
- Norma ISO/IEC 27004: Especificará las métricas y técnicas de medición utilizadas para determinar la efectividad del SGSI y sus medidas de control. Aplicación específica en el período do (Do); según el método PHVA.

Norma ISO 27001-2014

ISO 27001 es una norma internacional que certifica los procesos de una organización para gestionar correctamente la seguridad de la información.

ISO 27001 también se basa en otras normas como ISO / IEC 17799: 2005, la serie ISO 13335, ISO / IEC TR 180:200 y las directrices de la OCDE sobre sistemas y redes de seguridad de la información, proporcionando orientación para el desarrollo. Implementar sistema de seguridad de la información.

Debido a esta conformidad con otros sistemas de gestión y la integración con los estándares de gestión relevantes, la implementación de ISO 27001 conduce a:

- Cumplir con los estándares del sistema de gestión como ISO 9001 e ISO 1001.
- Énfasis en la mejora continua de los procesos del sistema de gestión de seguridad de la información.
- Claridad de la documentación y los requisitos de registro.
- Procesos de evaluación y gestión de riesgos involucrados utilizando el modelo de ciclo de calidad de Deming: Planificar, Hacer, Verificar, Actuar (PDCA).
- Proteja los activos comerciales, desde la información digital, los documentos y los activos físicos (computadoras y redes) hasta el conocimiento de los empleados.

Proteger sus activos de información es muy importante porque las amenazas no solo provienen del exterior de nuestra empresa, sino también del interior. El contenido de la información son los elementos que contienen información y se clasifican de la siguiente manera:

- Información impresa.
- Información electrónica.
- Sistemas de información
- Personas
- Equipos informáticos.

Norma Técnica Peruana (NTP-ISO/IEC 27001:2014)

(INDECOPI, NORMA TECNICA PERUANA NTPISO / IEC 2700: 2014, 2014) esta norma técnica peruana define los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de administración de seguridad de la información.

Esta norma técnica peruana cubre requisitos de evaluación y procesamiento de riesgos de seguridad de la información ajustados a las necesidades de la organización. Los requisitos establecidos en esta Norma Técnica Peruana son de carácter general y se aplican a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.

De acuerdo a las normas peruanas, el primer paso, la organización y su contexto deben ser entendidos, deben ser identificados

- Interesados en el sistema de gestión de seguridad de la información.
- Requerimientos de las partes inquietudes relacionadas con la seguridad de la información Estos requerimientos pueden ser legales o regulatorios.

Una entidad determinará las limitaciones y aplicabilidad del SGSI, con el fin de establecer la medida en que está disponible como información documentada.

Liderazgo

La alta dirección debe evidenciar liderazgo y compromiso con la administración de la seguridad de la información

a) Asegurar que la política y los objetivos de seguridad de la información se establezcan en línea con la dirección estratégica de la organización, en caso de que esta persona se convierta en director de DRTPE

b) Asegurar la integración de CMSI Requisito

c) Asegurar los recursos necesarios para iniciar el proyecto de políticas

d) Promover la mejora continua

El estándar específico al que se debe adaptar la política de seguridad a cada caso, dependiendo de la entidad, la política de seguridad debe estar disponible como información documentada, comunicada dentro de la organización (a través de entrevistas confidenciales, capacitaciones, etc.), y están disponibles para todos. preocupado.

Planificación

En esta sección se establecen acciones para abordar riesgos y oportunidades, asegurando que las políticas se desarrollen e implementen exitosamente en la prevención y reducción de impactos indeseables, a través de acciones para abordar los riesgos que surgen después del evento. 'Análisis de riesgo.

Valoración del riesgo de seguridad de la información

El NTP establece que una organización debe definir e implementar un proceso de evaluación de riesgos de seguridad de la información. Que:
a) Establecer y mantener estándares de riesgo de seguridad de la información
b) Garantizar evaluaciones de riesgo de seguridad
c) Identificar riesgos de seguridad asociados con la pérdida de confidencialidad, integridad y disponibilidad.
d) Desarrollar un correcto análisis de riesgos (valorando las consecuencias, determinando la probabilidad, para finalmente generar una planificación de riesgos que permita realizar una correcta valoración

Tratamiento de los riesgos de seguridad de información

La misma entidad debe establecer objetivos de seguridad, a niveles que se consideren aceptables por esta.

- Los objetivos deben ser consistentes
- Deben ser medibles (si es practico)
- Ser comunicados (se establece que, con charlas de seguridad, capacitación a todo el personal de la entidad, dentro de este requisito podemos poner la etapa de concientización)
- Ser actualizados según sea apropiado

Objetivos de seguridad de la información

La misma entidad debe establecer objetivos de seguridad, en la medida que lo estime aceptable.

- Los objetivos deben ser consistentes
- Deben ser medibles (si son realistas)
- Comunicarse (se establece que, con entrevistas de seguridad, se capacita a todo el personal de la unidad., En esta solicitud podemos incluir en la etapa de sensibilización)
- Actualizado si es necesario

Para alcanzar sus finalidades, una organización debe establecer y proporcionar los recursos necesarios para determinar, implementar, mantener y mejorar continuamente una política de seguridad de la información, teniendo en cuenta que cualquier acción que se realice se realizará de forma integral.

Evaluación de riesgos de seguridad de la información

NTPISO / IEC 2700: 2014 requiere que una entidad realice una evaluación de riesgos de seguridad a intervalos establecidos, además de que la entidad mantenga información documentada sobre los resultados de su evaluación de riesgos de seguridad.

Según (INDECOPI, NORMA TECNICA PERUANA NTPISO / IEC 2700: 2014, 2014), una organización debe implementar un plan de tratamiento de riesgos

de seguridad de la información y de igual manera, debe retener información sobre los resultados del procesamiento.

La organización realizará auditorías para evaluar el estado de la seguridad de la información, de acuerdo con (INDECOPI, NORMA TECNICA PERUANA NTPISO / IEC 2700: 2014, 2014), la organización debe:

a) Planificar, establecer, implementar y mantener uno o más programas de auditoría, incluidas frecuencias, métodos, etc.

b) Definir criterios y alcance de cada auditoría

c) Seleccionar auditores y realizar auditorías

A continuación, se hará referencia a algunos puntos clave de la determinación de controles de las políticas de seguridad, de acuerdo a (INDECOPI, NORMA TECNICA PERUANA NTP-ISO/IEC 2700:2014, 2014):

Tabla 8, Norma Técnica Peruana NTP-ISO/IEC 27001:2014

A. Política de Seguridad	
A.1. Política de Seguridad de la Información	
Objetivo de control: "Proporcionar apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes"	
A.1.1. "Documentar política de seguridad de la información"	Control El director de esta unidad será el responsable de aprobar la política de privacidad y los cambios futuros.
A.1.2. "Análisis de la política de seguridad de la información"	Control Esta Política es revisada anualmente por el Comité de Gestión de Seguridad de la Información y actualizada para asegurar su efectividad.
A.2. Organización de la seguridad de la información	
Objetivo: "Implantar un patrón de administración para el inicio y el control de la implementación y operación de la seguridad de la información en la entidad".	
A.2.1. "Acuerdo de la gerencia con la seguridad de la información"	Control La gerencia debe promover activamente la seguridad dentro de la entidad mediante la asignación de fondos a través de una dirección clara y un compromiso demostrado.
A.2.2. "Concertación de la seguridad de información"	Control Todas las secciones de liderazgo de la organización deben coordinar las actividades de seguridad de la información.
A.2.3. "Establecimiento de responsabilidades de la seguridad de la información"	Control La responsabilidad por la seguridad de la información debe estar claramente establecida y asignada a la gerencia.
A.2.4. "Autorización para los medios de	Control

procesamiento de información”	Definir e implementar procedimientos de autorización administrativa para nuevas actividades de procesamiento de información.
A.2.5. “Acuerdos de confidencialidad”	Control Los requisitos de confidencialidad deben establecerse y revisarse periódicamente teniendo en cuenta la necesidad de la agencia de proteger la información.
A.2.6. “Verificación independiente de la seguridad de la información”	Control El enfoque de la organización para la implementación y gestión de la seguridad de la información (es decir, los objetivos y procesos de control de la seguridad de la información) debe revisarse de forma independiente a intervalos de tiempo establecidos para determinar la eficacia de las medidas de implementación. .
A.3. Dispositivos móviles y teletrabajo	
Objetivo: “Asegurar la seguridad del teletrabajo y el uso de los equipos móviles”	
A.3.1. “Política de equipos móviles”	Control Para gestionar los riesgos asociados con el uso de dispositivos móviles, se requieren políticas y medidas de seguridad de apoyo.
A.3.2. “Teletrabajo”	Control Deben existir políticas y medidas de seguridad de apoyo para proteger la información disponible a través del trabajo remoto.
A.4. Gestión de activos	
A.4.1. Compromiso por los activos	
Objetivo: “Mantener la protección óptima de los activos de la entidad”	
A.4.1. “Inventariado de activos”	Control Debe usar el registro de contenido para identificar qué información debe actualizarse.
A.4.2. “Propiedad de los activos”	Control A quién se deben delegar los recursos de una organización para designar recursos para realizar un seguimiento del ciclo de vida del recurso.
A.4.3. “Uso aceptable de los activos”	Control Deben definirse, documentarse y aplicarse estándares para el uso justo de la información y los activos. .
A.4.2. Categorización de la información	
Objetivo: “Fijar que la información reciba un nivel de protección apropiado”	
A.4.2.1 “Lineamiento de clasificación”	Control

	La información debe clasificarse de acuerdo con su valor, requisitos legales, confidencialidad e importancia para la organización.
A.4.2.2 “Etiquetado y uso de la información”	Control Se recomienda a los operadores que implementen un conjunto de procesos vinculados con el etiquetado y el uso de la información.
A.4.3. Manejo de los medios	
Objetivo: “Prevenir la difusión, manipulación, eliminación de los activos de información”	
A.4.3.1. “Gestión de medios removibles”	Control Dependiendo de las necesidades de la organización, se debe implementar un programa de administración de medios extraíbles.
A.4.3.2. “Transferencia de medios físicos”	Control Los medios de almacenamiento de información deben estar protegidos contra el acceso no autorizado.
A.4.3.3. “Procedimiento de manejo de la información”	Deben implementarse procedimientos de almacenamiento y gestión de la información para evitar el acceso no autorizado.
“Seguridad de documentación del sistema”	Los documentos deben estar protegidos contra el acceso no autorizado.
A.5. Monitoreo	
Objetivo: “Detectar actividades de procesamiento de información no autorizadas”	
A.5.1. “Registro de auditoría”	Se recomienda crear un registro de actividades de auditoría, excepciones e incidentes de seguridad de la información.
A.5.2. “Uso del sistema de monitoreo”	Los procesos para evaluar el uso de los recursos de procesamiento de información deben ser oportunos y estos procedimientos deben revisarse periódicamente.
A.5.3. “Protección de la información del registro”	Los medios de grabación y la información registrada deben protegerse contra la manipulación y el acceso no autorizado.
A.5.4. “Registro de fallas”	Los defectos deben registrarse, analizarse y tomarse las medidas apropiadas.
A.6 Seguridad de los recursos humanos.	
A.6.1. Antes del empleo	
Objetivo: “Asegurar que los empleados, contratistas y terceros entiendan sus compromisos, y sean apropiados para los roles de acuerdo a sus requerimientos laborales, y así de disminuir el riesgo de a que están expuestos los activos de información”	
A.6.1.1.” Roles y responsabilidades”	Control Se recomienda que las funciones y responsabilidades de los trabajadores vinculados con la seguridad, etc., se establezcan y documenten de acuerdo con la

	política de seguridad de la información de la organización.
A.6.1.2. “Selección”	Control Se recomiendan verificaciones de antecedentes de todos los posibles empleados, contratistas y terceros de acuerdo con las leyes, los reglamentos y la ética aplicables y deben ser acordes con los requisitos comerciales, se accede a la clasificación de la información y se perciben los riesgos.
A.6.1.3. “Términos y condiciones de empleo”	Control Recomendado como parte de los deberes del personal; los trabajadores, contratistas y terceros deben aceptar los términos de sus contratos de trabajo, los cuales deben establecer claramente sus responsabilidades y obligaciones en materia de confidencialidad.
A.6.2. Durante el empleo	
Objetivo: “Asegurar que todos los empleados, etc., estén al tanto de las amenazas sobre la seguridad de información, para que puedan desarrollar su trabajo de forma normal, y reducir los riesgos de error humano, esto va de la mano de una correcta concientización en estos temas por parte de la gerencia mediante capacitaciones”.	
A.6.2.1. “Gestión de responsabilidades”	Control La gerencia debe exigir a los trabajadores que apliquen medidas de seguridad consistentes con las políticas y procedimientos establecidos de la organización.
A.6.2.2. “Capacitación y educación en seguridad de la información”	Control Los empleados de la entidad propuesta deben recibir capacitación adecuada y mantener las políticas y procesos de la entidad actualizados con sus funciones.
A.6.2.3. “Proceso disciplinario”	Control Se recomiendan procedimientos disciplinarios para los empleados que no respeten las normas de confidencialidad o no informen incidentes de seguridad de la información.
A.6.3. Terminación o cambio del empleo	
Objetivo: “Asegurar que los empleados que salgan de la Institución, lo realicen de manera ordenada, sin violar ninguna regla de seguridad”.	
A.6.3.1. “Devolución de activos”	Control Todos los trabajadores deben devolver todos los activos de la organización en su poder al momento de la terminación.
A.6.3.2. “Terminación o cambio de responsabilidades”	Control El acceso de los empleados que dejan la organización debe ser revocado al final del contrato.
A.7. Seguridad física y ambiental	
A.7.1. Áreas seguras.	
Objetivo: “Evitar el acceso no autorizado, daño e interferencia a los locales de acceso restringido”.	
A.7.1.1. “Controles de ingreso físico”	Las áreas seguras deben estar aseguradas con medidas de control de acceso apropiadas para

	garantizar que solo las personas autorizadas puedan ingresar.
A.7.1.2. "Protección contra amenazas externas y ambientales"	La protección física debe diseñarse y aplicarse para evitar daños por incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o provocados por el sujeto.
A.7.2. Seguridad de los equipos informáticos	
Objetivo: "Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la institución"	
A.7.2.1. "Ubicación y protección de los equipos"	Control El equipo debe estar en ubicaciones estratégicas y protegido para reducir el riesgo de peligros como robo o vandalismo.
A.7.2.2. "Servicios de suministro"	Control El equipo aún debe estar protegido contra cortes de energía debido al grupo electrógeno.
A.7.2.3. "Seguridad en el cableado"	Control Las líneas eléctricas y de telecomunicaciones que transportan datos deben estar protegidas contra intercepciones, interferencias o daños.
A.7.2.4. "Mantenimiento de equipos"	Control El equipo debe mantenerse y actualizarse periódicamente para garantizar su disponibilidad e integridad.
A.7.2.5. "Remoción de equipos"	Control Eliminación no autorizada de hardware o software de su ubicación.
A.7.2.6. "Reutilización segura de equipos"	Control Todos los elementos de hardware que contengan medios de almacenamiento deben verificarse para garantizar que los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de manera segura.
A.7.2.7. "Política de escritorio Limpio y Pantalla limpia"	Control Para optimizar el procesamiento de la información, se debe utilizar la estrategia de pantalla limpia.
A.8 Administración de las comunicaciones y operaciones	
A.8.1. Procedimientos y responsabilidad operacionales	
Objetivo: "Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras"	
A.8.1.1 "Procedimientos de operación documentados"	Control Se recomienda que los procesos de gestión de los sistemas de información se documenten y mantengan, y que estén disponibles para todos los usuarios que los necesiten.
A.8.1.2. "Gestión de cambio de control"	Los cambios en los diversos sistemas utilizados por la agencia deben ser controlados.

A.8.2. Respaldo	
Objetivo: “Se recomienda preservar la integridad y disponibilidad de los servicios de procesamiento de información”	
A.8.2.1. “Respaldo de información”	Control La información mantenida por la organización debe respaldarse periódicamente y, además, las copias de seguridad deben probarse para demostrar que funcionan correctamente.
A.9. Administración de seguridad de redes.	
Objetivo: “Asegurar la protección de la información en redes y la protección de la estructura de soporte”	
A.9.1. “Controles de red”	Control La red debe estar debidamente administrada y controlada, y gestionada con estándares para asegurar la información.
A.9.2. “Seguridad de los servicios de red”	Control Controles de seguridad, niveles de servicio, tanto internos como proporcionados por terceros.
A.10 Criptografía	
A.10.1. Controles criptográficos	
Objetivo: “Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y la integridad de la información”	
A.10.1.1 “Gestión de Claves”	Control Las reglas para el uso, la protección y la vida útil de las claves criptográficas deben desarrollarse e implementarse dentro de la entidad. La distribución de claves debe controlarse a través de un proceso de gestión formal. Genere claves con más de ocho caracteres usando mayúsculas, minúsculas, números y caracteres especiales
A.11.1. Control de acceso	
Objetivo: “Limitar el acceso de información”	
A.11.1.1. “Política de control de acceso”	Control Se deben implementar procedimientos formales para el alta y baja de categorías o grupos de usuarios en función del nivel de acceso a la información y/o servicios solicitados (impresión, etc.), grupos o permisos, esto se gestiona a través de Workgroup, una aplicación de Windows.
A.11.1.2. “Aprovisionamiento de acceso a usuario”	Control La dirección de la unidad debe revisar periódicamente los derechos de acceso de los usuarios mediante procedimientos formales.
A.11.2. Responsabilidades de los usuarios	
Objetivo: “Hacer que los usuarios respondan por la salvaguarda de su información”.	
A.11.2.1. “Uso de Información: Control-> Los usuarios deben ser exigidos que sigan las prácticas de la organización en el manejo de información sensible”.	
A.11.3. Control de acceso a redes	

Objetivo: "Evitar el acceso no autorizado a los servicios en red"	
A.11.3.1. "Política sobre el uso de servicios de red"	Control Los usuarios sólo deben tener acceso a los servicios para los que hayan sido expresamente autorizados.
A.11.3.2 "Autenticación del usuario para conexiones externas"	Control El método de autenticación debe usarse para controlar el acceso de los usuarios a través del trabajo remoto o el acceso remoto.
A.11.3.3 "Identificación del equipo de red"	Control Piense en la autenticación automática de computadoras como un método para autenticar conexiones desde computadoras y ubicaciones específicas.
A.11.3.4 "Control de conexión de redes"	Control De acuerdo con la política de control de acceso, el ancho de banda de conexión de los usuarios en una red compartida debe limitarse para permitir el acceso solo a los recursos necesarios para el crecimiento de su negocio.
A.12. Seguridad en las operaciones	
A.12.1. Administración de vulnerabilidades técnicas	
Objetivo: "Prevenir la explotación de vulnerabilidades técnicas"	
A.12.2. "Restricciones sobre instalación de software"	Control Establecer e implementar políticas que identifiquen el software adecuadamente monitoreado e instalado por el usuario.
A.13. Gestión de incidentes de seguridad de la información	
Objetivo: "Asegurar un tratamiento consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad"	
A.13.1. "Responsabilidades y procedimientos"	Control Establecer responsabilidades y procedimientos de gestión para garantizar una respuesta rápida.
A.13.2. "Reporte de debilidades de seguridad de la información"	Control Se requerirá que los usuarios de los sistemas de información de la organización informen cualquier debilidad o falla observada.
A.13.3. "Evaluación y decisión sobre eventos de seguridad de la información"	Control Se debe evaluar un incidente de seguridad de la información y tomar una decisión sobre si clasificar el incidente como un incidente de seguridad.
A.13.4. "Respuesta a incidentes de seguridad de la información"	Control

	Debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.
A.14 Cumplimiento de los requisitos legales y contractuales	
Objetivo: "Evitar infracciones de las obligaciones legales, estatutarias, regulatorias, relacionadas a la seguridad de la información"	
A.14.1. "Identificación de requisitos contractuales y de legislación aplicables"	Control Todos los requisitos legales, regulatorios y contractuales relevantes y el enfoque de la entidad para el cumplimiento organizacional.
A.14.2. "Privacidad y protección de datos personales"	Control La privacidad y la protección de los datos personales deben garantizarse según lo exigen las leyes y los reglamentos.
A.15. Revisiones de seguridad de la información	
Objetivo: "Asegurar que la seguridad de la información esta implementada y es operada de acuerdo con las políticas y procedimientos organizativos".	
A.15.1. "Revisión independiente de la seguridad de la información"	Control El enfoque de la organización para la implementación y gestión de la seguridad de la información, es decir,(evaluar si los objetivos, controles y procedimientos están bien definidos)
A.15.2. "Cumplimiento de políticas y normas de seguridad"	El director de la unidad deberá evaluar periódicamente el cumplimiento de los procesos y manejo de la información en su área de responsabilidad.

Fuente. (INDECOPI, NORMA TECNICA PERUANA NTP-ISO/IEC 2700:2014, 2014)

2.2.9. Ley de Delitos Informáticos

Ley N°30096 (REPUBLICA, 2013), La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

Ley de Protección de Datos Personales

De acuerdo a (Briceño Huaygua, 2019), acota que la Ley N° 29733 (PCM, 2016) de Protección de Datos Personales del Perú tiene como objetivo proteger todos los datos de las personas naturales gestionados por las compañías: clientes, colaboradores y proveedores, entre otros. Para ello se requiere la implementación de un marco integrado de medidas técnicas, organizacionales y legales

Las normas sobre protección de datos personales brindan a los ciudadanos las herramientas necesarias para proteger sus datos personales y controlar el uso que se realiza de los mismos. Para garantizar la protección de los datos personales las entidades públicas deben cumplir con sus obligaciones de acuerdo a ley

Políticas de Seguridad de la Información

Las políticas son medios para definir un comportamiento deseado en los miembros del personal interno de las instituciones, estas surgen como una herramienta que ayuda a concientizar sobre la importancia de la seguridad de la información dentro de los procesos y actividades que se desarrollan diariamente, a la vez que mediante las políticas de seguridad podemos establecer un conjunto de reglas, controles, etc. A su vez nos permite establecer claramente los roles que participaran en la definición de estas, adecuándose a cada entidad de estudio, que por ejemplo a nivel de acceso de información se definirán de acuerdo al nivel de acceso de información que requiera el desempeño de una actividad realizada por un miembro de la entidad.

Una política de seguridad debe establecer un conjunto de controles que se deben implementar, así como la política debe abarcar un contexto amplio. La política de seguridad se implementa mediante procedimientos técnicos de acuerdo a las necesidades de la organización, estableciendo su cumplimiento

Para definir las políticas necesarias para una institución, se debe realizar un proceso de análisis de los riesgos de información, este análisis debe incluir a toda los niveles y actores de la institución, estas políticas tienen que estar documentadas y ser aprobadas por la dirección de la organización y comunicada a todo el personal.

Etapas para la implementación de políticas de seguridad de información

1. Desarrollo de las políticas: Etapa en la que la entidad debe delegar la responsabilidad a un auditor en temas de seguridad de la información, este personal puede interno o externo, la entidad debe de participar en la creación, actualización y aprobación de estas, esta etapa tiene los siguientes ítems:

- Justificación de la creación de política: Las políticas deben crearse de acuerdo a los requerimientos que esta tenga, de acuerdo a su contexto, una identificado este paso se debe definir los controles que fortalezcan esta política.

- Alcance: Se debe definir a quienes (hace referencia a procesos, niveles jerárquicos, empleados, etc.) abarca el cumplimiento de estas políticas

- Roles y Responsabilidades: El establecimiento de roles y responsabilidades es de suma importancia para el proceso de aplicación de las políticas, para futuras auditorías este esquema es fundamental.

- Revisión de la política: Una vez que se desarrolla una política, otros evaluarán la actividad para examinar la adopción y hacer recomendaciones para el desarrollo y desarrollo de políticas.

- Aprobación de la Política: Este ítem indica que la gerencia de la institución debe de publicar las políticas y establecer un cronograma de cumplimiento, así como debe mostrar interés en la implementación de estas

2. Cumplimiento: Etapa en la que las políticas redactadas deben de estar implementadas, así como sus respectivos controles, es muy importante que l gerencia participe activamente y desarrolle planes para su cumplimiento

3. Comunicación: Etapa en la que difunde las políticas de seguridad, diversos autores señalan que la instituciones deben de implementar programas de capacitación a todos los empleados, personal externo, contratistas, etc. para que de esta forma conozcan y den cumplimiento de las normativas, las políticas deben de ser proporcionada en formato digital para su ágil difusión

4. Monitoreo: Etapa en la que se evalúan la eficiencia de las políticas de seguridad al momento de mitigar los riesgos a las que está expuesta la institución, este monitoreo o auditoría debe realizarse por especialistas en seguridad de la información

5. Mantenimiento: Una vez que se ha realizado una auditoría informática de las políticas de seguridad, estas darán recomendaciones acerca de cómo se debe mejorar la seguridad, sobre qué políticas deben de ser actualizadas, que procedimientos extras se deben implementar, etc., se deben de seguir las recomendaciones

6. Retiro: Fase en la cual una política de seguridad ya ha cumplido su finalidad o ha quedado obsoleta, cada retiro o actualización de una política debe contar con autorizaciones de la parte directiva de la organización

Estos componentes determinarán el alcance de las políticas de seguridad (Plan director de Seguridad) a nivel genérico, de acuerdo a (CIBERSEGURIDAD, 2018) para la elaboración e implementación de un Plan de políticas de seguridad se siguen las fases o etapas que muestra la ilustración:

Gráfico 12,: Implantando un Plan director de Seguridad,

Fuente (CIBERSEGURIDAD, 2018)

Conocer la situación actual de la organización

El primer paso es comprender el contexto de la organización, determinar sus requisitos de seguridad y realizar un análisis de riesgos de seguridad de la información desde una perspectiva holística.

Este es el paso más importante y complejo en el proceso de la política de seguridad ya que esta autoridad involucra a diferentes actores, se deben brindar todas las facilidades a las personas que se encargan de desarrollar esta fase, como por ejemplo entrevistas, encuestas, recogida de información, etc. Es fundamental el apoyo de la dirección, el buen inicio de esta etapa garantiza el éxito del planteo de políticas de Seguridad.

Establecer el alcance

Una vez delimitada el contexto y teniendo los primeros requerimientos de seguridad se determinará cuál será el aspecto a mejorar a través de las políticas de seguridad con sus controles respectivos, se recomienda que el alcance abarque a toda la institución, o en algunos casos se empiece por el departamento de tics.

Responsables de la gestión de los activos

Los activos de una organización son todos los activos que tienen valor para ella. Así, los activos de información son todos los procesos, personas, dispositivos, software o archivos que los contienen, procesan o gestionan de alguna forma.

Deben identificarse claramente los pasivos contra los activos de una organización, que pueden ser hardware, dispositivos móviles, aplicaciones, instalaciones, servicios e información. Esto le facilitará el seguimiento a lo largo de la vida útil del activo.

Esto nos facilitará el seguimiento de la implementación de las iniciativas implementadas, así como el análisis y la recopilación de información.

Valoración inicial

Un buen comienzo significa una evaluación inicial de la situación actual de la organización para determinar los controles y requisitos apropiados, que pueden ser de algún tipo (técnicos, legales u organizativos) para contrarrestar los riesgos de seguridad de la información.

Una vez que los controles de seguridad están en su lugar, se debe permitir un período de tiempo para medir su madurez, que se refiere a la efectividad de los controles para reducir el riesgo que la organización tiene que enfrentar.

Modelo de madurez

Como guía, podemos comenzar con los cinco niveles de la Escala de Madurez de Competencias de la siguiente manera:

Tabla 9, Modelo de madures de las salvaguardas implantadas

Inexistente	El control de seguridad en el sistema de TI no está implementado.	0
Inicial	Existen reglas o controles de seguridad, pero no se administran, no existe un proceso formal de aplicación y su adopción depende de la buena voluntad de los empleados.	1
Repetible	Las medidas de seguridad se implementan de manera completamente informal (con sus propios procedimientos informales). La responsabilidad es personal. No está lloviendo.	2
Definido	Los controles se implementan de acuerdo con procedimientos documentados, pero sin la aprobación del director de seguridad o del comité de gestión.	3
Administrado	Los controles se realizan de acuerdo con procedimientos documentados, aprobados y formales.	4
Optimizado	Los controles se aplican de acuerdo con procedimientos documentados, validados y distribuidos, cuya eficacia se mide periódicamente en auditorías informatizadas.	5

Fuente: (CIBERSEGURIDAD, 2018)

Análisis de cumplimiento

Para verificar el cumplimiento de las políticas de seguridad, se deben realizar encuestas, reuniones y monitoreo de la gestión de la información para evaluar el cumplimiento de los controles implementados.

Es importante registrar todas las incidencias y problemas detectados durante la evaluación, se medirá también cuánto o qué nivel de aplicación (nivel de madurez de los controles) real mantienen los trabajadores, para ello, es útil emplear tablas y listas de verificación que contengan aspectos que deben revisarse y verificarse.

Establecer los objetivos

Una vez de realizado el análisis de cumplimiento se obtendrá cuáles son los puntos a mejorar, y de acuerdo a estos la institución se enfocará que puntos aborda primero de acuerdo a la importancia de la seguridad de información.

Referencia la norma ISO/IEC 27002:2017.

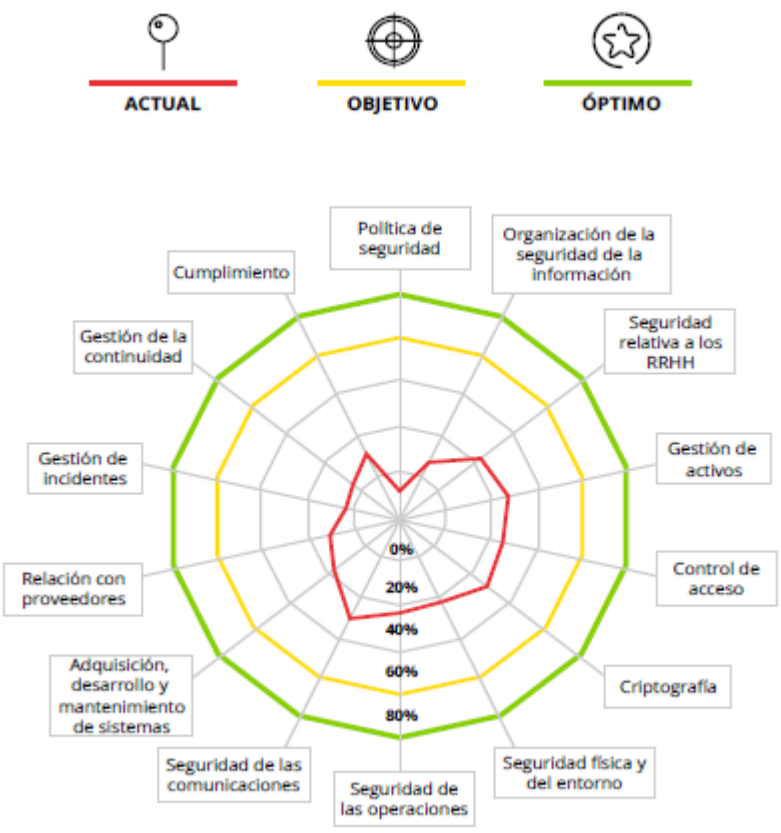


Gráfico 13, Ejemplo del resultado de la evaluación,

Fuente (CIBERSEGURIDAD, 2018)

La línea roja muestra el cumplimiento actual, la línea amarilla muestra los posibles objetivos de cumplimiento a mediano plazo y la línea verde muestra el cumplimiento óptimo.

Análisis de riesgos

Necesitábamos realizar un análisis de las amenazas que enfrenta nuestra organización. Como resultado de este análisis de riesgos, obtendremos una lista de amenazas con las que nos enfrentamos

Gráfico 14, Etapas del análisis de riesgos,

Fuente (CIBERSEGURIDAD, 2018)

Para realizar el análisis de riesgos de seguridad, utilizaremos la metodología Magerit v3, una vez implementada la metodología obtendremos un mapa de riesgos, que nos servirá de base para desarrollar el plan de seguridad estableciendo los controles mínimos para reducir el riesgo hasta un nivel aceptable por la DRTPE

Las políticas de seguridad de la información se crean para combatir las amenazas a la información de una organización. Esto se logra a través de controles de seguridad que deben verificarse periódicamente. Tenga en cuenta que cada organización determinará su política más conveniente y se asegurará de que cumpla con los requisitos reglamentarios aplicables.

Debe estimar el costo de sus propuestas de seguridad de la información e identificar un cronograma factible para su adopción.

2.2.9.1. Marco de Políticas para la Seguridad de la Información

Las políticas proporcionan un marco de referencia que proporciona la estructura (jerárquica) que debe gestionarse para lograr las finalidades de la organización.

Se definen en la política:

- El sujeto que aprueba la política de la empresa.
- Consecuencias del incumplimiento de la política.
- Mecanismos de gestión de excepciones.
- Comprobar y medir el cumplimiento de las políticas

Una política de seguridad de la información proporciona a una organización pautas detalladas para ayudar a desarrollar y hacer cumplir los principios que establecen estándares y normas; esto requiere un alto grado de compromiso por parte de las autoridades institucionales, además de la revisión y actualización periódica de la política identificada para determinar cómo evoluciona Los controles establecidos tienen fallas y debilidades.

Las políticas de seguridad de la información implementadas principalmente en las organizaciones públicas y privadas son:

- Política del Sistema de Gestión de Seguridad de la Información (SGSI).
- Política de control de acceso físico.
- Política de descarga de ficheros (red externa/interna).
- Política de estrategia de contingencia.
- Política de retención de documentos.
- Política para el uso de los servicios de Internet.
- Política de comunicación y uso de computadoras en movimiento.
- Política de teletrabajo.
- Política para el uso del control de contraseñas
- Política de cumplir con las normas exigidas por la ley.
- Política de uso de licencias de software.
- Política de privacidad y protección de datos

Adaptar las Políticas al Entorno de la Empresa

Las políticas y los marcos de políticas deben ser relevantes para los objetivos, la estrategia y el apetito de riesgo de la empresa, y se debe considerar la situación de la empresa, ya que depende del tipo de organización y el contexto en el que se encuentra. El contenido de la política debe determinarse.

Los factores a considerar al adaptar una política para su negocio incluyen:

- Solo se aplican las normas y reglamentos de la empresa.
- Requerimientos funcionales operativos de negocio.

- Demandas competitivas de propiedad intelectual y protección de datos.
- Políticas avanzadas existentes y protección de datos competitiva.
- Diseño único de la arquitectura TI de la empresa
- Regulaciones gubernamentales, etc.

Una vez que se implementa una política de seguridad de la información, debe evaluarse y actualizarse regularmente como parte del proceso de revisión.

2.2.9.2. Recomendaciones para la redacción de una política de seguridad de la información

Aquí hay un conjunto de recomendaciones para crear políticas de privacidad y seguridad de la información en las organizaciones:

- Una correcta política de seguridad debe perseguir un objetivo, debe especificar a quiénes afecta su aplicación, como impacta en los otros procesos de la institución
- Ser coherente con la legislación del país, respecto a la privacidad de la Información, tomando como referencia los estándares internacionales como la ISO 27001
- Definición de los roles para la correcta aplicación de las políticas
- Definición de las consecuencias a las que los trabajadores puedan estar inmersos por el no cumplimiento de estas
- Fecha que inicia la vigencia de las políticas.

2.2.9.3. Roles o Estructuras de la Seguridad de la Información

Cada entidad tiene un rol o estructura específica de seguridad de la información que, dependiendo de su tamaño y necesidades organizacionales, permite identificar a los sujetos adecuados para delegar el trabajo relacionado con la protección de información sensible, sistemas y procesos.

Tabla 10, Descripción de roles definidos en gestión de las políticas de seguridad de información dentro de la entidad

Director de la entidad	El director regional de Trabajo y Promoción del Empleo-Hco, será el responsable de aprobar la política de privacidad y los cambios futuros.
Comité de Gestión de Seguridad	El Comité de Seguridad de la Agencia Regional de Empleo y Promoción del Trabajo - Hco iniciará la planificación y coordinación de la operación del sistema de seguridad de la información y podrá recomendar otras actividades o proyectos según sea necesario para lograr los objetivos del sistema de seguridad de la DRTPE-Hco. Estará conformado por: El Administrador, el director de la oficina técnico administrativa, el asesor legal y el responsable del área de informática. Este comité será el órgano responsable de que las políticas de seguridad y los procedimientos y prácticas se cumplan y además se las adecuadas con los lineamientos y objetivos de la Institución
El director de la Oficina Técnica Administrativa	El director de la Oficina de Gestión de Tecnología deberá designar a una persona responsable de realizar reuniones periódicas, levantar actas, notificar a los miembros del comité e informar a cualquier persona que tenga solicitudes.
El especialista de Seguridad de la información	El oficial de seguridad de la información será responsable de coordinar la seguridad de la información en la planificación, operación, mantenimiento y verificación de las actividades que apoyen el desarrollo de la política de seguridad. Los expertos serán actores internos o externos seleccionados por el Comité de Gestión de Seguridad.
Responsable de Informática	El responsable de TI realizará funciones entre las que se encuentran los requisitos de seguridad informática establecidos para la operación, gestión y comunicación de los sistemas y recursos técnicos (clasificación de la información por nivel de reputación, de los documentos y facilitará el acceso según el nivel de seguridad que requiera su ubicación).
Responsable de RR HH	El director de Recursos Humanos será responsable de informar a todas las personas que ingresan sobre el cumplimiento de la Política de Seguridad de la Información y de las normas a las que se somete la entidad.

***Fuente**: "Elaboración Propia"*

Una vez establecido los roles para dar inicio al plan del proyecto de las políticas de seguridad de la información, según (CIBERSEGURIDAD, 2018):

Tabla 11, Esquema de proyecto de políticas de seguridad de la información

ID	PROYECTO	DESCRIPCION
01	Desarrollar e implementar políticas de seguridad.	Desarrollo e implementación de políticas de seguridad en los siguientes proyectos: a) Compromiso de gestión b) Uso del correo electrónico e Internet. c) Usando un dispositivo móvil. d) Protección de Datos.
02	Implementar el programa de concientización sobre seguridad de la información	Llevar a cabo sesiones de formación y concientización a todos los integrantes de la organización
03	Desarrollar política de gestión de incidentes de seguridad	Definir, documentar e implantar un proceso para la gestión de incidentes de seguridad
04	Desarrollar políticas de acceso de información	Precisar, documentar e implementar procesos de gestión de acceso o información en función de tipo de función desempeñada y da información requerida.
05	Desarrollar políticas de copias de seguridad	Analice la información e implemente una estrategia de respaldo, lo que significa realizar restauraciones periódicas.
06	Clasificación de la información	Precisar un sistema de clasificación de la información que contemple al menos tres niveles de seguridad (público, privado y confidencial)
07	Definir los aspectos generales para que la entidad realice auditorias en el futuro	Definir un proceso para realizar futuras auditorias del cumplimiento de políticas de seguridad.

Fuente: (CIBERSEGURIDAD, 2018)

2.2.9.4. Métricas de seguridad

Son aquellas que proveen mediciones o valores concretos, sus características más importantes son:

- Fáciles de recolectar
- Expresadas en números o porcentajes
- Detalladas con unidades de medida, relevante para la toma de decisiones

Para el desarrollo de esta investigación va a estar en torno a los incidentes que se presentan en la entidad, a nivel de Confidencialidad, Integridad, Disponibilidad, Autenticidad, Trazabilidad.

Tabla 12, Métricas de la seguridad de información

¿Cuál es el nivel de confianza en de la organización en temas de seguridad informática – Políticas de Seguridad? % de empleados que adquieren conocimientos en temas de seguridad, nivel de conocimiento, del total de empelados	**Medir el Desempeño de la concientización de los usuarios en los temas de seguridad de la información**
¿Qué tan efectivas son las políticas de seguridad de información? % de reducción de los riesgos en las dimensiones de seguridad de la información ¿Cuál es el nivel de cumplimiento de las políticas de seguridad? N° del modelo de madurez de la Política de Seguridad de información	**Desempeño de las políticas de Seguridad de la información**
¿Qué tipos de incidentes se presentan en la organización? N° de incidentes asociados con la confidencialidad/Total de incidentes N° de incidentes asociados con la disponibilidad/Total de incidentes N° de incidentes asociados con la integridad/Total de incidentes N° de incidentes asociados con la Autenticidad/Total de incidentes N° de incidentes asociados con la Trazabilidad/Total de incidentes	**Desempeño de la administración de incidentes de seguridad**

Fuente: (CIBERSEGURIDAD, 2018)

2.3. Marco Situacional

Organigrama de la Dirección Regional de Trabajo y Promoción del Empleo – Hco

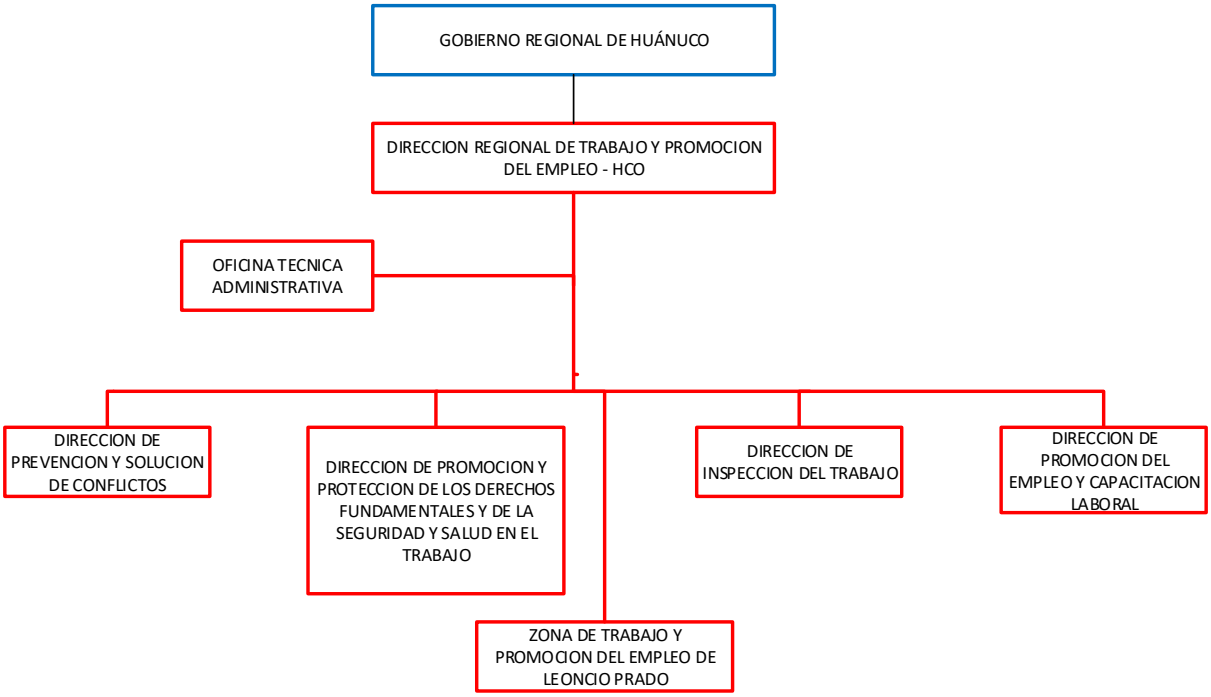


Gráfico 15, Organigrama DRTPE

Fuente: *Dirección Regional de Trabajo y Promoción del Empleo Dirección: Jirón Mayro N° 379*

En resumen, la DRTPE, brinda orientación y asesoría en temas laborales, seguridad, salud en el trabajo, a través de los diferentes profesionales, establecidas en las 6 sub áreas que la conforman, donde brindan los siguientes servicios de:

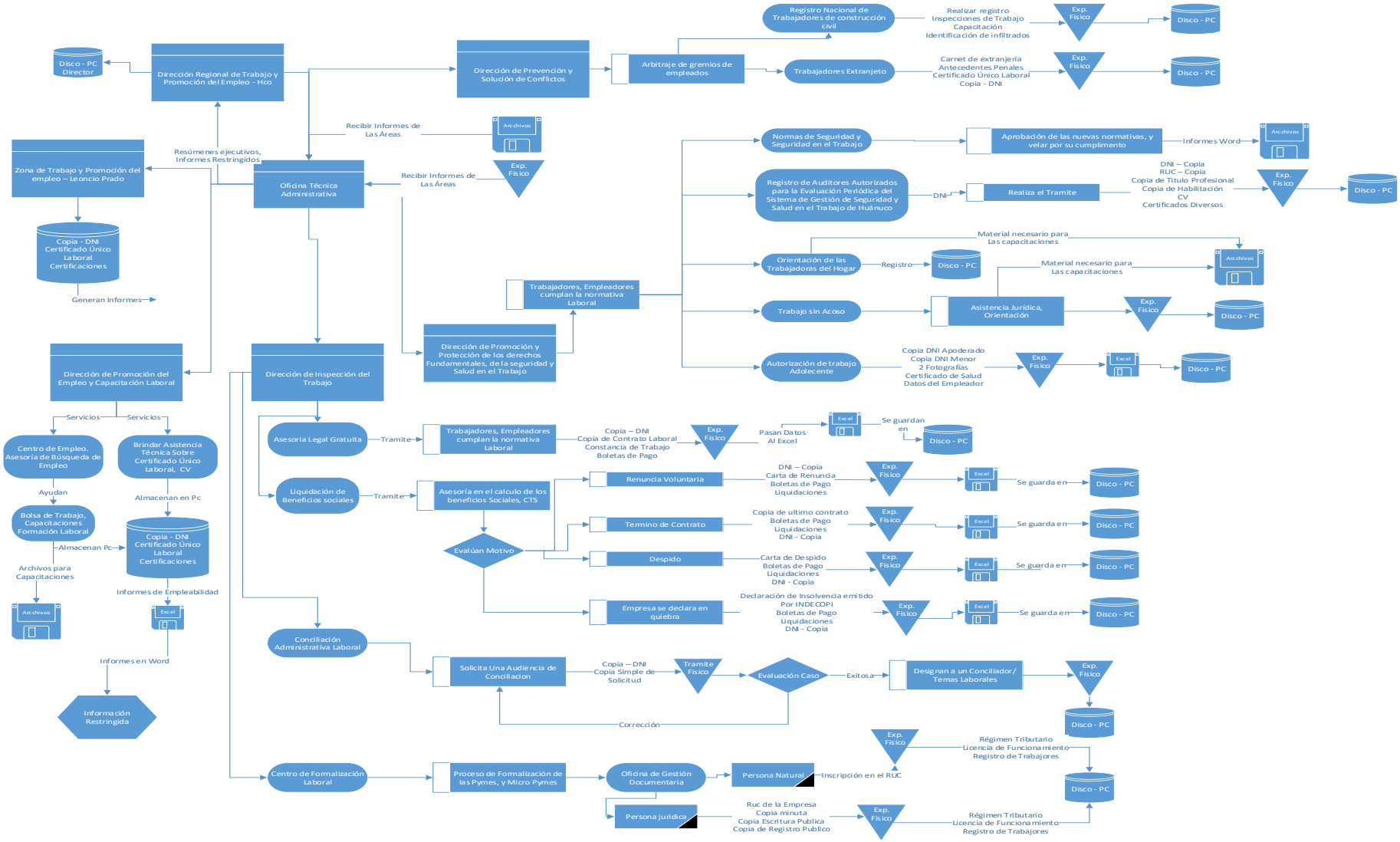
- Orientación sobre formalización laboral
- Certificado único Laboral (CertiJoven - CertiAdulto)
- Orientación Vocacional e Información Ocupacional
- Orientación sobre seguridad y salud en el trabajo

Así como asesoría y defensa legal gratuita, además de orientación sobre los derechos del trabajador, conciliación administrativa laboral, se pueden realizar los siguientes tramites de:

- Autorización de trabajo adolescente
- Registro de Organizaciones Sindicales
- Registro de empresas de Personal con Discapacidad
- Registro de Empresas de Intermediación Laboral (Contrato de Services, de terceros), centro de empleo

Gráfico 16, Flujo de información en la DRTPE

Fuente: Elaboración Propia


Registro Nacional de Trabajadores de construcción civil
Realizar registro
Inspecciones de Trabajo
Capacitación
Identificación de infiltrados
Exp. Fisico
Disco - PC
Disco - PC Director
Dirección Regional de Trabajo y Promoción del Empleo - Hco
Dirección de Prevención y Solución de Conflictos
Arbitraje de gremios de empleados
Trabajadores Extranjeto
Carnet de extranjería
Antecedentes Penales
Certificado Unico Laboral
Copia - DNI
Exp. Fisico
Disco - PC
Recibir Informes de Las Áreas
Archivos
Exp. Fisico
Zona de Trabajo y Promoción del empleo – Leoncio Prado
Resúmenes ejecutivos, Informes Restringidos
Oficina Técnica Administrativa
Recibir Informes de Las Áreas
Normas de Seguridad y Seguridad en el Trabajo
Aprobación de las nuevas normativas, y velar por su cumplimento
Informes Word
Archivos
Registro de Auditores Autorizados para la Evaluación Periódica del Sistema de Gestión de Seguridad y Salud en el Trabajo de Huánuco
DNI
Realiza el Tramite
DNI – Copia
RUC – Copia
Copia de Titulo Profesional
Copia de Habilitación
CV
Certificados Diversos
Exp. Fisico
Disco - PC
Copia - DNI
Certificado Único Laboral
Certificaciones
Generan Informes
Material necesario para Las capacitaciones
Orientación de las Trabajadoras del Hogar
Registro
Disco - PC
Material necesario para Las capacitaciones
Archivos
Trabajadores, Empleadores cumplan la normativa Laboral
Trabajo sin Acoso
Asistencia Jurídica, Orientación
Exp. Fisico
Disco - PC
Dirección de Promoción y Protección de los derechos Fundamentales, de la seguridad y Salud en el Trabajo
Autorización de trabajo Adolecente
Copia DNI Apoderado
Copia DNI Menor
2 Fotografías
Certificado de Salud
Datos del Empleador
Exp. Fisico
Excel
Disco - PC
Dirección de Promoción del Empleo y Capacitación Laboral
Dirección de Inspección del Trabajo
Servicios
Servicios
Centro de Empleo. Asesoría de Búsqueda de Empleo
Brindar Asistencia Técnica Sobre Certificado Único Laboral, CV
Asesoria Legal Gratuita
Tramite
Trabajadores, Empleadores cumplan la normativa Laboral
Copia – DNI
Copia de Contrato Laboral
Constancia de Trabajo
Boletas de Pago
Exp. Fisico
Pasan Datos Al Excel
Excel
Se guardan en
Disco - PC
Ayudan
Almacenan en Pc
Liquidación de Beneficios sociales
Tramite
Asesoría en el calculo de los beneficios Sociales, CTS
Bolsa de Trabajo, Capacitaciones Formación Laboral
Almacenan Pc
Copia - DNI
Certificado Único Laboral
Certificaciones
Evalúan Motivo
Renuncia Voluntaria
DNI – Copia
Carta de Renuncia
Boletas de Pago
Liquidaciones
Exp. Fisico
Excel
Se guarda en
Disco - PC
Archivos para Capacitaciones
Informes de Empleabilidad
Termino de Contrato
Copia de ultimo contrato
Boletas de Pago
Liquidaciones
DNI - Copia
Exp. Fisico
Excel
Se guarda en
Disco - PC
Archivos
Excel
Despido
Carta de Despido
Boletas de Pago
Liquidaciones
DNI - Copia
Exp. Fisico
Excel
Se guarda en
Disco - PC
Empresa se declara en quiebra
Declaración de Insolvencia emitido Por INDECOPI
Boletas de Pago
Liquidaciones
DNI - Copia
Exp. Fisico
Excel
Se guarda en
Disco - PC
Informes en Word
Conciliación Administrativa Laboral
Solicita Una Audiencia de Conciliacion
Copia – DNI
Copia Simple de Solicitud
Tramite Fisico
Evaluación Caso
Exitosa
Designan a un Conciliador/ Temas Laborales
Exp. Fisico
Disco - PC
Información Restringida
Corrección
Exp. Fisico
Régimen Tributario
Licencia de Funcionamiento
Registro de Trabajores
Centro de Formalización Laboral
Proceso de Formalización de las Pymes, y Micro Pymes
Oficina de Gestión Documentaria
Persona Natural
Inscripción en el RUC
Disco - PC
Persona juridica
Ruc de la Empresa
Copia minuta
Copia Escritura Publica
Copia de Registro Publico
Exp. Fisico
Régimen Tributario
Licencia de Funcionamiento
Registro de Trabajores

Se observa en la entidad que existen falencias que se describen a continuación:

Divulgación no Autorizada: Existen tramites o expedientes que los trabajadores realizan según los servicios que requieran porque la DRTPE brinda múltiples servicios, por medio de entrevista y/o conversaciones con los mismos usuarios y/o trabajadores se mencionó que existe en determinados casos filtraciones de información en los casos de conciliaciones Laborales, como también en casos donde se ha denunciado Acoso Laboral, estos expedientes son tramitados de forma física como virtual, pero la DRTPE, almacena esta información en algunas computadoras, las cuales no tienen ni siquiera la autenticación por usuario y contraseña, lo cual es muy preocupante.

Ingeniería Social: No existe charlas o capacitaciones al personal sobre la seguridad de información que manejan, como también no existe políticas de seguridad definidas para estos casos, al no haber recibido capacitación alguna, lo más relevante que se observo es que las computadoras con las que cuenta la entidad no tiene instalado ningún programa de antivirus, lo que las hace muy vulnerables a la entrada de virus informáticos, que puedan corromper la información, así mismo se observó que el acceso a internet es libre y no tiene restricción alguna hacia cualquier página y/o aplicación, lo cual agrava el problema de seguridad de la información.

El encargado de informática nos comentó que existe un **uso inapropiado de los equipos informáticos** (computadoras de escritorio, Laptops, Tablet's), ya que no existe restricción al momento de ingresar al internet, una parte de los trabajadores de la entidad la usan para entrar a redes sociales, como a la descarga de series y música, lo que, al no haber ningún programa de antivirus, el equipo se infecta y daña la información almacenada, que en muchas ocasiones el encargado de informática tiene que formatear el equipo informático para solucionar el problema

2.4. Definición de términos básicos

estos son los términos básicos que se van a utilizar a lo largo del desarrollo del proyecto de tesis:

- **Aceptación del riesgo:** La decisión de aceptar el riesgo.
- **Activo:** Elementos vinculados con el sistema de información necesarios para el funcionamiento normal de la organización.
- **Amenaza:** Causa potencial de eventos inesperados que podrían dañar los sistemas o activos de TI.
- **Análisis de impacto**: "Estudio de las consecuencias que tendría una parada de X tiempo sobre la Organización"
- **Análisis de riesgo:** Utilice la información sistemáticamente para identificar las fuentes y estimar el riesgo. Reconocer los activos que requieren ser protegidos o valorados.
- **Confidencialidad:** Como resultado, la seguridad de la información asegura que los datos almacenados en el sistema no serán revelados a otras organizaciones o sujetos que no tengan derecho a acceder a la información.
- **Integridad:** Para que el sistema autentique, los datos no deben ser manipulados. Esto asegura que la información recopilada es correcta y no ha sido modificada, es decir, asegura la exactitud de nuestros datos.
- **Disponibilidad:** Que la información que tenemos sea fácilmente accesible para quienes dentro de la organización deban tener esa información
- **Autenticidad:** Se refiere a cuando una persona, entidad o fuente de la que proviene los datos sea veraz y real, la suplantación es el principal factor que pone en riesgo la autenticidad.
- **Trazabilidad:** El objetivo de esta característica es permitir que en todo momento se pueda determinar quién hizo qué y en qué momento, con la finalidad de poder conocer todos los incidentes y así poder analizarlos
- **Control:** Las medidas de gestión de riesgos, incluida la organización, las políticas, los procedimientos, las directrices, las prácticas o las estructuras, pueden ser de carácter administrativo, técnico, de gestión o legal.
- **Declaración de aplicabilidad:** Documentación que describe las finalidades de control y las medidas de control que son relevantes y aplicables a la entidad del SGSI.
- **Evaluación del riesgo:** El procedimiento de comparar el nivel de riesgo estimado durante un análisis de riesgo con criterios dados para determinar las ponderaciones de riesgo.
- **Evento de seguridad de información:** Este es un evento identificado del estado del sistema, servicio o red que indica una posible política de seguridad de la información o una falla de control o una situación previamente desconocida que puede estar relacionada con la seguridad.
- **Frecuencia (probabilidad de ocurrencia):** La posibilidad de que una amenaza se convierta en realidad, sin importar qué protecciones existan para hacer frente a la amenaza.
- **Gestión del riesgo:** Acciones coordinadas para dirigir y controlar la organización con respecto al riesgo. Por lo general, incluye evaluación de riesgos, tratamiento, aprobación y comunicación. Estas actividades se centran en gestionar la incertidumbre relativa de las amenazas detectadas.

- **Impacto:** Mide el daño a la propiedad debido al reconocimiento de amenazas
- **Incidente de seguridad de información:** Esto se indica mediante un solo incidente o una serie de eventos de seguridad de la información inesperados que tienen el potencial de impactar significativamente las operaciones comerciales y afectar la seguridad de la información.
- **Política:** Intención y dirección general expresada formalmente por la gerencia.
- **Probabilidad:** Se refiere a la mayor o menor posibilidad de que ocurra un suceso
- **Políticas de Seguridad:** Una política de seguridad es una norma y un proceso que rige cómo una organización previene, protege y administra el riesgo de dañar varias computadoras.
- **Riesgo:** Es la probabilidad de que ocurra un evento y la combinación de su ocurrencia.
- **Salvaguardas o contra medidas:** Son procesos o mecanismos técnicos o normativos para disminuir el nivel de peligro.
- **Tratamiento del riesgo:** Seleccionar e implementar salvaguardas y controles para modificar el procedimiento de gestión de riesgos.
- **Vulnerabilidad:** Ciertos estados inherentes al activo facilitan la ejecución de amenazas y hacen que el activo sea vulnerable a los ataques.
- **Magerit:** “Respuestas al llamado “Procedimiento de Gestión de los Riesgos” (Escuela Nacional de Seguridad, 2012)
- **No repudio:** “Evitar que una entidad que haya enviado o recibido información o intercambiados datos, alegue ante terceros que no los envió o no los recibió.” (Digital, 2017)
- **Información:** Es un conjunto de datos, que al unirse nos indica algo.
- **Software:** Son los sistemas operativos, programas y aplicaciones instaladas en los equipos informativos que reciben, procesan y transforman los datos.
- **Equipos informáticos:** Son dispositivos que contienen aplicaciones que permiten el mismo funcionamiento.
- **Instalaciones**: Son los lugares en los cuales están ubicados los equipos informáticos.
- **Redes:** Es la que ayuda a la comunicación y transportación de los datos, lo cual implica importancia de seguridad.
- **Personal:** Son los sujetos que tienen derecho a acceder a la información: administradores, desarrolladores, usuarios internos y externos, y demás empleados de la empresa, todos con diferentes niveles de acceso a la información.

2.4.1. Definición de acrónimos.

DRTPE: Dirección Regional de Trabajo y Promoción del Empleo.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

ISO: Organismo Internacional de Normalización.

COBIT: Control para sistemas de información y telecomunicaciones.

ITIL: Biblioteca de infraestructura de tecnología e información.

TI: tecnología de información.

CSAE: Consejo Superior de Administración Electrónica

GORECO: Gobierno Regional de Huánuco.

HCO: Huánuco.

III. MARCO METODOLÓGICO

3.1. Nivel y Tipo de Investigación

El nivel y tipo de estudio se detallan a continuación, de acuerdo a diversos autores se llega a lo siguiente:

- **Según el nivel de investigación:** Este estudio es explicativo ya que determinaremos el impacto del enfoque Magerit v3 para mejorar la seguridad de la información.

- **Según el tipo de la investigación:** En nuestro caso, esta aplicación aborda el problema que, al implementar la metodología Magerit v3 y NTP ISO-27001:2014, que aborda la estrategia de seguridad de la gestión de riesgos de activos informáticos, mejorará la seguridad de la información para nuestra investigación, brindando herramientas de gestión de riesgos en la información.

3.2. Diseño de la Investigación

Según (Sampieri, 2014) "Los **diseños cuasiexperimentales** también manipulan deliberadamente, al menos, una variable independiente para observar su efecto sobre una o más variables dependientes", es decir la experimentación permite controlar la variable dependiente según la influencia de la independiente, de esta forma, el análisis se realizará antes (pre-test) y después (post-test) al aplicar el método Magerit V3.
Donde:

Tabla 13, Información del Diseño

Símbolo	Descripción
G	Activos informáticos – Activos de información
O1	Pre - Observación, medición
O2	Post - Observación, medición
X	Estimulo

Fuente: elaboración propia

Esquema de la Investigación

En el diseño de pre prueba – post prueba:

G: O1 ---- X ---- O2

Tabla 14, Diseño de la investigación

Pre - Observación, Medición Análisis de la seguridad de la información	Estimulo (Implementación)	Post - Observación, medición Análisis de la seguridad de la información
O1	X	O2
Activos de información estado inicial	Metodología Magerit v3	Activos de información estado final

***Fuente**: Elaboración propia*

3.3. Determinación del Universo/Población

La población incluye los recursos informáticos de la Dirección Regional de Empleo y Promoción Laboral, divididos en 6 componentes:

Tabla 15, Universo – Población de estudio

Universo/Población	N°
Oficina técnica administrativa	12
Dirección de prevención y solución de conflictos	8
Dirección de promoción y protección de los derechos fundamentales y de la seguridad	10
Dirección de implementaciones de trabajo	8
Dirección de promoción del empleo y capacitación laboral	10
Zona de trabajo y promoción del empleo de Leoncio Prado	6
Total	52

Fuente: elaboración propia

N	**54**

3.4. Selección de la Muestra

Para la obtención de la muestra se aplicó un muestreo no pirobalística de ser por finalidad o conveniencia, se tuvo en cuenta todos los recursos de cómputo pertenecientes a la DRTPE - Hco

.

n	**54**

3.5. Técnicas e instrumentos de recolección de datos

Las herramientas que utilizamos para recopilar información para el desarrollo y análisis de la investigación son:

Tabla 16, Técnicas de recolección de datos

TÉCNICAS	INSTRUMENTOS
Revisión documental: Revise varios documentos de DRTPE, incluido el inventario de hardware y software, y varios documentos organizativos proporcionados por el propietario del sistema de gestión. Para entender el funcionamiento del sistema se tiene en cuenta el mecanismo de protección de la seguridad de la información al implementar el sistema, la estructura organizacional de la DRTPE, etc.	• Documentos Administrativos
La observación: **Se realizo la forma de como el personal de entidad maneja la información, así como los activos** .	• Fichas de Observación • Cámara fotográfica • Formato de Control
Encuesta: Instrumento elaborado con ítems y alternativas cerradas y/o abiertas de acuerdo a lo que se desea estudiar en la problemática	• Cuestionario
Entrevista: La entrevista con fines de investigación puede ser entendida como la conversación que sostendremos con los encargados de sistemas de la DRTPE	• Apuntes

***Fuente**: elaboración propia*

3.6. Procesamiento y presentación de datos

Para el proceso de data se analizarán los resultados de los proyectos medibles utilizando SPSS y Excel.

- Preparación de muestras en recursos de Excel 2016: la plantilla de Excel preparada se ajusta a los parámetros de la metodología Magerit v3 para que los datos de recursos puedan ingresarse, procesarse y analizarse.

- Proceso y presentación de respuestas de investigación. SPSS se empleará para el análisis y la prueba de hipótesis.

Mediante las técnicas ya mencionadas el procesamiento de datos y la información obtenida, podemos tener el contexto de la situación actual de la seguridad de la información en la DRTPE, de esta manera podremos conocer las soluciones, a nuestra problemática planteada.

IV. APLICACIÓN DE LA METODOLOGÍA MAGERIT V3

A continuación, se realizará un análisis de riesgo cuantitativo para tratar de entender qué y cuánto cuantificando de todos los aspectos posibles. Después de completar el análisis de riesgos, entrará en la fase de gestión de riesgos.

4.1. Análisis de Riesgo

Para llevar a cabo el proceso y aplicar adecuadamente la metodología Magerit V3, cuyo objetivo principal es identificar, estimar los activos y posibles amenazas al recurso, esta información se recolecta a través de entrevistas, consultorías, encuestas, postulaciones a los gerentes de TI, así como al personal administrativo de la Dirección Regional de Trabajo y Promoción del Empleo. El presente análisis se va a desarrollar a través de un análisis cuantitativo.

El análisis de riesgos incluye una serie de actividades que se describen a continuación:

4.1.1. Caracterización de Activos

En esta actividad se identificarán los activos relacionados con la gestión de la información y luego de este paso se evaluará cada activo por su relevancia para la entidad.

a) Identificación de activos

Tabla 17, Identificación de Activos de información, Lista de Activos – DRTPE – Hco

	N°	CAPA	CÓDIGO	ACTIVO	UN
ACTIVOS ESENCIALES [essential]	AED1	DATOS [data]	[mult]	Multimedia (Información de audio, videos, material de capacitación)	-
	AED2		[dgi]	Datos de gestión interna	-
	AED3		[dct]	Datos de las certificaciones	-
	AED4	INFORMACIÓN [info]	[doc]	Documentos	-
	AED5		[inf]	Informes	-
	AED6		[exp]	Expedientes	-
	AED7		[tram]	Trámites	-
	AED8		[ipu]	Información pública	-
	AED9		[ipe]	Información personal	-
	AED10		[icl]	Información restringida	-
	AED11		[rde]	Registro de datos de entrada, formato físico, Datos de control de acceso	-
	AED12	SERVICIO [service]	[sei]	Servicio de Internet	1
	AED13		[email]	Correo electrónico entidad - DRTPE-Hco	-

APLICACIONES INFORMÁTICAS [apps]	APS1	SOFTWARE [SW]	[ehs]	S.O Windows	**25**
	APS2		[afp]	Adobe flash player	**5**
	APS3		[sql]	SIGA (Sistema Integrado de Gestión Administrativa)	**1**
	APS4		[off]	Microsoft Office Professional 2016	**25**
	APS5		[msp]	Ms Project 2016	**25**
	APS6		[vis]	Visio	**25**
	APS7		[brw]	Navegador web Google Chrome	**25**
	APS8		[pwi]	Página web Institucional DRTPE - Hco (http://direcciontrabajo.regionhuanuco.gob.pe/)	**1**
	APS9		[bck]	Sistema de Backup (RESPALDOS)	**-**
EQUIPOS INFORMÁTICOS [einf]	EIH1	HARDWARE [HW]	[cde]	Computadoras de escritorio	**20**
	EIH2		[cpp]	Computadora personal portátil de 2.0 GHz - Laptop	**3**
	EIH3		[ipl]	Impresora Laser	**1**
	EIH4		[ipt]	Impresora de Inyección a tinta	**2**
	EIH5		[emcfc]	Equipo multifuncional copiadora fax impresor escáner de inyección a tinta color	**2**
	EIH6		[sva]	EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER Y/O FAX	**2**
	EIH7		[cpu]	Unidad Central de Proceso - CPU	**25**
	EIH8		[pm]	Placa madre o Motherboard	**25**
	EIH9			Lectores Ópticos	**25**
	EIH10			Memoria RAM	**25**
	EIH11			Disco Duro HDD	**25**
	EIH12			Tarjeta de Red, Grafica y sonido	**25**
	EIH13			Mouse	**25**
	EIH14			Teclado – Keyboard	**25**
	EIH15			Cámaras de Seguridad Fijas	**2**
	EIH16			Tableta Pad	**3**
	EIH17			Router	**4**
	EIH18			Monitor Led 21.5 in	**18**
	EIH19			Monitor Led PLANO	**4**
	EIH20			Pozo a Tierra	**1**
COMUNICACIONES	CRC1	REDES DE COMUNIC	[lan]	Red local LAN	**-**
	CRC2		[rpv]	Red privada virtual (Zoom) - corporativo - Pro	**1**

	CRC3		[rte]	Red telefónica	**1**
	CRC4		[wif]	Red inalámbrica - Access Point	**4**
	CRC5		[mob]	Telefonía móvil	**-**
SOPORTE DE INFORMACION [spi]	SPI1	**SOPORTE DE INFORMACION [spi]**	[dav]	Almacenamiento en la nube (Google Drive)	
	SPI2		[cdv]	CD / DVD	**-**
	SPI3		[pml]	Proyector multimedia	**1**
	SPI4		[usb]	Dispositivo USB - 8 GB	**8**
	SPI5		[aux]	cable adaptador USB 3.0 a SATA	**2**
	SPI6		[tjm]	Tarjeta de memoria	**2**
	SPI7		[hdv]	Hard drive - HDD - Externo	**3**
EQUIPAMIENTO AUXILIAR **[eax]**	EAE1	EQUIPAMIENTO **[aux]**	[ups]	Estabilizador de energía - Regulador de voltaje	**6**
	EAE2		[fal]	Fuentes de alimentación - Conectores	**-**
	EAE3		[cbl]	Cableado de red - CAT 6A	**-**
	EAE4		[mbl]	Mobiliario	**-**
	EAE6		[ib]	Identificador biométrico	
	EAE7		[cbl]	Cableado eléctrico	**-**
INSTALACIONES **[ins]**	INI1	INSTALACIONES **[L]**	[off]	Oficinas	**6**
	INI2		[slc]	Sala de orientaciones - Capacitaciones	**1**
	INI3		[sla]	Sala de atención	**2**
PERSONAL **[per]**	PSP1	PERSONAL **[P]**	[drt]	Director Regional de Trabajo y Promocion del Empleo	**1**
	PSP2		[dota]	Director de la Oficina Tecnico Administrativo	**1**
	PSP3		[dpsc]	Director de Prevencion y Solucion de Conflictos	**1**
	PSP4		[dss]	Director de promoción y protección de los derechos fundamentales y de la seguridad y salud en el trabajo	**1**
	PSP5		[dga]	Director de dirección de inspección del trabajo	**1**
	PSP6		[dpe]	Director de dirección de promoción del empleo y capacitación laboral	**1**
	PSP7		[dzl]	Director zona de trabajo y promoción del empleo de leoncio prado	**1**
	PSP8		[jrrhh]	Jefe de Recursos Humanos	**1**
	PSP9		[pa]	Personal Administrativo	**12**
	PSP10		[inf]	Encargado de Informática	**1**
	PSP11		[pct]	Personal encargado de brindar asistencia técnica y capacitaciones diversas	**5**

Fuente: Obtenido de la información y observación en campo

b) Valoración de Activos

En esta actividad se especificarán las dimensiones o aspectos en que el activo es valioso para la unidad y la valoración se hará de acuerdo a la siguiente tabla:

Tabla 18, Criterios de valoración de activos

VALOR			CRITERIO
10		Muy alto	Daño muy grave a la Entidad.
7	**9**	Alto	Daño grave a la Entidad.
4	**6**	Medio	Daño importante a la Entidad.
1	**3**	Bajo	Daño menor a la Entidad.
0		Despreciable	Irrelevante a efectos prácticos

Fuente: Magerit V3

Tabla 19, Dimensiones de seguridad

[D]	Recursos estén disponibles en el momento en que se necesiten	Disponibilidad
[I]	La información no puede ser manipulada en el proceso de envío	Integridad
[C]	Asegura el secreto de las comunicaciones	Confidencialidad
[A]	Enviada por quien aparece como emisor	Autenticidad
[N_R]	No puede negar la autoría del mensaje enviado	No repudio

Fuente: Magerit V3

A continuación, se muestra la tabla N° 20, de valoración de activos

	N°	CAPA	CÓDIGO	ACTIVO	UN	COSTO UNITARIO	COSTO TOTAL	DIMENSIONES				
								[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [essential]	AED1	DATOS [data]	[mult]	Multimedia (Información de audio, videos, material de capacitación)	-	-	-	6	6	3	6	4
	AED2		[dgi]	Datos de gestión interna	-	-	-	9	8	6	7	7
	AED3		[dct]	Datos de las certificaciones	-	-	-	7	6	6	6	5
	AED4	INFORMACIÓN [info]	[doc]	Documentos	-	-	-	8	7	6	10	8
	AED5		[inf]	Informes	-	-	-	9		5	7	6
	AED6		[exp]	Expedientes	-	-	-	8	8	7		5
	AED7		[tram]	Trámites	-	-	-	9	8	7	8	7
	AED8		[ipu]	Información pública	-	-	-	8	7	6	7	
	AED9		[ipe]	Información personal	-	-	-	9	8	7	8	8
	AED10		[icl]	Información restringida	-	-	-	9	8	7	8	7
	AED11		[rde]	Registro de datos de entrada, formato físico, Datos de control de acceso	-	-	-	7	5	3	6	3
	AED12	SERVICIO [service]	[sei]	Servicio de Internet	1	S/ 1,500.00	S/ 1,500.00	10	8	7	6	7
	AED13		[email]	Correo electrónico entidad - DRTPE-Hco	-	-	-	9	6	9	9	7
APLICACIONES INFORMÁTICAS [apps]	APS1	SOFTWARE [SW]	[ehs]	S.O Windows	25	$90.00	$2,250.00	8	5	2	7	5
	APS2		[afp]	Adobe flash player	5	S/ 25.00	S/ 125.00	4	3		4	
	APS3		[sql]	SIGA (Sistema Integrado de Gestión Administrativa)	1	-	-	6	6	7	8	6
	APS4		[off]	Microsoft Office Professional 2016	25	$78.00	$1,950.00	7	3	4	7	4
	APS5		[msp]	Ms Project 2016	25	S/ 24.00	S/ 600.00	3	4		3	
	APS6		[vis]	Visio	25	S/ 45.00	S/ 1,125.00	5	4	4	3	3
	APS7		[brw]	Navegador web Google Chrome	25	-	-	10	3	8	10	2
	APS8		[pwi]	Página web Institucional DRTPE - Hco (http://direcciontrabajo.regionhuanuco.gob.pe/)	1	S/ 1,500.00	S/ 1,500.00	9	7	6	7	6
	APS9		[bck]	Sistema de Backup (RESPALDOS)	-	-	-	7	9	4	6	4
EQUIPOS INFORMÁTICOS [einf]	EIH1	HARDWARE [HW]	[cde]	Computadoras de escritorio	20	$2,300.00	$46,000.00	10	9	9	7	4
	EIH2		[cpp]	Computadora personal portátil de 2.0 GHz - Laptop	3	$2,300.00	$6,900.00	10	9	8	7	4
	EIH3		[ipl]	Impresora Laser	1	$12,640.00	$12,640.00	9	7	7	7	4
	EIH4		[ipt]	Impresora de Inyección a tinta	2	$730.00	$1,460.00	9	9		3	
	EIH5		[emcfc]	Equipo multifuncional copiadora fax impresora escáner de inyección a tinta color	2	$879.15	$1,758.29	9	7		7	

	EIH6		[sva]	EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER Y/O FAX	2	$1,900.00	$3,800.00	9	7		7	
	EIH7		[cpu]	Unidad Central de Proceso – CPU	25	$1,350.00	$33,750.00	10	8	7	8	
	EIH8		[pm]	Placa madre o Motherboard	25	$260.00	$6,500.00	10	9	9		
	EIH9			Lectores Ópticos	25	$150.00	$3,750.00	7	7	8		
	EIH10			Memoria RAM	25	$180.00	$4,500.00	10	9	9		
	EIH11			Disco Duro HDD	25	$220.00	$5,500.00	9	7	8	6	
	EIH12			Tarjeta de Red, Grafica y sonido	25	$50.00	$1,250.00	8	7	8		
	EIH13			Mouse	25	$25.00	$625.00	9	7	6		
	EIH14			Teclado – Keyboard	25	$20.00	$500.00	9	7	6		
	EIH15			Cámaras de Seguridad Fijas	2	$559.00	$1,118.00	7	4	4		
	EIH16			Tableta Pad	3	$615.00	$1,845.00	10	9	9	7	
	EIH17			Router	4	$450.00	$1,800.00	10	8	9		
	EIH18			Monitor Led 21.5 in	18	$392.00	$7,056.00	7	8	8		
	EIH19			Monitor Led PLANO	4	$651.00	$2,604.00	7	7	8		
	EIH20			Pozo a Tierra	1	$980.00	$980.00	8	7			
COMUNICACIONES [ccm]	CRC1	REDES DE COMUNICACIÓN [scn]	[lan]	Red local LAN	-	-	-	9	7	9	3	
	CRC2		[rpv]	Red privada virtual (Zoom) - corporativo – Pro	1	S/ 561.30	S/ 561.30	9	8	7	5	
	CRC3		[rte]	Red telefónica	1	S/ 100.00	S/ 100.00	7	8	9	2	
	CRC4		[wif]	Red inalámbrica - Access Point	4	S/ 160.00	S/ 640.00	8	7	7	3	5
	CRC5		[mob]	Telefonía móvil	-	-		7	3	2	3	
SOPORTE DE INFORMACION [spi]	SPI1	SOPORTE DE INFORMACION [spi]	[dav]	Almacenamiento en la nube (Google Drive)				4	5	4		3
	SPI2		[cdv]	CD / DVD	-	-	-	2	3	3	4	
	SPI3		[pml]	Proyector multimedia	1	S/ 2,629.00	S/ 2,629.00	3	4			4
	SPI4		[usb]	Dispositivo USB - 8 GB	8	S/ 25.00	S/ 200.00	8	3	3	3	
	SPI5		[aux]	cable adaptador USB 3.0 a SATA	2	S/ 100.00	S/ 200.00	6				
	SPI6		[tjm]	Tarjeta de memoria	2	S/ 20.00	S/ 40.00	2		3	2	4
	SPI7		[hdv]	Hard drive - HDD – Externo	3	S/ 250.00	S/ 750.00	4	5	3	3	4
EQUIPAM	EAE1	EQUIPAM	[ups]	Estabilizador de energia - Regulador de voltaje	6	S/ 50.00	S/ 300.00	7	6		2	

	EAE2		[fal]	Fuentes de alimentación – Conectores	-	-	-	9	4	2	3	
	EAE3		[cbl]	Cableado de red - CAT 6 A	-	-	-	9	5		2	5
	EAE4		[mbl]	Mobiliario	-	-	-	5		4		3
	EAE6		[ib]	Identificador biométrico				7	5			2
	EAE7		[cbl]	Cableado eléctrico	-	-	-	7	5	2		
INSTALACIONES [ins]	INI1	INSTALACIONES [L]	[off]	Oficinas	6	-	-	8	5	3	8	
	INI2		[slc]	Sala de orientaciones - Capacitaciones	1	-	-	8	6	4	10	3
	INI3		[sla]	Sala de atención	2	-	-	8	5	4		
PERSONAL [per]	PSP1	PERSONAL [P]	[drt]	Director Regional de Trabajo y Promoción del Empleo	1	-	-	9	8	7	3	3
	PSP2		[dota]	Director de la Oficina Técnico Administrativo	1			9	8	7	3	3
	PSP3		[dpsc]	Director de Prevención y Solución de Conflictos	1			9	8	7	3	3
	PSP4		[dss]	Director de promoción y protección de los derechos fundamentales y de la seguridad y salud en el trabajo	1			9	8	7	3	3
	PSP5		[dga]	Director de dirección de inspección del trabajo	1			9	8	7	3	3
	PSP6		[dpe]	Director de dirección de promoción del empleo y capacitación laboral	1			9	8	7	3	3
	PSP7		[dzl]	Director zona de trabajo y promoción del empleo de leoncio prado	1			9	8	7	3	3
	PSP8		[jrrhh]	Jefe de Recursos Humanos	1			8	7	7		
	PSP9		[pa]	Personal Administrativo	12			8	7	8		
	PSP10		[inf]	Encargado de Informática	1			10	7	7		
	PSP11		[pct]	Personal encargado de brindar asistencia técnica y capacitaciones diversas	5			10	8	8		

Tabla 20, valoración de activos,

Fuente: "Elaboración Propia"

4.1.2. Caracterización de las Amenazas

Como parte de esta actividad, identificamos la amenaza que se puede presentar sobre el recurso y estimamos la frecuencia y la degradación que ocasiona.

a) Identificación de amenazas

El primer paso es el de reconocer las amenazas a las que están los activos, para ello se tomara en cuenta el listado de amenazas que nos ofrece la metodología, luego identificaremos las amenazas para nuestro caso de estudio, específicamente los activos de la entidad.
Las amenazas están clasificadas en 4 grupos:

- [N] Desastres Naturales
- [1] De origen industrial
- [E] Errores y fallos no intencionados
- [A]Ataque deliberados

Tabla 21, Identificación de Amenazas, DRTPE-Hco

N°		AMENAZA	DESCRIPCIÓN
DESASTRES NATURALES [N]	DN1	Fuego **[N.1]**	Incendios: posibilidad de que el fuego acabe con recursos del sistema, información física
	DN2	Daños por agua **[N.2]**	Inundaciones: posibilidad de que el agua acabe con recursos del sistema
	DN3	Tormentas Eléctricas **[N.3]**	Descarga natural de electricidad que afecte los recursos del sistema
	DN4	Fenómenos Climáticos **[N.4]**	Modificaciones del clima previsto como una amenaza específica
DE ORIGEN INDUSTRIAL [I]	OI1	Contaminación Electromagnética **[I1]**	Interferencias de radio, campos magnéticos, radiaciones térmicas
	OI2	Contaminación Mecánica **[I2]**	Vibraciones, polvo, suciedad, etc.
	OI3	Desastres Industriales **[I3]**	Sobrecarga eléctrica, explosiones, contaminación química
	OI4	Avería de origen físico o lógico **[I4]**	Fallos en los equipos, de funcionamiento del hardware o falla en los programas
	OI5	Corte del suministro eléctrico **[I5]**	Pérdida o cese de la alimentación de potencia
	OI6	Condiciones inadecuadas de temperatura o humedad **[I6]**	Fallas en la climatización, excediendo los márgenes de trabajo de los equipos
	OI7	Fallo de servicios de comunicaciones **[I7]**	Pérdida de los medios de telecomunicación, destrucción o detención de los medios o centros de conmutación
	OI8	Interrupción de otros servicios y suministros esenciales **[I8]**	Servicios o recursos de los que depende la operación de los equipos
	OI9	Degradación de los soportes de almacenamiento de la información **[I9]**	Avería o falla del funcionamiento como consecuencia del paso del tiempo

ERRORES Y FALLOS NO INTENCIONADOS [E]	EF1	Errores de los usuarios **[F1]**	Error de uso de los servicios o datos
	EF2	Errores del administrador **[F2]**	Error de uso de los responsables de instalación y operación
	EF3	Errores de monitorización (log) **[F3]**	Registros de actividades fallidos, incompletos, faltantes
	EF4	Errores de configuración **[F4]**	Privilegios de acceso, flujos de actividades, registro de actividad erróneos
	EF5	Deficiencias en la organización **[F5]**	Acciones del personal descoordinadas, errores por omisión
	EF6	Difusión de software dañino **[F6]**	Propagación de virus, spyware, gusanos, troyanos, etc.
	EF7	Errores de re - encaminamiento **[F7]**	Envío de información a través de una ruta, sistema o red incorrecta
	EF8	Errores de secuencia **[F8]**	Alteración accidental del orden de los mensajes transmitidos y almacenados en algún soporte informático
	EF9	Fugas de información **[F9]**	Transferencia o revelación accidental de información almacenada en algún soporte informático
	EF10	Destrucción de información **[F10]**	Pérdida accidental de información almacenada en algún soporte informático
	EF11	Vulnerabilidades de los programas (software) **[F11]**	Defectos en el código o funcionalidad de los programas
	EF12	Errores de mantenimiento o actualización de software **[F12]**	Defectos en los procedimientos o controles de actualización, perjuicio a la mantenibilidad del sistema de información
	EF13	Errores de mantenimiento o actualización de equipos o hardware **[F13]**	Defectos en los procedimientos o controles de actualización, perjuicio a la mantenibilidad del sistema de información
	EF14	Caída del sistema por agotamiento de recursos **[F14]**	Saturación o caída del sistema informático por carencia de recursos
	EF15	Pérdida de equipos **[F15]**	Pérdida de equipos y soportes de información
	EF16	Indisponibilidad del personal **[F16]**	Ausencia accidental del puesto de trabajo
ATAQUES INTENCIONADOS [A]	AI1	Manipulación de la configuración **[A1]**	Configuración de procesos y flujos de actividades por personal no responsable del mismo
	AI2	Suplantación de la identidad del usuario **[A2]**	Usurpación de derechos y privilegios de acceso
	AI3	Abuso de privilegios de acceso **[A3]**	Abuso de derecho y nivel de privilegios ajenos a su competencia
	AI4	Uso no previsto **[A4]**	Utilización de los recursos del sistema para fines no previstos
	AI5	Difusión de software dañino **[A5]**	Propagación intencionada de virus, spyware, gusanos, troyanos, etc.
	AI6	Re - encaminamiento o alteración de mensajes **[A6]**	Envío o alteración del orden de los mensajes transmitidos
	AI7	Acceso no autorizado **[A7]**	Acceso y uso ilícito de los recursos del sistema
	AI8	Monitorización de tráfico **[A8]**	Extrae contenido de las comunicaciones: destino, volumen, frecuencia de los intercambios

	AI9	Repudio **[A9]**	Negación de acciones: de origen, de recepción o de entrega
	AI10	Interceptación de información **[A10]**	Escucha pasiva de información que no le corresponde
	AI11	Modificación deliberada de la información **[A11]**	Alteración intencional de la información
	AI12	Destrucción de información **[A12]**	Eliminación intencional de información
	AI13	Divulgación de información **[A13]**	Divulgación, geolocalización y copia ilegal de software
	AI14	Manipulación de programas **[A14]**	Alteración intencionada del funcionamiento de los programas
	AI15	Manipulación de los equipos **[A15]**	Sabotaje del hardware
	AI16	Robo **[A16]**	Sustracción de hardware
	AI17	Ataque destructivo **[A17]**	Destrucción de hardware o de soportes
	AI18	Ocupación enemiga **[A18]**	Locales invadidos y falta de control sobre los equipos
	AI19	Indisponibilidad del personal **[A19]**	Daño a la disponibilidad del personal
	AI20	Extorsión **[A20]**	Consiste en obligar a una persona a realizar un acto involuntario a través de medios tecnológicos
	AI21	Ingeniería social **[A21]**	Abuso de la buena fe de las personas para que realicen actividades que interesan a terceros

Fuente: Magerit v3, Libro II – Catalogo

b) Valoración de las amenazas

Como parte de esta actividad, estimar la probabilidad (en %) de ocurrencia y degradación de la realización de la amenaza por recurso identificado.

Tabla 22, Probabilidad de Ocurrencia amenaza

PROBABILIDAD DE OCURRENCIA	
1	Muy raro
2	Improbable
3	Posible
4	Probable
5	Prácticamente segura

Fuente: Magerit v3, Libro II – Catalogo

DEGRADACIÓN %		
Despreciable	**0%**	**10%**
Bajo	**20%**	**30%**
Medio	**40%**	**60%**
Alto	**70%**	**80%**
Muy Alto	**90%**	**100%**

Fuente: Magerit v3, Libro II – Catalogo

De acuerdo a estos parámetros, se procede a la identificación de amenazas por cada activo, asignándole una probabilidad de ocurrencia, así como la degradación del activo en caso se materialice la amenaza, a continuación, se muestra la siguiente tabla N° 23 de caracterización de amenazas por cada activo.

	N°	CODIGO	ACTIVO	PROB DE OCURRENCIA DE MATERIALIZACION DE AMENAZAS	DEGRADACION EN LAS DIMENCIONES				
					[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [esencial]	AED1	[mult]	Multimedia (Información de audio, videos, material de capacitación)	3	**50%**	**70%**	**70%**	**60%**	**50%**
		OI9	Degradación de los soportes de almacenamiento de la información [I9]	4		70%			50%
		EF8	Errores de secuencia [F8]	3	20%	20%	70%		30%
		AI4	Uso no previsto [A4]	4	50%	40%			
		EF10	Destrucción de información [F10]	2		50%			
		AI11	Modificación deliberada de la información [A11]	4	20%	70%	20%	60%	
	AED2	[dge]	Datos de gestión interna	**3**	**80%**	**70%**	**70%**	**70%**	**20%**
		AI11	Modificación deliberada de la información [A11]	3		50%	30%	70%	
		OI8	Interrupción de otros servicios y suministros esenciales [I8]	2	80%	40%			
		EF10	Destrucción de información [F10]	4	40%	70%	30%		
		AI13	Divulgación de información [A13]	4			70%	20%	20%
	AED3	[mul]	Datos de las certificaciones	**4**	**40%**	**40%**	**90%**	**40%**	**30%**
		AI11	Modificación deliberada de la información [A11]	5		20%	90%		
		OI9	Degradación de los soportes de almacenamiento de la información [I9]	3	40%	40%			
		AI4	Uso no previsto [A4]	5	40%			40%	
		EF7	Errores de re – encaminamiento [F7]	3		40%	30%		30%
	AED4	[doc]	Documentos	**4**	**60%**	**60%**	**50%**	**80%**	**40%**
		AI13	Divulgación de información [A13]	4			50%	80%	40%
		EF10	Destrucción de información [F10]	3	30%	60%	40%		
		OI9	Degradación de los soportes de almacenamiento de la información [I9]	4	60%	50%			
	AED5	[inf]	Informes	**2**	**20%**	**40%**	**70%**	**80%**	**30%**
		EF9	Fugas de información [F9]	3	10%		70%	80%	30%
		DN1	Fuego [N.1]	1	20%	40%			

AED6	[exp]	**Respaldos Backup - Expedientes**	**3**	**60%**	**40%**	**50%**	**30%**	**30%**
	DN1	Fuego [N.1]	**1**	**20%**	**40%**			
	EF1	Errores de los usuarios [F1]	5	60%	30%		30%	30%
	OI9	Degradación de los soportes de almacenamiento de la información [I9]	4			50%		
AED7	[tram]	**Trámites**	**4**	**70%**	**50%**	**60%**	**50%**	**30%**
	EF10	Destrucción de información [F10]	4	70%	50%		30%	30%
	EF9	Fugas de información [F9]	3			60%	50%	
	AI4	Uso no previsto [A4]	5	70%				
AED8	[ipu]	**Información pública**	**4**	**70%**	**30%**	**40%**	**30%**	**40%**
	EF1	Errores de los usuarios [F1]	4		30%		30%	40%
	EF9	Fugas de información [F9]	4	70%	30%	40%	20%	
	EF5	Deficiencias en la organización [F5]	4	40%		20%		
AED9	[ipe]	**Información personal**	**4**	**70%**	**60%**	**50%**	**40%**	**50%**
	EF9	Fugas de información [F9]	2	50%		50%	40%	50%
	EF10	Destrucción de información [F10]	5	70%	50%	20%		
	AI3	Abuso de privilegios de acceso [A3]	4	50%	60%	40%		
AED10	[icl]	**Información restringida**	**4**	**70%**	**70%**	**50%**	**30%**	**40%**
	AI4	Uso no previsto [A4]	4	70%	70%		30%	
	EF9	Fugas de información [F9]	4	30%		50%	20%	40%
	EF10	Destrucción de información [F10]	4	60%	50%	20%		
AED11	[log]	**Registro de datos de entrada, formato físico, digital Datos de control de acceso**	**3**	**30%**	**30%**	**0%**	**0%**	**10%**
	EF16	Indisponibilidad del personal [F16]	2	20%	30%			10%
	EF12	Errores de mantenimiento o actualización de software [F12]	3	30%	20%			10%
AED12	[sei]	**Servicio de Internet**	**4**	**90%**	**50%**	**70%**	**70%**	**30%**
	EF7	Errores de re – encaminamiento [F7]	5	20%			70%	30%

		OI4	Avería de origen físico o lógico [I4]	2	60%	50%			20%
		OI5	Corte del suministro eléctrico [I5]	4	70%		40%		
		OI7	Fallo de servicios de comunicaciones [I7]	4	40%		40%		
		EF14	Caída del sistema por agotamiento de recursos [F14]	4	90%	50%	70%		
	AED13	[email]	**Correo electrónico entidad - DRTPE-Hco**	**3**	**70%**	**90%**	**70%**	**60%**	**60%**
		EF1	Errores de los usuarios [F1]	3	40%	20%	40%	30%	30%
		OI4	Avería de origen físico o lógico [I4]	2	60%	30%			
		OI7	Fallo de servicios de comunicaciones [I7]	4	70%	60%			
		EF6	Difusión de software dañino [F6]	5	50%	90%	70%	60%	60%
		EF7	Errores de re – encaminamiento [F7]	4	60%	60%	50%	50%	40%
		EF8	Errores de secuencia [F8]	3	60%		70%		50%
		OI8	Interrupción de otros servicios y suministros esenciales [I8]	3	50%	40%			
APLICACIONES INFORMÁTICAS **[apps]**	APS1	[ehs]	S.O Windows	**3**	**60%**	**60%**	**70%**	**60%**	**50%**
		OI4	Avería de origen físico o lógico [I4]	4	20%	20%			
		AI4	Uso no previsto [A4]	3	40%				
		AI7	Acceso no autorizado [A7]	2	60%		50%		
		EF6	Difusión de software dañino [F6]	4	60%	60%	70%	60%	50%
		EF2	Errores del administrador [F2]	4	30%	50%	40%	10%	
	APS2	[sql]	SIGA (Sistema Integrado de Gestión Administrativa)	**4**	**80%**	**30%**	**30%**	**20%**	**40%**
		EF11	Vulnerabilidades de los programas (software) [F11]	4	40%	30%			
		EF9	Fugas de información [F9]	3	80%		30%	20%	40%
		EF14	Caída del sistema por agotamiento de recursos [F14]	4	40%			10%	
	APS3	[mac]	Microsoft Office Professional 2016	**4**	**70%**	**90%**	**50%**	**60%**	**40%**
		AI1	Manipulación de la configuración [A1]	3	70%	90%		60%	40%
		EF12	Errores de mantenimiento o actualización de software [F12]	5	30%	20%	50%	20%	
	APS4	[off]	Ms Project 2016	3	**40%**	**40%**	**50%**	**40%**	**10%**

		EF11	Vulnerabilidades de los programas (software) [F11]	3	40%	40%		40%	
		EF12	Errores de mantenimiento o actualización de software [F12]	3	20%		50%		10%
	APS5	[msp]	Visio - 2016	3	40%	40%	50%	40%	10%
		EF11	Vulnerabilidades de los programas (software) [F11]	3	40%	40%		40%	
		EF12	Errores de mantenimiento o actualización de software [F12]	3	40%		50%	20%	10%
	APS6	[brw]	Navegador web Google Chrome	**4**	**100%**	**80%**	**90%**	**100%**	**50%**
		EF11	Vulnerabilidades de los programas (software) [F11]	4	100%	80%	90%	100%	50%
		EF12	Errores de mantenimiento o actualización de software [F12]	4	70%				
	APS7	[msp]	Página web Institucional DRTPE - Hco (http://direcciontrabajo.regionhuanuco.gob.pe/)	**3**	**80%**	**70%**	**40%**	**20%**	**20%**
		AI1	Manipulación de la configuración [A1]	3	50%	60%	40%	20%	
		AI7	Acceso no autorizado [A7]	3	80%	70%			20%
		EF14	Caída del sistema por agotamiento de recursos [F14]	2	60%				
		EF11	Vulnerabilidades de los programas (software) [F11]	4	70%	40%	30%		
EQUIPOS INFORMÁTICOS **[einf]**	EIH1	[tlp]	Computadoras de escritorio	**4**	**70%**	**50%**	**70%**	**20%**	**50%**
		OI3	Desastres Industriales [I3]	2	30%		30%		
		OI2	Contaminación Mecánica [I2]	3	50%			20%	
		OI4	Avería de origen físico o lógico [I4]	5	70%	40%			
		OI5	Corte del suministro eléctrico [I5]	4	50%				
		AI1	Manipulación de la configuración [A1]	4	60%	50%	60%		50%
		AI15	Manipulación de los equipos [A15]	5	60%		60%		20%
		EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	5	60%	20%			
		AI16	Robo [A16]	3	60%		70%		10%
	EIH2	[ipm]	Computadora personal portátil de 2.0 GHz - Laptop	**3**	**90%**	**50%**	**80%**	**60%**	**50%**
		OI3	Desastres Industriales [I3]	2	30%		30%		
		OI2	Contaminación Mecánica [I2]	3	50%			40%	

	OI4	Avería de origen físico o lógico [I4]	4	70%	40%				
	OI5	Corte del suministro eléctrico [I5]	4	50%					
	AI1	Manipulación de la configuración [A1]	3	60%	50%	60%	60%	50%	
	AI15	Manipulación de los equipos [A15]	4	60%		60%		20%	
	EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	90%	20%				
	AI16	Robo [A16]	2	60%		80%		10%	
EIH3		Impresora laser	**3**	**80%**	**50%**	**60%**	**20%**	**0%**	
	OI3	Desastres Industriales [I3]	2	30%		30%			
	OI2	Contaminación Mecánica [I2]	3	50%			20%		
	OI4	Avería de origen físico o lógico [I4]	5	80%	40%				
	OI5	Corte del suministro eléctrico [I5]	4	50%					
	AI1	Manipulación de la configuración [A1]	3	60%	50%	60%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	80%	20%				
EIH4	[sva]	Impresora de inyección de tinta	**3**	**80%**	**50%**	**60%**	**20%**	**0%**	
	OI3	Desastres Industriales [I3]	2	30%		30%			
	OI2	Contaminación Mecánica [I2]	3	50%			20%		
	OI4	Avería de origen físico o lógico [I4]	5	80%	40%				
	OI5	Corte del suministro eléctrico [I5]	4	50%					
	AI1	Manipulación de la configuración [A1]	3	60%	50%	60%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	80%	20%				
EIH5	[swt]	Equipo multifuncional copiadora fax impresora escáner de inyección a tinta color	**3**	**80%**	**50%**	**60%**	**20%**	**0%**	
	OI3	Desastres Industriales [I3]	2	30%		30%			
	OI2	Contaminación Mecánica [I2]	3	50%			20%		
	OI4	Avería de origen físico o lógico [I4]	5	80%	40%				
	OI5	Corte del suministro eléctrico [I5]	4						

		AI1	Manipulación de la configuración [A1]	3	60%	50%	60%		
		EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	80%	20%			
	EIH6	[swt]	EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER Y/O FAX	**3**	**80%**	**50%**	**60%**	**20%**	**0%**
		OI3	Desastres Industriales [I3]	2	30%		30%		
		OI2	Contaminación Mecánica [I2]	3	50%			20%	
		OI4	Avería de origen físico o lógico [I4]	5	80%	40%			
		OI5	Corte del suministro eléctrico [I5]	4					
		AI1	Manipulación de la configuración [A1]	3	60%	50%	60%		
		EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	80%	20%			
	EIH7	[swb]	Unidad Central de Proceso – CPU	**3**	**70%**	**50%**	**60%**	**10%**	**20%**
		OI3	Desastres Industriales [I3]	3	30%		30%		
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	4	50%				
		OI2	Contaminación Mecánica [I2]	4	50%			10%	
		OI4	Avería de origen físico o lógico [I4]	4	70%	40%			
		AI15	Manipulación de los equipos [A15]	3	60%	50%	60%		20%
		EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	4	60%		60%		20%
		OI5	Corte del suministro eléctrico [I5]	3		20%			
		AI16	Robo [A16]	2	60%				
	EIH8		Placa madre o Motherboard	**3**	**60%**	**20%**	**60%**	**10%**	**10%**
		OI3	Desastres Industriales [I3]	3	30%		30%		
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	4	50%				
		OI2	Contaminación Mecánica [I2]	4	50%				
		OI4	Avería de origen físico o lógico [I4]	3	60%			10%	
		AI15	Manipulación de los equipos [A15]	4	50%				
		EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	50%	20%	60%		
		OI5	Corte del suministro eléctrico [I5]	4			60%		10%
		AI16	Robo [A16]	2	40%				

EIH9		Lectores Ópticos	**3**	**70%**	**20%**	**60%**	**10%**	**10%**
	OI3	Desastres Industriales [I3]	3	30%		30%		
	OI6	Condiciones inadecuadas de temperatura o humedad [I6]	4	50%				
	OI2	Contaminación Mecánica [I2]	4	50%				
	OI4	Avería de origen físico o lógico [I4]	3	60%			10%	
	AI15	Manipulación de los equipos [A15]	4	50%				
	EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	60%	20%	60%		
	OI5	Corte del suministro eléctrico [I5]	4					10%
	AI16	Robo [A16]	1	70%				
EIH10		Memoria RAM	**3**	**50%**	**20%**	**60%**	**10%**	**10%**
	OI3	Desastres Industriales [I3]	3	30%		30%		
	OI6	Condiciones inadecuadas de temperatura o humedad [I6]	4	50%				
	OI2	Contaminación Mecánica [I2]	4	50%				
	OI4	Avería de origen físico o lógico [I4]	3	50%			10%	
	AI15	Manipulación de los equipos [A15]	4	50%				
	EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	50%	20%	60%		
	OI5	Corte del suministro eléctrico [I5]	4					10%
	AI16	Robo [A16]	2	30%				
EIH11		Disco Duro HDD	**4**	**60%**	**70%**	**70%**	**10%**	**20%**
	OI3	Desastres Industriales [I3]	3	30%		30%		
	OI6	Condiciones inadecuadas de temperatura o humedad [I6]	4	50%				
	OI2	Contaminación Mecánica [I2]	4	50%				
	OI4	Avería de origen físico o lógico [I4]	3	60%			10%	
	AI13	Divulgación de información [A13]	4	50%	70%			20%
	EF12	Errores de mantenimiento o actualización de software [F12]	4	50%		60%		
	AI7	Acceso no autorizado [A7]	4	50%		70%		10%
	AI16	Robo [A16]	3	30%				

EIH12		Tarjeta de Red, Grafica y sonido	**3**	**60%**	**40%**	**0%**	**0%**	**0%**
	OI3	Desastres Industriales [I3]	3	30%				
	OI6	Condiciones inadecuadas de temperatura o humedad [I6]	4	50%	40%			
	OI2	Contaminación Mecánica [I2]	4	50%				
	OI4	Avería de origen físico o lógico [I4]	3	60%				
	AI15	Manipulación de los equipos [A15]	4	50%	30%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	60%	20%			
	OI5	Corte del suministro eléctrico [I5]	4	60%				
	AI16	Robo [A16]	1	30%				
EIH13		Mouse	**3**	**70%**	**30%**	**0%**	**0%**	**0%**
	OI3	Desastres Industriales [I3]	3	30%				
	OI2	Contaminación Mecánica [I2]	4	50%				
	OI4	Avería de origen físico o lógico [I4]	3	60%				
	AI15	Manipulación de los equipos [A15]	4	50%	30%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	60%	20%			
	OI5	Corte del suministro eléctrico [I5]	4	60%				
	AI16	Robo [A16]	2	70%				
EIH14		Teclado – KEYBOARD	**3**	**70%**	**30%**	**0%**	**0%**	**0%**
	OI3	Desastres Industriales [I3]	3	30%				
	OI2	Contaminación Mecánica [I2]	4	50%				
	OI4	Avería de origen físico o lógico [I4]	3	60%				
	AI15	Manipulación de los equipos [A15]	4	50%	30%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	60%	20%			
	OI5	Corte del suministro eléctrico [I5]	4	60%				
	AI16	Robo [A16]	2	70%				
EIH15		Cámara de seguridad Fija	**3**	**60%**	**0%**	**50%**	**0%**	**0%**
	OI3	Desastres Industriales [I3]	3	30%		40%		

		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	4	50%				
		OI2	Contaminación Mecánica [I2]	4	50%		50%		
		OI4	Avería de origen físico o lógico [I4]	3	60%				
		AI15	Manipulación de los equipos [A15]	4	50%				
		EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	60%				
		OI5	Corte del suministro eléctrico [I5]	4	60%				
		AI16	Robo [A16]	1	30%				
	EIH16		Tableta Pad	**4**	**70%**	**50%**	**50%**	**40%**	**40%**
		OI3	Desastres Industriales [I3]	3	30%				
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	4	50%	50%			
		OI2	Contaminación Mecánica [I2]	4	60%		20%		
		OI4	Avería de origen físico o lógico [I4]	3	60%				
		AI15	Manipulación de los equipos [A15]	4	70%		50%		
		EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	60%			40%	
		OI5	Corte del suministro eléctrico [I5]	4	60%				
		AI16	Robo [A16]	3	70%			40%	40%
	EIH17		Router	**4**	**90%**	**70%**	**50%**	**40%**	**20%**
		OI3	Desastres Industriales [I3]	4	30%				
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	4	50%				
		OI2	Contaminación Mecánica [I2]	4	50%	20%			
		OI4	Avería de origen físico o lógico [I4]	4	60%				
		AI15	Manipulación de los equipos [A15]	4	90%	70%			
		EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	80%			10%	
		OI5	Corte del suministro eléctrico [I5]	3	60%		50%		
		AI16	Robo [A16]	2	40%			40%	20%
	EIH18		Monitor LED 21.5 in	**3**	**70%**	**50%**	**40%**	**0%**	**10%**
		OI3	Desastres Industriales [I3]	3	30%				
		OI2	Contaminación Mecánica [I2]	4	50%				
		OI4	Avería de origen físico o lógico [I4]	3	60%	30%			

		AI15	Manipulación de los equipos [A15]	4	50%				10%
		OI5	Corte del suministro eléctrico [I5]	3	60%		40%		
		AI4	Uso no previsto [A4]	3		50%			
		AI16	Robo [A16]	1	70%				
	EIH19		Monitor Plano	**3**	**70%**	**50%**	**40%**	**0%**	**10%**
		OI3	Desastres Industriales [I3]	3	30%				
		OI2	Contaminación Mecánica [I2]	4	50%				
		OI4	Avería de origen físico o lógico [I4]	3	60%	30%			
		AI15	Manipulación de los equipos [A15]	4	50%				10%
		OI5	Corte del suministro eléctrico [I5]	3	60%		40%		
		AI4	Uso no previsto [A4]	3		50%			
		AI16	Robo [A16]	1	70%				
	EIH20		Pozo a Tierra	**3**	**70%**	**0%**	**40%**	**10%**	**0%**
		DN4	Fenómenos Climáticos [N.4]	3	50%				
		OI3	Desastres Industriales [I3]	3	30%				
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	4	50%			10%	
		OI2	Contaminación Mecánica [I2]	4	50%				
		OI4	Avería de origen físico o lógico [I4]	3	60%			10%	
		AI15	Manipulación de los equipos [A15]	3	40%				
		AI1	Manipulación de la configuración [A1]	4	50%				
		EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	60%		20%		
		OI5	Corte del suministro eléctrico [I5]	4	60%		40%		
		AI16	Robo [A16]	1	70%				
COMUNICACIONES [ccm]	CRC1	[lan]	Red local LAN	**4**	**80%**	**70%**	**50%**	**80%**	**30%**
		OI7	Fallo de servicios de comunicaciones [I7]	4	80%	40%	50%	80%	
		EF12	Errores de mantenimiento o actualización de software [F12]	4	20%	20%			20%
		EF14	Caída del sistema por agotamiento de recursos [F14]	3	20%				20%
		OI5	Corte del suministro eléctrico [I5]	4	60%	40%			
		OI4	Avería de origen físico o lógico [I4]	4	60%	70%	50%	40%	30%
	CRC3	[ptp]	Red privada virtual (Zoom) - corporativo - Pro	**4**	**50%**	**60%**	**40%**	**30%**	**40%**
		OI7	Fallo de servicios de comunicaciones [I7]	4	50%	50%	30%	10%	

	OI8	Interrupción de otros servicios y suministros esenciales [I8]	3	30%	60%			
	OI1	Contaminación Electromagnética [I1]	3	30%				
	EF4	Errores de configuración [F4]	4	40%	30%	40%	30%	40%
CRC4	[rte]	**Red telefónica**	**4**	**50%**	**50%**	**20%**	**20%**	**30%**
	OI7	Fallo de servicios de comunicaciones [I7]	3	50%				10%
	OI4	Avería de origen físico o lógico [I4]	4		50%	20%	20%	30%
CRC5	[wif]	**Red inalámbrica - Access Point**	**3**	**60%**	**50%**	**50%**	**30%**	**50%**
	EF4	Errores de configuración [F4]	3	40%	50%		10%	50%
	EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	3	40%	40%			
	OI1	Contaminación Electromagnética [I1]	3	40%				
	EF14	Caída del sistema por agotamiento de recursos [F14]	3	60%	40%	50%	30%	10%
CRC6	[mob]	**Telefonía móvil**	**3**	**60%**	**50%**	**40%**	**30%**	**20%**
	EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	4	40%	50%			
	OI1	Contaminación Electromagnética [I1]	3	40%	50%			
	EF7	Errores de re – encaminamiento [F7]	3	60%	50%	40%	30%	20%
SOPORTES DE INFORMACIÓN [spi]	SPI1	[dsk]	Almacenamiento en la nube (Google Drive)	**4**	**60%**	**50%**	**70%**	**30%**	**30%**
	OI8	Interrupción de otros servicios y suministros esenciales [I8]	2	30%	50%	30%	20%	30%
	AI4	Uso no previsto [A4]	4	20%	50%	30%	20%	30%
	AI2	Suplantación de la identidad del usuario [A2]	3			40%		20%
	AI13	Divulgación de información [A13]	4	40%	50%	70%	10%	10%
	EF7	Errores de re – encaminamiento [F7]	5	60%	50%	40%	30%	20%
	SPI2	[cdv]	CD / DVD	**4**	**50%**	**50%**	**40%**	**30%**	**20%**
	AI4	Uso no previsto [A4]	4	20%	50%	40%	30%	20%
	OI4	Avería de origen físico o lógico [I4]	3	50%				
	SPI3	[pml]	Proyector multimedia	**3**	**50%**	**40%**	**0%**	**0%**	**0%**
	OI4	Avería de origen físico o lógico [I4]	3	40%	0%	0%	0%	0%
	EF5	Deficiencias en la organización [F5]	2	30%				

	OI5	Corte del suministro eléctrico [I5]	4	50%	40%			
SPI4	[usb]	Dispositivo USB - 8 GB	**3**	**70%**	**60%**	**60%**	**40%**	**30%**
	AI4	Uso no previsto [A4]	4	20%	50%	30%	20%	30%
	EF5	Errores de los usuarios [F1]	4	30%	60%	60%	10%	20%
	EF6	Difusión de software dañino [F6]	3	70%	60%			
	OI4	Avería de origen físico o lógico [I4]	2	30%	40%			
	EF1	Errores de los usuarios [F1]	3	40%	30%	40%	40%	30%
SPI5	[tjm]	cable adaptador USB 3.0 a SATA	**3**	**60%**	**40%**	**0%**	**30%**	**0%**
	OI4	Avería de origen físico o lógico [I4]	3	20%	20%		30%	
	OI9	Degradación de los soportes de almacenamiento de la información [I9]	3	10%	40%			
	AI16	Robo [A16]	3	60%				
SPI6	[tjm]	Tarjeta de memoria	**3**	**50%**	**50%**	**50%**	**40%**	**30%**
	EF10	Destrucción de información [A12]	3	50%	40%	50%	30%	
	OI4	Avería de origen físico o lógico [I4]	2	30%	40%			
	EF1	Errores de los usuarios [F1]	3	40%	30%	40%	40%	30%
	EF6	Difusión de software dañino [F6]	3	50%	50%			
	AI4	Uso no previsto [A4]	4	20%	50%	30%	20%	30%
SPI7	[hdv]	Hard drive - HDD – Externo	**3**	**70%**	**60%**	**50%**	**40%**	**30%**
	EF10	Destrucción de información [F10]	3	50%	40%	50%	30%	
	EF1	Errores de los usuarios [F1]	3	40%	30%	40%	40%	30%
	OI4	Avería de origen físico o lógico [I4]	2	30%	40%			
	EF6	Difusión de software dañino [F6]	3	70%	60%			
	AI4	Uso no previsto [A4]	4	20%	50%	30%	20%	30%
EAE1	[ede]	Estabilizador de energía - Regulador de voltaje	**4**	**50%**	**70%**	**10%**	**80%**	**10%**
	OI7	Fallo de servicios de comunicaciones [I7]	3	50%	10%		10%	10%
	OI9	Degradación de los soportes de almacenamiento de la información [I9]	4	40%	70%	10%	80%	
	OI4	Avería de origen físico o lógico [I4]	4	50%	20%		10%	10%
EAE2	[fal]	Fuentes de alimentación – Conectores	**3**	**60%**	**50%**	**0%**	**0%**	**0%**
	OI4	Avería de origen físico o lógico [I4]	2	60%	50%			
	OI5	Corte del suministro eléctrico [I5]	3	50%	20%			
EAE3	[cbl]	Cableado de red - CAT 6 A	**3**	**70%**	**60%**	**40%**	**20%**	**10%**

EQUIPAMIENTO AUXILIAR [eax]

		OI1	Contaminación Electromagnética [I1]	3	40%	40%			
		OI7	Fallo de servicios de comunicaciones [I7]	4	50%	60%	40%	20%	10%
		OI3	Desastres Industriales [I3]	3	60%	50%			
		OI9	Degradación de los soportes de almacenamiento de la información [I9]	3	70%	50%			10%
		DN4	Fenómenos Climáticos [N.4]	3	40%	20%			
	EAE4	[mbl]	**Mobiliario**	**3**	**40%**	**30%**	**20%**	**0%**	**20%**
		OI9	Degradación de los soportes de almacenamiento de la información [I9]	3	40%	30%	20%		20%
		DN4	Fenómenos Climáticos [N.4]	2	20%	10%			
	EAE5	[eqc]	**Identificador biométrico**	**4**	**80%**	**50%**	**20%**	**80%**	**50%**
		OI4	Avería de origen físico o lógico [I4]	4	80%	50%	20%	80%	50%
		OI9	Degradación de los soportes de almacenamiento de la información [I9]	3	40%	30%	20%		20%
		OI5	Corte del suministro eléctrico [I5]	4	40%				
	EAE6	[cbl]	**Cableado eléctrico**	**4**	**60%**	**60%**	**40%**	**30%**	**20%**
		OI5	Corte del suministro eléctrico [I5]	4	60%				
		OI1	Contaminación Electromagnética [I1]	3		40%			10%
		OI4	Avería de origen físico o lógico [I4]	4	50%	60%	40%	30%	20%
INSTALACIONES [ins]	INI1	[off]	**Oficinas**	**2**	**80%**	**70%**	**40%**	**10%**	**40%**
		DN1	Fuego [N.1]	1	80%	70%	20%		
		AI4	Uso no previsto [A4]	3	20%	20%	40%	10%	40%
		OI2	Contaminación Mecánica [I2]	3	50%				
	INI2	[slc]	**Sala de orientaciones - Capacitaciones**	**3**	**50%**	**50%**	**40%**	**20%**	**40%**
		OI7	Fallo de servicios de comunicaciones [I7]	3	50%	40%		0%	0%
		AI4	Uso no previsto [A4]	3	20%	20%	40%		40%
		AI7	Acceso no autorizado [A7]	4	50%	50%	40%	20%	20%
	INI3	[sla]	**Sala de atención**	**4**	**70%**	**50%**	**40%**	**30%**	**40%**
		AI4	Uso no previsto [A4]	4	70%	20%	40%		40%
		OI2	Contaminación Mecánica [I2]	3	10%	50%		30%	10%
PERSONAL [per]	PSP1	[spt]	Director Regional de Trabajo y Promoción del Empleo	**4**	**80%**	**40%**	**70%**	**80%**	**20%**
		EF9	Fugas de información [F9]	3	30%		70%	10%	
		AI21	Ingeniería social [A21]	5	80%	40%	60%	80%	20%

	AI19	Indisponibilidad del personal [A19]	3	30%	30%				
PSP2	[jft]	Director de la Oficina Técnico Administrativo	**3**	**80%**	**60%**	**80%**	**80%**	**60%**
	AI19	Indisponibilidad del personal [A19]	3	30%	30%			
	AI3	Abuso de privilegios de acceso [A3]	4	80%	60%	80%	80%	60%
	EF9	Fugas de información [F9]	3	30%		70%	10%	
	AI21	Ingeniería social [A21]	3	30%	40%	60%	40%	20%
PSP3	[pnf]	Director de Prevención y Solución de Conflictos	**3**	**80%**	**40%**	**70%**	**80%**	**20%**
	AI19	Indisponibilidad del personal [A19]	3	30%	30%			
	EF9	Fugas de información [F9]	3	30%		70%	10%	
	AI3	Abuso de privilegios de acceso [A3]	4	80%		60%	80%	
	AI21	Ingeniería social [A21]	4	80%	40%	60%	40%	20%
PSP4	[pad]	Director de promoción y protección de los derechos fundamentales y de la seguridad y salud en el trabajo	**4**	**80%**	**40%**	**70%**	**80%**	**20%**
	AI19	Indisponibilidad del personal [A19]	3	30%	30%			
	EF9	Fugas de información [F9]	3	30%		70%	10%	
	AI3	Abuso de privilegios de acceso [A3]	4	80%		60%	80%	
	AI21	Ingeniería social [A21]	4	80%	40%	60%	40%	20%
PSP5	[sym]	Director de dirección de inspección del trabajo	**4**	**80%**	**40%**	**70%**	**80%**	**20%**
	AI19	Indisponibilidad del personal [A19]	3	30%	30%			
	EF9	Fugas de información [F9]	3	30%		70%	10%	
	AI3	Abuso de privilegios de acceso [A3]	4	80%		60%	80%	
	AI21	Ingeniería social[A21]	4	80%	40%	60%	40%	20%
PSP6	[mme]	Director de dirección de promoción del empleo y capacitación laboral	**4**	**80%**	**40%**	**70%**	**80%**	**20%**
	AI19	Indisponibilidad del personal [A19]	3	30%	30%			
	EF9	Fugas de información [F9]	3	30%		70%	10%	
	AI3	Abuso de privilegios de acceso [A3]	4	80%		60%	80%	
	AI21	Ingeniería social [A21]	4	80%	40%	60%	40%	20%
PSP7	[mmm]	Director zona de trabajo y promoción del empleo de leoncio prado	**4**	**80%**	**40%**	**70%**	**80%**	**20%**
	AI19	Indisponibilidad del personal [A19]	3	30%	30%			

		EF9	Fugas de información [F9]	3	30%		70%	10%	
		AI3	Abuso de privilegios de acceso [A3]	4	80%		60%	80%	
		AI21	Ingeniería social [A21]	4	80%	40%	60%	40%	20%
	PSP8	[opr]	Jefe de Recursos Humanos	**4**	**80%**	**50%**	**70%**	**80%**	**50%**
		AI19	Indisponibilidad del personal [A19]	3	30%	30%			
		EF9	Fugas de información [F9]	3	30%		70%	10%	
		AI3	Abuso de privilegios de acceso [A3]	4	80%		60%	80%	
		AI21	Ingeniería social [A21]	4	80%	40%	60%	40%	20%
		AI7	Acceso no autorizado [A7]	4		50%	40%	60%	50%
	PSP9	[lya]	Personal Administrativo	**4**	**80%**	**50%**	**70%**	**80%**	**50%**
		AI19	Indisponibilidad del personal [A19]	3	30%	30%			
		EF9	Fugas de información [F9]	3	30%		70%	10%	
		AI3	Abuso de privilegios de acceso [A3]	4	80%		60%	80%	
		AI21	Ingeniería social [A21]	4	80%	40%	60%	40%	20%
		AI7	Acceso no autorizado [A7]	4		50%	40%	60%	50%
	PSP10	[seg]	Encargado de Informática	**4**	**80%**	**50%**	**70%**	**80%**	**50%**
		AI19	Indisponibilidad del personal [A19]	3	30%	30%			
		EF9	Fugas de información [F9]	3	30%		70%	10%	
		AI3	Abuso de privilegios de acceso [A3]	4	80%		60%	80%	
		AI21	Ingeniería social [A21]	4	80%	40%	60%	40%	20%
		AI7	Acceso no autorizado [A7]	4		50%	40%	60%	50%
	PSP11	[ctr]	Personal encargado de brindar asistencia técnica y capacitaciones diversas	**4**	**80%**	**50%**	**70%**	**80%**	**50%**
		AI19	Indisponibilidad del personal [A19]	3	30%	30%			
		EF9	Fugas de información [F9]	3	30%		70%	10%	
		AI3	Abuso de privilegios de acceso [A3]	4	80%		60%	80%	
		AI21	Ingeniería social [A21]	4	80%	40%	60%	40%	20%
		AI7	Acceso no autorizado [A7]	4		50%	40%	60%	50%

Tabla 23, caracterización de amenazas por activo

Fuente: Elaboración Propia

4.1.3. Caracterización de las salvaguardas

Esta actividad consta de dos subtareas:

a) Identificación de las salvaguardas pertinentes

b) Valoración de las salvaguardas

El propósito de estas actividades es comprender qué necesitamos para proteger el sistema y ver si tenemos un sistema de protección que satisfaga nuestros requerimientos. Ambas actividades se van a catalogar en una sola tabla general, donde van a estar identificadas las salvaguardas que la entidad necesita para reducir los riesgos, así como la valoración de esas salvaguardas en referencia de su nivel de efectividad para reducir los riesgos.

Tabla Tipo de Protección salvaguarda

Tipo de Mecanismo de Protección	
1	Preventivo
2	Detectivo
3	Correctivo

Tabla 24 Grado de Implementación de la

0	No Implementado
1	Implementado

Tabla 25, Grado de Efectividad de la salvaguarda

Factor	Nivel	Significado
0%	L0 - Inexistente	Inexistente
10%	L1 - inicial	inicial / ad hoc
30%	L2 - reproducible	reproducible, pero intuitivo
50%	L3 - definido	proceso definido
75%	L4 - gestionado	gestionado y medible
95% - 100%	L5 - Optimizado	Optimizado

Fuente Magerit v3

A continuación, se hace un resumen del porque se escoge cada agrupamiento de salvaguardas, y a que amenazas combate

Se procede a explicar el agrupamiento de salvaguardas:

- **Protecciones Generales**: Se incluye este tipo de salvaguarda porque define los controles de identificación, autenticidad, monitorización de accesos.

- **Protección de los Servicios:** Este tipo de protección se incluye porque garantiza la disponibilidad, la gestión de cambios y utiliza perfiles de seguridad que se esfuerzan por brindar servicios de alta calidad.

- **Protección de las aplicaciones informáticas:** Se incluye este tipo de protección porque permite gestionar el uso y la seguridad del software empleado para prestar el servicio final.

- **Protección de los equipos informáticos**: Se considera este tipo de protección porque nos permite asegurar la disponibilidad, seguridad y mantenimiento de los equipos durante el cambio y operación.
- **Protección de las comunicaciones.** Se incluye este tipo de protección porque permite gestionar la integridad y confidencialidad de los datos intercambiados, el acceso a los servicios y perfiles de seguridad para garantizar la disponibilidad y el empleo justo de las conexiones entrantes y salientes.
- **Protección de los soportes de información**: Este tipo de protección se incluye porque le permite administrar la seguridad de los dispositivos físicos o documentos y la integridad de la información almacenada en ellos.

- **Elementos auxiliares:** Estos tipos de protección se incluyen para la gestión del plan de energía, la climatización y la protección del cableado de red.

- **Protección de las Instalaciones:** Considere el control de acceso y el estado de diseño del entorno físico para acomodar dichas protecciones.

- **Gestión del personal:** Se incluye este tipo de salvaguardas porque plantea la formación y concienciación, disponibilidad del personal.

- **Adquisición / desarrollo:** Dichas salvaguardas se incluyen porque se relacionan con la compra o el desarrollo de aplicaciones, hardware, comunicaciones, soporte informativo o de comunicaciones que mejoran el servicio.

Luego de la descripción del grupo de salvaguardas se procede a evaluar las salvaguardas implantadas actualmente en la DRTPE, así mismo su nivel de efectividad de la misma, ambas actividades se desarrollarán en la siguiente tabla N° 26:

	N°	SALVAGUARDAS	TIPO	ESTADO DE CONTROL	NIVEL DE MADUREZ DE SALVAGUARDA	% EFECTIVIDAD	NIVEL DE EFECTIVIDAD	OBJETIVO DE SALVAGUARDA
PROTECCIONES GENERALES U HORIZONTALES	PGH1	Identificación y autenticación	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
	PGH2	Gestión de incidencias	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
	PGH3	Herramientas de seguridad - Antivirus Corporativo	Detectivo	No Implementado	L1 - inicial	10%	1	L5
	PGH4	Herramienta de detección / prevención de intrusión (Físico, Lógico)	Detectivo	No Implementado	L0 - Inexistente	0%	0	L5
	PGH5	Herramienta de chequeo de configuración	Correctivo	No Implementado	L1 - inicial	10%	1	L5
	PGH6	Herramienta de análisis de vulnerabilidades	Detectivo	No Implementado	L0 - Inexistente	0%	0	L5
	PGH7	Herramienta de monitorización de tráfico – Firewall	Detectivo	No Implementado	L0 - Inexistente	0%	0	L5
	PGH8	DLP: Herramienta de monitorización de contenidos	Detectivo	No Implementado	L0 - Inexistente	0%	0	L5
	PGH9	Gestión de vulnerabilidades	Correctivo	No Implementado	L0 - Inexistente	0%	0	L5
	PGH10	Registro y auditoría	Correctivo	No Implementado	L1 - inicial	10%	1	L5
PROTECCIÓN DE LOS DATOS / INFORMACIÓN	PDI1	Copias de seguridad (Backup)	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
	PDI2	Aseguramiento de la integridad de la información	Detectivo	No Implementado	L0 - Inexistente	0%	0	L5
	PDI3	Cifrado de la información	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
	PDI4	Protección de la información	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
PROTECCIÓN DE	PCC1	Gestión de claves criptográficas - Usuarios PC, etc	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5

	PCC2	Gestión de claves de comunicaciones - Red Wifi, Red de datos	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
PROTECCIÓN DE LOS SERVICIOS	PPS1	Aseguramiento de la disponibilidad de los servicios (internet, etc)	Detectivo	No Implementado	L1 - inicial	10%	1	L5
	PPS2	Aceptación y puesta en operación	Preventivo	No Implementado	L1 - inicial	10%	1	L5
	PPS3	Perfiles de seguridad	Detectivo	No Implementado	L1 - inicial	10%	1	L5
	PPS4	Gestión de cambios	Correctivo	No Implementado	L1 - inicial	10%	1	L5
	PPS5	Protección de servicios y aplicaciones web	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
	PPS6	Protección del correo electrónico	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
PROTECCIÓN DE LAS APLICACIONES (SOFTWARE)	PPA1	Copias de seguridad (Backup)	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
	PPA2	Actualizaciones y mantenimiento	Correctivo	No Implementado	L0 - Inexistente	10%	1	L5
	PPA3	Protección de las aplicaciones informáticas	Detectivo	No Implementado	L0 - Inexistente	0%	0	L5
PROTECCIÓN DE LOS EQUIPOS (HARDWARE)	PPH1	Aseguramiento de la disponibilidad de los equipos de hardware	Preventivo	No Implementado	L1 - inicial	30%	2	L5
	PPH2	Operación - Manual del correcto uso	Correctivo	No Implementado	L1 - inicial	10%	1	L5
	PPH3	Cambios (Actualizaciones y mantenimiento)	Correctivo	No Implementado	L2 - reproducible	30%	2	L5
	PPH4	Informática móvil - Tablet's	Correctivo	No Implementado	L1 - inicial	10%	1	L5
	PPH5	Reproducción de documentos	Detectivo	No Implementado	L2 - reproducible	30%	2	L5
	PPH6	Protección de los equipos informáticos	Preventivo	No Implementado	L1 - inicial	10%	1	L5

PROTECCIÓN DE LAS COMUNICACIONES	PPC1	Entrada en servicio	Detectivo	No Implementado	L1 - inicial	10%	1	L5
	PPC2	Protección de la integridad de los datos intercambiados	Detectivo	No Implementado	L0 - Inexistente	0%	0	L5
	PPC3	Operación - Manual del correcto uso	Correctivo	No Implementado	L2 - reproducible	30%	2	L5
	PPC4	Perfiles de seguridad	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
	PPC5	Seguridad Wireless	Preventivo	No Implementado		0%	0	L5
	PPC6	Protección de las comunicaciones	Detectivo	No Implementado	L0 - Inexistente	0%	0	L5
PROTECCIÓN EN LOS PUNTOS DE	PPI1	Puntos de interconexión: conexiones entre zonas de confianza	Preventivo	No Implementado	L1 - inicial	10%	1	L5
	PPI2	Protección de los equipos informáticos	Preventivo	No Implementado	L1 - inicial	10%	1	L5
PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN	PSI1	Aseguramiento de la disponibilidad	Detectivo	No Implementado	L1 - inicial	10%	1	L5
	PSI2	Limpieza de contenidos	Preventivo	No Implementado	L1 - inicial	10%	1	L5
	PSI3	Destrucción de soportes	Correctivo	No Implementado	L0 - Inexistente	0%	0	L5
	PSI4	Protección de los soportes de información	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
PROTECCIÓN DE LOS ELEMENTOS AUXILIARES	PEA1	Correcta Instalación Cableado Cat 6A	Correctivo	No Implementado	L0 - Inexistente	0%	0	L5
	PEA2	Protección del cableado CAT 6A	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
	PEA3	Climatización	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
	PEA4	Suministro eléctrico, Pozo a tierra	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
	PEA5	Aseguramiento de la disponibilidad	Detectivo	No Implementado	L1 - inicial	10%	1	L5

PROTECCIÓN DE LAS INSTALACIONES	PPI1	Diseño de las instalaciones	Correctivo	No Implementado	L1 - inicial	10%	1	L5
	PPI2	Control de acceso físico	Preventivo	Implementado	L5 - Optimizado	95%	5	L5
	PPI3	Aseguramiento de la disponibilidad - Recursos como extintores, etc	Detectivo	No Implementado	L0 - Inexistente	0%	0	L5
	PPI4	Protección de las instalaciones	Preventivo	No Implementado	L1 - inicial	10%	1	L5
SALVAGUARDAS RELATIVAS AL PERSONAL	SRP1	Gestión del personal	Preventivo	No Implementado	L1 - inicial	10%	1	L5
	SRP2	Formación y concienciación	Correctivo	No Implementado	L0 - Inexistente	0%	0	L5
	SRP3	Aseguramiento de la disponibilidad - Personal	Detectivo	No Implementado	L1 - inicial	10%	1	L5
SALVAGUARDAS DE TIPO ORGANIZATIVO	STO2	Gestión de riesgos	Correctivo	No Implementado	L1 - inicial	10%	1	L5
	STO3	Planificación de la seguridad	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
	STO4	Inspecciones de seguridad	Detectivo	No Implementado	L0 - Inexistente	0%	0	L5
CONTINUIDAD DE LAS OPERACIONE	CDO2	Análisis de impacto	Detectivo	No Implementado	L0 - Inexistente	0%	0	L5
	CDO3	Plan de recuperación de desastres	Correctivo	No Implementado	L1 - inicial	10%	1	L5
EXTERNALIZACION	EXT1	Compromiso de confidencialidad	Preventivo	No Implementado	L1 - inicial	10%	1	L5
	EXT2	Identificación y calificación del personal encargado	Detectivo	No Implementado	L0 - Inexistente	0%	0	L5
	EXT3	Procedimiento de escalado y resolución de incidencias	Correctivo	No Implementado	L1 - inicial	10%	1	L5
ADQUISICIÓN Y DESARRO	AYD1	Servicios	Preventivo	No Implementado	L1 - inicial	10%	1	L5
	AYD2	Aplicaciones - Originales	Preventivo	No Implementado	L1 - inicial	10%	1	L5

	AYD3	Salvaguarda de ciclo de vida de los equipos	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5
	AYD4	Comunicaciones	Preventivo	No Implementado	L1 - inicial	10%	1	L5
	AYD5	Soportes de información	Preventivo	No Implementado	L0 - Inexistente	0%	0	L5

Tabla 26,, Identificación y valoración de salvaguardas

Fuente: Elaboración Propia

4.1.4 ESTIMACIÓN DEL ESTADO DE RIESGO

En esta acción se va a utilizar la información recabada hasta el momento a Entidad. DRTPE, son las siguientes:

a) Estimación del Impacto Potencial

En este paso se va a determinar el impacto potencial al que está predispuesto la entidad DRTPE – Hco, este paso se logra determinar señalando el valor de los activos en las dimensiones establecidas, así como la degradación que causan las amenazas sobre esos activos.
El impacto es el valor de cada recurso multiplicado por el valor de degradación de cada amenaza.

I = Valor activo x Degradación de Materialización de la amenaza sobre activo

VALOR		
9	10	Muy alto
7	8	Alto
4	6	Medio
2	3	Bajo
0	1	Despreciable

Tabla de Valoración de Dimensiones

IMPACTO		
9	10	Desastroso
7	8	Mayor
4	6	Moderado
2	3	Menor
0	1	Insignificante

Tabla de Impacto

Según esos valores se ha establecido el impacto potencial por activo de la entidad – DRTPE, en la siguiente tabla podemos observar con mayor detalle

Tabla 27, Valoración de Impacto

		Despreciable		Bajo		Medio			Alto		Muy Alto	
		0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
Muy Alto	10	0	1	2	3	4	5	6	7	8	9	10
Alto	9	0	1	2	3	4	5	5	6	7	8	9
	8	0	1	2	2	3	4	5	6	6	7	8
	7	0	1	1	2	3	4	4	5	6	6	7
Medio	6	0	1	1	2	2	3	4	4	5	5	6
	4	0	0	1	1	2	2	2	3	3	4	4
Bajo	3	0	0	1	1	1	2	2	2	2	3	3
	2	0	0	0	1	1	1	1	1	2	2	2
	1	0	0	0	0	0	1	1	1	1	1	1
Despreciable	0	0	0	0	0	0	0	0	0	0	0	0

Fuente: Elaboración Propia

Posteriormente, se muestra la tabla de Impacto,

Tabla 28, Tabla de Impacto de las amenazas a los activos de información

	N°	CAPA	COD.	ACTIVO	PROB.	DIMENCIONES				
						[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [essential]	AED1	DATOS [data]	[ast]	Multimedia (Información de audio, videos, material de capacitación)	3	3	4	2	4	2
	AED2		[ots]	Datos de gestión interna	3	7	6	4	5	1
	AED3		[dge]	Datos de las certificaciones	4	3	2	5	2	2
	AED4	INFORMACIÓN [info]	[doc]	Documentos	4	5	4	3	8	3
	AED5		[inf]	Informes	2	2	0	4	6	2
	AED6		[exp]	Expedientes	3	5	3	4	0	2
	AED7		[tram]	Trámites	4	6	4	4	4	2
	AED8		[ipu]	Información pública	4	6	2	2	2	0
	AED9		[ipe]	Información personal	4	6	5	4	3	4
	AED10		[icl]	Información restringida	4	6	6	4	2	3
	AED11		[log]	Registro de datos de entrada, formato físico, Datos de control de acceso	3	2	2	0	0	0
	AED12	SERVICIO [service]	[sei]	Servicio de Internet	4	9	4	5	4	2
	AED15		[dir]	Correo electrónico entidad - DRTPE-Hco	3	6	5	6	5	4
APLICACIONES INFORMÁTICAS [apps]	APS1	SOFTWARE [SW]	[ehs]	S.O Windows	3	5	3	1	4	3
	APS3		[afp]	Adobe flash player	3	2	1	0	2	0
	APS4		[sql]	SIGA (Sistema Integrado de Gestión Administrativa)	4	5	2	2	2	2
	APS5		[mac]	Microsoft Office Professional 2016	4	5	3	2	4	2
	APS6		[off]	Ms Project 2016	3	1	2	0	1	0
	APS7		[msp]	Visio	3	2	2	2	1	0
	APS8		[vis]	Navegador web Google Chrome	4	10	2	7	10	1
	APS9		[brw]	Página web Institucional DRTPE - Hco (http://direcciontrabajo.regionhuanuco.gob.pe/)	3	7	5	2	1	1
	APS10		[msp]	Sistema de Backup (RESPALDOS)	3	6	5	0	4	0
EQUIPOS INFORMÁTICOS [einf]	EIH1	HARDWARE [HW]	[cpe]	Computadoras de escritorio	4	7	5	6	1	2
	EIH2		[cpp]	Computadora personal portátil de 2.0 GHz - Laptop	3	9	5	6	4	2
	EIH3		[iml]	Impresora Laser	3	7	4	4	1	0
	EIH4		[ipt]	Impresora de Inyección a tinta	3	7	5	0	1	0
	EIH5		[emc]	Equipo multifuncional copiadora fax impresor escáner de inyección a tinta color	3	7	4	0	1	0

	EIH6		[Emi]	EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER Y/O FAX	3	7	4	0	1	0
	EIH7		[cpu]	Unidad Central de Proceso - CPU	3	7	4	4	1	0
	EIH8		[mtb]	Placa madre o Motherboard	3	6	2	5	0	0
	EIH9		[lo]	Lectores Ópticos	3	5	1	5	0	0
	EIH10		[ram]	Memoria RAM	3	5	2	5	0	0
	EIH11		[hdd]	Disco Duro HDD	4	5	5	6	1	0
	EIH12		[trg]	Tarjeta de Red, Grafica y sonido	3	5	3	0	0	0
	EIH13		[Mou]	Mouse	3	6	2	0	0	0
	EIH14		[Key]	Teclado - Keyboard	3	6	2	0	0	0
	EIH15		[dis]	Camaras de Seguridad Fijas	3	4	0	2	0	0
	EIH16		[tpad]	TABLETA PAD	4	7	5	5	3	0
	EIH17		[rout]	Router	4	9	6	5	0	0
	EIH18		[ml]	MONITOR LED 21.5 in	3	5	4	3	0	0
	EIH19		[mp]	MONITOR PLANO	3	5	4	3	0	0
	EIH20		[pt]	Pozo a Tierra	3	6	0	0	0	0
COMUNICACIONES [ccm]	CRC1	REDES DE COMUNICACIÓN [COM]	[lan]	Red local LAN	4	7	5	5	2	0
	CRC3		[ptp]	Red privada virtual (Zoom) - corporativo - Pro	4	5	5	3	2	0
	CRC4		[rte]	Red telefónica	4	4	4	2	0	0
	CRC5		[wif]	Red inalámbrica - Access Point	3	5	4	4	1	3
	CRC6		[mob]	Telefonía móvil	3	4	2	1	1	0
SOPORTES DE INFORMACIÓN [spi]	SPI1	SOPORTE [media]	[dsk]	Almacenamiento en la nube (Google Drive)	4	2	3	3	0	1
	SPI2		[cdv]	CD / DVD	4	1	2	1	1	0
	SPI3		[pml]	Proyector multimedia	3	2	2	0	0	0
	SPI4		[usb]	Dispositivo USB - 8 GB	3	6	2	2	1	0
	SPI5			cable adaptador USB 3.0 a SATA	3	4	0	0	0	0
	SPI6		[tjm]	Tarjeta de memoria	3	1	0	2	1	1
	SPI7		[hdv]	Hard drive - HDD - Externo	3	3	3	2	1	1
EQUIPAMIENTO AUXILIAR [eax]	EAE1	EQUIPAMIENTO [aux]	[ups]	Estabilizador de energía - Regulador de voltaje	4	4	4	0	2	0
	EAE2		[fal]	Fuentes de alimentación - Conectores	3	5	2	0	0	0
	EAE3		[cbl]	Cableado de red - CAT 6 A	3	6	3	0	0	1
	EAE4		[mbl]	Mobiliario	3	2	0	1	0	1
	EAE5		[eqc]	Identificador biométrico	4	6	3	0	0	1
	EAE6		[cbl]	Cableado eléctrico	4	4	3	1	0	0
INS TAL	INI1	INS TAL ACI	[off]	Oficinas	2	6	4	1	1	0

	INI2		[slc]	Sala de orientaciones - Capacitaciones	3	4	3	2	2	1
	INI3		[sla]	Sala de atención	4	6	3	2	0	0
PERSONAL [per]	PSP1	PERSONAL [P]	[spt]	Director Regional de Trabajo y Promoción del Empleo	4	7	3	5	2	1
	PSP2		[jft]	Director de la Oficina Técnico Administrativo	3	7	5	6	2	2
	PSP3		[pnf]	Director de Prevención y Solución de Conflictos	3	7	3	5	2	1
	PSP4		[pad]	Director de promoción y protección de los derechos fundamentales y de la seguridad y salud en el trabajo	4	7	3	5	2	1
	PSP5		[sym]	Director de dirección de inspección del trabajo	4	7	3	5	2	1
	PSP6		[mme]	Director de dirección de promoción del empleo y capacitación laboral	4	7	3	5	2	1
	PSP7		[mmm]	Director zona de trabajo y promoción del empleo de leoncio prado	4	7	3	5	2	1
	PSP8		[opr]	Jefe de Recursos Humanos	4	6	4	5	0	0
	PSP9		[lya]	Personal Administrativo	4	6	4	6	0	0
	PSP10		[seg]	Encargado de Informática	4	8	4	5	0	0
	PSP11		[ctr]	Personal encargado de brindar asistencia técnica y capacitaciones diversas	4	8	4	6	0	0

Fuente: "Elaboración propia"

b) Estimación del Riesgo

Esta tarea estima el riesgo para los activos de la entidad: riesgo potencial para el sistema, revisión del valor de los activos y evaluación de amenazas.

Tabla 29, Referencia para estimación de Riesgo

RIESGO		
0	1	Controlable
2	5	Aceptable
6	16	Tolerable
17	30	Intolerable
31	50	Extremo

PROBABILIDAD DE OCURRENCIA	
1	Muy Raro
2	Improbable
3	Posible
4	Probable
5	Prácticamente segura

Fuente: (Escuela Nacional de Seguridad, 2012)

Según la Metodología Magerit v3, el riesgo se calcula con la siguiente formula

Riesgo = Impacto x Probabilidad

Tabla 30, Tabla para mapeo de riesgos detallado

Muy Alto	10	10	20	30	40	50
Alto	9	9	18	27	36	45
	8	8	16	24	32	40
	7	7	14	21	28	35
Medio	6	6	12	18	24	30
	5	5	10	15	20	25
	4	4	8	12	16	20
Bajo	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
Despreciable	0	0	0	0	0	0
		1	2	3	4	5
		Muy raro	Improbable	Posible	Probable	Prácticamente segura

Fuente: Elaboración Propia

posteriormente, se muestra el Mapa de Riesgos:

Tabla 31, Riesgo potencial por activo de valor de la Entidad

	N°	CAPA	CÓDIGO	ACTIVO	PROB	DIMENCIONES				
						[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [esencial]	AED1	DATOS [data]	[ast]	Multimedia (Información de audio, videos, material de capacitación)	3	9	12	6	12	6
	AED2		[ots]	Datos de gestión interna	3	21	18	12	15	3
	AED3		[dge]	Datos de las certificaciones	4	12	8	20	8	8
	AED4	INFORMACIÓN [info]	[doc]	Documentos	4	20	16	12	32	12
	AED5		[inf]	Informes	2	4	0	8	12	4
	AED6		[exp]	Expedientes	3	15	9	12	0	6
	AED7		[tram]	Trámites	4	24	16	16	16	8
	AED8		[ipu]	Información pública	4	24	8	8	8	0
	AED9		[ipe]	Información personal	4	24	20	16	12	16
	AED10		[icl]	Información restringida	4	24	24	16	8	12
	AED11		[log]	Registro de datos de entrada, formato físico, Datos de control de acceso	3	6	6	0	0	0
	AED12	SERVICIO [service]	[sei]	Servicio de Internet	4	36	16	20	16	8
	AED15		[dir]	Correo electrónico entidad - DRTPE-Hco	3	18	15	18	15	12
APLICACIONES INFORMÁTICAS	APS1	SOFTWARE [SW]	[ehs]	S.O Windows	3	15	9	3	12	9
	APS3		[afp]	Adobe flash player	3	6	3	0	6	0
	APS4		[sql]	SIGA (Sistema Integrado de Gestión Administrativa)	4	20	8	8	8	8
	APS5		[mac]	Microsoft Office Professional 2016	4	20	12	8	16	8

	APS6		[off]	Ms Project 2016	3	3	6	0	3	0
	APS7		[msp]	Visio	3	6	6	6	3	0
	APS8		[vis]	Navegador web Google Chrome	4	40	8	28	40	4
	APS9		[brw]	Página web Institucional DRTPE - Hco (http://direcciontrabajo.regionhuanuco.gob.pe/)	3	21	15	6	3	3
	APS10		[msp]	Sistema de Backup (RESPALDOS)	3	18	15	0	12	0
EQUIPOS INFORMÁTICOS **[einf]**	EIH1	HARDWARE **[HW]**		Computadoras de escritorio	4	28	20	24	4	8
	EIH2			Computadora personal portátil de 2.0 GHz - Laptop	3	27	15	18	12	6
	EIH3			Impresora Laser	3	21	12	12	3	0
	EIH4			Impresora de Inyección a tinta	3	21	15	0	3	0
	EIH5			Equipo multifuncional copiadora fax impresor escáner de inyección a tinta color	3	21	12	0	3	0
	EIH6			EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER Y/O FAX	3	21	12	0	3	0
	EIH7			Unidad Central de Proceso - CPU	3	21	12	12	3	0
	EIH8			Placa madre o Motherboard	3	18	6	15	0	0
	EIH9			Lectores Ópticos	3	15	3	15	0	0
	EIH10			Memoria RAM	3	15	6	15	0	0
	EIH11			Disco Duro HDD	4	20	20	24	4	0
	EIH12			Tarjeta de Red, Grafica y sonido	3	15	9	0	0	0
	EIH13			Mouse	3	18	6	0	0	0
	EIH14			Teclado - Keyboard	3	18	6	0	0	0
	EIH15			Cámaras de Seguridad Fijas	3	12	0	6	0	0
	EIH16			Tableta Pad	4	28	20	20	12	0
	EIH17			Router	4	36	24	20	0	0
	EIH18			MONITOR LED 21.5 in	3	15	12	9	0	0
	EIH19			MONITOR PLANO	3	15	12	9	0	0
	EIH20			Pozo a Tierra	3	18	0	0	0	0
COMUNICACIONES **[ccm]**	CRC1	REDES DE COMUNICACIÓN	[lan]	Red local LAN	4	28	20	20	8	0
	CRC3		[ptp]	Red privada virtual (Zoom) - corporativo - Pro	4	20	20	12	8	0
	CRC4		[rte]	Red telefónica	4	16	16	8	0	0
	CRC5		[wif]	Red inalámbrica - Access Point	3	15	12	12	3	9
	CRC6		[mob]	Telefonía móvil	3	12	6	3	3	0
SOPORTES DE INFORMACIÓN	SPI1	SOPORTE **[media]**	[dsk]	Almacenamiento en la nube (Google Drive)	4	8	12	12	0	4
	SPI2		[cdv]	CD / DVD	4	4	8	4	4	0
	SPI3		[pml]	Proyector multimedia	3	6	6	0	0	0
	SPI4		[usb]	Dispositivo USB - 8 GB	3	18	6	6	3	0

	SPI5			cable adaptador USB 3.0 a SATA	3	12	0	0	0	0
	SPI6		[tjm]	Tarjeta de memoria	3	3	0	6	3	3
	SPI7		[hdv]	Hard drive - HDD - Externo	3	9	9	6	3	3
EQUIPAMIENTO AUXILIAR [eax]	EAE1	EQUIPAMIENTO [aux]	[ups]	Estabilizador de energía - Regulador de voltaje	4	16	16	0	8	0
	EAE2		[fal]	Fuentes de alimentación - Conectores	3	15	6	0	0	0
	EAE3		[cbl]	Cableado de red - CAT 6A	3	18	9	0	0	3
	EAE4		[mbl]	Mobiliario	3	6	0	3	0	3
	EAE5		[eqc]	Identificador biométrico	4	24	12	0	0	4
	EAE6		[cbl]	Cableado eléctrico	4	16	12	4	0	0
INSTALACIONES [...]	INI1	INSTALACIONES [...]	[off]	Oficinas	2	12	8	2	2	0
	INI2		[slc]	Sala de orientaciones - Capacitaciones	3	12	9	6	6	3
	INI3		[sla]	Sala de atención	4	24	12	8	0	0
PERSONAL [per]	PSP1	PERSONAL [P]	[spt]	Director Regional de Trabajo y Promoción del Empleo	4	28	12	20	8	4
	PSP2		[jft]	Director de la Oficina Técnico Administrativo	3	21	15	18	6	6
	PSP3		[pnf]	Director de Prevención y Solución de Conflictos	3	21	9	15	6	3
	PSP4		[pad]	Director de promoción y protección de los derechos fundamentales y de la seguridad y salud en el trabajo	4	28	12	20	8	4
	PSP5		[sym]	Director de dirección de inspección del trabajo	4	28	12	20	8	4
	PSP6		[mme]	Director de dirección de promoción del empleo y capacitación laboral	4	28	12	20	8	4
	PSP7		[mmm]	Director zona de trabajo y promoción del empleo de leoncio prado	4	28	12	20	8	4
	PSP8		[opr]	Jefe de Recursos Humanos	4	24	16	20	0	0
	PSP9		[lya]	Personal Administrativo	4	24	16	24	0	0
	PSP10		[seg]	Encargado de Informática	4	32	16	20	0	0
	PSP11		[ctr]	Personal encargado de brindar asistencia técnica y capacitaciones diversas	4	32	16	24	0	0

Fuente: Elaboración Propia

Una vez obtenido la matriz de riesgos de los activos de la DRTPE, se comienza a seleccionar los activos para su tratamiento de riesgos, en esta parte se debe tener en cuenta que la entidad va a decidir sobre cual es nivel de riesgos que puede aceptar, la entidad determino que los riesgos de color dorado – riesgo intolerable, y de color rojo – riesgo extremo se deben dar una solución, con esa condición se van a priorizar esos activos sobre el resto, a continuación, se mostraran en la Tabla priorización:

Tabla de Priorización de Activos

Se observa que hay 6 activos con riesgo intolerable, se deben implementar salvaguardas, para mitigar el riesgo

Tabla 32, Tabla Matriz de Priorización v1 de Activos general

RIESGOS INTOLERABLES

N°	ACTIVO	[D]	[I]	[C]	[A]	[N_R]
1	Navegador web Google Chrome	Muy Urgente	No Definido	Urgente	Muy Urgente	No Definido
2	Router	Muy Urgente	Urgente	Urgente	No Definido	No Definido
3	Servicio de Internet	Muy Urgente	No Definido	Urgente	No Definido	No Definido
4	Documentos	Urgente	No Definido	No Definido	Muy Urgente	No Definido
5	Personal encargado de brindar asistencia técnica y capacitaciones diversas	Muy Urgente	No Definido	Urgente	No Definido	No Definido
6	Encargado de Informática	Muy Urgente	No Definido	Urgente	No Definido	No Definido

	RIESGOS INTOLERABLES					
1	Computadoras de escritorio	Urgente	Urgente	Urgente	No Definido	No Definido
2	Tableta Pad	Urgente	Urgente	Urgente	No Definido	No Definido
3	Disco Duro HDD	Urgente	Urgente	Urgente	No Definido	No Definido
4	Red local LAN	Urgente	Urgente	Urgente	No Definido	No Definido
5	Correo electrónico entidad - DRTPE-Hco	Urgente	No Definido	Urgente	No Definido	No Definido
6	Datos de gestión interna	Urgente	Urgente	No Definido	No Definido	No Definido
7	Red privada virtual (Zoom) - corporativo – Pro	Urgente	Urgente	No Definido	No Definido	No Definido
8	Información personal	Urgente	Urgente	No Definido	No Definido	No Definido
9	Información restringida	Urgente	Urgente	No Definido	No Definido	No Definido
10	Computadora personal portátil de 2.0 GHz - Laptop	Urgente	No Definido	Urgente	No Definido	No Definido
11	Personal Administrativo	Urgente	No Definido	Urgente	No Definido	No Definido
12	Director Regional de Trabajo y Promoción del Empleo	Urgente	No Definido	Urgente	No Definido	No Definido

13	Director de la Oficina Técnico Administrativo	Urgente	No Definido	Urgente	No Definido	No Definido
14	Director de promoción y protección de los derechos fundamentales y de la seguridad y salud en el trabajo	Urgente	No Definido	Urgente	No Definido	No Definido
15	Director de dirección de inspección del trabajo	Urgente	No Definido	Urgente	No Definido	No Definido
16	Director de dirección de promoción del empleo y capacitación laboral	Urgente	No Definido	Urgente	No Definido	No Definido
17	Director zona de trabajo y promoción del empleo de leoncio prado	Urgente	No Definido	Urgente	No Definido	No Definido
18	Jefe de Recursos Humanos	Urgente	No Definido	Urgente	No Definido	No Definido
19	Página web Institucional DRTPE - Hco (http://direcciontrabajo.regionhuanuco.gob.pe/)	Urgente	No Definido	No Definido	No Definido	No Definido
20	Trámites	Urgente	No Definido	No Definido	No Definido	No Definido
21	Información pública	Urgente	No Definido	No Definido	No Definido	No Definido
22	SIGA (Sistema Integrado de Gestión Administrativa)	Urgente	No Definido	No Definido	No Definido	No Definido
23	Impresora Laser	Urgente	No Definido	No Definido	No Definido	No Definido
24	Impresora de Inyección a tinta	Urgente	No Definido	No Definido	No Definido	No Definido
25	Equipo multifuncional copiadora fax impresor escáner de inyección a tinta color	Urgente	No Definido	No Definido	No Definido	No Definido
26	EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER Y/O FAX	Urgente	No Definido	No Definido	No Definido	No Definido
27	Unidad Central de Proceso - CPU	Urgente	No Definido	No Definido	No Definido	No Definido
28	Placa madre o Motherboard	Urgente	No Definido	No Definido	No Definido	No Definido
29	Mouse	Urgente	No Definido	No Definido	No Definido	No Definido
30	Teclado – Keyboard	Urgente	No Definido	No Definido	No Definido	No Definido
31	Pozo a Tierra	Urgente	No Definido	No Definido	No Definido	No Definido
32	Cableado de red - CAT 6 A	Urgente	No Definido	No Definido	No Definido	No Definido

33	Datos de las certificaciones	No Definido	No Definido	Urgente	No Definido	No Definido
34	Microsoft Office Professional 2016	Urgente	No Definido	No Definido	No Definido	No Definido
35	Sistema de Backup (RESPALDOS)	Urgente	No Definido	No Definido	No Definido	No Definido
36	Dispositivo USB - 8 GB	Urgente	No Definido	No Definido	No Definido	No Definido
37	Identificador biométrico	Urgente	No Definido	No Definido	No Definido	No Definido
38	Sala de atención	Urgente	No Definido	No Definido	No Definido	No Definido
39	Director de Prevención y Solución de Conflictos	Urgente	No Definido	No Definido	No Definido	No Definido

Fuente: "Elaboración Propia"

4.1.5. Proceso de Gestión de Riesgos

Cuando ejecuta un método de análisis de riesgos, puede obtener resultados sobre los impactos y las amenazas a los activos. Evalúe cada riesgo significativo con base en la tabla de riesgos.

Una vez completadas las actividades del proyecto de reducción de riesgos, la gerencia es responsable de implementar las medidas de control. A los efectos de este tipo de tesis y su ámbito de trabajo, se terminará en esta fase. Encontrar una manera de crear un plan de trabajo coherente y efectivo creará una nueva visión dentro de la organización. En la siguiente tabla se muestra a detalle la tabla de priorización de activos, detallando el nombre del activo, tipo de activo, las dimensiones de seguridad a priorizar de acuerdo al mapa de riesgos, los riesgos asociados a esos activos, y la estrategia de acción.

Tabla 33, Numero de Activos priorisables, según la entidad

Activos totales	54
Activos identificados en riesgo intolerable (Color Dorado)	39
Activos identificados en riesgo extremo (Color Rojo)	6

Fuente: Elaboración Propia

N°	ACTIVO	Tipo de Activo	[D]	[I]	[C]	[A]	[N_R]	Estrategia
1	Navegador web Google Chrome	Software	40	8	28	40	4	Mitigar
2	Router	Equipo Informático – Hardware	36	24	20	0	0	Mitigar
3	Servicio de Internet	Servicio	36	16	20	16	8	Mitigar
4	Documentos	Información	20	16	12	32	12	Mitigar
5	Personal encargado de brindar asistencia técnica y capacitaciones diversas	Personal	32	16	24	0	0	Mitigar
6	Encargado de Informática	Personal	32	16	20	0	0	Mitigar
		RIESGOS INTOLERABLES						
1	Computadoras de escritorio	Equipo Informático – Hardware	28	20	24	4	8	Mitigar
2	Tableta Pad	Equipo Informático – Hardware	28	20	20	12	0	Mitigar
3	Disco Duro HDD	Equipo Informático – Hardware	20	20	24	4	0	Mitigar
4	Red local LAN	Redes de Comunicación	28	20	20	8	0	Mitigar
5	Correo electrónico entidad - DRTPE-Hco	Servicio	18	15	18	15	12	Mitigar
6	Datos de gestión interna	Datos	21	18	12	15	3	Mitigar
7	Red privada virtual (Zoom) - corporativo – Pro	Redes de Comunicación	20	20	12	8	0	Mitigar
8	Información personal	Información	24	20	16	12	16	Mitigar
9	Información restringida	Información	24	24	16	8	12	Mitigar

10	Computadora personal portátil de 2.0 GHz - Laptop	Equipo Informático – Hardware	27	15	18	12	6	Mitigar
11	Personal Administrativo	Personal	24	16	24	0	0	Mitigar
12	Director Regional de Trabajo y Promoción del Empleo	Personal	28	12	20	8	4	Mitigar
13	Director de la Oficina Técnico Administrativo	Personal	21	15	18	6	6	Mitigar
14	Director de promoción y protección de los derechos fundamentales y de la seguridad y salud en el trabajo	Personal	28	12	20	8	4	Mitigar
15	Director de dirección de inspección del trabajo	Personal	28	12	20	8	4	Mitigar
16	Director de dirección de promoción del empleo y capacitación laboral	Personal	28	12	20	8	4	Mitigar
17	Director zona de trabajo y promoción del empleo de Leoncio prado	Personal	28	12	20	8	4	Mitigar
18	Jefe de Recursos Humanos	Personal	24	16	20	0	0	Mitigar
19	Página web Institucional DRTPE - Hco (http://direcciontrabajo.regionhuanuco.gob.pe/)	Software	21	15	6	3	3	Mitigar
20	Trámites	Información	24	16	16	16	8	Mitigar
21	Información pública	Información	24	8	8	8	0	Mitigar
22	SIGA (Sistema Integrado de Gestión Administrativa)	Software	20	8	8	8	8	Mitigar
23	Impresora Laser	Equipo Informático – Hardware	21	12	12	3	0	Mitigar
24	Impresora de Inyección a tinta	Equipo Informático – Hardware	21	15	0	3	0	Mitigar
25	Equipo multifuncional copiadora fax impresor escáner de inyección a tinta color	Equipo Informático – Hardware	21	12	0	3	0	Mitigar
26	EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER Y/O FAX	Equipo Informático – Hardware	21	12	0	3	0	Mitigar

27	Unidad Central de Proceso - CPU	Equipo Informático – Hardware	21	12	12	3	0	Mitigar
28	Placa madre o Motherboard	Equipo Informático – Hardware	18	6	15	0	0	Mitigar
29	Mouse	Equipo Informático – Hardware	18	6	0	0	0	Mitigar
30	Teclado – Keyboard	Equipo Informático – Hardware	18	6	0	0	0	Mitigar
31	Pozo a Tierra	Equipo Informático – Hardware	18	0	0	0	0	Mitigar
32	Cableado de red - CAT 6 A	Equipamiento Auxiliar	18	9	0	0	3	Mitigar
33	Datos de las certificaciones	Datos	12	8	20	8	8	Mitigar
34	Microsoft Office Professional 2016	Software	20	12	8	16	8	Mitigar
35	Sistema de Backup (RESPALDOS)	Software	18	15	0	12	0	Mitigar
36	Dispositivo USB - 8 GB	Soporte	18	6	6	3	0	Mitigar
37	Identificador biométrico	Equipamiento Auxiliar	24	12	0	0	4	Mitigar
38	Sala de atención	Instalaciones	24	12	8	0	0	Mitigar
39	Director de Prevención y Solución de Conflictos	Personal	21	9	15	6	3	Mitigar

Tabla 34, Matriz de priorización específica,

Fuente: "Elaboración Propia"

4.5.1.1 Plan de seguridad – dirección regional de trabajo y promoción del empleo – Hco

Tabla 35, Información general Propuesta de políticas de seguridad

Código	PROPOL-001
Versión	1
Fecha de aprobación	XX/XX/2021
Resumen	Propuesta de Políticas, basadas en buenas prácticas, para la gestión de seguridad de la información
Aprobado por	Director Regional de Trabajo y Promoción del Empleo
Área Involucrada	Todas las áreas
Paginas	26 paginas

Fuente: Modelo de Plantilla aprobado por la ONGEI

Historial de Revisiones

Tabla 36, Historial de revisiones

Fecha	Versión	Modificado/Creado por	Descripción de las modificaciones
18/05/2021	1.5	Tesistas	

Fuente: Modelo de Plantilla aprobado por la ONGEI

Cuadro de Aprobación

Tabla 37, Cuadro de Aprobación

Fecha	Nombre	Cargo	Sello y Firma

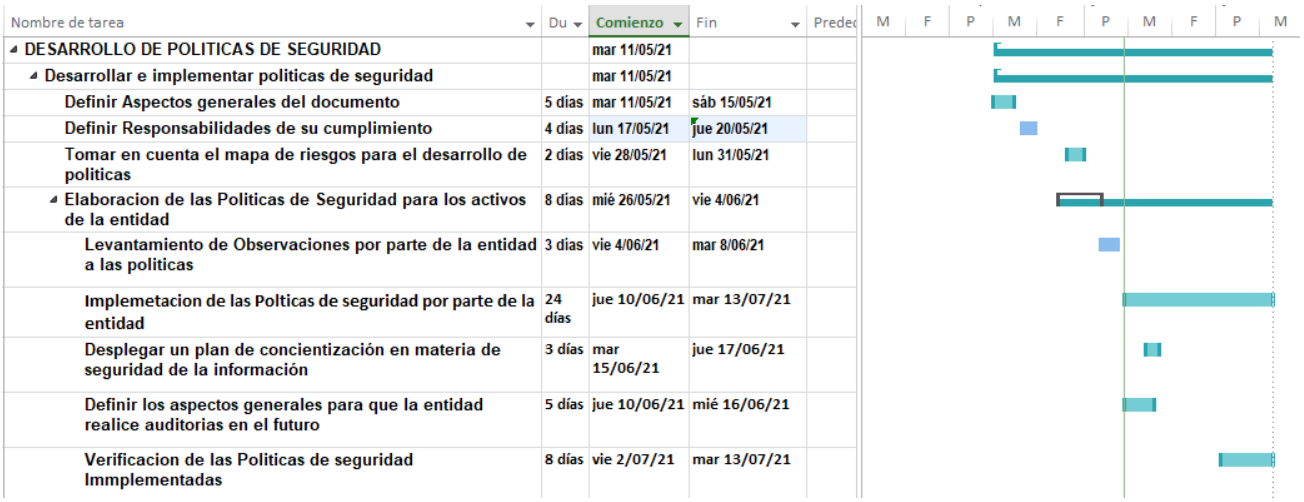
Fuente: Modelo de Plantilla aprobado por la ONGEI

Modelo de encabezado de las políticas de seguridad

Trabajo DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO - HUÁNUCO	**DIRECCION REGIONAL DE TRABAJO Y PROMOCION DEL EMPLEO – HCO**	**CODIGO PROPOL-001**
	PROPUESTA DE POLÍTICAS, BASADAS EN BUENAS PRÁCTICAS, PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**FECHA: XX/05/2021 VERSION: 1.x**

Fuente: Elaboración propia

Cronograma Plan de seguridad



Nombre de tarea	Du	Comienzo	Fin	Predec
DESARROLLO DE POLITICAS DE SEGURIDAD		mar 11/05/21		
Desarrollar e implementar politicas de seguridad		mar 11/05/21		
Definir Aspectos generales del documento	5 días	mar 11/05/21	sáb 15/05/21	
Definir Responsabilidades de su cumplimiento	4 días	lun 17/05/21	jue 20/05/21	
Tomar en cuenta el mapa de riesgos para el desarrollo de politicas	2 días	vie 28/05/21	lun 31/05/21	
Elaboracion de las Politicas de Seguridad para los activos de la entidad	8 días	mié 26/05/21	vie 4/06/21	
Levantamiento de Observaciones por parte de la entidad a las politicas	3 días	vie 4/06/21	mar 8/06/21	
Implemetacion de las Polticas de seguridad por parte de la entidad	24 días	jue 10/06/21	mar 13/07/21	
Desplegar un plan de concientización en materia de seguridad de la información	3 días	mar 15/06/21	jue 17/06/21	
Definir los aspectos generales para que la entidad realice auditorias en el futuro	5 días	jue 10/06/21	mié 16/06/21	
Verificacion de las Politicas de seguridad Immplementadas	8 días	vie 2/07/21	mar 13/07/21	

Gráfico 17, Cronograma del plan de Seguridad

Fuente: Elaboración Propia

a. Objetivo

Dar a la Dirección Regional de trabajo y Promoción del Empleo, un marco de gestión para los objetivos de seguridad de la información, la dirección general y los principios operativos, amparado en los lineamientos de estado en una política de Ciberseguridad

b. Finalidad

Determinar puntos de referencia para el desarrollo e implementación de procedimientos y actividades de gestión para proteger la seguridad de la información y minimizar el impacto de amenazas o eventos adversos en la continuidad del funcionamiento de la Dirección Regional de trabajo y Promoción del Empleo.

c. Base Legal

- “Ley N° 27444 Ley del Procedimiento Administrativo General”. Resolución Jefatural N° 340-94-INEI, que aprueba la Directiva N° 015-94-INEI/SJI.
- Resolución Ministerial Nº 246-2007-PCM que aprueba el Uso Obligatorio de la “Norma Técnica Peruana” NTP-ISO/IEC 17799:2007.
- Resolución de Contraloría General Nº 458-2008-CG “Guía para la Implementación del Sistema de Control Interno de las entidades del Estado”.
- Resolución Ministerial Nº 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”.

4.1.6.2. Alcance

Esta política se aplica a toda la de la Dirección Regional de trabajo y Promoción del Empleo, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

4.1.6.3. Responsabilidad de su cumplimiento

Cada uno de los funcionarios, empleados, subgerencias o personal técnico, independientemente de su cargo, son responsables de implementar esta Política de privacidad como parte de sus funciones y del cumplimiento de esta política anterior, de la siguiente manera:

Director de la entidad	"El director regional de Trabajo y Promoción del Empleo-Hco, tendrá la función de aprobar la política de seguridad y sus futuras modificaciones".
Comité de Gestión de Seguridad	"El Comité de Seguridad de la Dirección Regional de Trabajo y Promoción del Empleo-Hco, procederá a Planificar y coordinar el funcionamiento del sistema de seguridad de la información, además podrá proponer otras acciones o proyectos que sean necesarias para alcanzar los fines y objetivos del sistema de seguridad de la DRTPE-Hco. Estará conformado por: El Administrador, el director de la oficina técnico administrativa, el asesor legal y el responsable del área de informática. Este comité será el órgano responsable de que las políticas de seguridad y los procedimientos y prácticas se cumplan y además se las adecuadas con los lineamientos y objetivos de la Institución".
El director de la Oficina Técnica Administrativa	"El director de la oficina técnico administrativa designará un responsable de convocar periódicamente las reuniones tanto ordinarias como extraordinarias, elaborar las actas, informar a los integrantes del comité y presentar los informes a quien lo solicite".
El especialista de Seguridad de la información	"El Especialista de Seguridad de la Información, será el responsable de la coordinación de Seguridad de la Información que apoya el desarrollo de actividades de planeación, operación, mantenimiento y verificación de las políticas de seguridad El especialista será un agente interno o externo, seleccionado por el comité de Gestión de seguridad. Para este caso será designado de acuerdo al área de informática".
Responsable de Informática	"El responsable de Informática, cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología (clasificar la información de acuerdo con el grado de confiabilidad de documentar y brindar los accesos de acuerdo a nivel de seguridad que requiera sus puestos)".
Responsable de RR HH	"El responsable del Área de Recursos Humanos, cumplirá la función de notificar a todo el personal que comience con sus labores respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, a las que se encuentre sometida la entidad".

Tabla 38, Descripción de roles definidos en gestión de las políticas de seguridad de información dentro de la entidad,

Fuente: Elaboración propia

4.1.6.4. Aspectos Generales

Esta política incluye una serie de lineamientos que abordan aspectos específicos de la seguridad de la información, incluyendo los siguientes temas:

- Organización de la Seguridad
- Seguridad de Recursos Humanos
- Gestión de Activos
- Control de Accesos
- Criptografía
- Seguridad Física y Ambiental
- Seguridad de las Operaciones y Comunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de la Seguridad de la Información
- Cumplimiento

El Comité de Gestión de la Seguridad revisará cada año la propuesta de Políticas, a efectos de mantenerla actualizada. Así mismo toda modificación será aprobada por esta.

El análisis se realizó como parte de la identificación y evaluación de riesgos utilizando la metodología MAGERIT v3 la cual se alinea con los objetivos y controles de la Norma Técnica Peruana para responder adecuadamente a los riesgos ya que nos permiten cumplir con los requisitos legales, regulatorios y contractuales. Los objetivos de control y las acciones sugeridas se enumeran a continuación.

La DRTPE, puede no aplicar la totalidad de las políticas de seguridad propuestas en este documento, todo no cumplimiento de las políticas debe ser sustentada y debidamente justificada indicando el porqué del no cumplimento de esa política de seguridad, este cambio debe ser aprobado por el director regional de Trabajo y Promoción del Empleo-Hco.

4.2 Políticas generales de seguridad de información

Tabla 39, Propuesta de Políticas de Seguridad

Sección – Dominio	Prioridad	Justificación	Apli. - Pre	PROPUESTA REALIZADA POR TESISTAS	Apli. - Post
DOMINIO: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN					
A.1. Política de Seguridad de la Información					
Objetivo de control: Orientación de la Dirección para la gestión de la seguridad de la información					
A.1.1. Documentar política de seguridad de la información	Aplica	Se deben establecer formalmente las directrices que se deben seguir en la entidad	10%	I. El director de la entidad, tendrá la función de aprobar la política de seguridad y sus futuras modificaciones, estas deberán ser comunicadas a todo el personal interno, y a las partes externas relevantes, para mayor referencia la Tabla 39, Descripción de roles definidos en gestión de las políticas de seguridad de información dentro de la entidad,	30%
A.1.2. Revisión de la política de seguridad de la información	Aplica	Es necesario realizar una revisión periódica de las políticas de seguridad	0%	I. El Comité de Gestión de la Seguridad de la Información revisará anualmente la presente Política, a efectos de mantenerla actualizada, y así garantizar la efectividad de las mismas, para mayor referencia la Tabla 39, Descripción de roles definidos en gestión de las políticas de seguridad de información dentro de la entidad,	30%
A.2. Organización de la seguridad de la información					
Objetivo: Implantar un patrón de administración para el inicio y el control de la implementación y operación de la seguridad de la información en la entidad.					

A.2.1. Acuerdo de la gerencia con la seguridad de la información	Aplica	La gerencia debe apoyar activamente la seguridad dentro de la institución a través de una dirección clara	0%	I. La entidad debe establecer en su política general de seguridad de la información el compromiso, organización y asignación de responsabilidades para su cumplimiento, así mismo determinar las sanciones correspondientes por el incumplimiento	50%
A.2.4. Acuerdos de confidencialidad	Aplica	Se deben identificar y revisar regularmente los requerimientos de confidencialidad	10%	I. Todo usuario que requiere acceso a información clasificada como “Restringida” debe ser autorizado por el propietario de la misma en el período establecido por la entidad. Las autorizaciones de acceso a la información deben ser documentadas para así mantener un seguimiento de auditoría.	30%
A.3. Dispositivos móviles y teletrabajo					
Objetivo: Asegurar la seguridad del teletrabajo y el uso de los dispositivos móviles					

A.3.1. Política de dispositivos portátiles, móviles	Aplica	Los trabajadores que manejen información de la entidad en dispositivos portátiles, móviles que debe ser utilizada de acuerdo a los lineamientos de seguridad de información	30%	I. Se prohíbe tener como herramientas de trabajo, computadores portátiles (laptops), USB´s o cualquier otro equipo de propiedad del usuario, salvo autorización previa emitida por el jefe de mayor jerarquía del área que corresponda a la subárea y el correspondiente registro por parte del encargado de informática. Se define este control para que el usuario no transfiera información a su laptop personal considerada “restringida”, por parte de la entidad. II. Es responsabilidad del Usuario utilizar los discos compactos, USB´s, etcétera, de manera adecuada. Queda terminantemente prohibido al Usuario usar dispositivos externos como USB u otros dispositivos de almacenamiento que previamente hayan sido utilizados en computadores de uso público o dudoso, como, por ejemplo: centros educativos, Internet, o incluso, su computador personal sin la debida	50%

				revisión por parte del antivirus corporativo, para descartar amenazas por parte de virus informáticos III. Es responsabilidad del Usuario que usa una Laptop de la entidad o personal proteger la información propiedad de la entidad guardada o archivada en el mismo, para lo cual deberá cumplir las siguientes reglas básicas: - Cifrar el contenido de la Laptop para evitar el acceso a los datos en caso de que el equipo sea objeto de robo. - Respaldar la información antes de viajar. IV. Es obligatorio para todo el personal que usa dispositivos inalámbricos, propiedad de la DRTPE-Hco, para el desarrollo de sus funciones, como: teléfonos celulares, Tablet's, etc., que utilice como mecanismo de seguridad el bloqueo automático de los mismos y el uso de contraseña de acceso, caso contrario se aplicarán las sanciones correspondientes. V. Es responsabilidad del usuario, realizar un respaldo periódico de la información contenida en los dispositivos móviles o portátiles asignados, para evitar la pérdida de dicha información por robo, extravío, daño del aparato o cualquier otra circunstancia.	

A.3.2. Teletrabajo	Aplica	Los trabajadores de la entidad pueden tener acceso remoto a la información de entidad, según los requerimientos de cada puesto	0%	I. Se debe capacitar a los empleados en ciberseguridad antes de que comiencen a teletrabajar para que conozcan las políticas II. Al realizar el trabajo de forma remota se debe elegir los dispositivos corporativos que la entidad proporciono para el trabajo de forma remota, ya que cuentan con las especificaciones que la entidad considera necesarias y tienen instalado el software preciso para realizar el trabajo de forma segura III. Todos los dispositivos, según el nivel de información que manejen y necesiten para el correcto desarrollo de sus actividades, deben almacenar la información cifrada, tanto para proteger los datos de la entidad para garantizar su confidencialidad e integridad.	50%
A.4. Gestión de activos					
A.4.1. Responsabilidad por los activos					
Objetivo: Lograr y mantener la protección apropiada de los activos de la organización					
A.4.1. Inventariado de activos	Aplica	Se recomienda que los activos de información estén identificados, a través de un registro de los activos, que deben de actualizarse	30%	I. La entidad debe de elaborar y mantener un inventario de los activos (tangibles e intangibles), las mejores prácticas indican que se debe mantener un inventariado general y otro con los activos de hardware y software existente en la institución, la responsabilidad del mantenimiento del inventario es conjuntamente entre el encargado de informática, y del designado por la Oficina de Informática.	50%
A.4.2. Propiedad de los activos	Aplica	Los activos de la entidad deben consignar a quien se le	30%	I. Cada uno de los activos tiene que estar correctamente identificado, clasificado y asignado a un propietario, además de ubicación vigente del mismo	50%

		asigna dicho activo, para mantener un seguimiento de la vida útil del activo			
A.4.3. Uso aceptable de los activos	Aplica	Se recomienda la identificación, documentación e implementación de las normas para el uso correcto de la información y los activos.	10%	I. Cada sub área de la entidad será responsable de la actualización del inventario de los activos, conjuntamente con el encargado de informática. II. La entidad debe definir y revisar periódicamente las restricciones de acceso y clasificaciones para los activos importantes. III. La entidad debe implementar un programa de capacitación de funcionarios de todas las áreas para el entendimiento y correcto uso de los activos definidos	75%
A.4.2. Categorización de la información					
Objetivo: Fijar que la información reciba un nivel de protección apropiado					
A.4.2.1 Lineamiento de clasificación	Aplica	Se recomienda que la información sea categorizada por su valor, requerimientos legales, confidencialidad e importancia para la organización.	0%	I. De acuerdo a la importancia de la información es necesario clasificar la información de la entidad basados en requisitos legales, valor, las etiquetas asignadas son de acuerdo a la normativa peruana NTP-ISO/IEC 27001:2014 son Restringida, uso Interno, General. II. La clasificación asignada a un tipo de información, solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.	50%

				III.	La información que existe en más de un medio (sean físico o lógico) debe de tener la misma clasificación sin importar el formato.	
				IV.	Los empleados de la entidad, tanto internos como externos deben de estar al tanto de los procedimientos de etiquetado.	
A.4.2.2 Etiquetado y manejo de la información formato digital	Aplica	Se recomienda que la entidad implemente un grupo de procedimientos para etiquetar y usar la información.	10%	I.	Todo contenedor de información en medio digital (CDs, USB, Memorias portables, etc.) debe presentar una etiqueta con la clasificación correspondiente. Es necesario establecer controles para evitar eventos como divulgación, modificación, retiro o destrucción de información no autorizada.	30%
				II.	La información en formato digital clasificada como de acceso “General”, puede ser almacenada en cualquier medio electrónico en la DRTPE (información para consultas, información de capacitaciones en temas de formación laboral, notas informativas, etc.). Sin embargo, se deben tomar las medidas necesarias para no mezclar información “General” con información correspondiente a otra clasificación (Restringida o de uso interno).	
				III.	El encargado de informática, antes de transmitir información clasificada como “Restringida”, debe asegurarse que el destinatario de la información esté autorizado (que se cumpla el No repudio). La característica de no repudio sirve a los emisores o a los receptores para que la otra parte no pueda negar un mensaje transmitido.	
				IV.	Información en formato digital, clasificada como “Restringida”, debe ser encriptado con un método aprobado por el encargado de informática, por ejemplo, comprimir la información usando	

				el programa WinRAR, y agregando una clave para su descompresión, cuando es almacenada en cualquier medio (CDs, Memorias portables, etc.). V. Toda transmisión de Información clasificada como “Restringida”, “Uso Interno” realizada hacia o a través de redes externas a la Institución debe contar con la debida autorización de la entidad, además debe realizarse utilizando un medio de transmisión seguro, utilizando el correo institucional para este fin drtpe2019@gmail.com. Para la información clasificada como “General” bastara con enviarla sin tener la autorización correspondiente. VI. Todo documento en formato digital, debe presentar la clasificación correspondiente en la parte superior (cabecera) e inferior (pie de página) de cada página del documento, indicando si es “Restringida”, “Uso Interno” o de “General”	
A.4.2.3 Etiquetado y manejo de la información formato físico	Aplica	Se recomienda que la entidad implemente un grupo de procedimientos para etiquetar y usar la información. En formato físico	30%	I. Todo documento o contenedor de información debe ser etiquetado (encabezado) como “Restringida”, “Uso interno”, y “General” dependiendo de la clasificación asignada. II. Todo documento clasificado como “Restringido” debe contar con una carátula en la cual se muestre la clasificación de la información que contiene. III. El ambiente donde se almacena la información clasificada como “Restringida”, debe contar con adecuados controles de acceso y protección cuando se encuentre sin vigilancia.	50%

				IV. El acceso debe ser permitido solo al personal formalmente autorizado, una vez obtenido la autorización podrá tener acceso a información clasificada como “Restringida” V. Los usuarios que utilizan documentos con información “Restringida” deben asegurarse de: -Almacenarlos en lugares adecuados. -Evitar que usuarios no autorizados accedan a dichos documentos.	
A.4.3. Manejo de los medios					
Objetivo: Prevenir la difusión, manipulación, eliminación de los activos de información					
A.4.3.1. Gestión de medios removibles	Aplica	Se recomienda la ejecución de procedimientos para la administración de los medios extraíbles, de acuerdo a las necesidades de la organización	10%	I. Los discos duros no deben contener datos sensibles salvo en las computadoras cuyo acceso físico sea restringido o que tengan instalados un programa de seguridad y que los accesos a la computadora y a sus archivos sean controlados adecuadamente.	30%
A.4.3.2. Transferencia de medios físicos	Aplica	Los medios que contienen información deben ser protegidos, contra el acceso no autorizado a estas	30%	I. La información enviada por servicios postales debe ser protegida de accesos no autorizados mediante la utilización de: Paquetes sellados Entrega en persona Firmado y sellado de un cargo	50%

A.4.3.3. Procedimiento de manejo de la información	Aplica	Se recomienda la implementación de procedimientos para el manejo y guardado de la información para resguardarse de un acceso no autorizado.	10%	I. Los mensajes de correo electrónico deben ser considerados de igual manera que un documento de comunicación formal, estos mensajes están sujetos a monitoreo y auditoria. Los sistemas de correo electrónico no deben ser utilizados para lo siguiente: Enviar cadenas de mensajes, spam Enviar propaganda de candidatos políticos Actividades ilegales, no éticas o impropias con la entidad. II. No deben realizarse el reenvío automático de correos a direcciones que no pertenecen a la institución. Puesto que no existe control sobre los mensajes de correo electrónico una vez que estos se encuentran fuera de la red de la Dirección Regional de Trabajo y Promoción del Empleo. III. El intercambio de información puede darse dentro de la entidad, siempre dentro de los parámetros que establecen los controles de seguridad que garanticen seguridad y protección a la información que se está intercambiando. Los aspectos que esta política debería incluir son: Procedimientos de un correcto uso de los medios. Controles para evitar la modificación, la interceptación, el copiado o la destrucción de la información. Buenas prácticas para contrarrestar ingeniería social. Uso de cifrado en datos que se consideren necesarios. IV. Debe establecerse un proceso formal para aprobar la publicación de información de la entidad por medio del correo electrónico, así como para las redes sociales como la cuenta institucional de Facebook	50%

				V. La información contenida en sistemas públicos, como la página web de la entidad no debe contener información restringida, confidencial. VI. Información restringida o confidencial solo debe imprimirse en equipos específicamente designados para esta tarea, estos equipos deben estar supervisados por la oficina del director de la DRTPE	

A.5. Monitoreo					
Objetivo: Detectar actividades de procesamiento de información no autorizadas					
A.5.1. Registro de auditoría	Aplica	Se recomienda generar registros de las actividades de auditoría, excepciones e incidentes de seguridad de la información	0%	I. Todas las herramientas, incluyendo programas, aplicaciones, documentación y papeles de trabajo, requeridos para la auditoria de sistemas deben protegerse de amenazas posibles como se indica en esta política de seguridad. II. La entidad debe llevar a cabo auditorías internas a intervalos planificados para determinar si son puestos en marcha de la manera correcta y su grado de cumplimiento, así mismo toda documentación respecto a análisis de riesgos o afines debe ser preservado para que sirva de base a futuras auditorias. La norma peruana NTP/ISO 27001-2014, recomienda que debe realizarse las auditorias cada año. Dichas auditorias deben verificar si se cumplen los requisitos de la presente norma y legislación afines de la entidad, Si los controles que se encuentran implementados, se mantienen eficazmente, si se tiene un desempeño de acuerdo al esperado III. La entidad debe mejorar continuamente la eficacia del plan de seguridad, mediante los resultados de auditorías de seguridad, así como de las acciones correctivas y preventivas por parte de la DRTPE, así como tener los recursos necesarios para este fin IV. Toda información relacionada con trabajos sobre análisis de riesgos que se hayan desarrollado en la entidad, asi como documentos afines debe de ser preservados para que sirva como referente a futuras auditorias	30%

A.5.3. Protección de la información del registro	Aplica	Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.	0%	I. Los registros de fallas deben ser almacenados en archivos de Excel, para tener un control posterior, para futuras auditorias II. Los registros de información deben estar almacenados en una computadora destinada para ello, y solo deben tener acceso a ella el encargado de informática, y/o, profesionales afines	30%
A.5.4. Registro de fallas	Aplica	Las fallas se deben registrar, analizar y se debe tomar la acción apropiada	0%	Formato del procedimiento I. Para el correcto registro de fallas o incidentes, se utilizará el Formato de procedimiento especificado en la tabla N 40, el cual contiene los siguientes ítems: Nro. de Registro de fallas, Cargo del personal, Nombre del personal Fecha y Hora, Descripción del error o problema	30%
A.6 Seguridad de los recursos humanos.					
A.6.1. Antes del empleo					
Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus compromisos, y sean apropiados para los roles de acuerdo a sus requerimientos laborales, y así de disminuir el riesgo de a que están expuestos los activos de información					
A.6.1.1. Roles y responsabilidades	Aplica	Se recomienda el establecimiento y documentación de los roles y responsabilidades de seguridad de los empleados, etc. ,de acuerdo con la política de	10%	I. Los estándares relacionados al personal deben ser aplicados para asegurarse que los empleados sean seleccionados adecuadamente antes de ser contratados y que el acceso sea denegado oportunamente cuando un empleado es despedido o transferido. II. Se tendrá una variación continua de las claves de acceso (referido al S.O., y la página web) al personal para mantener la seguridad de los sistemas de información.	50%

		la seguridad de información de la organización		III. Deben de establecerse controles para comunicar los cambios del personal y los requerimientos de recursos de cómputo al responsable de informática. Es crucial que estos cambios sean atendidos a tiempo.	
A.6.1.3. Términos y condiciones de empleo	Aplica	Se recomienda que como parte de su obligación laboral; los empleados, contratistas y terceros deben aceptar las condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades en la seguridad de la información	0%	I. Cuando se contrate a un empleado nuevo y/o el servicio de algún tercero, se debe de entregar una copia de las políticas en formato digital, para que así se tenga una referencia de cómo desarrollar su labor II. El personal debe de ser comunicado de las implicancias de seguridad en relación a las responsabilidades de su trabajo	30%
A.6.2. Durante el empleo					
Objetivo: Asegurar que todos los empleados, etc., estén al tanto de las amenazas sobre la seguridad de información, para que puedan desarrollar su trabajo de forma normal, y reducir los riesgos de error humano, esto va de la mano de una correcta concientización en estos temas por parte de la gerencia mediante capacitaciones.					

A.6.2.1. Gestión de responsabilidades	Aplica	La administración debe solicitar que los empleados apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización	10%	I. Cuando se notifique un despido o transferencia, el encargado de informática debe de asegurarse que la cuenta de acceso usuario de la computadora debe ser cambiada para el nuevo personal.	50%
A.6.2.2. Capacitación y educación en seguridad de la información	Aplica	Se recomienda que los empleados de la entidad deban recibir la adecuada capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral	0%	I. Es responsabilidad del encargado de informática promover constantemente la importancia de la seguridad a todos los usuarios de los sistemas de información. II. El programa de concientización en seguridad debe de contener continuas actualizaciones y charlas, adicionalmente se puede emplear diversos métodos como afiches, avisos, ppts, videos de seguridad de la información., los cuales recuerden permanentemente al usuario el papel importante que cumplen en el mantenimiento de la seguridad de la información, así como el correcto uso de los equipos.	30%
A.6.2.3. Proceso disciplinario	Aplica	Se recomienda implementar un proceso disciplinario para los empleados que han cometido una falta en la seguridad, o que	10%	I. En caso de una incidencia, o falta que infrinja la vulneración de la información restringida, se aplicaran las sanciones administrativas, y legales son: -Destitución del cargo y consiguiente despido de la entidad. -Penalidad de acuerdo a lo estipulado en el contrato, por transgresión de una de las políticas de seguridad. -Otros de acuerdo a la gravedad de la incidencia.	30%

		no hayan reportado un incidente respecto a la seguridad de información			
A.6.3. Terminación o cambio del empleo					
Objetivo: Asegurar que los empleados que salgan de la Institución, lo realicen de manera ordenada, sin violar ninguna regla de seguridad.					
A.6.3.1. Devolución de activos	Aplica	Los empleados deben devolver todos los activos de la institución que estén en su poder a la terminación de su contrato.	30%	I. Cualquier ítem entregado al empleado como computadoras portátiles, datos, documentación, manuales, etc. deben de ser entregados a jefe inmediato con cargo.	50%
A.6.3.2. Terminación o cambio de responsabilidades	Aplica	Los derechos de acceso de los empleados que salen de la organización deben ser eliminados al término de su contrato.	0%	I. El área de RRHH de la entidad debe de notificar al encargado de informática, la renuncia o despido de los empleados, así como el inicio y fin de los periodos de vacaciones de los mismos. II. Luego del despido o renuncia de algún empleado, es responsabilidad del jefe inmediato del empleado revisar cualquier archivo físico o digital elaborado o modificado por el usuario. Además de ello el encargado de informática debe de asegurarse que la cuenta de acceso usuario de la computadora debe ser cambiada para el nuevo personal.	50%

A.7. Seguridad física y ambiental					
A.7.1. Áreas seguras.					
Objetivo: Evitar el acceso no autorizado, daño e interferencia a los locales de acceso restringido.					
A.7.1.1. Controles de ingreso físico	Aplica	Se recomienda la protección de las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado	50%	I. Se deben implementar medidas de seguridad física para asegurar la integridad de las instalaciones y de las computadoras de cada estación de trabajo dentro de la entidad II. Las medidas de protección deben ser consistentes con el nivel de clasificación de los activos y el valor de la información procesada y almacenada en las instalaciones. III. El acceso a cualquier instalación u oficina debe estar restringido únicamente al personal autorizado, o a ciudadanos previamente identificados. IV. Todas las consultas por parte del público en general que requieran la entrada a la entidad, deben ser correctamente identificadas por medio de los datos del DNI de la persona y se debe mantener un registro escrito, asimismo se debe registrar la fecha y hora, así mismo esa información debe ser almacenado en un archivo Excel, para su posterior monitoreo. V. Se debe de poner en marcha el control biométrico con que cuenta la entidad, pero actualmente está sin funcionamiento, deben de ser utilizadas para proteger las instalaciones VI. En aquellas oficinas en donde existen computadoras con información confidencial, o con acceso al equipo de Router que se encarga de proveer internet, se deberán tomar medidas	75%

				para el resguardo, y solo deben tener acceso a ello las personas previamente autorizadas	
A.7.2. Seguridad de los equipos informáticos					
Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la institución					
A.7.2.1. Ubicación y protección de los equipos	Aplica	Los equipos deben estar ubicados en lugares estratégicos y protegidos, para reducir el riesgo de amenazas como, robo o daño intencional.	30%	I. Es muy importante que la fuente de alimentación cuente con una potencia ideal que le permita trabajar de una manera más holgada, ya que, en el caso de estar conectada a una computadora, a esta se le suelen añadir otros elementos (teclados, ratones, grabadoras, disco duro, luces, etc.) que terminarán demandándole la energía para poder funcionar; por lo tanto si la potencia es insuficiente, es probable que se origine un fallo en algunos de los dispositivos, impidiéndole funcionar al no llegarle la potencia requerida, originando que la computadora no funcione. II. Los medios de almacenamiento, incluyendo discos duros de computadoras, que albergan información clasificada como “Restringida”, deben ser puestos en una ubicación especial designada por el encargado de informática, asimismo se deberá monitorear la transferencia de información de esos equipos.	50%
A.7.2.3. Seguridad en el cableado	Aplica	El cableado de la energía y las telecomunicaciones que transportan datos deben ser protegidos de las	30%	I. Se deben de conservar los cables en buen estado, ordenados y correctamente conectados. No debe existir ningún tipo de tensión, evitando siempre el doblado de los mismos. II. El cableado eléctrico requiere el cumplimiento de las normas o reglamentos, Norma Técnica Peruana NTP 370.301:2002 instalaciones eléctricas en edificios	50%

		interceptación, interferencia o daño		III. Se debe comprobar que el cableado de red cumple las normativas necesarias y que tiene la calidad necesaria, normalmente CAT5 o CAT6. Para evitar el posible seccionamiento del cableado de red lo mejor es entubarlo o integrarlo en la estructura del edificio.	
A.7.2.4. Mantenimiento de equipos	Aplica	Los equipos deben ser mantenidos periódicamente, actualizando, para asegurar su continua disponibilidad e integridad	10%	I. Todos los programas instalados en las computadoras deben ser legales, aprobados y periódicamente inventariados, solo los programas adquiridos o aprobados por la institución, serán instalados en las computadoras. II. La instalación y/o uso de programas de juegos, de distribución gratuita (freeware) o de propiedad personal está totalmente prohibido.	50%
A.7.2.5. Remoción de equipos	Aplica	Los equipos de información, o el software no deben ser retirados de su lugar sin autorización	10%	I. Todo traslado o asignación de equipos, es de responsabilidad del encargado de informática de la DRTPE, la verificación y realización del requerimiento.	30%
A.7.2.6. Reutilización segura de equipos	Aplica	Todo elemento de equipo que contengan medios de almacenamiento debe ser verificados para asegurar su correcto uso	30%	I. Es de responsabilidad del usuario, efectuar un correcto uso del equipo de cómputo que le fue asignado, así como de los programas en él instalados; cualquier cambio y/o traslado deberá ser solicitado con anticipación por su respectiva Sub Área. Asimismo, el usuario debe verificar que cualquier cambio y/o traslado del Equipo de Cómputo que le fue asignado, se realice por personal de informática, así como también la instalación o retiro de software.	50%

A.7.2.7. Política de escritorio Limpio y Pantalla limpia	Aplica	Debe ser adoptada una política de escritorio limpio, así como de pantalla limpia	10%	I. II. III. IV.	El responsable del área de informática debe realizar el mantenimiento preventivo y correctivo de los equipos informáticos. Siempre que el personal se ausente de su estación de trabajo, deberá bloquear las sesiones de sus equipos de cómputo. Todos los equipos de cómputo y dispositivos portátiles deberán tener aplicado el cierre de sesión por inactividad, definido por el equipo de seguridad de la información, se sugiere que cuando los equipos se encuentren inactivas por más de 15 minutos deben ser configurados con un protector de pantalla con contraseña, cuando sea aplicable. Es responsabilidad del Usuario evitar el deterioro del Hardware, para lo cual deberá cumplir las siguientes reglas básicas: No ingerir ni dejar alimentos y/o bebidas cerca y/o encima del Hardware. No colocar objetos pesados encima del Hardware. Mantener alejado del Hardware cualquier elemento electromagnético como imanes, teléfonos, radios, etc. No colocar el Hardware en lugares inestables y/o expuestos a ser golpeados involuntariamente o que estén en riesgo de caer y dañarse parcial o totalmente. No abrir el Hardware. De ser necesaria dicha labor será llevada a cabo por el encargado de informática. Es responsabilidad de los Usuarios conservar siempre limpio su lugar de trabajo, así como su Hardware asignado.	50%
A.8 Gestión de las comunicaciones y operaciones						
A.8.1. Procedimientos y responsabilidad operacionales						

Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras					
A.8.1.1 Procedimientos de operación documentados	Aplica	Se recomienda documentar y mantener los procedimientos de manejo de los Sistemas de información, y se deben poner a distribución de todos los usuarios que los necesiten	0%	I. Para la asignación de cuentas de usuario en las estaciones de trabajo, el director de cada área usuaria es el responsable de presentar la 'Solicitud de Usuarios y/o Perfiles de Acceso a los Sistemas de Cómputo', al encargado de informática, quien generará los Usuarios y Contraseñas correspondientes, para luego remitirlas al área de Recursos Humanos, para que éste a su vez los entregue al Usuario Final, con la confidencialidad requerida. II. Se debe otorgar a los usuarios acceso solamente a la información mínima necesaria para la realización de sus labores. III. Es responsabilidad del encargado de informática ver que los privilegios de acceso de los diversos usuarios estén alineados con las necesidades para la realización correcta de sus actividades en la entidad.	30%
A.8.2. Respaldo					
Objetivo: Se recomienda preservar la integridad y disponibilidad de los servicios de procesamiento de información					

A.8.2.1. Respaldo de información	Aplica	Se recomienda la realización de copias de respaldo de la información que maneja la institución, de forma periódica, además de ello las copias de seguridad deben ser probadas para demostrar su correcto funcionamiento	10%	I. El encargado de informática es responsable de asegurar que se generen copias de respaldo institución, en medios físicos o en la nube, para ello se deberán capacitar al personal. II. Debe formalmente definirse procedimientos para la creación y recuperación de copias de respaldo. III. Cada 2 meses deben efectuarse pruebas para asegurar el correcto funcionamiento de los archivos guardados, así como el funcionamiento de las memorias usb, pendrive, esto ayudara a fortalecer la capacidad de restaurar información en caso de que suceda un imprevisto. IV. Los usuarios deben generar copias de respaldo de información restringida transfiriendo archivos a la carpeta personal establecida para dicho fin por el encargado de informática, a la vez que esa información debe ser almacenada a la par en un pendrive exclusivo para dicha categoría información	50%
A.9. Gestión de seguridad de redes.					
Objetivo: Asegurar la protección de la información en redes y la protección de la estructura de soporte					
A.9.1. Controles de red	Aplica	Las redes deben ser correctamente manejadas, controladas, y gestionadas mediante estándares, para asegurar la información	0%	I. Todas las conexiones realizadas entre la red interna (esto abarca la red física, como también la red inalámbrica) de la institución e Internet, deben ser controladas por un firewall para prevenir accesos no autorizados.	50%

A.9.2. Seguridad de los servicios de red	Aplica	Controles de seguridad, niveles de servicio, ya sean servicios internos o provisto de terceros	0%	I.	Todas las conexiones de red internas y externas, sean por cableado o por Access point, deberán tener una contraseña para poder hacer uso de ellas, estarán delimitadas el Control A.10 Criptografía, de igual manera deben cumplir con las políticas de la Institución sobre servicios de red y control de acceso. Es responsabilidad del encargado de informática, determinar que los servicios sean los óptimos, o realizar requerimientos para la adecuación que necesite la entidad	50%
A.10 Criptografía						
A.10.1. Controles criptográficos						
Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y la integridad de la información						
A.10.1.1 Gestión de Claves	Aplica	Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada en la entidad	0%	I. II. III. IV.	Todas las contraseñas deben expirar dentro de un periodo que no exceda los ciento cincuenta (150) días. Los usuarios no deben poder cambiar sus contraseñas al menos 1 vez por mes. Se recomienda que los encargados de administrar la página web de la entidad, que son la Dirección de Informática del gobierno Regional de Huánuco, que el sistema web este configurado para deshabilitar los identificadores de los usuarios en caso de ocurrir (3) intentos fallidos de autenticación. En los casos que los sistemas utilizados no soporten controles para las características establecidas para la estructura, vigencia, reutilización e intentos fallidos de ingreso, en el punto de gestión de claves, se debe documentar la excepción a la política, detallando la viabilidad de modificar la aplicación para soportar las características establecidas para las contraseñas.	50%

		La asignación de claves se debe controlar a través de un proceso de gestión formal. Generando una clave con más de ocho caracteres, usando mayúsculas, minúsculas, números y caracteres especiales	0%	I. Todas las contraseñas deben tener una longitud mínima de ocho (8) caracteres y no deben contener espacios en blanco. II. Las contraseñas deben ser difíciles de adivinar. Palabras de diccionario, identificadores de usuario y secuencias comunes de caracteres, como, por ejemplo “12345678” o “ABCDEFG”, no deben ser empleadas. III. Detalles personales como los nombres de familiares, número de documento de identidad, número de teléfono o fechas de cumpleaños no deben ser usados salvo acompañados con otros caracteres adicionales que no tengan relación directa. IV. contraseñas deben incluir al menos un carácter no alfanumérico. Las contraseñas deben contener al menos un carácter alfabético en mayúscula y uno en minúscula.	30%
A.11 Control de acceso					
Objetivo: Limitar el acceso de información considerada como "Restringida", en la entidad					

A.11.1 Política de control de acceso	Aplica	Se recomienda la implementación u n procedimiento formal para la inscripción y desinscripción de categorías o grupos de usuarios de acuerdo al nivel de acceso de información que requieran y/o servicios (impresión, etc.), estos grupos o	30%	I. Cada usuario deberá identificarse para el acceso a su computadora de su estación de trabajo a través de una cuenta de usuario local, el SO. Windows 10, trae esa exigencia de identificación II. Cada usuario de un sistema debe tener una cuenta de usuario PC que no sea compartido con otro usuario. III. Debe establecerse un procedimiento para asegurar que cuenta de usuario sea retirado cuando un empleado es despedido o transferido. IV. Las computadoras personales deben bloquearse luego de quince (15) minutos de inactividad. El usuario tendrá que autenticarse antes de reanudar su actividad. V. El usuario debe ser instruido en el uso correcto de las características de seguridad del terminal y funciones de todas las plataformas, estaciones de trabajo, computadoras	50%

		permisos se gestionan a través de Workgroups, una de las aplicaciones de Windows.		personales, etc., y debe cerrar la sesión o bloquear la estación de trabajo cuando se encuentre desatendida. VI. Es importante que todos los empleados protejan sus contraseñas respecto al login de sesión de inicio en su estación de trabajo, cada usuario es responsable de su uso y protección VII. Las contraseñas no deben ser divulgadas a ningún otro usuario salvo bajo el pedido de su jefe inmediato, con autorización del Encargado de informática. Si se divulga la contraseña, esta debe ser cambiada durante el próximo ingreso. VIII. El usuario autorizado es responsable de todas las acciones realizadas por alguna persona a quién se le ha comunicado la contraseña o identificador de usuario. IX. Las contraseñas deben estar siempre encriptados cuando se encuentren almacenadas o cuando sean transmitidas a través de redes.	
A.11.1.2. Aprovisionamiento de acceso a usuario	Aplica	Se recomienda que la administración de la entidad deba revisar los derechos de acceso de los usuarios en periodos regulares de tiempo utilizando un proceso formal..	10%	I. Debe existir un procedimiento formal para la inscripción y des inscripción de categorías o grupos de usuarios de acuerdo al nivel de acceso de información que requieran y/o servicios (impresión, etc.), estos grupos o permisos se gestionaran a través de Workgroups, una de las aplicaciones de Windows	50%
A.11.2. Responsabilidades de los usuarios					

Objetivo: Hacer que los usuarios respondan por la salvaguarda de su información					
A.11.2.1. Uso de Información:	Aplica	Los usuarios deben ser exigidos que sigan las prácticas de la organización en el manejo de información sensible	10%	I. Todo equipo de cómputo de propiedad de la entidad, serán usados solo para actividades relacionadas al puesto del usuario según el manual de funciones definidos para cada puesto dentro de la entidad II. Toda la actividad realizada utilizando un identificador de usuario determinado, es de responsabilidad del empleado a quién le fue asignado. Por consiguiente, los usuarios no deben compartir la información de su identificador con otros o permitir que otros empleados utilicen su identificador de usuario para realizar cualquier acción.	30%
A.11.3. Control de acceso a redes					
Objetivo: Evitar el acceso no autorizado a los servicios en red					
A.11.3.1. Política sobre el uso de servicios de red	Aplica	Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.	0%	I. El encargado de informática debe aprobar todas las conexiones con redes o dispositivos externos. II. El esquema de direccionamiento interno de la red no debe ser visible desde redes o equipos externos. Esto evita que “hackers” u otras personas pueden obtener fácilmente información sobre la estructura de red de la DRTPE y computadoras internas, para conocer las vulnerabilidades de la red se deben realizar análisis de las vulnerabilidades con softwares especializados como por ejemplo nmap, que es sencillo de utilizar, que nos detalla las falencias de la red (puertos de red abiertos, los firewalls actualizados, etc.). el uso de ese software es gratuito	30%

A.11.3.3 Identificación del equipo de red	Aplica	Se debe considerar la autenticación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.	0%	I. Todas las conexiones de red internas y externas deben cumplir con las políticas de la Institución sobre servicios de red y control de acceso. Es responsabilidad del encargado de informática, determinar lo siguiente: Elementos de la red que pueden ser accedidos El procedimiento de autorización para la obtención de acceso Controles para la protección de la red.	30%
A.11.3.4 Control de conexión de redes	Aplica	Se debe restringir la capacidad de conexión de los usuarios en las redes	30%	I. Al no tener desplegado programa de antivirus en la entidad, se hace prioritario limitar la capacidad de conexión a paginas (Facebook, páginas de ocio, etc), que no son de necesarios para el correcto desempeño de sus actividades, una recomendación seria que, a través de la instalación de algún programa, o bloqueadores de host cuya característica viene determinada en el S:O: Windows 10 II. Todos los servicios habilitados en los sistemas de acceso a información deben contar con una justificación coherente con las necesidades de la entidad. Los riesgos asociados a los servicios de red deben determinarse y ser resueltos antes de la implementación del servicio.	50%
A.12. Seguridad en las operaciones					
A.12.1. Gestión de vulnerabilidades técnicas					
Objetivo: Prevenir la explotación de vulnerabilidades técnicas					

A.12.2. Restricciones sobre instalación de software	Aplica	Reglas que determinen la instalación de software por parte de los usuarios, deben ser establecidas e implementadas	30%	I.	Es obligación del personal de la institución, emplear sólo los programas cuyas licencias han sido obtenidas por la institución y forman parte de su plataforma estándar. II. No se descargarán e instalaran software adicional a las necesarias para el desarrollo de sus actividades en la entidad, así mismo que el usuario de la red no hará uso de este para entrar a páginas web, que no sean necesarios para el desarrollo de sus actividades, ni redes sociales. III. Todos aquellos usuarios no administradores del equipo tendrán bloqueada la instalación de aplicaciones de cualquier origen en el equipo de la entidad, para lograr esto se recomienda realizar los siguientes pasos: Abrimos una ventana ejecutar de Windows mediante el atajo de teclado Win+R. Escribimos gpedit.msc y pulsamos Aceptar o Enter. Vamos a Configuración del Equipo. Entramos en Plantillas Administrativas. A continuación, en Componentes de Windows Y ahora seleccionamos Windows Installer. En el panel derecho seleccionamos Prohibir instalaciones de usuario. Marcamos la opción Habilitada. Salimos del editor.	50%

A.12.3. Protección contra virus informáticos			0%	I.	Se requiere la instalación urgente de un Antivirus corporativo para las computadoras, laptops, Tablet's, porque actualmente la entidad no cuenta con ningún programa de antivirus, esta situación hace que los equipos se encuentren vulnerables a los virus informáticos, fallas del Sistema Operativo, lo cual aumenta el riesgo de pérdida de información de los archivos almacenados en los equipos informáticos, además de ello el programa antivirus que la entidad implemente debe encontrarse licenciado y habilitado en todas las computadoras y debe ser actualizado periódicamente.	0%
				II.	Todos los archivos adjuntos recibidos a través del correo electrónico desde Internet deben ser revisados por un antivirus antes de ejecutarlos.	
				III.	El programa antivirus debe ser configurado para realizar revisiones periódicas para la detección de virus en los medios de almacenamiento de las computadoras de la institución.	
				IV.	La actualización del software SO, aplicaciones, y programas deben ser realizadas solo por el encargado de informática, con la debida autorización	
A.13. Gestión de incidentes de seguridad de la información						
Objetivo: Asegurar un tratamiento consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad						

A.13.1. Responsabilidades y procedimientos	Aplica	Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida	10%	I. II. III.	Si un empleado detecta o sospecha la ocurrencia de un incidente de seguridad, tiene la obligación de notificarlo al encargado de informática. Si un empleado detecta una vulnerabilidad (por ejemplo, que el antivirus este desactualizado, que el office no esté correctamente activado, etc.), esto debe ser notificado al encargado de informática El encargado de informática debe documentar todos los reportes de incidentes de seguridad	30%
A.13.2. Reporte de debilidades de seguridad de la información	Aplica	Los usuarios de los sistemas de información que posea la organización deben ser exigidos de reportar cualquier debilidad o mal funcionamiento observado	10%	I. II. III.	Si se sospecha la presencia de un virus en un sistema, el usuario debe notificar al encargado de informática, quien se encargará de la eliminación del virus, o incidente detectado El personal encargado de operar los sistemas de información debe registrar todos los errores y fallas que ocurren en el procesamiento de información (que en este caso sería la página web de la entidad) o en los sistemas de comunicaciones y notificar al Administrador de Red. En el caso de la DRTPE-Hco, la dirección debe considerar el contrato de un especialista en red, quien ocupe el cargo de Encargado de red, el formato de documentar una falla es de la siguiente manera: Nombre y cargo de quien reporta la falla, Hora y fecha de ocurrencia de la falla, Descripción del error o problema. Es responsabilidad del encargado de informática asegurarse que el virus haya sido eliminado por completo del sistema antes de conectar nuevamente el equipo a la red de datos.	30%

A.13.3. Evaluación y decisión sobre eventos de seguridad de la información	Aplica	Los eventos de seguridad de la información deben ser evaluados, y deben decidirse si son clasificados como incidentes de seguridad	0%	I. Los registros de fallas deben ser almacenados en archivos de Excel, para tener un control posterior, para futuras auditorias II. Los registros de fallas deben ser revisados semanalmente. III. Los registros de errores no solucionados deben permanecer abiertos hasta que se encuentre una solución al problema, este plazo para solución debe de ser máximo 2 días hábiles, si no se ha solucionado se deberá comunicar al área de informática GOREHCO. Además, estos registros deben ser almacenados para una posterior verificación independiente.	30%
A.14 Cumplimiento de los requisitos legales y contractuales					
Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias, relacionadas a la seguridad de la información					
A.14.1. Identificación de requisitos contractuales y de legislación aplicables	Aplica	Todos los requisitos legislativos, regulatorios y contractuales relevantes, así como el enfoque de la entidad para el cumplimiento por parte de la organización	0%	I. Para el planteamiento de estas políticas de seguridad, se tomó la siguiente Base Legal: • Ley N° 27444 “Ley del Procedimiento Administrativo General”. - Resolución Jefatural N° 340-94-INEI, que aprueba la Directiva N° 015-94-INEI/SJI. • Resolución de Contraloría General Nº 458-2008-CG “Guía para la Implementación del Sistema de Control Interno de las entidades del Estado”. • Resolución Ministerial Nº 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”.	50%

A.14.2. Privacidad y protección de datos personales	Aplica	La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulaciones	0%	I. La información manejada por los sistemas de información (página web de la DRTPE) y las redes asociadas debe estar adecuadamente protegida contra modificaciones no autorizadas, divulgación o destrucción, el uso de controles de acceso reduce la posibilidad del acceso no autorizado	30%
A.15. Revisiones de seguridad de la información					
Objetivo: Fijar que la seguridad de la información se encuentre implementada y que su uso se ajuste de acuerdo a los requerimientos de la organización					
A.15.1. Revisión independiente de la seguridad de la información	Aplica	El enfoque de la organización para manejar la seguridad de la información y su implementación.,	0%	I. La entidad debe mejorar continuamente la eficacia del plan de seguridad, mediante los resultados de auditorías de seguridad, así como de las acciones correctivas y preventivas por parte de la DRTPE, así como tener los recursos necesarios para este fin, la NTP ISO/IEC 27001:2014, recomienda que las instituciones hagan auditorias cada año, con el fin de afinar los controles de seguridad e considerar otros	30%

Fuente: Elaboración Propia

La tabla N 39, que es el planteamiento de las propuestas de políticas de seguridad de la información, fue propuesta mediante el estándar de la norma técnica peruana NTP¨:ISO27001-2014, la cual nos brinda el formato, así como sugerencias en las diversas categorías, que, según los requerimientos de la entidad, las cuales están basadas en un análisis de riesgos, la cual nos permitió estimar los riesgos a los cuales están expuestos los activos, así como las salvaguardas que debería tener, esta data permitió entender el contexto, para realizar un correcto tratamiento de riesgos de los activos informáticos. La siguiente tabla tiene la función de estimar los controles de seguridad necesarios, que de acuerdo a los requerimientos de seguridad de la información la entidad debería contar, estos controles se definen de la Sección – Dominio de la normativa, se le asigna una Prioridad, que significa si es aplicable en la entidad, la justificación del porque debe ir esos controles, así como de la propuesta en sí, que a criterio de la entidad esta puede

modificada, etc; y por último la tabla también muestra los valores de “aplicación-Pre”, que significa que controles se estaban aplicando al inicio por la entidad, la “aplicación-Post”, que es después de la propuesta cual es la escala o nivel de cumplimiento

El siguiente formato, se propone para el registro de fallas, el cual se hace referencia en la tabla N 39.

Tabla 40, Formato del procedimiento

Nro. De registro	Registro de fallas
Cargo del personal	
Nombre del personal	
Fecha y Hora	
Descripción del error o problema	

Fuente: Elaboración Propia

Después de realizado el planteo de las políticas de seguridad de la información, levantado las observaciones de la entidad, se evaluaron el Grado de Efectividad de la salvaguarda (% de madures salvaguarda o control de seguridad), en 2 momentos “pre” y “post”, de acuerdo a la tabla 25, esta evaluación se basó en información recogida de las entrevistas y revisión de documentos, se determinó un nivel de cumplimiento a cada uno de los controles de seguridad propuestos, la siguiente tabla especifica más detalladamente

Tabla 41 (Detalle de % madures salvaguarda o control de seguridad)

Inexistente	“No se lleva a cabo el control de seguridad en los sistemas de información”.	0
Inicial	“Las políticas o controles de seguridad existen, pero no se administran, no existe un proceso formal para realizarlas, su aplicación depende de la buena voluntad de los trabajadores”.	1
Repetible	“Las medidas de seguridad se realizan de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación”.	2
Definido	“El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección”.	3
Administrado	“El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado”.	4
Optimizado	“El control se aplica de acuerdo a un procedimiento documentado, aprobado y distribuido, su eficacia se mide periódicamente durante las auditorías informáticas mediante indicadores”.	5

Fuente: Elaboración Propia

La siguiente tabla muestra el impacto de los controles propuestos sobre los riesgos encontrados, de acuerdo a los dominios de la norma NTP-ISO 27001:2014, teniendo en cuenta el análisis de riesgos se puede observar porcentaje de cumplimiento de cada control, en 2 tiempos “Pre” y “Post”. Esta información nos ayuda a calcular el % de cumplimiento de las salvaguardas (% Mecanismos salvaguardas implantadas)

Tabla 42, % de cumplimiento Pre – Post controles o salvaguardas

No. Dom	DOMINIO DE LA NORMA	SECCIONES NORMA	% PRE SECCION	% PRE DOMINIO	% POST SECCION	% POST DOMINIO	% META CUMPLIMIENTO
5	A.1. Política de Seguridad de la Información	A.1. Orientación de la Dirección para la gestión de la seguridad de la información	5.0%	5.0%	30.0%	30.0%	40.0%
6	A.2. Organización de la seguridad de la información	A.2.1. Establecer Marco de Referencia	5.0%	10.0%	40.0%	30.0%	46.3%
		A.2.2 Asegurar Dispositivos móviles y teletrabajo	15.0%		20.0%		
7	A.3. Gestión de activos	A.3.1. Responsabilidad por los activos	23.3%	18.9%	43.3%	36.1%	71.5%
		A.3.2. Clasificación de la información	13.3%		30.0%		
		A.3.3. Manejo de los medios	20.0%		35.0%		
8	A.5. Monitoreo	A.5. Detectar actividades de procesamiento de información no autorizadas	0.0%	0.0%	30.0%	30.0%	50.0%
9	A.6 Seguridad de los recursos humanos.	A.6.1. Antes del empleo	5.0%	8.9%	30.0%	33.3%	64.3%
		A.6.2. Durante el empleo	6.7%		30.0%		
		A.6.3. Terminación o cambio del empleo	15.0%		40.0%		
10	A.7. Seguridad física y ambiental	A.7.1. Áreas seguras.	50.0%	35.0%	75.0%	59%	74%
		A.7.2. Seguridad de los equipos informáticos	20.0%		43.3%		
11	A.8 Gestión de las comunicaciones y operaciones	A.8.1. Procedimientos y responsabilidad operacionales	0.0%	5.0%	30.0%	30.0%	75.0%
		A.8.2. Respaldo (Back-Up)	10.0%		30.0%		

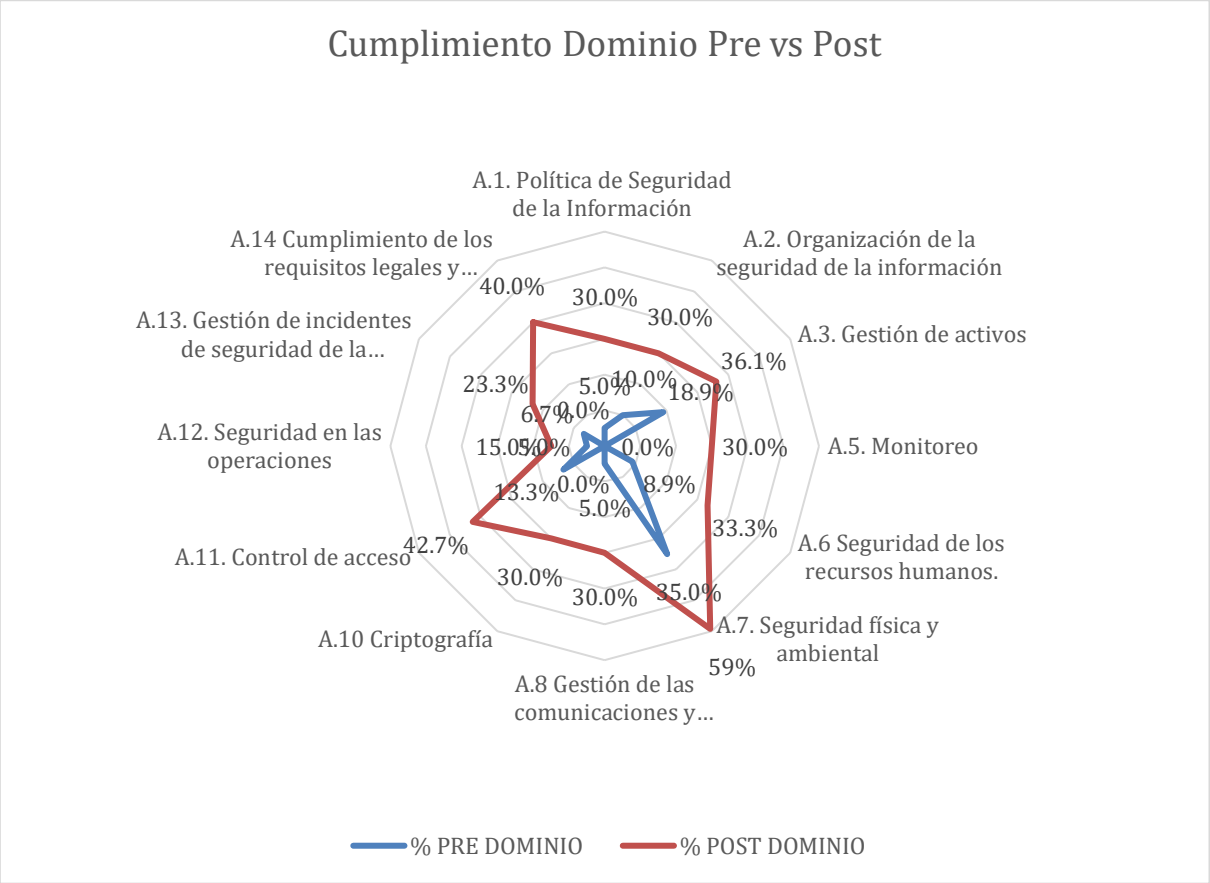
12	A.10 Criptografía	A.10. Controles criptográficos	0.0%	0.0%	30.0%	30.0%	75.0%
13	A.11. Control de acceso	A.11.1 Limitación de acceso a la información	0.0%	13.3%	40.0%	42.7%	65.6%
		A.11.2. Responsabilidades de los usuarios	30.0%		50.0%		
		A.11.3. Control de acceso a redes	10.0%		38.0%		
14	A.12. Seguridad en las operaciones	A.12. Gestión de vulnerabilidades técnicas	5.0%	5.0%	15.0%	15.0%	40.0%
15	A.13. Gestión de incidentes de seguridad de la información	A.13. Gestión de incidentes de seguridad de la información	6.7%	6.7%	23.3%	23.3%	75.0%
16	A.14 Cumplimiento de los requisitos legales y contractuales	A.14.1. Evitar infracciones de las obligaciones legales, estatutarias, regulatorias	0.0%	0.0%	50.0%	40.0%	66.7%
		A.14.2 Revisiones de seguridad de la información	0.0%		30.0%		
	Cumplimiento			8.98%		33.30%	61.91%

Fuente Elaboración Propia

Se puede observar que ha habido un incremento saludable del % de cumplimiento en los diferentes dominios de la normativa, al establecerse los controles necesarios, y también gracias a las correcciones de la entidad, se pudo llegar a este resultado, sim embargo, la mayoría de los objetivos de control están ubicados en porcentajes menores a 50%, esto se explica por el corto tiempo que la entidad ha tenido para el inicio del proyecto de implementación de las políticas, estas actividades requieren tiempo y recursos.

A continuación, se muestra un gráfico 18 de Comparación de % Cumplimiento, resalta la mejora del cumplimiento de los controles o salvaguardas

Gráfico 18, Comparación de % Cumplimiento



Fuente: Elaboración Propia

Una vez teniendo estos resultados, se procedió a realizar la siguiente tabla que contiene los activo con mayor riesgo de la entidad DRTPE, de acuerdo al mapa de riesgos, se identificó para cada riesgo la política que podría mitigar el riesgo una vez se implemente, la siguiente tabla muestra esa información

Tabla 43, Clasificación de Políticas por cada riesgo encontrado,

N°	ACTIVO	Tipo de Activo	Prob - Pre	[D]	[I]	[C]	[A]	[N_R]	Políticas				Estado	% Efectividad
1	Navegador web Google Chrome	Software	4	40	8	**28**	40	4	A.11. Control de acceso	A.5. Monitoreo	A.13. Gestión de incidentes de seguridad de la información	A.8 Gestión de las comunicaciones y operaciones	Proceso	**31.5%**
2	Router	Equipo Informático – Hardware	4	36	**24**	**20**	0	0	A.3. Gestión de activos	A.5. Monitoreo	A.7. Seguridad física y ambiental		Proceso	**41.8%**
3	Servicio de Internet	Servicio	4	36	16	**20**	16	8	A.10 Criptografía	A.5. Monitoreo	A.13. Gestión de incidentes de seguridad de la información		Proceso	**30.0%**
4	Encargado de Informatica	Información	4	32	16	**20**	0	4	A.11. Control de acceso	A.2. Organización de la seguridad de la información	A.1. Política de Seguridad de la Información		Proceso	**34.2%**
5	Personal encargado de brindar asistencia tecnica y capacitaciones diversas	Personal	4	32	16	**24**	0	4	A.6 Seguridad de los recursos humanos.	A.1. Política de Seguridad de la Información			Proceso	**31.7%**
6	Correo electrónico entidad - DRTPE-Hco	Servicio	4	**24**	**20**	**24**	**20**	16	A.11. Control de acceso	A.5. Monitoreo	A.10 Criptografía		Proceso	**34.2%**
	RIESGOS INTOLERABLES													
1	Computadoras de escritorio	Equipo Informático – Hardware	4	**28**	**20**	**24**	4	8	A.3. Gestión de activos	A.5. Monitoreo	A.7. Seguridad física y ambiental	A.2. Organización de la seguridad de la información	Proceso	**38.82%**

2	Disco Duro HDD	Equipo Informático – Hardware	4	**20**	**20**	**24**	4	0	A.3. Gestión de activos	A.5. Monitoreo	A.7. Seguridad física y ambiental	A.2. Organización de la seguridad de la información	Proceso	**38.82%**
3	Tableta Pad	Equipo Informático – Hardware	4	**28**	**20**	**20**	12	0	A.3. Gestión de activos	A.5. Monitoreo	A.7. Seguridad física y ambiental	A.2. Organización de la seguridad de la información	Proceso	**38.82%**
4	Red local LAN	Redes de Comunicación	4	**28**	**20**	**20**	8	0	A.3. Gestión de activos	A.5. Monitoreo	A.7. Seguridad física y ambiental	A.11. Control de acceso	Proceso	**41.99%**
5	Datos de gestion interna	Datos	3	**21**	**18**	12	15	15	A.11. Control de acceso	A.13. Gestión de incidentes de seguridad de la información	A.8 Gestión de las comunicaciones y operaciones	A.10 Criptografía	Proceso	**31.50%**
6	Información personal	Datos	4	**24**	**20**	16	12	16	A.11. Control de acceso	A.5. Monitoreo	A.2. Organización de la seguridad de la información	A.1. Política de Seguridad de la Información	Proceso	**33.17%**
7	Información restringida	Datos	4	**24**	**24**	16	8	12	A.3. Gestión de activos	A.11. Control de acceso	A.13. Gestión de incidentes de seguridad de la información		Proceso	**34.04%**
8	Computadora personal portatil de 2.0 GHz - Laptop	Equipo Informático – Hardware	3	**27**	15	**18**	12	6	A.11. Control de acceso	A.5. Monitoreo	A.2. Organización de la seguridad de la información	A.1. Política de Seguridad de la Información	Proceso	**33.17%**
9	Red privada virtual (Zoom) - corporativo - Pro	Redes de Comunicación	4	**20**	**20**	12	8	0	A.11. Control de acceso	A.5. Monitoreo	A.1. Política de Seguridad de la Información		Proceso	**34.22%**

10	Director Regional de Trabajo y Promocion del Empleo	Equipo Informático – Hardware	4	**28**	12	**20**	8	4	A.3. Gestión de activos	A.5. Monitoreo	A.7. Seguridad física y ambiental		Proceso	**41.76%**
11	Director de la Oficina Tecnico Administrativo	Personal	3	**21**	15	**18**	6	6	A.1. Política de Seguridad de la Información	A.6 Seguridad de los recursos humanos.			Proceso	**31.67%**
12	Director de promoción y protección de los derechos fundamentales y de la seguridad y salud en el trabajo	Personal	4	**28**	12	**20**	8	4	A.1. Política de Seguridad de la Información	A.6 Seguridad de los recursos humanos.			Proceso	**31.67%**
13	Director de dirección de inspección del trabajo	Personal	4	**28**	12	**20**	8	4	A.1. Política de Seguridad de la Información	A.6 Seguridad de los recursos humanos.			Proceso	**31.67%**
14	Director de dirección de promoción del empleo y capacitación laboral	Personal	4	**28**	12	**20**	8	4	A.1. Política de Seguridad de la Información	A.6 Seguridad de los recursos humanos.			Proceso	**31.67%**
15	Director zona de trabajo y promoción del empleo de leoncio prado	Personal	4	**28**	12	**20**	8	4	A.1. Política de Seguridad de la Información	A.6 Seguridad de los recursos humanos.			Proceso	**31.67%**
16	Jefe de Recursos Humanos	Personal	4	**24**	16	**20**	0	0	A.1. Política de Seguridad de la Información	A.6 Seguridad de los recursos humanos.			Proceso	**31.67%**
17	Personal Administrativo	Personal	4	**24**	16	**24**	0	0	A.1. Política de Seguridad	A.6 Seguridad de los			Proceso	**31.67%**

									de la Información	recursos humanos.					
18	S.O Windows	Software	4	**28**	**20**	4	16	12	A.5. Monitoreo	A.13. Gestión de incidentes de seguridad de la información	A.8 Gestión de las comunicaciones y operaciones	A.10 Criptografía	Proceso	**28.33%**
19	Datos de las certificaciones	Software	4	12	12	**20**	8	8	A.3. Gestión de activos	A.11. Control de acceso	A.1. Política de Seguridad de la Información		Proceso	**36.26%**
20	SIGA (Sistema Integrado de Gestión Administrativa)	Software	4	**20**	8	8	8	8	A.11. Control de acceso	A.5. Monitoreo	A.2. Organización de la seguridad de la información	A.1. Política de Seguridad de la Información	Proceso	**33.17%**
21	Microsoft Office Professional 2016	Software	4	**20**	12	8	16	8	A.11. Control de acceso	A.5. Monitoreo	A.8 Gestión de las comunicaciones y operaciones		Proceso	**34.22%**
22	Pagina web Institucional DRTPE - Hco (http://direcciontrabajo.regionhuanuco.gob.pe/)	Servicio	3	**21**	15	6	6	6	A.11. Control de acceso	A.13. Gestión de incidentes de seguridad de la información	A.8 Gestión de las comunicaciones y operaciones	A.10 Criptografía	Proceso	**31.50%**
23	Sistema de backup (RESPALDOS)	Equipo Informático – Hardware	3	**18**	15	0	12	0	A.3. Gestión de activos	A.7. Seguridad física y ambiental			Proceso	**47.64%**
24	Impresora Laser	Equipo Informático – Hardware	3	**21**	12	12	3	0	A.3. Gestión de activos	A.7. Seguridad física y ambiental			Proceso	**47.64%**
25	Impresora de Iyeccion a tinta	Equipo Informático – Hardware	3	**21**	15	0	3	0	A.3. Gestión de activos	A.7. Seguridad			Proceso	**47.64%**

										física y ambiental					
26	Equipo multifuncional copiadora fax impresora escanner de inyeccion a tinta color	Equipo Informático – Hardware	3	**21**	12	0	3	0	A.3. Gestión de activos	A.7. Seguridad física y ambiental			Proceso	**47.64%**
27	Equipo multifuncional copiadora impresora	Equipo Informático – Hardware	3	**21**	12	0	3	0	A.3. Gestión de activos	A.7. Seguridad física y ambiental			Proceso	**47.64%**
28	Unidad Central de Proceso - CPU	Equipo Informático – Hardware	3	**21**	12	12	3	0	A.3. Gestión de activos	A.7. Seguridad física y ambiental			Proceso	**47.64%**
29	Placa madre o Motherboard	Equipo Informático – Hardware	3	**18**	6	15	0	0	A.3. Gestión de activos	A.7. Seguridad física y ambiental			Proceso	**47.64%**
30	Mouse	Equipo Informático – Hardware	3	**18**	6	0	0	0	A.3. Gestión de activos	A.7. Seguridad física y ambiental			Proceso	**47.64%**
31	Teclado - Keyboard	Equipo Informático – Hardware	3	**18**	6	0	0	0	A.3. Gestión de activos	A.7. Seguridad física y ambiental			Proceso	**47.64%**
32	Pozo a Tierra	Equipamiento Auxiliar	3	**18**	0	0	0	0	A.3. Gestión de activos	A.7. Seguridad física y ambiental			Proceso	**47.64%**
33	Dispositivo USB - 8 GB	Equipamiento Auxiliar	3	**18**	6	6	3	0	A.3. Gestión de activos	A.7. Seguridad física y ambiental			Proceso	**47.64%**
34	Cableado de red - CAT 6A	Equipamiento Auxiliar	3	**18**	9	0	0	3	A.3. Gestión de activos	A.7. Seguridad física y ambiental			Proceso	**47.64%**

35	Identificador biometrico	Equipamiento Auxiliar	4	**24**	12	0	0	4	A.3. Gestión de activos	A.7. Seguridad física y ambiental			Proceso	**47.64%**
36	Sala de atención	Instalaciones	4	**24**	12	8	0	0	A.11. Control de acceso	A.7. Seguridad física y ambiental			Proceso	**50.92%**
37	Director de Prevencion y Solucion de Conflictos	Personal	3	**21**	9	15	6	3	A.1. Política de Seguridad de la Información	A.11. Control de acceso			Proceso	**36.33%**
38	Informes	Datos	3	3	9	12	**18**	9	A.1. Política de Seguridad de la Información	A.11. Control de acceso			Proceso	**36.33%**

Fuente: "Elaboración Propia"

Luego se va proceder a poner la tabla de riesgos post implementación de las políticas de seguridad para ver su efecto

Tabla 44, Estado de riesgos post Implementación

	N°	CAPA	CÓDIGO	ACTIVO	% EFICACIA DE LA SALVAGUARDA EN LA PROBABILIDAD	DIMENCIONES				
						[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [essential]	AED1	DATOS [data]	[ast]	Multimedia (Información de audio, videos, material de capacitación)	3	8	10	5	10	5
	AED2		[ots]	Datos de gestión interna	3	19	16	11	13	13
	AED3		[dge]	Datos de las certificaciones	2	4	4	6	2	2
	AED4	INFORMACIÓN [info]	[doc]	Documentos	4	15	12	9	24	15
	AED5		[inf]	Informes	2	3	4	6	8	4
	AED6		[exp]	Expedientes	2	7	4	6	3	3
	AED7		[tram]	Trámites	3	13	8	8	8	8
	AED8		[ipu]	Información pública	3	14	5	5	5	0
	AED9		[ipe]	Información personal	3	14	12	10	7	10
	AED10		[icl]	Información restringida	4	21	21	14	7	11
	AED11		[log]	Registro de datos de entrada, formato físico, Datos de control de acceso	2	3	2	0	0	1
	AED12	SERVICIO [service]	[sei]	Servicio de Internet	3	22	10	12	10	5
	AED14		[dir]	Correo electrónico entidad - DRTPE-Hco	4	22	18	22	18	15
APLICACIONES INFORMÁTICAS [apps]	APS1	SOFTWARE [SW]	[ehs]	S.O Windows	2	8	5	2	6	5
	APS3		[afp]	Adobe flash player	2	3	2	0	3	0
	APS4		[sql]	SIGA (Sistema Integrado de Gestión Administrativa)	3	10	4	4	4	4
	APS5		[mac]	Microsoft Office Professional 2016	3	12	7	5	10	5
	APS6		[off]	Ms Project 2016	2	2	3	2	2	0
	APS7		[msp]	Visio	2	3	3	3	2	0
	APS8		[vis]	Navegador web Google Chrome	3	23	5	16	23	2
	APS9		[brw]	Página web Institucional DRTPE - Hco (http://direccionTrabajo.regionhuanuco.gob.pe/)	2	11	8	3	3	3
	APS10		[msp]	Sistema de Backup (RESPALDOS)	2	10	8	0	6	0
EQUIPOS INFORMÁTICOS	EIH1	HARDWARE [HW]		Computadoras de escritorio	3	14	10	12	2	4
	EIH2			Computadora personal portátil de 2.0 GHz - Laptop	2	12	7	8	5	3
	EIH3			Impresora Laser	2	9	5	5	1	0
	EIH4			Impresora de Inyección a tinta	2	9	7	0	1	0

	EIH5			Equipo multifuncional copiadora fax impresor escáner de inyección a tinta color	2	9	5	0	1	0
	EIH6			Equipo multifuncional copiadora impresora scanner y/o fax	2	9	5	0	1	0
	EIH7			Unidad Central de Proceso - CPU	2	9	5	5	1	0
	EIH8			Placa madre o Motherboard	2	8	3	7	0	0
	EIH9			Lectores Ópticos	2	7	1	7	0	0
	EIH10			Memoria RAM	2	7	3	7	0	0
	EIH11			Disco Duro HDD	3	10	10	12	2	0
	EIH12			Tarjeta de Red, Grafica y sonido	2	7	4	0	0	0
	EIH13			Mouse	2	8	3	0	0	0
	EIH14			TECLADO - KEYBOARD	2	8	3	0	0	0
	EIH15			Disipador de calor (culer)	2	6	0	3	0	0
	EIH16			TABLETA PAD	3	15	11	11	6	0
	EIH17			Router	3	18	12	10	0	0
	EIH18			MONITOR LED 21.5 in	2	7	5	4	0	0
	EIH19			MONITOR PLANO	2	7	6	4	0	0
	EIH20			Pozo a Tierra	2	8	0	0	0	0
COMUNICACIONES [ccm]	CRC1	REDES DE COMUNICACIÓN [COM]	[lan]	Red local LAN	2	7	5	5	2	0
	CRC3		[ptp]	Red privada virtual (Zoom) - corporativo - Pro	3	10	10	6	4	0
	CRC4		[rte]	Red telefónica	3	9	9	5	0	0
	CRC5		[wif]	Red inalámbrica - Access Point	2	7	5	5	1	4
	CRC6		[mob]	Telefonía móvil	2	6	3	2	2	0
SOPORTES DE INFORMACIÓN [spi]	SPI1	SOPORTE [media]	[dsk]	Almacenamiento en la nube (Google Drive)	3	5	7	7	0	2
	SPI2		[cdv]	CD / DVD	3	2	4	2	2	0
	SPI3		[pml]	Proyector multimedia	2	3	3	0	0	0
	SPI4		[usb]	Dispositivo USB - 8 GB	2	8	3	3	1	0
	SPI5			cable adaptador USB 3.0 a SATA	2	6	0	0	0	0
	SPI6		[tjm]	Tarjeta de memoria	2	1	0	3	1	1
	SPI7		[hdv]	Hard drive - HDD - Externo	2	4	4	3	1	1
EQUIPAMIENTO AUXILIAR	EAE1	EQUIPAMIENTO [aux]	[ups]	Estabilizador de energía - Regulador de voltaje	4	16	16	0	8	0
	EAE2		[fal]	Fuentes de alimentación - Conectores	3	15	6	0	0	0
	EAE3		[cbl]	Cableado de red - CAT 6A	2	9	5	0	0	2
	EAE4		[mbl]	Mobiliario	3	6	0	3	0	3

	EAE5		[eqc]	Identificador biométrico	4	24	12	0	0	4
	EAE6		[cbl]	Cableado eléctrico	2	4	3	1	0	0
INSTALACIONES [ins]	INI1	INSTALACIONES [L]	[off]	Oficinas	1	2	2	0	0	0
	INI2		[slc]	Sala de orientaciones - Capacitaciones	1	2	1	1	1	0
	INI3		[sla]	Sala de atención	2	5	2	2	0	0
PERSONAL [per]	PSP1	PERSONAL [P]	[spt]	Director Regional de Trabajo y Promoción del Empleo	3	15	6	11	4	2
	PSP2		[jft]	Director de la Oficina Técnico Administrativo	2	10	7	9	3	3
	PSP3		[pnf]	Director de Prevención y Solución de Conflictos	2	10	4	7	3	1
	PSP4		[pad]	Director de promoción y protección de los derechos fundamentales y de la seguridad y salud en el trabajo	3	15	6	11	4	2
	PSP5		[sym]	Director de dirección de inspección del trabajo	3	15	6	11	4	2
	PSP6		[mme]	Director de dirección de promoción del empleo y capacitación laboral	3	15	6	11	4	2
	PSP7		[mmm]	Director zona de trabajo y promoción del empleo de leoncio prado	3	15	6	11	4	2
	PSP8		[opr]	Jefe de Recursos Humanos	3	12	8	10	0	0
	PSP9		[lya]	Personal Administrativo	3	14	9	14	0	0
	PSP10		[seg]	Encargado de Informática	3	18	9	12	0	2
	PSP11		[ctr]	Personal encargado de brindar asistencia técnica y capacitaciones diversas	3	18	9	14	0	2

Fuente: Elaboración Propia

V. RESULTADOS

5.1. Procesamiento de datos

Se describe a través de figuras y tablas cada dato general, a lo largo de la implementación de la metodología Magerit v3, mediante las propuestas de políticas de seguridad en la entidad DRTPE, para el tratamiento de riesgos respectivo

Esta sección 5.1 se ha dividido en 3 partes, las 2 primeras partes 5.1.1. Datos de implementación, 5.1.2. Datos post Implementación, son de relación de encuestas realizadas al personal administrativo para ver el impacto de la implementación de la metodología Magerit v3, mediante charlas, entrega de la propuesta de políticas de seguridad y la presentación del archivo Excel donde está todo el proceso de análisis y gestión de riesgos, todos estos datos nos permiten tener una idea del manejo de los activos informáticos post implementación la cual nos servirá para medir nuestros indicadores en la parte 5.1.3.

que es la muestra para la realización de la tesis

5.1.1. Datos de implementación (encuesta)

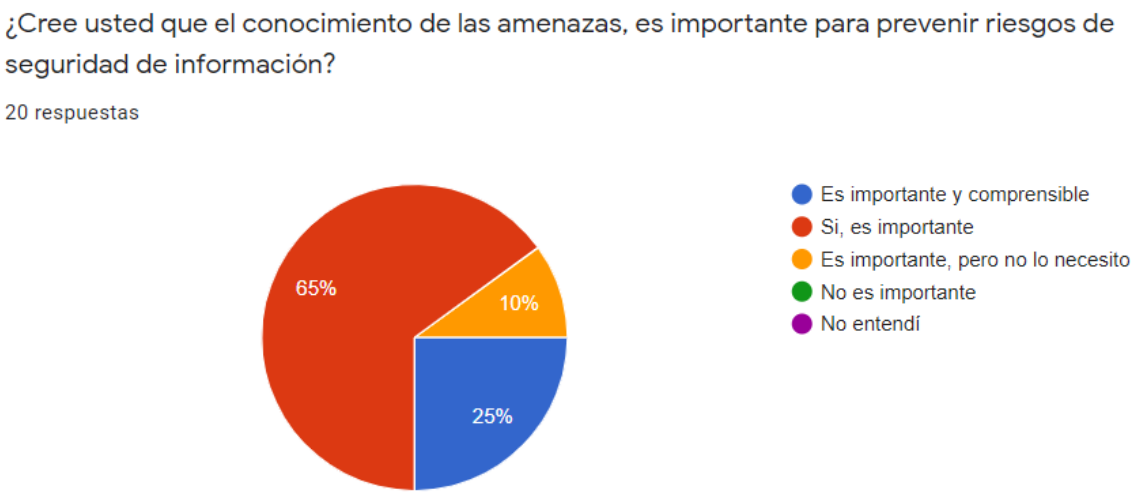
Los siguientes datos fueron obtenidos el día martes 20 de julio, día en el cual se implementó y explico a los trabajadores lo que se trataba de lograr, y una breve capacitación sobre las salvaguardas y temas de seguridad de la información, por lo que posterior a ello se realizó la siguiente encuesta de siete preguntas a una muestra de 20 personas.

Pregunta 1

Resumen de la pregunta 1: aquí podemos observar que los trabajadores en su mayoría piensan que la metodología y políticas de seguridad si ayudará a mejorar y reducir los riesgos de seguridad en la entidad en un 25% y 35%.

Escala	Personal entidad	
	Fi	hi%
1 = No entiende el tema	1	5%
2 = No ayuda ni mejora	0	0%
3 = Ayuda, pero es insuficiente	7	35%
4 = si ayuda	7	35%
5 = Mejora Considerablemente	5	25%
	20	100%

Pregunta 2:



Resumen de la pregunta 2: aquí podemos observar que los trabajadores piensan en un 65% que el identificar las amenazas es importante para prevenir los riesgos en la entidad.

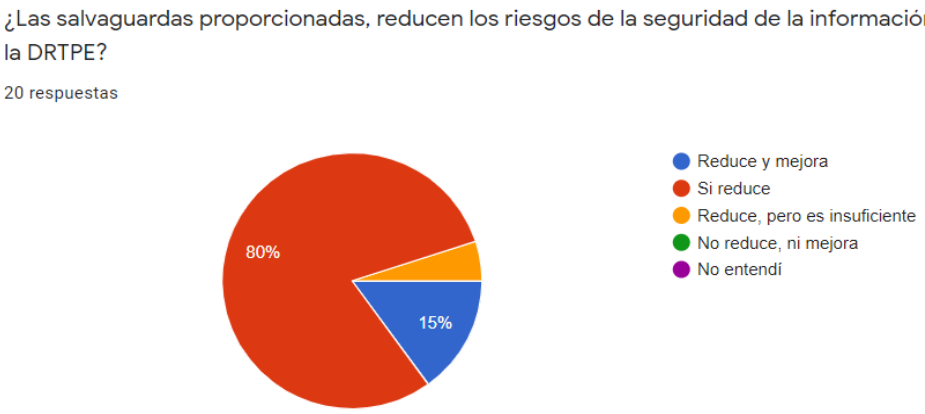
Escala	Personal entidad	
	Fi	hi%
1 = No entiende el tema	0	0%
2 = No es importante	0	0%
3 = No es tan importante	2	10%
4 = Si es importante	13	65%
5 = Importante y comprensible	5	25%
	20	100%

Pregunta 3

Resumen de la pregunta 3: aquí podemos observar que los trabajadores piensan que el conocimiento de las vulnerabilidades es visibles y posibles de evitarlas para prevenir perdidas de información.

Escala	Personal entidad	
	Fi	hi%
1 = No entiende los temas	0	0%
2 = No es importante	0	0%
3 = Si en su mayoría	14	70%
4 = Si Opino que son vulnerabilidades latentes	6	30%
	20	100%

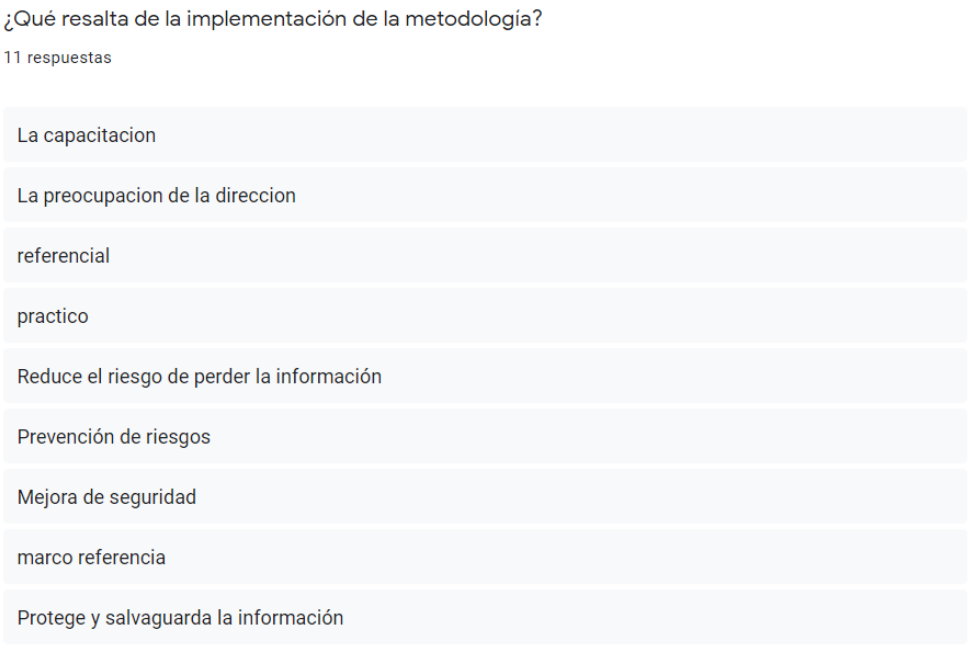
Pregunta 4:



Resumen de la pregunta 4: Aquí podemos observar que los trabajadores piensan que las salvaguardas proporcionadas son las adecuadas para reducir los riesgos de seguridad de la información en la entidad.

Escala	Personal entidad	
	Fi	hi%
1 = No entiende los temas	0	0%
2 = reduce ni mejora	0	0%
3 = Reduce per es insuficiente	1	5%
4 = Si reduce	16	80%
5 = Reduce y mejora mucho	3	15%
	20	100%

Pregunta 5



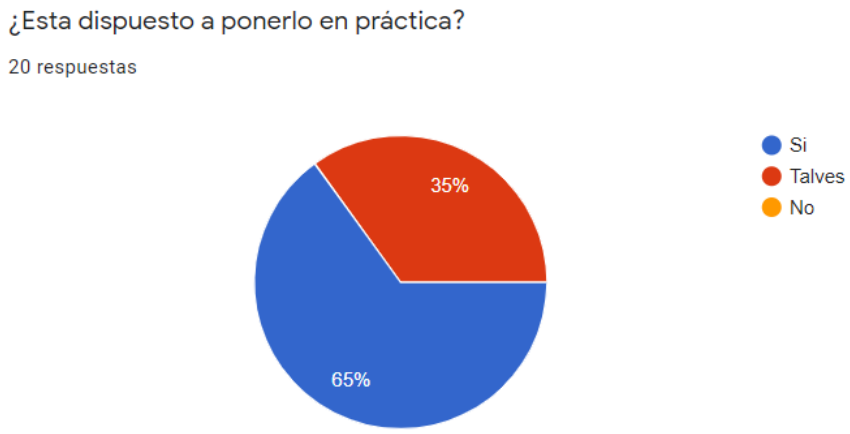
Resumen de la pregunta 5: En general se observa que los trabajadores creen que la capacitación, la propuesta de las políticas, como parte de la implementación, mejora la comprensión en los temas de seguridad

Pregunta 6:

Resumen de la pregunta 6: Aquí podemos observar que los trabajadores piensan que la implementación de la metodología es en promedio complicada, dado que interfiere en la rapidez de sus labores diarias.

Escala	Personal entidad	
	Fi	hi%
1 = Entendible	5	25%
2 = Promedio	14	70%
3 = Complicado	1	5%
	20	100%

Pregunta 7:



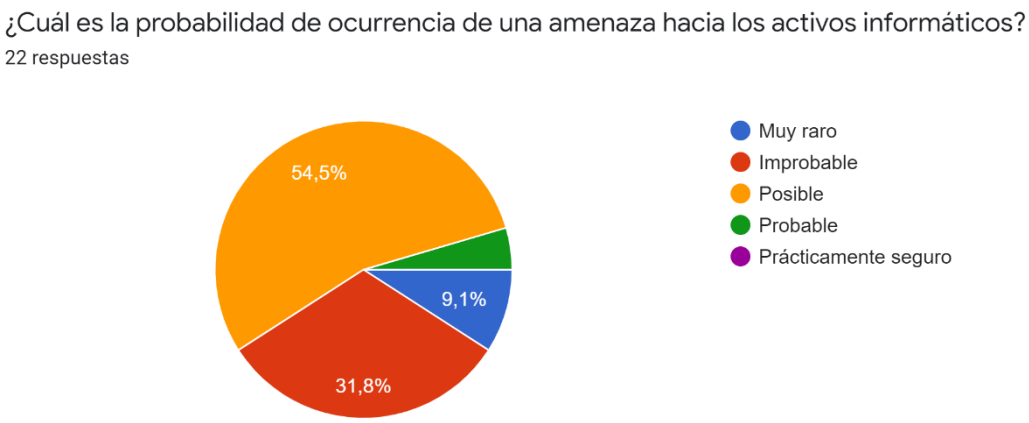
Resumen de la pregunta 7: la mayoría de los trabajadores están dispuestos a poner en prácticas las salvaguardas propuestas mediante las políticas de seguridad.

Escala	Personal entidad	
	Fi	hi%
No	0	0%
Talvez	7	35%
Si	13	65%
	20	100%

5.1.2. Datos Post Implementación (encuesta)

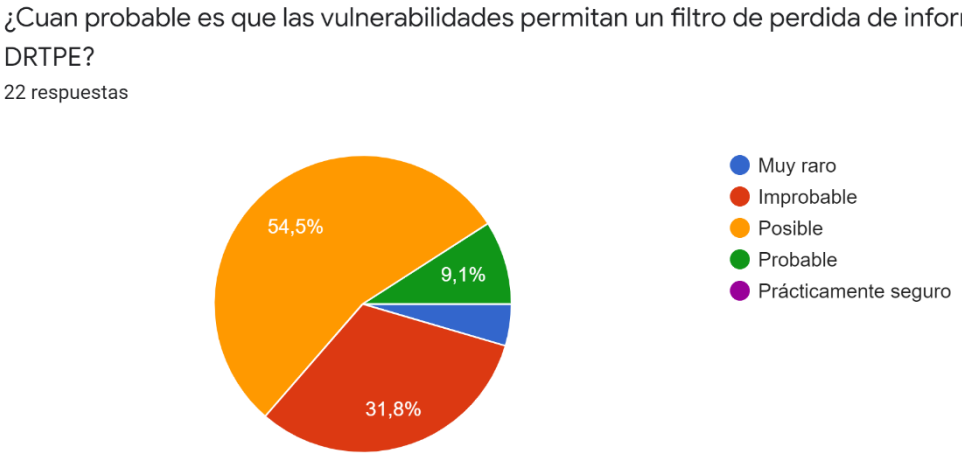
Los siguientes datos fueron obtenidos el día miércoles 4 de agosto, posterior a la implementación, día en el cual se recolecto los datos a través de una encuesta para identificar el impacto que se logró con la implementación de la metodología, esta encuesta se realizo a una muestra de 22 personas con un total de cinco preguntas, en la cual se tomó como variables la amenaza, riesgo, vulnerabilidad, salvaguardas y políticas de seguridad.

Pregunta 1

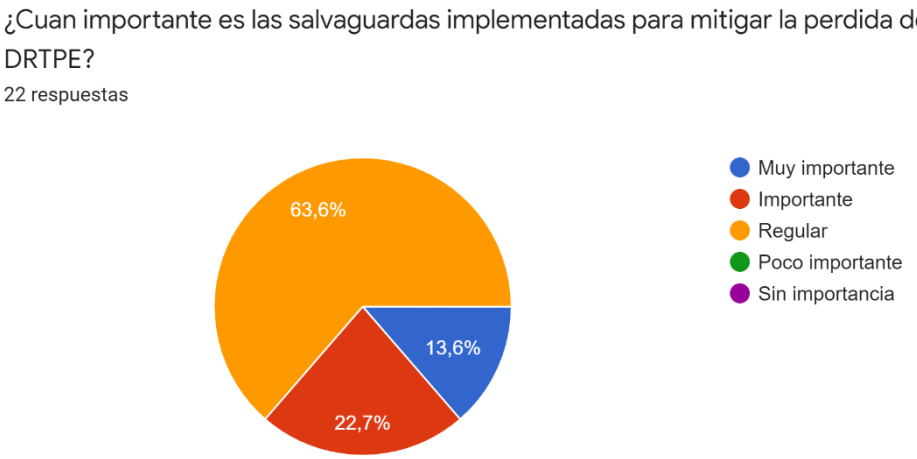


Resumen de la pregunta 1: Según los datos, podemos observar que la probabilidad de ocurrencia redujo en referencia al inicio del proyecto, teniendo un total de 54.5% de posibilidad de ocurrencia de una amenaza.

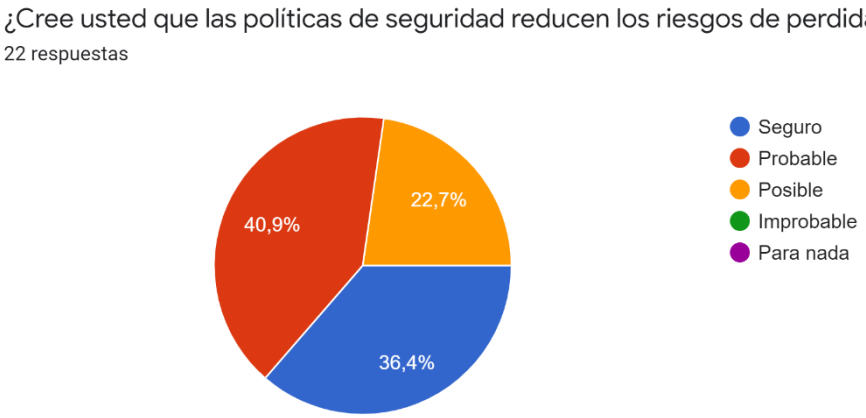
Pregunta 2: Aquí podemos observar que la probabilidad de ocurrencia de perdida de información es de 45.5%, siendo de esta manera un porcentaje menor al inicio del proyecto.



Pregunta 3: Aquí podemos observar que las vulnerabilidades aun son latentes de perder información, haciendo que el porcentaje de probabilidad sea de 54.5%.



Pregunta 4: como podemos observar, las salvaguardas son importantes en un rango de 40% a 60%, con un promedio de 63.6% de aceptación posterior a la implementación del proyecto.



Pregunta 5: Aquí podemos observar que los trabajadores piensan que las políticas de seguridad reducen los riesgos de perdida de información y ayudan a la seguridad en la entidad.

5.1.3. Procesamiento de datos en relación a las variables de estudio

Mediante los datos obtenidos en las 2 secciones anteriores (referente al proceso de implementación de la metodología Magerit v3, mediante políticas de seguridad), nos permiten describir mediante figuras y tablas en las respectivas dimensiones de las variables.

Análisis descriptivo de la variable independiente: metodología Magerit v3

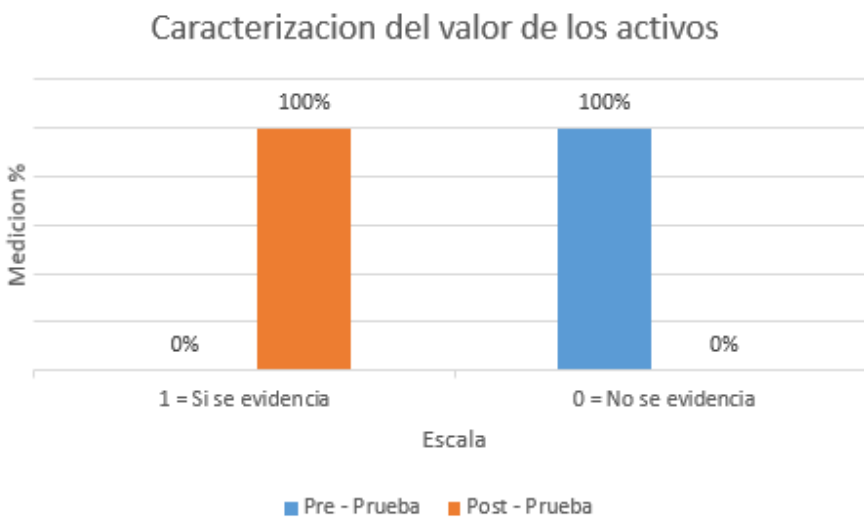
Dimensión: Mapa de Valor
Indicador: Caracterización del valor que representan los activos para la Entidad

Tabla 45, Resultado del indicador – Caracterización del valor de los activos

Dimensión - Mapa de Valor Indicador - Caracterización del valor que representan los activos para la Entidad	Pre prueba "Activos informáticos antes de la implementación Magerit v3"		Post prueba "Activos informáticos después de la implementación Magerit v3"	
Escala	Activos		Activos	
	Fi	hi%	Fi	hi%
1 = Si se evidencia	0	0%	54	100%
0 = No se evidencia	54	100%	0	0%
	54	100%	54	100%

Fuente: Elaboración Propia

Gráfico 19, Resultado de la Caracterización del valor de los activos



Fuente: Elaboración Propia

Interpretación

Del gráfico N° 19, se observa que en los resultados alcanzados antes de la implementación de la metodología Magerit v3, el 100% que representa a 54 activos, no contaban con una correcta caracterización de los activos, Mientras que en la etapa de post – implementación, se puede observar que incrementó la cantidad de activos que cuentan con la debida caracterización a 100%

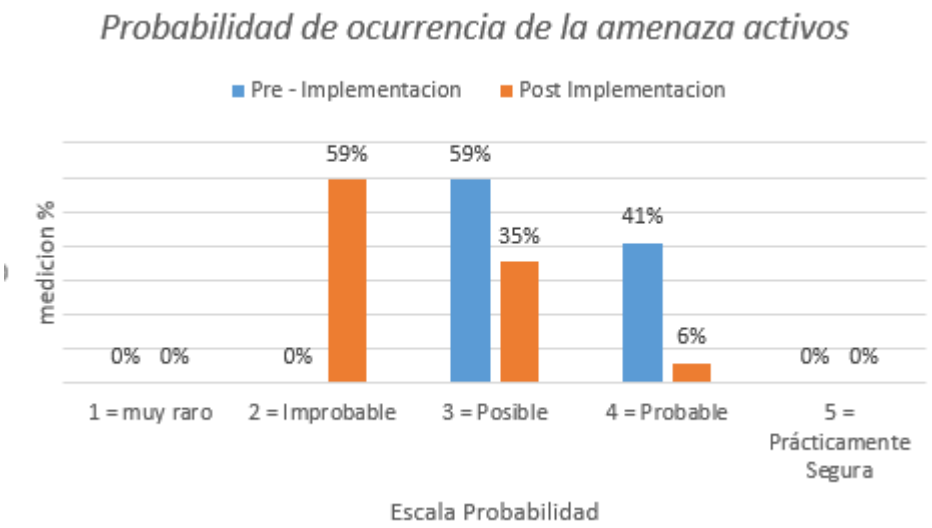
Dimensión: Amenazas
Indicador: Probabilidad de ocurrencia de la amenaza

Tabla 46, Resultado del indicador "Probabilidad de ocurrencia de la amenaza"

Dimensión – Amenaza Indicador - Probabilidad de ocurrencia de amenaza	Pre prueba "Activos informáticos antes de la implementación Magerit v3"		Post prueba "Activos informáticos después de la implementación Magerit v3"	
Escala	Activos		Activos	
	Fi	hi%	Fi	hi%
1 = muy raro	0	0%	0	0%
2 = Improbable	0	0%	32	59%
3 = Posible	32	59%	19	35%
4 = Probable	22	41%	3	6%
5 = Prácticamente Segura	0	0%	0	0%
	54	100%	54	100%

Fuente: "Elaboración Propia"

Gráfico 20, Probabilidad de ocurrencia de amenaza



Fuente: "Elaboración Propia"

Interpretación:

La tabla N° 46 señala los resultados del indicador “probabilidad de ocurrencia” para el análisis de los activos informáticos antes de la implementación de la metodología Magerit v3, se aprecia que, de los 54 activos evaluados, 32 activos, que representan al 59% del total, se encuentran en la categoría de probabilidad de amenaza posible, así como 22 activos, que representan 41%, se encuentran en la categoría de amenaza probable, se puede establecer en esta primera parte que es muy probable que se materialicen las amenazas a las cuales están expuestos los activos de información de la entidad. En cuanto a la post implementación de la metodología Magerit v3, se aprecia que a comparación de la prueba de pre-implementacion ahora solo 19 activos de información, que representan 35%, se ubican en la categoría de probabilidad posible, así como 3 activos de información, que representan 6%, se ubica en la categoría de riesgo probable, de esta comparativa se puede visualizar que hubo una reducción en la probabilidad de afectación de las amenazas, así como ahora 32 activos se ubican en la categoría Improbable, que ahora representa 59% del total de activos.

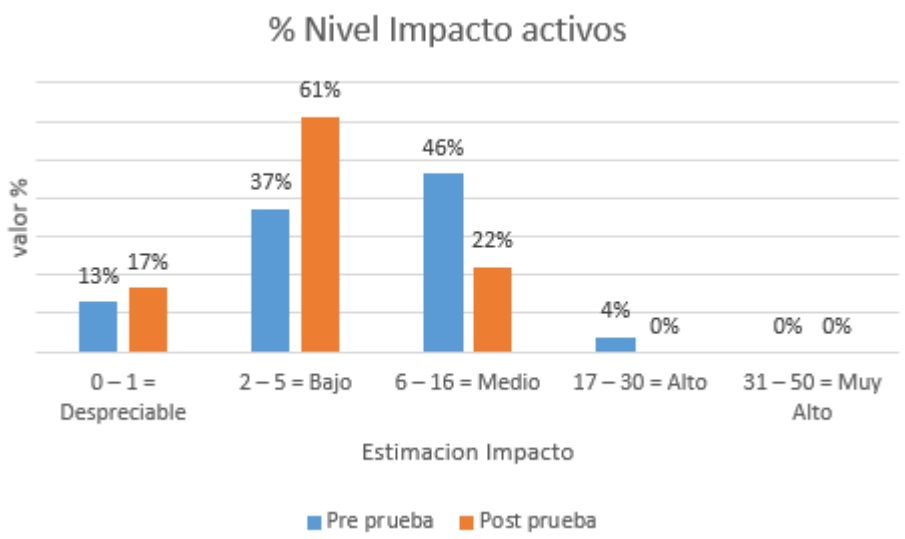
Dimensión: Impacto
Indicador: % Nivel de Impacto

Tabla 47, Resultado del Indicador % Nivel de Impacto

Dimensión – Impacto	Pre prueba “Activos informáticos antes de la implementación Magerit v3”		Post prueba “Activos informáticos antes de la implementación Magerit v3”	
Indicador - % Nivel de Impacto				
Escala	Activos		Activos	
	fi	hi%	fi	hi%
0 – 1 = Despreciable	7	13%	9	17%
2 – 5 = Bajo	20	37%	33	61%
6 – 16 = Medio	25	46%	12	22%
17 – 30 = Alto	2	4%	0	0%
31 – 50 = Muy Alto	0	0%	0	0%
	54	100%	54	100%

Fuente: Elaboración Propia

Gráfico 21, Resultado de dimensión Impacto activos



Fuente: Elaboración Propia

Interpretación:

La tabla N°47 señala los resultados del indicador “% nivel de impacto” para el análisis de los activos informáticos antes de la implementación de la metodología Magerit v3; se observa que, de los 54 activos informáticos evaluados, 4% que representan a 2 activos informáticos se encuentran en la categoría de impacto “Alto”, 46% que representan a 25 activos informáticos se encuentran en la categoría de impacto “medio”, estos datos nos indican que si estos activos tuviesen la materialización de las amenazas, el impacto en los activos que sufriría la entidad sería un daño importante.

En cuanto a lapost prueba para el análisis de los activos después de la implementación de la metodología Magerit v3, se observa una reducción a 0% de los activos informáticos que se encuentran en la categoría de impacto “Alto”, asimismo la categoría de impacto “Medio” disminuyo a 22%, que representan solamente a 12 activos informáticos

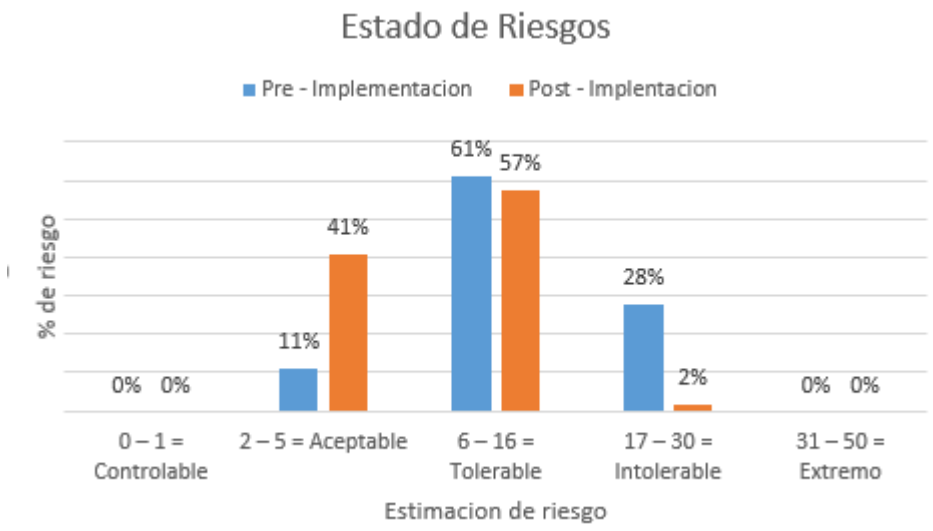
Dimensión: Riesgo
Indicador: Estimación de riesgo

Tabla 48, Resultado del indicador "Estimación de riesgo"

Dimensión – Riesgo Indicador - Estimación de riesgo	Pre prueba "Activos informáticos antes de la implementación Magerit v3"		Post prueba "Activos informáticos después de la implementación Magerit v3"	
Escala	Activos		Activos	
	Fi	hi%	Fi	hi%
0 – 1 = Controlable	0	0%	0	0%
2 – 5 = Aceptable	6	11%	22	41%
6 – 16 = Tolerable	33	61%	31	57%
17 – 30 = Intolerable	15	28%	1	2%
31 – 50 = Extremo	0	0%	0	0%
	54	100%	54	100%

Fuente: "Elaboración Propia"

Gráfico 22, Resultado del indicador "Estimación de riesgo"



Fuente: "Elaboración Propia"

Interpretación:
La tabla N°44 señala los resultados del indicador "estimación de riesgo" para el análisis de los activos informáticos antes de la implementación de la metodología Magerit v3; se aprecia que, de los 54 tipos de activos de información evaluados, 15 activos, que representan al 28% se encuentran la categoría de riesgo Intolerable, el 61%, que son 33 activos se encuentran se encuentran en la categoría de riesgo Tolerable. En cuanto al análisis de los activos después de la implementación de la Metodología Magerit v3, se observa que a comparación del pre – implementación ahora el estado de riesgo intolerable se redujo a 2%, la categoría de riesgo Tolerable disminuyo a 57%, ya que la categoría de riesgo aceptable aumento a 41%

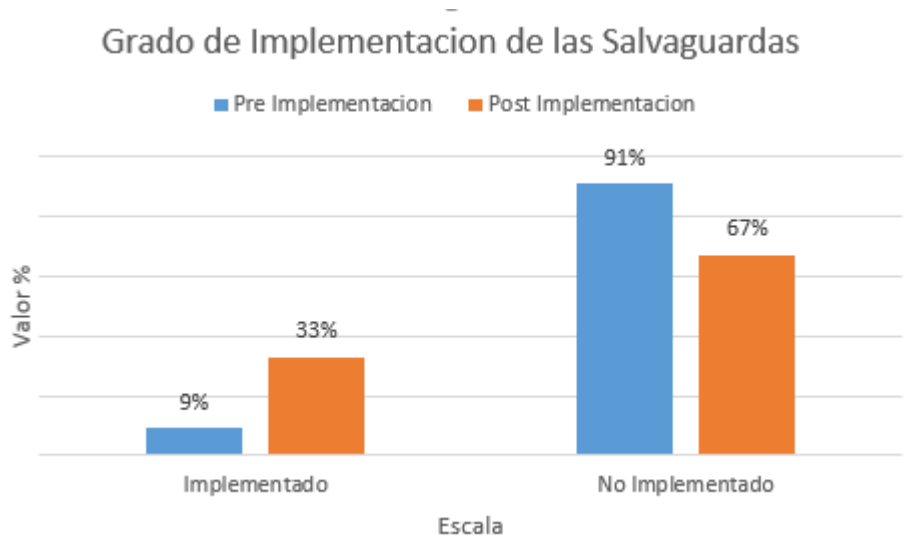
Dimensión: Salvaguardas
Indicador 1.1: Mecanismos de salvaguarda implantados actualmente

Tabla 49, Resultado del indicador "Mecanismos de salvaguarda implantados actualmente"

Dimensión Salvaguarda				
Grado de Implementación	**Antes de la Implementación**		**después de la Implementación**	
	FI	**%**	**FI**	**%**
Implementado	5	9%	18	33%
No Implementado	49	91%	36	67%
Total	54	100%	54	100%

Fuente: "Elaboración Propia"

Gráfico 23, Resultado del indicador "Mecanismos de salvaguarda implantados actualmente"



Fuente: "Elaboración Propia"

Del gráfico N° 22, se aprecia que en los resultados alcanzados antes de la implementación de la metodología Magerit v3, el 91% que representa a 49 activos, no cuentan con mecanismos de salvaguarda implantados, en tanto que en la etapa de post – implementación, se puede observar que incremento la cantidad de activos de 9% a 33%, que si cuentan con algún mecanismo de salvaguarda implementado

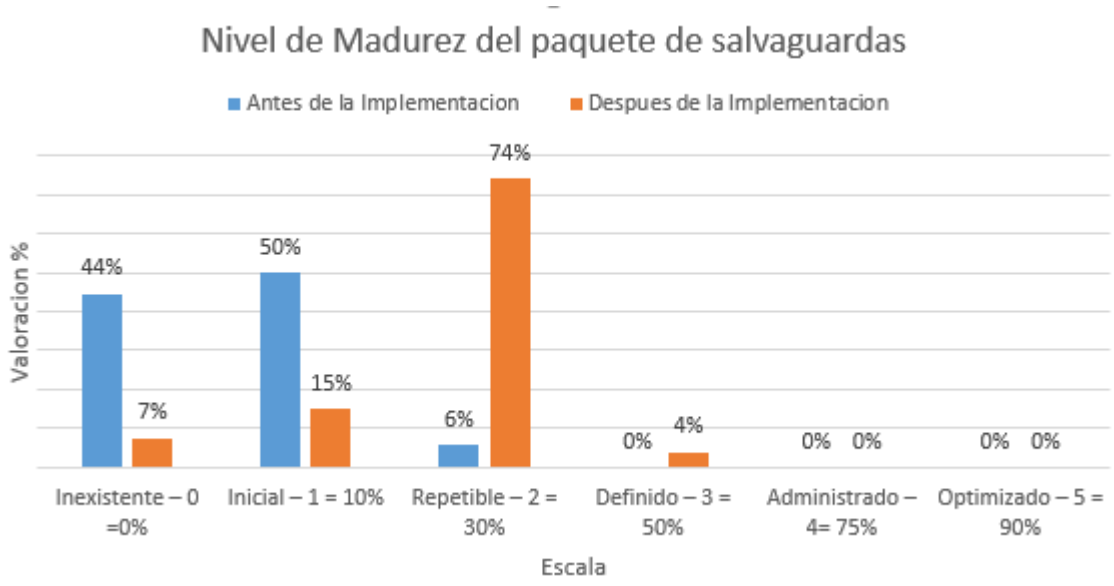
Dimensión: Salvaguardas
Indicador 1.2: Nivel de Madurez del paquete de salvaguardas

Tabla 50, Resultado del indicador "Nivel de Madurez del paquete de salvaguardas"

Nivel de Madurez del paquete de salvaguardas	Antes de la Implementación		Después de la Implementación	
	FI	%	FI	%
Inexistente – 0 =0%	23	44%	4	7%
Inicial – 1 = 10%	27	50%	8	15%
Repetible – 2 = 30%	3	6%	40	74%
Definido – 3 = 50%	0	0%	2	4%
Administrado – 4= 75%	0	0%	0	0%
Optimizado – 5 = 90%	0	0%	0	0%
Total	54	100%	54	100%

Fuente: "Elaboración Propia"

Gráfico 24, Resultado del indicador "Nivel de Madurez del paquete de salvaguardas"



Fuente: "Elaboración Propia"

Del gráfico N° 22, se aprecia que en los resultados alcanzados antes de la implementación de la metodología Magerit v3 en la dimensión "Nivel de madurez del paquete de salvaguardas, que significa el nivel de eficacia de las salvaguardas desplegadas", para cada activo informático, el 44 %, que representan a 23 activos informáticos, se encuentran en la categoría de salvaguarda "inexistente" que significa que estos activos cuentan con un paquete de salvaguardas que ofrecen una eficacia 0% en la reducción de riesgos, el 50%, que representan 27 activos informáticos se encuentran en la categoría de salvaguarda "inicial" que significa que estos activos cuentan con un paquete de salvaguardas que ofrecen una eficacia 10% en la reducción de riesgos y solamente el 6% de los activos, se encuentran en la categoría de salvaguarda "definido", que significa que estos activos cuentan con un paquete de salvaguardas que ofrecen una eficacia 30% en la reducción de riesgos.
Mientas que después de la implementación de la metodología Magerit v3, se observa una reducción al 7%, en la categoría de salvaguarda "inexistente" que significa que

estos activos que son 4 cuentan con un paquete de salvaguardas que ofrecen una eficacia 0% en la reducción de riesgos, así mismo se da la reducción a 15%, en la categoría de salvaguarda “inicial” que significa que estos activos que son 8 cuentan con un paquete de salvaguardas que ofrecen una eficacia 10% en la reducción de riesgos, esto se debe a que la categoría de paquete de salvaguarda “repetible” aumento a 74%, que significa que estos activos que son 40 cuentan con un paquete de salvaguardas que ofrecen una eficacia de 30% en la reducción de riesgos

Dimensión: Políticas
Indicador: Verificación de la formulación de políticas para los activos informáticos

Tabla 51, Resultado del indicador “Verificación de políticas en las dimensiones de seguridad”

Verificación de políticas en las dimensiones de seguridad	Antes de la Implementación		Después de la Implementación	
	FI	%	FI	%
Si se evidencia	0	0%	54	100%
No se evidencia	54	100%	0	0%
Total	54	100%	54	100%

Fuente: “Elaboración Propia”

Gráfico 25, Resultado del indicador “Verificación de políticas en las dimensiones de seguridad”

Fuente: “Elaboración Propia”

Del gráfico N° 23, se aprecia que, en los resultados alcanzados en la pre - implementación, el 100% que representa a 54 activos de información, “No” cuentan con políticas de seguridad definidas. En tanto que después de la implementación se puede visualizar que incfementó la cantidad de activos en 100%, que “Si” cuentan con políticas de seguridad definidas

Análisis descriptivo de la variable dependiente: Gestión de riesgos de la Seguridad de la información

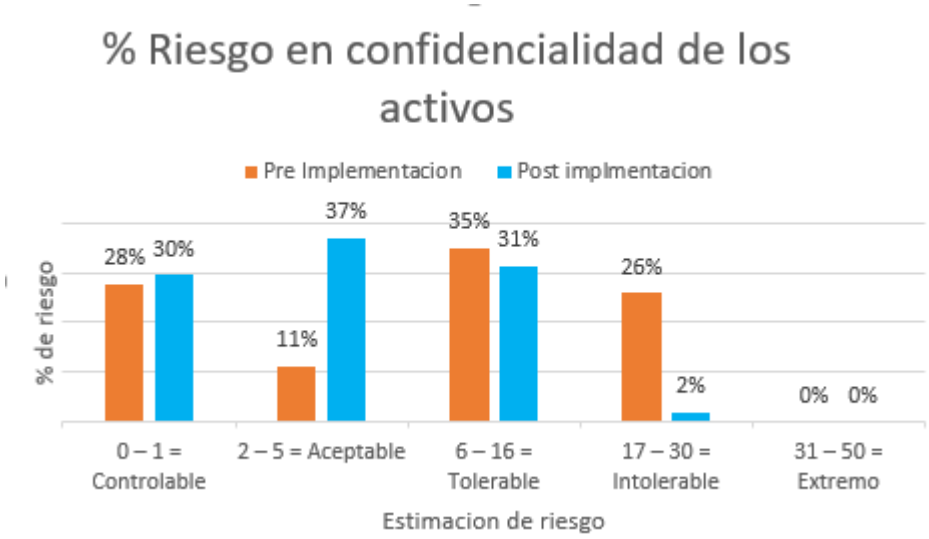
Dimensión: Confidencialidad
Indicador: % Riesgo en la confidencialidad de los Activos

Tabla 52, Resultado del indicador % Riesgo en la confidencialidad de los Activos

Dimensión – Confidencialidad Indicador - % Riesgo en la confidencialidad de los Activos	Pre prueba "Activos informáticos antes de la implementación Magerit v3"		Post prueba "Activos informáticos antes de la implementación Magerit v3"	
Escala	Activos		Activos	
	Fi	hi%	fi	hi%
0 – 1 = Controlable	15	28%	16	30%
2 – 5 = Aceptable	6	11%	20	37%
6 – 16 = Tolerable	19	35%	17	31%
17 – 30 = Intolerable	14	26%	1	2%
31 – 50 = Extremo	0	0%	0	0%
	54	100%	54	100%

Fuente: "Elaboración Propia"

Gráfico 26, Resultado del indicador % Riesgo en la confidencialidad de los Activos



Fuente: "Elaboración Propia"

Del gráfico N° 25, se aprecia que en los resultados alcanzados en la pre implementación, 26% que representan a 14 activos informáticos, se encuentra en un estado de riesgo en la confidencialidad, categoría de riesgo "intolerable", Mientras que en el post – implementación se puede observar que el estado de riesgo en la dimensión de confidencialidad "intolerable" se redujo a 2%, que representa a 1 activo informático esto se debe a que la categoría de riesgo "aceptable" aumento de 11% a 37%

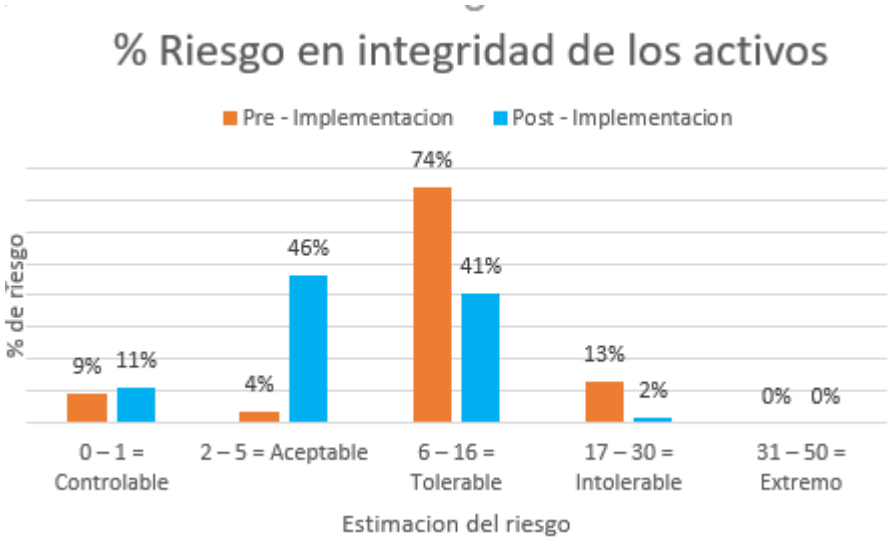
Dimensión: Integridad
Indicador: % Riesgo en la Integridad de los Activos

Tabla 53, Resultado del indicador % Riesgo en la Integridad de los Activos

Dimensión – Integridad Indicador - % Riesgo en la integridad de los Activos	Pre prueba "Activos informáticos antes de la implementación Magerit v3"		Post prueba "Activos informáticos antes de la implementación Magerit v3"	
Escala	Activos		Activos	
	Fi	hi%	fi	hi%
0 – 1 = Controlable	5	9%	6	11%
2 – 5 = Aceptable	2	4%	25	46%
6 – 16 = Tolerable	40	74%	22	41%
17 – 30 = Intolerable	7	13%	1	2%
31 – 50 = Extremo	0	0%	0	0%
	54	100%	54	100%

Fuente: "Elaboración Propia"

Gráfico 27, Resultado del indicador % Riesgo en la Integridad de los Activos



Fuente: "Elaboración Propia"

Del gráfico N° 26, se aprecia que en los resultados alcanzados en la pre implementación, 13% que representan a 7 activos informáticos, se encuentra en un estado de riesgo en la integridad, categoría de riesgo "intolerable", el 74% que son 40 activos informáticos se encuentran en la categoría "tolerable", Mientras que en la post - implementación se puede observar que el estado de riesgo en la dimensión de integridad "intolerable" se redujo a 2%, de igual manera la categoría de riesgo "tolerable" disminuyo a 41% que representan 22 activos informáticos, esta disminución se da porque la categoría de riesgo aceptable aumento de 4% a 46%, que representan a 25 activos informáticos

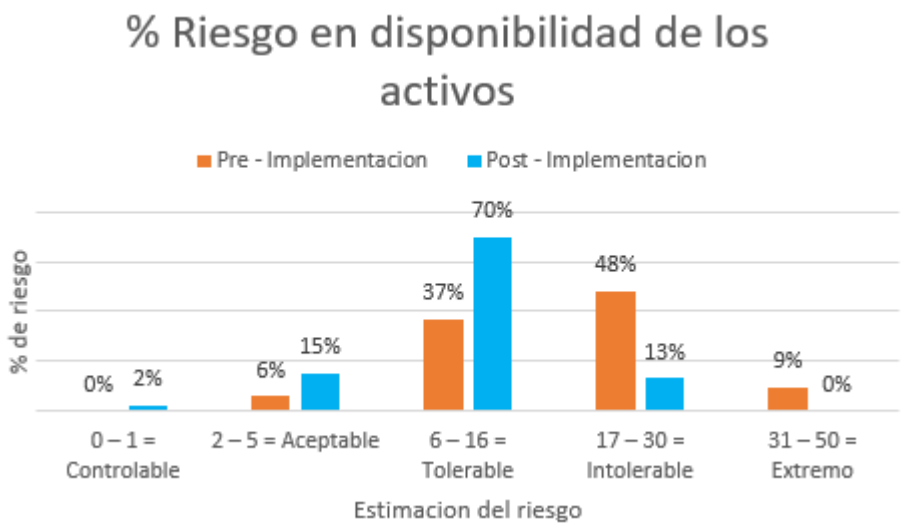
Dimensión: Disponibilidad
Indicador: % Riesgo en la disponibilidad de los Activos

Tabla 54, Resultado del indicador % Riesgo en la Disponibilidad de los Activos

Dimensión – Disponibilidad Indicador - % Riesgo en la disponibilidad de los Activos	Pre prueba "Activos informáticos antes de la implementación Magerit v3"		Post prueba "Activos informáticos antes de la implementación Magerit v3"	
Escala	Activos		Activos	
	Fi	hi%	fi	hi%
0 – 1 = Controlable	0	0%	1	2%
2 – 5 = Aceptable	3	6%	8	15%
6 – 16 = Tolerable	20	37%	38	70%
17 – 30 = Intolerable	26	48%	7	13%
31 – 50 = Extremo	5	9%	0	0%
	54	100%	54	100%

Fuente: "Elaboración Propia"

Gráfico 28, Resultado del indicador % Riesgo en la Disponibilidad de los Activos



Fuente: "Elaboración Propia"

Del gráfico N° 27, se aprecia que en los resultados alcanzados en la pre implementación, 9% que representan a 5 activos informáticos, se encuentra en un estado de riesgo en la dimensión de disponibilidad, categoría de riesgo "extremo", 48% que representan a 26 activos se encuentran en la categoría de riesgo "intolerable", el 37% que representan 20 de activos se encuentran en la categoría de riesgo "tolerable", en tanto que en la post – implementación se puede observar que el estado de riesgo en la dimensión de disponibilidad, categoría de riesgo "extremo" disminuyo a 0%, de igual manera la categoría de riesgo "intolerable" disminuyo a 13%, así como la categoría de riesgo "tolerable" incrementó a 70%

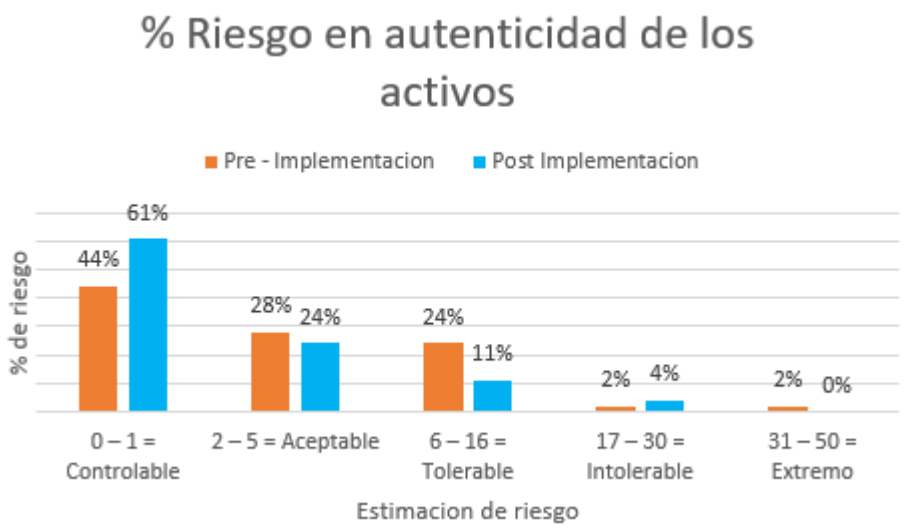
Dimensión: Autenticidad
Indicador: % Riesgo en la Autenticidad de los Activos

Tabla 55, Resultado del indicador % Riesgo en la Autenticidad de los Activos

Dimensión – Autenticidad Indicador - % Riesgo en la autenticidad de los Activos	Pre prueba "Activos informáticos antes de la implementación Magerit v3"		Post prueba "Activos informáticos antes de la implementación Magerit v3"	
Escala	Activos		Activos	
	Fi	hi%	fi	hi%
0 – 1 = Controlable	24	44%	33	61%
2 – 5 = Aceptable	15	28%	13	24%
6 – 16 = Tolerable	13	24%	6	11%
17 – 30 = Intolerable	1	2%	2	4%
31 – 50 = Extremo	1	2%	0	0%
	54	100%	54	100%

Fuente: "Elaboración Propia"

Gráfico 29, Resultado del indicador % Riesgo en la Autenticidad de los Activos



Fuente: "Elaboración Propia"

Del gráfico N° 27, se aprecia que en los resultados obtenidos en la pre implementación, 2% que representa a 1 activo informático, se encuentra en un estado de riesgo en la dimensión de autenticidad, categoría de "extremo", 2% que representa a 1 activo se encuentran en la categoría de riesgo "intolerable", el 24% que representan 13 de activos se encuentran en la categoría de riesgo "tolerable", Mientras que en la post – implementación se puede observar que el estado de riesgo en la dimensión de disponibilidad, la categoría "intolerable" aumento a 4%, ya que la categoría de riesgo "extremo" disminuyo a 0%, así como la categoría de riesgo "tolerable" disminuyo a 11%, ya que la categoría de riesgo "controlable" aumento a 61%

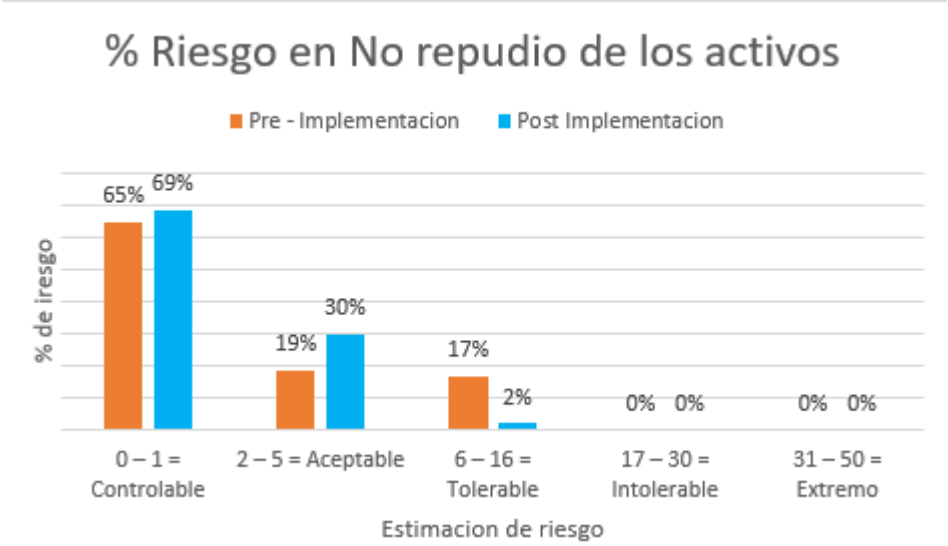
Dimensión: No repudio
Indicador: % Riesgo en el No repudio de los Activos

Tabla 56, Resultado del indicador % Riesgo en el No repudio de los Activos

Dimensión - No repudio Indicador - % Riesgo no repudio de los Activos	Pre prueba "Activos informáticos antes de la implementación Magerit v3"		Post prueba "Activos informáticos antes de la implementación Magerit v3"	
Escala	Activos		Activos	
	Fi	hi%	fi	hi%
0 – 1 = Controlable	35	65%	37	69%
2 – 5 = Aceptable	10	19%	16	30%
6 – 16 = Tolerable	9	17%	1	2%
17 – 30 = Intolerable	0	0%	0	0%
31 – 50 = Extremo	0	0%	0	0%
	54	100%	54	100%

Fuente: "Elaboración Propia"

Gráfico 30, Resultado del indicador % Riesgo en el No repudio de los Activos



Fuente: "Elaboración Propia"

Del gráfico N° 29, se aprecia que en los resultados alcanzados en la pre implementación, se observa que 17% que representan a 9 activos informáticos se encuentran en la categoría de riesgo "tolerable", el 19% que representan 10 de activos se encuentran en la categoría de riesgo "aceptable", Mientras que en la post - implementación se puede observar que el estado de riesgo en la categoría "tolerable" se redujo a 2%, ya que la categoría de riesgo "aceptable" aumento de 19% a 30%.

5.2. Contrastación de Hipótesis

Las pruebas de la Hipótesis General y Específicas, se efectuarán a través el Test de Wilcoxon (Pruebas No Paramétricas, cuando no provienen de una normalidad), debido a que se efectúa para muestras relacionadas (pre y post) y las variables son numéricas. Se efectuará de la manera siguiente:

a) Se calcula la Normalidad: Kolmogorov Smirnov, para muestras que rondan alrededor de (> 50 datos).
Criterios para determinar la Normalidad:

- P-valor => α ; Ha: Los datos provienen de una distribución Normal.
- P-valor < α ; Ho: Los datos NO provienen de una distribución Normal.

Como se trata de Pruebas No Paramétricas, P- Valor < α .

b) Se calcula P-Valor de la PRUEBA DE WILCOXON

Prueba de hipótesis general

Ha: La implementación de la metodología Magerit v3 y la Norma Técnica Peruana ISO 27001-2014 **mejora** la gestión de riesgos de la seguridad de la información de la DRTPE-Hco 2021.

Ho: La implementación de la metodología Magerit v3 y la Norma Técnica Peruana ISO 27001-2014 **no mejora** la gestión de riesgos de la seguridad de la información de la DRTPE-Hco 2021.

a) Calculo de la Normalidad

Resumen de procesamiento de casos

		Casos					
		Válido		Perdidos		Total	
	Estado	N	Porcentaje	N	Porcentaje	N	Porcentaje
RiesgoCuantitativo	PostImpl	54	100,0%	0	0,0%	54	100,0%
	PreImple	54	100,0%	0	0,0%	54	100,0%

Descriptivos

	Estado			Estadístico	Desv. Error
Riesgo Cuantitativo	PostImp	Media		6,90	,570
		95% de intervalo de confianza para la media	Límite inferior	5,75	
			Límite superior	8,04	
		Media recortada al 5%		6,63	
		Mediana		5,67	
		Varianza		17,555	
		Desv. Desviación		4,190	
		Mínimo		1	
		Máximo		21	
		Rango		19	
		Rango intercuartil		7	
		Asimetría		1,032	,325
		Curtosis		,801	,639
	PreImple	Media		12,92	,916
		95% de intervalo de confianza para la media	Límite inferior	11,08	
			Límite superior	14,76	
		Media recortada al 5%		12,77	
		Mediana		12,00	
		Varianza		45,358	
		Desv. Desviación		6,735	
		Mínimo		3	
		Máximo		27	
		Rango		24	
		Rango intercuartil		12	
		Asimetría		,466	,325
		Curtosis		-,844	,639

Pruebas de normalidad

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estado	Estadístico	gl	Sig.	Estadístico	gl	Sig.
RiesgoCuantitativo	PostImpl	,183	54	,000	,908	54	,001
	PreImple	,162	54	,001	,930	54	,004

a. Corrección de significación de Lilliefors

Como son 54 datos, se verificará la parte de Kolmogorov-Smirnov, en ambos casos se observa que el valor de Sig., tanto para la pre - implementación de la metodología Magerit v3, como después de la implementación, son valores menores a 0.05, esto se debe a que estamos trabajando con una confiabilidad del 95%

Se verificará lo siguiente: P-valor < α ; Ho: Los datos NO provienen de una distribución Normal.

- P-valor (pre-implementacion de la metodología Magerit v3) => 0,000 < α=0.05
- P-valor (post-implementacion de la metodología Magerit v3) => 0,001 < α=0.05

Se puede **concluir** que los datos no provienen de una distribución normal, y por consiguiente se procede a aplicar el Test de Wilcoxon

b) Test de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
PostImplementacionMageritv3 - PreImplementacionMageritv3	Rangos negativos	51[a]	26,00	1326,00
	Rangos positivos	0[b]	,00	,00
	Empates	3[c]		
	Total	54		

a. PostImplementacionMageritv3 < PreImplementacionMageritv3

b. PostImplementacionMageritv3 > PreImplementacionMageritv3

c. PostImplementacionMageritv3 = PreImplementacionMageritv3

Estadísticos de prueba

	PostImplementacionMageritv3 - PreImplementacionMageritv3
Z	-6,216[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Interpretación: Estamos trabajando al nivel de significancia α=5%=0.05**,** valor P es: 0,000 < 0,05, como es inferior al valor de significancia se rechaza la hipótesis nula y se acepta la hipótesis alterna (Ha), en otras palabras, la implementación de la metodología Magerit v3 y la Norma Técnica Peruana ISO 27001-2014 mejora la gestión de riesgos de la seguridad de la información de la DRTPE-Hco, a un grado de 95% de confiabilidad.

prueba de hipótesis específica N° 2

Ha: La identificación de las amenazas a los que están expuestos los activos informáticos **permite** estimar el alcance del daño de la seguridad de la información en la DRTPE-Hco 2021.

Ho: La identificación de las amenazas a los que están expuestos los activos informáticos **no permite** estimar el alcance del daño de la seguridad de la información en la DRTPE-Hco 2021.

a) Cálculo de la Normalidad

		Casos					
		Válido		Perdidos		Total	
	Estado	N	Porcentaje	N	Porcentaje	N	Porcentaje
ProbabilidadOcurrenciaAmenaza	PostImpl	54	100,0%	0	0,0%	54	100,0%
	PreImple	54	100,0%	0	0,0%	54	100,0%

Descriptivos

	Estado			Estadístico	Desv. Error
ProbabilidadOcurrenciaAmenaza	PostImpl	Media		2,46	,082
		95% de intervalo de confianza para la media	Límite inferior	2,30	
			Límite superior	2,63	
		Media recortada al 5%		2,40	
		Mediana		2,00	
		Varianza		,367	
		Desv. Desviación		,605	
		Mínimo		2	
		Máximo		4	
		Rango		2	
		Rango intercuartil		1	
		Asimetría		,941	,325
		Curtosis		-,064	,639
	PreImple	Media		3,41	,067
		95% de intervalo de confianza para la media	Límite inferior	3,27	
			Límite superior	3,54	
		Media recortada al 5%		3,40	
		Mediana		3,00	
		Varianza		,246	
		Desv. Desviación		,496	
		Mínimo		3	
		Máximo		4	
		Rango		1	
		Rango intercuartil		1	
		Asimetría		,388	,325
		Curtosis		-1,922	,639

Pruebas de normalidad

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estado	Estadístico	gl	Sig.	Estadístico	gl	Sig.
ProbabilidadOcurrenciaAmenaza	PostImpl	,370	54	,000	,698	54	,000
	PreImple	,387	54	,000	,624	54	,000

a. Corrección de significación de Lilliefors

Como son 54 datos, se verificará la parte de Kolmogorov-Smirnov, en ambos casos se observa que el valor de Sig., tanto para la pre - implementación de la metodología Magerit v3, como después de la implementación, son valores menores a 0.05, esto se debe a que estamos trabajando con una confiabilidad del 95%

Se verificará lo siguiente: P-valor < α ; Ho: Los datos NO provienen de una distribución Normal.

- P-valor (pre-implementacion de la metodología Magerit v3) => 0,000 < α=0.05
- P-valor (post-implementacion de la metodología Magerit v3) => 0,000 < α=0.05

Se puede **concluir** que los datos no provienen de una distribución normal, y por consiguiente se procede a aplicar el Test de Wilcoxon

b) Test de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
PostImplementacionMageritv3 - PreImplementacionMageritv3	Rangos negativos	49[a]	25,00	1225,00
	Rangos positivos	0[b]	,00	,00
	Empates	5[c]		
	Total	54		

a. PostImplementacionMageritv3 < PreImplementacionMageritv3

b. PostImplementacionMageritv3 > PreImplementacionMageritv3

c. PostImplementacionMageritv3 = PreImplementacionMageritv3

Estadísticos de prueba

	PostImplementacionMageritv3 - PreImplementacionMageritv3
Z	-6,872[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Interpretación: Estamos trabajando al nivel de significancia α=5%=0.05**,** valor P es: 0,000 < 0,05, como es menor al valor de significancia se rechaza la hipótesis nula y se acepta la hipótesis alterna (Ha), en otras palabras, la identificación de las amenazas a los que están expuestos los activos informáticos **permite** estimar el alcance del daño de la seguridad de la información en la DRTPE-Hco, a un grado de 95% de confiabilidad.

prueba de hipótesis específica N° 3

Ha: La verificación del nivel de cumplimiento de las salvaguardas **reduce** el nivel de **impacto** de los activos informáticos en la DRTPE-Hco 2021.

Ho: La verificación del nivel de cumplimiento de las salvaguardas **reduce** el nivel de **impacto** de los activos informáticos en la DRTPE-Hco 2021.

a) Cálculo de la normalidad

Resumen de procesamiento de casos

		Casos					
		Válido		Perdidos		Total	
	Estado	N	Porcentaje	N	Porcentaje	N	Porcentaje
Nivel_impacto	PostImpl	54	100,0%	0	0,0%	54	100,0%
	PreImple	54	100,0%	0	0,0%	54	100,0%

Descriptivos

	Estado			Estadístico	Desv. Error
Nivel_impacto	PostImpl	Media		2,69	,158
		95% de intervalo de confianza para la media	Límite inferior	2,37	
			Límite superior	3,00	
		Media recortada al 5%		2,63	
		Mediana		3,00	
		Varianza		1,352	
		Desv. Desviación		1,163	
		Mínimo		1	
		Máximo		6	
		Rango		5	
		Rango intercuartil		1	
		Asimetría		,428	,325
		Curtosis		,073	,639
	PreImple	Media		3,61	,222
		95% de intervalo de confianza para la media	Límite inferior	3,17	
			Límite superior	4,06	
		Media recortada al 5%		3,58	
		Mediana		3,50	
		Varianza		2,657	
		Desv. Desviación		1,630	
		Mínimo		1	
		Máximo		7	
		Rango		6	
		Rango intercuartil		2	
		Asimetría		,174	,325
		Curtosis		-,569	,639

Pruebas de normalidad

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estado	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Nivel_impacto	PostImpl	,171	54	,000	,916	54	,001
	PreImple	,146	54	,006	,938	54	,008

a. Corrección de significación de Lilliefors

Como son 54 datos, se verificará la parte de Kolmogorov-Smirnov, en ambos casos se observa que el valor de Sig., tanto para la pre - implementación de la metodología Magerit v3, como después de la implementación, son valores menores a 0.05, esto se debe a que estamos trabajando con una confiabilidad del 95%.

Se verificará lo siguiente: P-valor < α ; Ho: Los datos NO provienen de una distribución Normal.

- P-valor (pre-implementacion de la metodología Magerit v3) => 0,000 < α=0.05
- P-valor (post-implementacion de la metodología Magerit v3) => 0,006 < α=0.05

Se puede **concluir** que los datos no provienen de una distribución normal, y por consiguiente se procede a aplicar el Test de Wilcoxon

b) Test de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
PostImplementacionMageritv3 - PreImplementacionMageritv3	Rangos negativos	38[a]	19,50	741,00
	Rangos positivos	0[b]	,00	,00
	Empates	16[c]		
	Total	54		

a. PostImplementacionMageritv3 < PreImplementacionMageritv3

b. PostImplementacionMageritv3 > PreImplementacionMageritv3

c. PostImplementacionMageritv3 = PreImplementacionMageritv3

Estadísticos de prueba

	PostImplementacionMageritv3 - PreImplementacionMageritv3
Z	-5,688[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Interpretación: Estamos trabajando al nivel de significancia α=5%=0.05**,** valor P es: 0,000 < 0,05, como es inferior al valor de significancia se rechaza la hipótesis nula y se acepta la hipótesis alterna (Ha), en otras palabras, la verificación del nivel de cumplimiento de las salvaguardas **reduce** el nivel de **impacto** de los activos informáticos en la DRTPE-Hco 2021, a un grado de 95% de confiabilidad.

VI. DISCUSIÓN O CONTRASTACIÓN DE RESULTADOS

De acuerdo a los resultados obtenidos en la tesis, luego de la implementación de la metodología Magerit v3 y la Norma Técnica Peruana ISO 27001-2014, mediante políticas de seguridad, en los gráficos N 20, N21, N22, que en conjunto se puede notar que hay una **reducción** de riesgos de los activos informáticos relacionados a la seguridad de información, así como un incremento de las salvaguardas desplegadas en la entidad, luego de la contrastación de hipótesis general se determinó que la implementación de la metodología Magerit v3, mediante un análisis de riesgos y la Norma Técnica Peruana ISO 27001-2014 **mejora** la gestión de riesgos de la seguridad de la información de la DRTPE, donde se consideró: el valor de significancia es: 0.000 < 0.05, con la cual **se acepta la hipótesis general alterna** y se rechaza la hipótesis nula, a un grado de 95% de confiabilidad. Esta investigación coincide con la de (FLORES, 2015), que después de realizar un análisis de riesgo en la institución policial de Chiclayo, e implementar políticas de seguridad basadas en ISO 27001, concluye que hay una mejora en el nivel de seguridad de los activos informáticos, que se evidencia con la disminución de los niveles de riesgo respecto a esos activos, dicha investigación también trabaja con un nivel de confiabilidad al 95%. La mejora en la gestión de riesgos de la seguridad de la información permite conseguir un mejor diagnóstico de los riesgos a los cuales están expuestos los activos de información, así como una forma de poder mitigarlos

La implementación de la Metodología Magerit v3 nos ayuda a una **mejor** identificación de las amenazas a los que están expuestos los activos informáticos y de esta manera entender el contexto en que se encuentra la seguridad de la información, que es el inicio para determinar el estado de riesgos a los cuales están expuestos los activos informáticos, y posteriormente permitirá realizar una gestión del riesgo mediante el planteo de políticas, estos datos se ven reflejados en el grafico N° 19 “Probabilidad de Ocurrencia de Amenazas”, donde de los 54 activos evaluados, 32 activos, que representan al 59% del total, se encuentran en la categoría de probabilidad de amenaza posible, así como 22 activos, que representan 41%, se encuentran en la categoría de amenaza probable, a comparación de la prueba de post-implementacion ahora solo 19 activos de información, que representan 35%, se ubican en la categoría de probabilidad posible, así como 3 activos de información, que representan 6%, se ubica en la categoría de amenaza probable, estos datos nos indican una mejora en la reducción de Probabilidad de ocurrencia de las amenazas, de los activos informáticos mediante una mejor estimación del alcance del daño de la seguridad de la información, así mismo luego de la contrastación de la hipótesis especifica N° 02, se obtiene que el valor P es: 0,000 < 0,05, como es menor al valor de significancia se rechaza la hipótesis nula y se acepta la hipótesis alterna (Ha), en otras palabras la identificación de las amenazas a los que están expuestos los activos informáticos **permite** estimar el alcance del daño de la seguridad de la información en la DRTPE-Hco, a un nivel de 95% de confiabilidad

El establecimiento de salvaguardas para reducir el impacto a los cuales se ubican los activos informáticos, permitió a la entidad DRTPE, obtener un marco de referencia para poder guiarse realizar la implementación de estas; una primera pista la podemos obtener del gráfico N° 23, referente a "salvaguarda implantados actualmente" y tabla N° 47, que muestra un incremento de las salvaguardas implantadas actualmente en los activos de 9% a 33%, por consiguiente, se puede establecer, que, al haber más activos con salvaguardas establecidas, se obtendrá una mejor reducción del nivel de impacto en los activos, de igual manera el grafico N °22 "Nivel de Madurez del paquete de salvaguardas" refuerza nuestro punto , al observarse un incremento de los activos informáticos que cuentan con un paquete de salvaguardas que ofrecen una eficacia de 30% en la reducción de impacto aumento de 9% a 74 % de los activos informáticos que representan 40 activos informáticos, además de ello en el grafico N° 21 referente al "% nivel de impacto" observamos una reducción del en la categoría de impacto "Alto" de 4% a 0%, así como una reducción de la categoría de impacto "Medio" de 46% a 22%, estos datos nos ayudaron a contrastar nuestra hipótesis específica N°03, donde se obtiene que el valor P es: 0,000 < 0,05, como es menor al valor de significancia se rechaza la hipótesis nula y se acepra la hipótesis alterna (Ha), esto quiere decir que la verificación del nivel de cumplimiento de las salvaguardas **reduce** el nivel de **impacto** de los activos informáticos en la DRTPE-Hco 2021, a un nivel de 95% de confiabilidad

CONCLUSIONES

Como resultado de la investigación presentada se puede concluir que la implementación de la metodología Magerit v3 y la Norma Técnica Peruana ISO 27001-2014, **mejora** la gestión de riesgos de la seguridad de la información de la DRTPE - Hco, debido a la **reducción** del estado de riesgos de los activos informáticos en las dimensiones de seguridad de la información como son confidencialidad, integridad, disponibilidad, así como la metodología Magerit v3 permitió **entender** el contexto en que se encuentra la seguridad de la información, que conocer el mapa de valor de los activos , que es el inicio para determinar el estado de riesgos a los cuales están expuestos los activos informáticos, y para posteriormente poder realizar un adecuado tratamiento de esos riesgos con la propuesta de políticas de seguridad, que consiste en darle un uso aceptable a sus activos informáticos, y de establecer estrategias, que permitan tener una buena gestión de los riesgos de la seguridad de información, en los en los resultados de contrastación de la hipótesis general se obtiene que el valor P es: 0,000 < 0,05, como es inferior al valor de significancia, se rechaza la hipótesis nula y se acepta la hipótesis alterna (Ha), a un nivel de 95% de confiabilidad.

Como resultado de la investigación presentada se puede concluir que la identificación de las amenazas a los que están expuestos los activos informáticos **permite** estimar el alcance del daño de la seguridad de la información en la DRTPE-Hco, debido a una mejora en la reducción de Probabilidad de ocurrencia de las amenazas, de los activos informáticos, en los resultados de contrastación de la hipótesis especifica N° 02. se consigue que el valor P es: 0,000 < 0,05, como es inferior al valor de significancia, se rechaza la hipótesis nula y se acepta la hipótesis alterna (Ha), a un nivel de 95% de confiabilidad

Como resultado de la investigación presentada se puede concluir que la verificación del nivel de cumplimiento de las salvaguardas **reduce** el nivel de **impacto** de los activos informáticos en la DRTPE-Hco 2021, debido a un incremento de las salvaguardas implantadas actualmente en los activos informáticos de 9% a 33%, por consiguiente, se puede establecer, que, al haber más activos con salvaguardas establecidas, se obtendrá una mejor reducción del nivel de impacto de los activos, lo cual es observado en el grafico N° 21 referente al "% nivel de impacto", en los resultados de contratación de la hipótesis especifica N° 03. Se consigue que el valor P es: 0,000 < 0,05, como es inferior al valor de significancia se rechaza la hipótesis nula y se acepta la hipótesis alterna (Ha), a un grado de 95% de confiabilidad.

RECOMENDACIONES O SUGERENCIAS

- Las entidades deben implementar el proceso de verificación y actualización de sus recursos informáticos para exponer continuamente el potencial de riesgos y amenazas que plantean los cambios tecnológicos en curso y las formas de comprometer la seguridad a través de nuevos mensajes que se descubren cada vez.

- La presente implementación de la metodología Magerit v3, que nos dio el marco para la formulación y verificación de la propuesta de políticas de seguridad se encuentra todavía en las primeras fases, esta propuesta puede ser modificada, actualizado de la mejor forma posible, de tal manera que, al darse cumplimiento a la mayoría de los controles propuestos, se logre contar con salvaguardas con un alto grado de efectividad para conservar la seguridad de información en valores óptimos

- Se debe capacitar a los usuarios para el óptimo uso de las normas de seguridad, estas capacitaciones deben formar parte de la estructura de la entidad, de igual forma se debe realizar encuestas a los usuarios para medir la concientización con respecto a estos ítems, para tener constancia de que los usuarios comprenden importancia de estos temas.

- Las dimensiones de confidencialidad, integridad y disponibilidad de la información deben estar en constante medición, que debe darse mediante un control de incidencias, porque ellas representan los pilares de la seguridad de la información

.

- El presente proyecto tiene la facultad de ser como fundamento para futuras auditorias de la Gestión de Seguridad de la Información en la entidad, ya que gracias a la metodología Magerit v3, cuenta con el análisis de riesgos de la entidad, así como una primera etapa de gestión de los riesgos, mediante la propuesta de las políticas de seguridad.

Referencias Bibliográficas

andreapazalejandro. (13 de 06 de 2017). *ONGEI (OFICINA NACIONAL DE GOBIERNO ELECTRÓNICO E INFORMÁTICA)*. Obtenido de ONGEI: https://andreapazalejandro.wordpress.com/2017/06/13/ongei-oficina-nacional-de-gobierno-electronico-e-informatica/#:~:text=Es%20el%20%C3%B3rgano%20especializado%20que,de%20Gobierno%20Electr%C3%B3nico%20e%20Inform%C3%A1tica.

ARGÜEZO RAMIREZ, E. D. (2019). *PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL ÁREA DE INFORMÁTICA DE LA MUNICIPALIDAD PROVINCIAL DE HUÁNUCO.* Huanuco: UDH.

Bach. Pedro PAJUELO GODOY, B. S. (2019). *“LA METODOLOGÍA MAGERIT V3 Y SU INCIDENCIA EN LA SEGURIDAD DE INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE PILLCO MARCA, 2019”.* Huanuco: Universidad Nacional Hermilio Valdizan.

Briceño Huaygua, C. A. (2019). *APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA LA ELABORACIÓN DE UN PLAN DE MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN DE LA ZONA ESPECIAL DE DESARROLLO – ZED PAITA.* Piura: UNIVERSIDAD NACIONAL DE PIURA - FACULTAD DE INGENIERÍA INDUSTRIAL.

Cabrejos Torres, Ramiro. (2020). *Influencia de la metodología Magerit v3 en la Seguridad de Información de la empresa Deco Interiors SAC.* Obtenido de http://repositorio.uss.edu.pe/handle/20.500.12802/7573

CAMPOS, I. O. (2019). *“MODELO DE GESTIÓN DE RIESGOS DE TI BASADOS EN LA NORMA ISO/IEC 27005 Y METODOLOGÍA MAGERIT PARA MEJORAR LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA – CHACHAPOYAS PERÚ”.* Lambayeque: UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO".

Carlos Barrantes P., & Javier Hugo H. (202). *Diseño e Implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos.* Obtenido de https://repositorio.usmp.edu.pe/handle/20.500.12727/609

Carlos Barrantes P., &. J. (2012). *Diseño e Implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos. .* Lima: USMP.

CEUPE. (2019). *Política de seguridad de la información.* Madrid: Blog de CEUPE.

CHÁVEZ, V. M. (2019). *PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS EN EL DATACENTER DE LA FACULTAD DE INGENIERA EN CIENCIAS APLICADAS CON LA METODOLOGÍA MAGERIT V3.0.* Ibarra: UNIVERSIDAD TÉCNICA DEL NORTE.

CHUMAN. (2015). *Aplicación de la metodología Magerit para el análisis y gestión de riesgos en los servidores de los sistemas de Gestión Académica de la universidad nacional Pedro Ruiz Gallo.* Obtenido de http://repositorio.unprg.edu.pe/handle/UNPRG/169

CHUMAN, B. J. (2015). *APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS EN LOS SERVIDORES DE LOS SISTEMAS DE GESTIÓN ACADÉMICA DE LA UNIVERSIDAD PEDRO RUIZ GALLO.* Lambayeque: Universidad Nacional Pedro Ruiz Gallo.

CIBERSEGURIDAD, I. N. (2018). *Plan Director de Seguridad.* Madrid: incibe_.

COTERA, B. G. (2016). *USO DE HERRAMIENTAS DE ETHICAL HACKING CON KALI LINUX PARA EL DIAGNOSTICO DE VULNERABILIDADES DE LA SEGURIDAD DE LA INFORMACION EN LA RED DE LA SEDE CENTRAL DE LA UNIVERSIDAD DE HUANUCO.* Huanuco: UDH.

COTERA, B. G. (2016). *USO DE HERRAMIENTAS DE ETHICAL HACKING CON KALI LINUX PARA EL DIAGNÓSTICO DE VULNERABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN EN LA RED DE LA SEDE CENTRAL DE LA UNIVERSIDAD DE HUÁNUCO.* Huanuco: UDH.

Digital, S. d. (2017). *POLÍTICA NACIONAL DE CIBERSEGURIDAD.* Lima: Persidencia del Consejo de Ministros.

Empleo, D. R. (15 de Mayo de 2021). *Dirección Regional de Trabajo y Promoción del Empleo*. Obtenido de http://direcciontrabajo.regionhuanuco.gob.pe/

Escuela Nacional de Seguridad. (2012). MAGERIT – versión 3.0 - Libro 1. En G. d. España, *Metodología de Análisis y Gestión de los Sistemas de Informacion* (pág. 7). Madrid: Ministerio de Hacienda y Administraciones Públicas.

Excellence, I. (18 de Marzo de 2015). *Blog especializado en Sistemas de Gestión*. Obtenido de https://www.pmg-ssi.com/2015/03/ntp-isoiec-17799-norma-tecnica-peruana/

Firma-e. (24 de Agosto de 2013). *Firma - E*. Obtenido de https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/

FLORES, J. C. (2015). *GUÍA DE IMPLEMENTACIÓN DE LA SEGURIDAD BASADO EN LA NORMA ISO/IEC 27001, PARA APOYAR LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS DE LA COMISARIA DEL NORTE P.N.P EN LA CIUDAD DE CHICLAYO .* Chiclayo: Universidad catolica Santo toribio de mogrobejo .

González, R. S. (2018). *ANALISIS DE ACTIVOS DE INFORMACION PARA UN SISTEMA MISIONAL BASADOS EN LA METODOLOGIA MAGERIT V3 Y LA NORMA ISO 27001:2013.* Bogota: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.

Guamán, V. L. (2019). *EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL SISTEMA DE EVALUACIÓN DE DOCENTES DE LA UNIVERSIDAD TÉCNICA DEL NORTE BASADO EN LA ISO 27002:2017 CON LA METODOLOGÍA MAGERIT V3 .* Ibarra: UNIVERSIDAD TÉCNICA DEL NORTE.

Hernandez, S. (16 de abril de 2018). *Etapas de la Gestión del Riesgo*. Obtenido de http://training.pensemos.com/pages/viewpage.action?pageId=17601635

INDECOPI. (2014). *NORMA TECNICA PERUANA NTP-ISO/IEC 2700:2014.* Lima: INDECOPI.

INDECOPI. (2016). *GUIA INFORMATIVA DE PROTECCION DE DATOS PERSONALES .* Lima: Direccion general de proteccion de datos personales.

ISOTools. (05 de 03 de 2018). *Blog Calidad y Excelencia*. Obtenido de Blog Calidad y Excelencia: https://www.isotools.org/2018/03/05/la-norma-iso-iec-27000-va-a-ser-revisada/

katerina, M. (2016). *Risk Analysis and Risk Management in Critical Infrastructures.* Grecia: UNIVERSITY OF PIRAEUS.

ONGEI. (2016). *ASPECTOS TECNICOS Y LEGALES.* Lima: INDECOPI.

Pajuelo Godoy, Pedro, & Velásquez Gudiño, Sesi Beatriz. (2019). *La Metodología Magerit v3 y su incidencia en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019.* Obtenido de http://renati.sunedu.gob.pe/handle/sunedu/1536569

Pérez, A. (27 de Marzo de 2021). *OBS Busines School*. Obtenido de https://www.obsbusiness.school/blog/seguridad-de-la-informacion-un-conocimiento-imprescindible

Ramiro, B. C. (2020). *INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC.* Pimentel: Universidad Señor de Sipan.

REPUBLICA, C. D. (2013). *LEY DE DELITOS INFORMÁTICOS - LEY Nº 30096.* Lima: Diario El Peruano.

Sampieri, R. H. (2014). *Metodologia de La Investigacion.* Mexico: Publicaciones El Oso Panda.

SB, R. (20 de 11 de 2017). *El Blog de Ricardo SB* . Obtenido de https://ricardo-sb.blogspot.com/2017/11/gestion-de-riesgos-en-seguridad-de-la.html

TecnoBlog. (08 de 02 de 2014). *Seguridad Informática*. Obtenido de http://infosaudit.blogspot.com/

Anexo 1, Formato de control para las políticas de seguridad

Sección – Dominio	Justificación	Estado - Control
DOMINIO: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		
A.1. Política de Seguridad de la Información		
Objetivo de control: Proporcionar apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes		
A.1.1. Documentar política de seguridad de la información	El director de la entidad, tendrá la función de aprobar la política de seguridad y sus futuras modificaciones.	
A.1.2. Revisión de la política de seguridad de la información	El Comité de Administración de la Seguridad de la Información evaluará cada año la presente Política, para mantenerla actualizada, y así garantizar la efectividad de las mismas	
Total, Cumplimiento		
A.2. Organización de la seguridad de la información		
A.2.1 Objetivo: Implantar un patrón de administración para el inicio y el control de la implementación y operación de la seguridad de la información en la entidad.		
A.2.1.1. Compromiso de la gerencia con la seguridad de la información	La administración debe estimular activamente la seguridad dentro de la entidad a través de una dirección clara, y compromiso demostrado, mediante asignación de presupuesto	
A.2.4.1. Acuerdos de confidencialidad	Se debe establecer y revisar periódicamente los requerimientos de confidencialidad teniendo en cuenta las necesidades de la institución para la protección de la información.	
A.2.2 Dispositivos móviles y teletrabajo		
Objetivo: Asegurar la seguridad del teletrabajo y el uso de los dispositivos móviles		
A.2.2.1 Política de dispositivos portátiles, móviles	Una política y medidas de seguridad de soporte deben ser adoptados para gestionar los riesgos por el uso de los equipos móviles	
A.2.2.2 Teletrabajo	Una política y medidas de seguridad de apoyo deben de ser implementadas para resguardar la información, a la que se accede a través del teletrabajo	
Total, Cumplimiento		
A.3. Gestión de activos		
A.3.1. Responsabilidad por los activos		
Objetivo: Mantener la protección óptima de los activos de la entidad		

A.3.1.1 Inventariado de activos	Se recomienda que los activos de información estén identificados, a través de un registro de los activos, que deben de actualizarse	
A.3.2.1 Propiedad de los activos	Los activos de la entidad deben consignar a quien se le asigna dicho activo, para mantener un seguimiento de la vida útil del activo	
A.3.3.1 Uso aceptable de los activos	Se recomienda la identificación, documentación e implementación de las normas para el uso correcto de la información y los activos.	
A.3.2. Clasificación de la información		
Objetivo: Fijar que la información reciba un nivel de protección apropiado		
A.3.2.1 Lineamiento de clasificación	Se recomienda que la información sea categorizada por su valor, requerimientos legales, confidencialidad e importancia para la organización.	
A.4.2.2 Etiquetado y manejo de la información formato digital	Se recomienda que la entidad implemente un grupo de procedimientos para etiquetar y usar la información, tanto para formato digital como físico	
A.3.2.3 Etiquetado y manejo de la información formato físico		
A.3.3. Manejo de los medios		
Objetivo: Prevenir la difusión, manipulación, eliminación de los activos de información		
A.3.3.1. Gestión de medios removibles	Se recomienda la ejecución de procedimientos para la administración de los medios extraíbles, de acuerdo a las necesidades de la organización	
A.3.3.2. Transferencia de medios físicos	Los medios que contienen información deben ser protegidos, contra el acceso no autorizado a estas	
A.3.3.3. Procedimiento de manejo de la información	Se recomienda la implementación de procedimientos para el manejo y guardado de la información para resguardarse de un acceso no autorizado.	
Total, Cumplimiento		
A.5. Monitoreo		
Objetivo: Detectar actividades de procesamiento de información no autorizadas		
A.5.1. Registro de auditoría	Se recomienda generar registros de las actividades de auditoría, excepciones e incidentes de seguridad de la información	

A.5.3. Protección de la información del registro	Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.	
A.5.4. Registro de fallas	Las fallas se deben registrar, analizar y se debe tomar la acción apropiada	
Total, Cumplimiento		
A.6 Seguridad de los recursos humanos.		
A.6.1. Antes del empleo		
Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus compromisos, y sean apropiados para los roles de acuerdo a sus requerimientos laborales, y así de disminuir el riesgo de a que están expuestos los activos de información		
A.6.1.1. Roles y responsabilidades	Se recomienda el establecimiento y documentación de los roles y responsabilidades de seguridad de los empleados, etc., de acuerdo con la política de la seguridad de información de la organización	
A.6.1.3. Términos y condiciones de empleo	Se recomienda que como parte de su obligación laboral; los empleados, contratistas y terceros deben aceptar las condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades, y obligaciones en la seguridad de la información	
A.6.2. Durante el empleo		
Objetivo: Asegurar que todos los empleados, etc., estén al tanto de las amenazas sobre la seguridad de información, para que puedan desarrollar su trabajo de forma normal, y reducir los riesgos de error humano, esto va de la mano de una correcta concientización en estos temas por parte de la gerencia mediante capacitaciones.		
A.6.2.1. Gestión de responsabilidades	La administración debe solicitar que los empleados apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización	
A.6.2.2. Capacitación y educación en seguridad de la información	Se recomienda que los empleados de la entidad deban recibir la adecuada capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral	
A.6.2.3. Proceso disciplinario	Se recomienda implementar un proceso disciplinario para los empleados que han cometido una falta en la seguridad, o que no hayan reportado un incidente respecto a la seguridad de información	
A.6.3. Terminación o cambio del empleo		
Objetivo: Asegurar que los empleados que salgan de la Institución, lo realicen de manera ordenada, sin violar ninguna regla de seguridad.		

A.6.3.1. Devolución de activos	Todos los empleados deben devolver todos los activos de la institución que estén en su poder a la terminación de su contrato.	
A.6.3.2. Terminación o cambio de responsabilidades	Los derechos de acceso de los empleados que salen de la organización deben ser eliminados al término de su contrato.	
Total, Cumplimiento		
A.7. Seguridad física y ambiental		
A.7.1. Áreas seguras.		
Objetivo: Evitar el acceso no autorizado, daño e interferencia a los locales de acceso restringido.		
A.7.1.1. Controles de ingreso físico	Se recomienda la protección de las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado	
A.7.2. Seguridad de los equipos informáticos		
Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la institución		
A.7.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados en lugares estratégicos y protegidos, para reducir el riesgo de amenazas como, robo o daño intencional.	
A.7.2.3. Seguridad en el cableado	El cableado de la energía y las telecomunicaciones que transportan datos deben ser protegidos de las interceptación, interferencia o daño	
A.7.2.4. Mantenimiento de equipos	Los equipos deben ser mantenidos periódicamente, actualizando, para asegurar su continua disponibilidad e integridad	
A.7.2.7. Política de escritorio Limpio y Pantalla limpia	Debe ser adoptada una política de escritorio limpio, así como de pantalla limpia	
Total, Cumplimiento		
A.8 Gestión de las comunicaciones y operaciones		
A.8.1. Procedimientos y responsabilidad operacionales		
Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras		
A.8.1.1 Procedimientos de operación documentados	Se recomienda documentar y mantener los procedimientos de manejo de los Sistemas de información, y se deben poner a distribución de todos los usuarios que los necesiten	

A.8.2. Respaldo (Back-Up)		
Objetivo: Se recomienda preservar la integridad y disponibilidad de los servicios de procesamiento de información		
A.8.2.1. Respaldo de información	Se recomienda la realización de copias de respaldo de la información que maneja la institución, de forma periódica, además de ello las copias de seguridad deben ser probadas para demostrar su correcto funcionamiento	
Total, Cumplimiento		
A.10 Criptografía		
A.10.1. Controles criptográficos		
Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y la integridad de la información		
A.10.1.1 Gestión de Claves	Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada en la entidad	
	La asignación de claves se debe controlar a través de un proceso de gestión formal. Generando una clave con más de ocho caracteres, usando mayúsculas, minúsculas, números y caracteres especiales	
Total, Cumplimiento		
A.11. Control de acceso		
Objetivo: Limitar el acceso de información considerada como "Restringida", en la entidad		
A.11.1.1. Política de control de acceso	Se recomienda la implementación un procedimiento formal para la inscripción y des inscripción de categorías o grupos de usuarios de acuerdo al nivel de acceso de información que requieran y/o servicios (impresión, etc.), estos grupos o permisos se gestionan a través de Workgroups, una de las aplicaciones de Windows.	
A.11.1.2. Aprovisionamiento de acceso a usuario	Se recomienda que la administración de la entidad deba revisar los derechos de acceso de los usuarios en periodos regulares de tiempo utilizando un proceso formal.	
A.11.2. Responsabilidades de los usuarios		
Objetivo: Hacer que los usuarios respondan por la salvaguarda de su información		
A.11.2.1. Uso de Información:	Los usuarios deben ser exigidos que sigan las prácticas de la organización en el manejo de información sensible	
A.11.3. Control de acceso a redes		
Objetivo: Evitar el acceso no autorizado a los servicios en red		

A.11.3.1. Política sobre el uso de servicios de red	Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.	
A.11.3.3 Identificación del equipo de red	Se debe considerar la autenticación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.	
A.11.5. Seguridad de los servicios de red	Mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red, ya sean servicios internos o provisto de terceros	
Total, Cumplimiento		
A.12. Seguridad en las operaciones		
A.12.1. Gestión de vulnerabilidades técnicas		
Objetivo: Prevenir la explotación de vulnerabilidades técnicas		
A.12.2. Restricciones sobre instalación de software	Reglas que determinen la instalación de software por parte de los usuarios, deben ser establecidas e implementadas	
A.12.3. Protección contra virus informáticos	Debe existir programas que ofrezcan protección de los virus informáticos	
Total, Cumplimiento		
A.13. Gestión de incidentes de seguridad de la información		
Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y las debilidades de la organización		
A.13.1. Responsabilidades y procedimientos	Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida	
A.13.2. Reporte de debilidades de seguridad de la información	Los usuarios de los sistemas de información que posea la organización deben ser exigidos de reportar cualquier debilidad o mal funcionamiento observado	
A.13.3. Evaluación y decisión sobre eventos de seguridad de la información	Los eventos de seguridad de la información deben ser evaluados, y deben ser respondidos de acuerdo con los procedimientos documentados	
Total, Cumplimiento		
A.14 Cumplimiento de los requisitos legales y contractuales		
A.14.1 Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias, relacionadas a la seguridad de la información		
A.14.1. Identificación de requisitos contractuales y de legislación aplicables	Todos los requisitos legislativos, regulatorios y contractuales relevantes, así como el enfoque de la organización para el cumplimiento por parte de la organización	

A.14.2. Privacidad y protección de datos personales	La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulaciones	
Total, Cumplimiento		
A.14.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información esta implementada y es operada de acuerdo con las políticas y procedimientos organizativos		
A.14.1. Revisión independiente de la seguridad de la información	El enfoque de la organización para manejar la seguridad de la información y su implementación., por ejemplo (evaluar si los objetivos de control, controles, procedimientos se encuentran bien definidos)	
Total, Cumplimento		
Cumplimiento Consolidado		

Anexo 2
Cuestionario

Estimado(a) Colaborador: Usuario General
El presente instrumento tiene como objetivo determinar la situación actual de cumplimiento de controles de seguridad en la. (DRTPE)

Agradeciéndole de antemano su colaboración.

Datos Específicos	
1	Nunca
2	Casi Nunca
3	A veces
4	Casi Siempre
5	Siempre

Variable Independiente: Metodología Magerit V3						
Dimensión 5: Cultura de riesgo de información - Desempeño de la concientización		**1**	**2**	**3**	**4**	**5**
1	¿La DRTPE le ha proporcionado capacitación sobre el resguardo de información que administra, o en algún tema relacionado a la seguridad de información?					
2	¿Pone en práctica alguna estrategia para la protección de la información?					
3	¿Se considera comprometido con el resguardo de la información que administra?					
4	En el uso de correo electrónico, ¿Comprueba el remitente de los correos electrónicos, para diferenciar si una comunicación es fraudulenta o no?					
5	¿Cuándo descarga archivos adjuntos al correo electrónico, antes de abrirlos, analiza el archivo con el programa de antivirus?					
6	¿Reutiliza las contraseñas de sus cuentas de Gmail, Facebook, para acceder a la computadora de su estación de trabajo?					
7	¿Al momento de usar memorias USB y/o discos duros externos deja conectado esos equipos a su computadora durante toda su jornada laboral?					
8	¿Los programas que usa en su estación de trabajo (Word, Excel, antivirus), se encuentran actualizados?					
9	¿La computadora de su estación de trabajo cuenta con una contraseña de sesión de inicio?					
10	En el navegador web Google ¿usted habilita la función «recordar contraseña»?					
11	Para el correcto desarrollo de su trabajo, ¿siempre cuenta con la información requerida?					
12	¿Su estación de trabajo cuenta con acceso libre de internet? (Con qué frecuencia accede a redes sociales, YouTube, etc.)					
13	¿Con que frecuencia instala programas adicionales a su computadora de trabajo en la entidad?					
14	La tecnología de su computadora y/o, laptop, en la DRTPE, es adecuada para el desarrollo de sus actividades diarias?					
15	¿El servicio de internet disponible en la DRTPE, es adecuado para realizar sus actividades?					
16	¿Requiere de algún tipo de asistencia para resolver problemas informáticos durante sus labores diarias?					

Fuente: Elaboración Propia

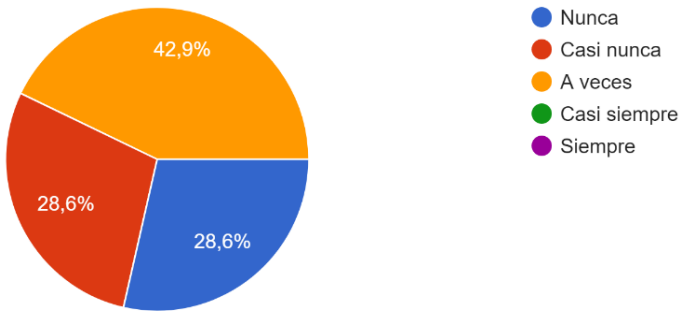
Anexo 3, Resultados de Encuesta

Para la investigación una vez analizada la fundamentación teórica de la metodología Magerit v3, se aplicaron los conceptos de cómo gestionar los riesgos, como medir el nivel de concientización en el tema. Por ello se utilizó una encuesta formulando interrogantes relacionadas al contexto. A continuación, se analiza el resultado obtenido en cada una de las preguntas:

1. ¿La DRTPE le ha proporcionado capacitación sobre el resguardo de información que administra, o en algún tema relacionado a la seguridad de información?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 – Nunca	2	28.6%
2 - Casi Nunca	2	28.6%
3 - A veces	3	42.9%
4 - Casi Siempre	0	0.0%
5 – Siempre	0	0.0%
Total	7	100.0%

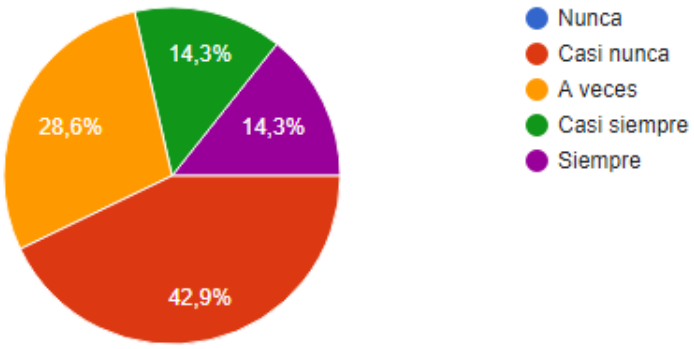
Fuente: “Elaboración Propia”



2. ¿Pone en práctica alguna estrategia para la protección de la información?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 – Nunca	0	0.0%
2 - Casi Nunca	3	42.9%
3 - A veces	2	28.6%
4 - Casi Siempre	1	14.3%
5 – Siempre	1	14.3%
Total	7	100.0%

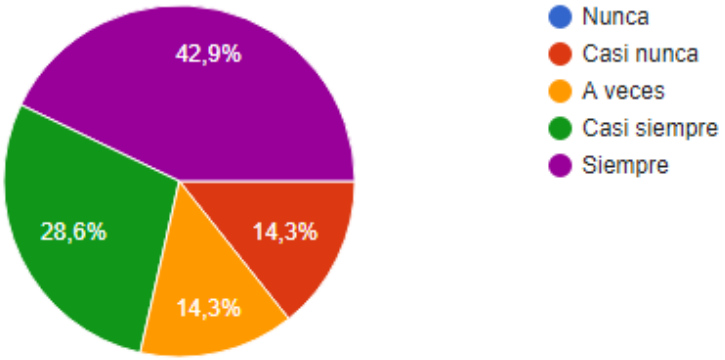
Fuente: “Elaboración propia”



3. ¿Se considera comprometido con el resguardo de la información que administra?

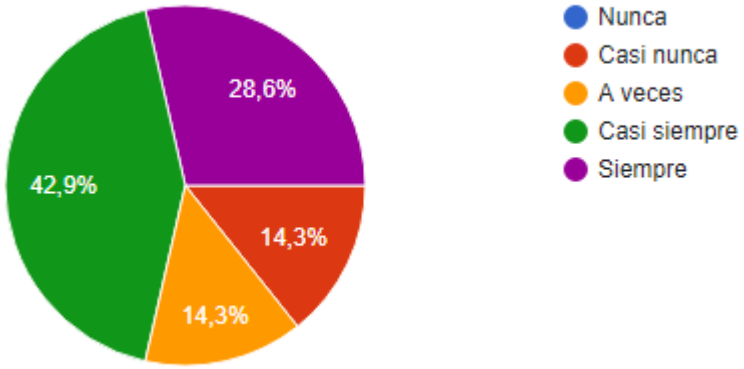
% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 – Nunca	0	0.0%
2 - Casi Nunca	1	14.3%
3 - A veces	1	14.3%
4 - Casi Siempre	2	28.6%
5 – Siempre	3	42.9%
Total	7	100.0%

Fuente: “Elaboración Propia”



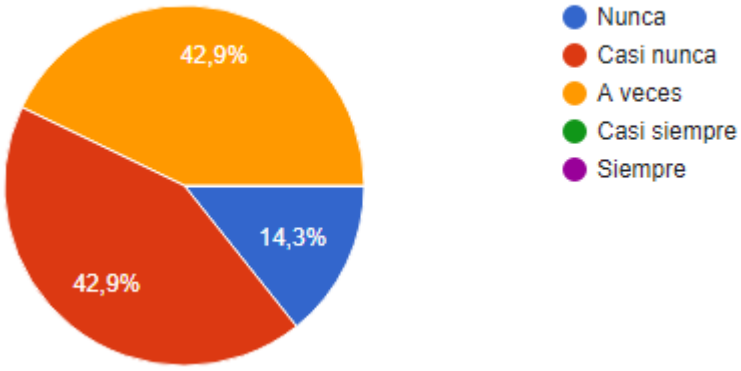
4. En el uso de correo electrónico, ¿Comprueba el remitente de los correos electrónicos, para diferenciar si una comunicación es fraudulenta o no?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 – Nunca	0	0.0%
2 - Casi Nunca	1	14.3%
3 - A veces	1	14.3%
4 - Casi Siempre	3	42.9%
5 – Siempre	2	28.6%
Total	7	100.0%



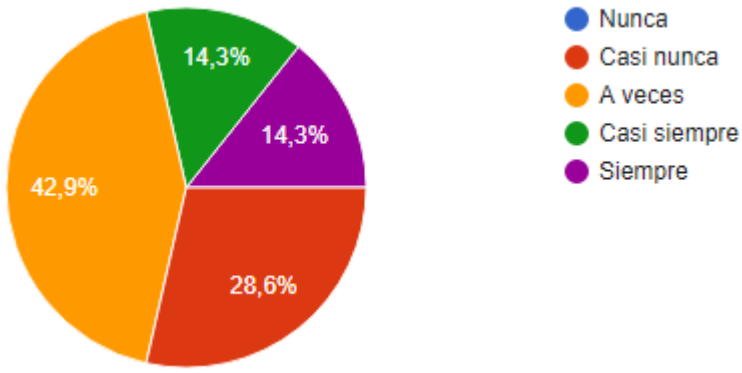
5. ¿Cuándo descarga archivos adjuntos al correo electrónico, antes de abrirlos, analiza el archivo con el programa de antivirus?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	Fi	hi%
1 - Nunca	1	14.3%
2 - Casi Nunca	3	42.9%
3 - A veces	3	42.9%
4 - Casi Siempre	0	0.0%
5 - Siempre	0	0.0%
Total	7	100.0%



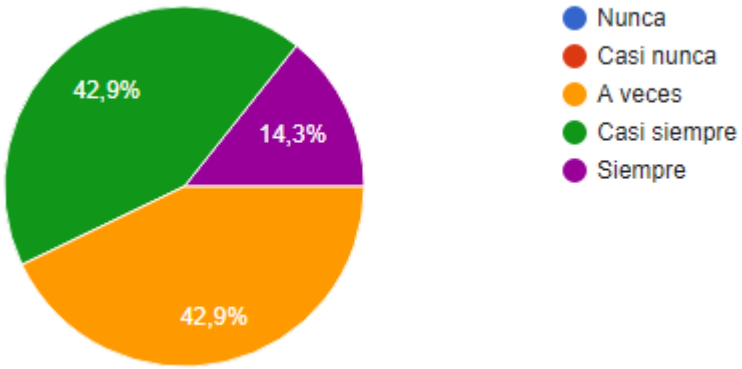
6. ¿Al momento de usar memorias USB y/o discos duros externos deja conectado esos equipos a su computadora durante toda su jornada laboral?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 – Nunca	0	0.0%
2 - Casi Nunca	2	28.6%
3 - A veces	3	42.9%
4 - Casi Siempre	1	14.3%
5 – Siempre	1	14.3%
Total	7	100.0%



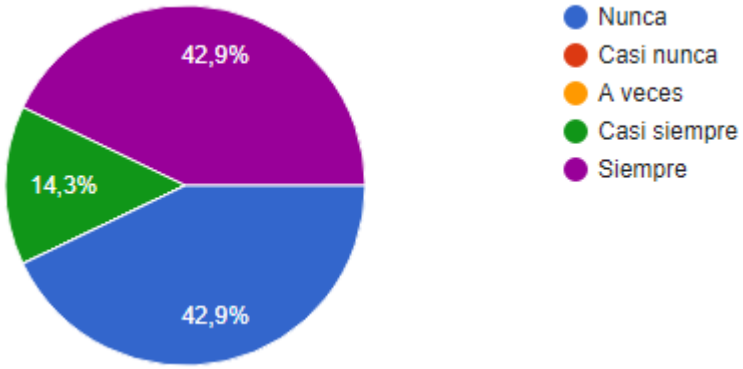
7. ¿Los programas que usa en su estación de trabajo (Word, Excel, antivirus), se encuentran actualizados?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 - Nunca	0	0.0%
2 - Casi Nunca	0	0.0%
3 - A veces	3	42.9%
4 - Casi Siempre	3	42.9%
5 - Siempre	1	14.3%
Total	7	100.0%



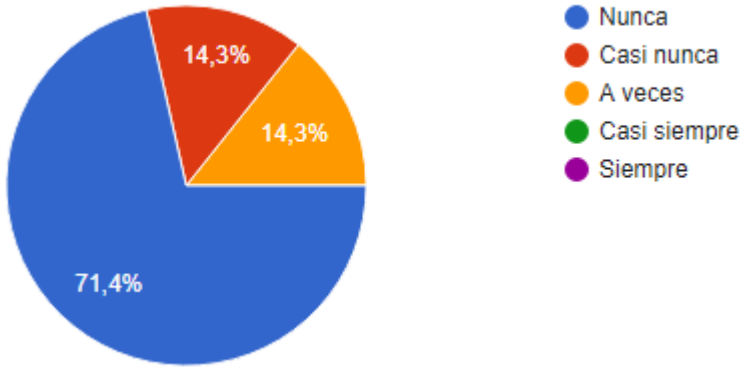
8. ¿La computadora de su estación de trabajo cuenta con una contraseña de sesión de inicio?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 – Nunca	3	42.9%
2 - Casi Nunca	0	0.0%
3 - A veces	0	0.0%
4 - Casi Siempre	1	14.3%
5 – Siempre	3	42.9%
Total	7	100.0%



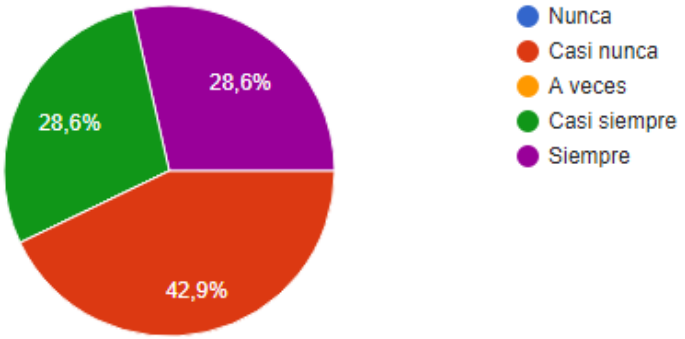
9. En el navegador web Google ¿usted habilita la función «recordar contraseña»?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 – Nunca	5	71.4%
2 - Casi Nunca	1	14.3%
3 - A veces	1	14.3%
4 - Casi Siempre	0	0.0%
5 – Siempre	0	0.0%
Total	7	100.0%



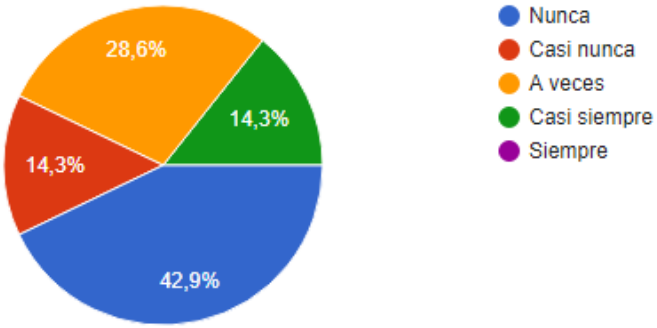
10. Para el buen desempeño de su trabajo ¿El acceso a internet es libre sin restricción a alguna página Web?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	Fi	hi%
1 - Nunca	0	0.0%
2 - Casi Nunca	3	42.9%
3 - A veces	0	0.0%
4 - Casi Siempre	2	28.6%
5 - Siempre	2	28.6%
Total	7	100.0%



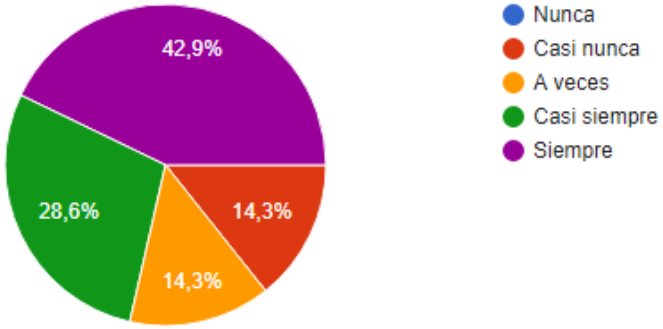
11. ¿Con que frecuencia instala programas adicionales a su computadora de trabajo en la entidad?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 – Nunca	3	42.9%
2 - Casi Nunca	1	14.3%
3 - A veces	2	28.6%
4 - Casi Siempre	1	14.3%
5 – Siempre	0	0.0%
Total	7	100.0%



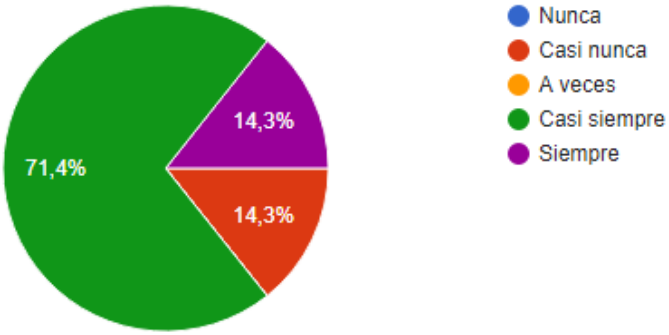
12. La tecnología de su computadora y/o, laptop, en la DRTPE, es adecuada para el desarrollo de sus actividades diarias?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 – Nunca	0	0.0%
2 - Casi Nunca	1	14.3%
3 - A veces	1	14.3%
4 - Casi Siempre	2	28.6%
5 – Siempre	3	42.9%
Total	7	100.0%



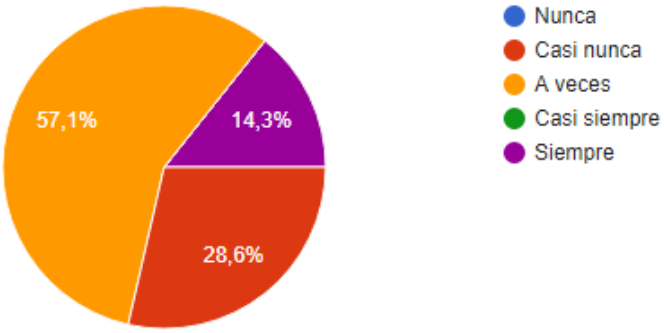
13. ¿El servicio de internet (la velocidad Megas) disponible en la DRTPE, es adecuado para realizar sus actividades?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 – Nunca	0	0.0%
2 - Casi Nunca	1	14.3%
3 - A veces	0	0.0%
4 - Casi Siempre	5	71.4%
5 – Siempre	1	14.3%
Total	7	100.0%



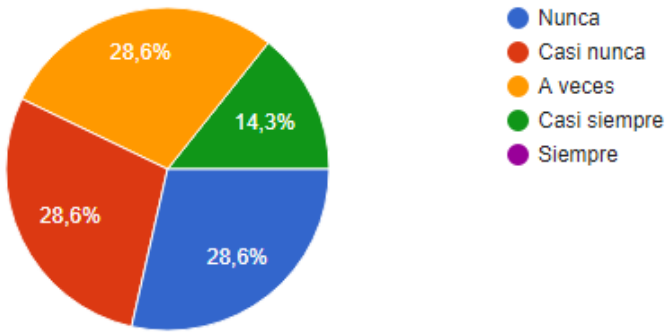
14. ¿Requiere de algún tipo de asistencia para resolver problemas informáticos durante sus labores diarias?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 – Nunca	0	0.0%
2 - Casi Nunca	2	28.6%
3 - A veces	4	57.1%
4 - Casi Siempre	1	14.3%
5 – Siempre	0	0.0%
Total	7	100.0%



15. ¿Reutiliza las contraseñas de sus cuentas de Gmail, Facebook, para acceder a la computadora de su estación de trabajo?

% Empleados que adquieren conocimientos en temas de seguridad	Antes de la Implementación	
	fi	hi%
1 – Nunca	2	28.6%
2 - Casi Nunca	2	28.6%
3 - A veces	2	28.6%
4 - Casi Siempre	1	14.3%
5 – Siempre	0	0.0%
Total	7	100.0%



Anexo 4: Pruebas de toma de datos


GOBIERNO REGIONAL
HUÁNUCO
GOBIERNO
Trabajo
LEO MOTO S
WALOR


APOLO CLUB

Anexo 5, Carta de Aceptación para el desarrollo del proyecto de tesis

GOBIERNO REGIONAL HUÁNUCO
Nuestro compromiso es contigo

GERENCIA REGIONAL DE DESARROLLO SOCIAL

DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO

"Año del Bicentenario del Perú: 200 años de Independencia"

HUÁNUCO, 05 DE ABRIL DE 2021

CARTA N° 003-2021-GRH-GRDS/DRTPE

SEÑORES:
Bach. DANIEL KEVIN RIVERA ANASTACIO
Bach. JHONATHAN HAROLD VALDIVIA ESCOBAR

HUÁNUCO. –

ASUNTO : AUTORIZACIÓN PARA REALIZACIÓN DE PROYECTO DE TESIS

Es grato dirigirme a ustedes para saludarlos cordialmente y a su vez manifestar que, habiendo recepcionado su solicitud de fecha 31 de marzo del año en curso, **se otorga el permiso correspondiente a efectos realizar su proyecto de tesis en la Dirección Regional de Trabajo y Promoción del Empleo Huánuco**. Para tal efecto, podrán efectuar las coordinaciones con el Lic. Adm. Elmo Martín Acosta – Director de la Oficina Técnica Administrativa.

Es todo cuanto informo para conocimiento y fines pertinentes.

Atentamente,

DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO · HUÁNUCO · REPÚBLICA DEL PERÚ

GOBIERNO REGIONAL DE HUANUCO
DIRECCION REGIONAL DE TRABAJO Y PROMOCION DEL EMPLEO

Mg. Miller Villanueva Santamaria
DIRECTOR REGIONAL DE TRABAJO Y PROMOCION DEL EMPLEO

Reg.	02383230
Exp.	01542180

Cc,
DRTPE

Anexo 6

Matriz de Consistencia

Titulo: Implementación de la metodología Magerit v3 para mejorar la gestión de riesgos de seguridad de la información y propuesta de políticas de seguridad basadas en norma técnica peruana ISO/IEC 27001:2014 en la dirección regional de trabajo y promoción del empleo de Huánuco - 2021.

Formulación de Problema	**Objetivos**	**Hipótesis**	**Variables**	**Dimensiones**	**Marco Metodológico**
General ¿En qué medida la implementación de la metodología Magerit V3 y la Norma Técnica Peruana ISO/IEC 27001-2014 mejorará de la gestión de riesgos de la seguridad de la información en la DRTPE-Hco - 2021? **Específicos** ¿De qué forma la identificación y valoración de los activos de información según las dimensiones de seguridad ayudan a mejorar el conocimiento actual de la información en la DRTPE-Hco 2021? ¿De qué manera la identificación de amenazas a los que están expuestos los activos de información permite estimar el alcance del daño de	**General** Implementar la metodología Magerit V3 y la Norma Técnica Peruana ISO 27001-2014 para mejorar la gestión de riesgos de la seguridad de la información en la DRTPE-Hco - 2021 **Específicos** Identificar y valorar los activos de información según las dimensiones de seguridad para **mejorar** el conocimiento actual de la información en la DRTPE-Hco 2021. Identificar de las amenazas a los que están expuestos los activos de información, para **estimar** el alcance del daño de la seguridad de la información en la DRTPE-Hco 2021.	**General** La implementación de la metodología Magerit v3 y la Norma Técnica Peruana ISO 27001-2014 **mejora** la gestión de riesgos de seguridad de la información de la DRTPE-Hco 2021. **Específicos** La identificación y valoración de los activos según las dimensiones de seguridad **mejora** el conocimiento actual de la información en la DRTPE-Hco 2021. La identificación de las amenazas a los que están expuestos los activos de información **permite** estimar el alcance del daño de la seguridad de la	**Variable Independiente** Metodología Magerit v3	Mapa de Valor Amenazas Impacto Riesgo Salvaguardas	**Nivel de investigación**: Explicativa **Tipo:** Aplicada **Población:** conformada por los activos informáticos que se encuentra dentro de la DRTPE – Hco, de 54 activos informáticos **Muestra**: Muestreo intencional o de conveniencia. n = 54 activos informáticos

la seguridad de la información en la DRTPE-Hco 2021? ¿Permitirá la verificación del nivel de cumplimiento de salvaguardas **reducir** el nivel de **impacto** en los activos informáticos en la DRTPE-Hco 2021? ¿Influye la propuesta de **políticas de seguridad** en la **reducción** del estado de riesgos a los que están expuestos los activos en la DRTPE-Hco 2021?	Verificar el nivel de cumplimiento de las salvaguardas para **reducir** el nivel de **impacto** de los activos informáticos en la DRTPE-Hco 2021. Proponer de políticas de seguridad para **reducir** el estado de riesgos en las dimensiones de seguridad de información de la información en la DRTPE-Hco – 2021.	información en la DRTPE-Hco 2021. La verificación del nivel de cumplimiento de las salvaguardas **reduce** el nivel de **impacto** de los activos informáticos en la DRTPE-Hco 2021. La propuesta de políticas de seguridad **reduce** el estado de riesgos en las dimensiones de seguridad de información de la información en la DRTPE-Hco – 2021	**Variable Dependiente** Gestión de Riegos de la Seguridad de la Información	Disponibilidad Integridad Confidencialidad Autenticidad No repudio	

Fuente: Elaboración Propia

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

RESOLUCIÒN Nº 0498-2021-UNHEVAL/FIIS-D/V.

Huánuco, 19 de noviembre de 2021.

CONSIDERANDO:

Que con Resolución Nº 077-2020-UNHEVAL-CEU, del 11.DIC.2020, se PROCLAMA Y ACREDITA a partir del 14 de diciembre de 2020 hasta el 13 de diciembre de 2024, al **Dr. MARCO ANTONIO VILLAVICENCIO CABRERA** como Decano de la Facultad de Ingeniería Industrial y de Sistemas, de la Universidad Nacional Hermilio Valdizán de Huánuco;

Que con Oficio N° 251-2021-UNHEVAL/PROFI-C, de fecha 10.NOV.2021, el Coordinador del PROCATP, remite el ejemplar de Tesis del Bachiller que estudio en el PROCATP ahora denominado PROFI correspondiente al Ciclo Académico 2021-I, con la finalidad de obtener el Título Profesional de la Escuela Profesional de Ingeniería de Sistemas, solicitando la designación de los Jurados Examinadores para la sustentación de Tesis y fijar fecha y hora, en base al Art. 49 del Reglamento del PROF;

Que visto el expediente, en mérito al Art. 49º del Reglamento del PROFI (ex PROCATP), mi Despacho considera procedente emitir una Resolución designando los Jurados Examinadores de tesis de los Bachilleres de la EP de Ingeniería de Sistemas – PROFI 2021-I, y fijar fecha, hora y lugar para la sustentación pública virtual, debiendo el Presidente del Jurado hacer conocer el Link respectivo;

BACHILLER	TÍTULO DE LA TESIS	JURADOS	DIA/HORA/LUGAR
✓ DANIEL KEVIN RIVERA ANASTACIO. ✓ JHONATHAN HAROLD VALDIVIA ESCOBAR	**IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT V3 PARA MEJORAR LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y PROPUESTA DE POLITICAS DE SEGURIDAD BASADAS EN NORMA TECNICA PERUANA ISO/IEC 27001:2014 EN LA DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO DE HUÁNUCO – 2021.**	Dra. Inés Jesús Tolentino **PRESIDENTE** Mg. Elmer Chuquiyauri Saldivar **SECRETARIO** Dr. Manuel Marín Mozombite **VOCAL**	**Día:** **VIERNES 26.NOV.2021** **Hora: 08:00 am-09.00 am** **LUGAR:Sustentación Virtual.**

Que estando a las atribuciones conferidas al Decano de la Facultad de Ingeniería Industrial y de Sistemas, por la Ley Universitaria N° 30220, Estatuto Universitario y Resolución N° 077-2020-UNHEVAL-CEU;

SE RESUELVE:

1° DESIGNAR Jurados Examinadores de tesis de Bachilleres de la EP de Ingeniería de Sistemas– PROFI 2021 - I, en mérito al Art. 49º del Reglamento del PROFI y fijar fecha, hora y lugar para la sustentación pública virtual, por lo manifestado en los considerandos de la presente Resolución:

BACHILLER	TÍTULO DE LA TESIS	JURADOS	DIA/HORA/LUGAR
✓ DANIEL KEVIN RIVERA ANASTACIO. ✓ JHONATHAN HAROLD VALDIVIA ESCOBAR	**IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT V3 PARA MEJORAR LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y PROPUESTA DE POLITICAS DE SEGURIDAD BASADAS EN NORMA TECNICA PERUANA ISO/IEC 27001:2014 EN LA DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO DE HUÁNUCO – 2021.**	Dra. Inés Eusebia Jesús Tolentino **PRESIDENTE** Mg. Elmer Chuquiyauri Saldivar **SECRETARIO** Dr. Manuel Marín Mozombite **VOCAL**	**Día:** **VIERNES 26.NOV.2021** **Hora: 08:00 am-09.00 am** **LUGAR:Sustentación Virtual.**

2° DAR A CONOCER a los órganos internos y a los interesados.

Regístrese, comuníquese y archívese

DECANO

Dr. Marco Villavicencio Cabrera
DECANO FIIS

c.c.:PROFI/Jurados/Interesados/Archivo.

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN"
HUÁNUCO – PERÚFACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL DEINGENIERO DE SISTEMAS - PROFI

En Huánuco, a los 26 días del mes de noviembre de 2021, siendo las 08 am horas de acuerdo al Reglamento del Programa de Fortalecimiento en Investigación PROFI de la Universidad NacionalHermilio Valdizán, Capítulo XII DE LA SUSTENTACIÓN DE LA TESIS, Art. 48º al 52º, se procedióa la evaluación de la sustentación de la tesis virtual, titulado**: IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT V3 PARA MEJORAR LA GESTIÓN DE RIESGOS DE SEGURIDADDE LA INFORMACIÓN Y PROPUESTA DE POLITICAS DE SEGURIDAD BASADAS EN NORMA TECNICA PERUANA ISO/IEC 27001:2014 EN LA DIRECCIÓN REGIONAL DE**

TRABAJO Y PROMOCIÓN DEL EMPLEO DE HUÁNUCO – 2021., presentado por el Bachiller en Ingeniería de Sistemas**: DANIEL KEVIN RIVERA ANASTACIO.**

Este evento se realizó vía Cisco Webex de la Facultad de Ingeniería Industrial y de Sistemas de la UNHEVAL, ante los miembros del Jurado Calificador, integrado por los siguientes catedráticos:

PRESIDENTE: Dra. INÉS EUSEBIA JESÚS

TOLENTINO SECRETARIO: Mg. ELMER

SANTIAGO CHUQUIYAURI SALDIVARVOCAL:

Dr. MANUEL MARÍN MOZOMBITE.

Finalizado el acto de sustentación, se procedió a la calificación conforme al Artículo 51º y 52º del Reglamento del Programa de Fortalecimiento en Investigación PROFI, obteniéndose e l siguienteresultado. **Nota: 17 (Diecisiete)** equivalente a la calificación de bueno Quedando el Bachiller en Ingeniería de Sistemas: **DANIEL KEVIN RIVERA ANASTACIO: aprobado**

Con lo que se dio por concluido el acto y en fe de la cual firman los miembros del jurado Calificador.

……

PRESIDENTE

…… ……

SECRETARIO **VOCAL**

" Año del Bicentenario del Perú: 200 Años de Independencia "

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" HUÁNUCO – PERÚ
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS - PROFI

En Huánuco, a los 26 días del mes de noviembre de 2021, siendo las 08 am horas de acuerdo al Reglamento del Programa de Fortalecimiento en Investigación PROFI de la Universidad Nacional Hermilio Valdizán, Capítulo XII DE LA SUSTENTACIÓN DE LA TESIS, Art. 48° al 52°, se procedió a la evaluación de la sustentación de la tesis virtual, titulado: **IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT V3 PARA MEJORAR LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y PROPUESTA DE POLITICAS DE SEGURIDAD BASADAS EN NORMA TECNICA PERUANA ISO/IEC 27001:2014 EN LA DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO DE HUÁNUCO – 2021.**, presentado por el Bachiller en Ingeniería de Sistemas: **JHONATHAN HAROLD VALDIVIA ESCOBAR.**

Este evento se realizó vía Cisco Webex de la Facultad de Ingeniería Industrial y de Sistemas de la UNHEVAL, ante los miembros del Jurado Calificador, integrado por los siguientes catedráticos:

PRESIDENTE: Dra. INÉS EUSEBIA JESÚS TOLENTINO
SECRETARIO: Mg. ELMER SANTIAGO CHUQUIYAURI SALDIVAR
VOCAL: Dr. MANUEL MARÍN MOZOMBITE.

Finalizado el acto de sustentación, se procedió a la calificación conforme al Artículo 51° y 52° del Reglamento del Programa de Fortalecimiento en Investigación PROFI, obteniéndose el siguiente resultado. **Nota: 17 (Diecisiete)** equivalente a la calificación de bueno Quedando el Bachiller en Ingeniería de Sistemas: **JHONATHAN HAROLD VALDIVIA ESCOBAR: aprobado**

Con lo que se dio por concluido el acto y en fe de la cual firman los miembros del jurado Calificador.

.....

PRESIDENTE

....

SECRETARIO **VOCAL**

<UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" DE HUÁNUCO
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS
CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

CONSTANCIA DE APTO

De acuerdo al Reglamento General de Grados y Títulos Modificado de la Universidad Nacional Hermilio Valdizán de Huánuco aprobado con Resolución del Consejo Universitario N° 1893-2021-UNHEVAL, de fecha 17 de agosto de 2021 y en atención a la Tercera Disposición Complementaria, donde estipula que los trabajos de investigación y tesis de pregrado deberán tener una similitud máxima del 30%.

Después de aplicado el Software Turnitin, se evidencia una similitud del 29% encontrándose bajo los parámetros reglamentados.

Tesis para optar el Título Profesional de Ingeniero de Sistemas:

"IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT V3 PARA MEJORAR LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y PROPUESTA DE POLITICAS DE SEGURIDAD BASADAS EN NORMA TECNICA PERUANA ISO/IEC 27001:2014 EN LA DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO DE HUÁNUCO – 2021".

Tesistas

Bach. Ing. Sistemas RIVERA ANASTACIO DANIEL
Bach. Ing. Sistemas VALDIVIA ESCOBAR JHONATHAN

Huánuco, 15 de febrero de 2022

Nérida del Carmen Pastrana Díaz
Directora de Investigación - FIIS

AUTORIZACIÓN PARA PUBLICACIÓN DE TESIS ELECTRÓNICA DE PREGRADO

IDENTIFICACIÓN PERSONAL (especificar los datos de los autores de la tesis)

Apellidos y Nombres: Daniel Kevin Rivera Anastacio **DNI.:** 74237163

Jhonathan Harold Valdivia Escobar **DNI.:** 48216218

Correo Electrónico: dannysisriv@gmail.com

Teléfono Casa: - **Celular:** 927313540 **Oficina:** _____

IDENTIFICACIÓN DE LA TESIS

Pregrado
Facultad de Ingeniería Industrial y de Sistemas **E.P.: Ingeniería de Sistemas**

Título Profesional obtenido:

Ingeniero de Sistemas

Título de la tesis:

IMPLEMENTACION DE LA METODOLOGIA MAGERIT V3 PARA MEJORAR LA GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 27001/2014 EN LA DIRECCION REGIONAL DE TRABAJO Y PROMOCION DEL EMPLEO DE HUANUCO – 2021

Tipo de acceso que autoriza(n) el (los) autor (es):

Marcar "X"	Categoría de Acceso	Descripción de Acceso
X	**PÚBLICO**	Es público y accesible al documento a texto completo por cualquier tipo de usuario que consulta el repositorio.
	RESTRINGIDO	Solo permite el acceso al registro del metadato con información básica más no al texto completo.

Al elegir la opción "Público", a través de la presente autorizo o autorizamos de manera gratuita al Repositorio Institucional – UNHEVAL, a publicar la versión electrónica de esta tesis en el Portal Web repositorio.unheval.edu.pe, por un plazo indefinido, consintiendo que con dicha autorización cualquier tercero podrá acceder a dichas páginas de manera gratuita, pudiendo revisarla, imprimirla o grabarla, siempre y cando se respete la autoría y sea citada correctamente.

En caso haya (n) marcado la opción "Restringido", por favor detallar las razones por las que se eligió este tipo de acceso:

Asimismo, pedimos indicar el período de tiempo en que la tesis tendría el tipo de acceso restringido:

( ) 1 año

( ) 2 años

( ) 3 años

( ) 4 años

Luego del período señalado por usted (es), automáticamente la tesis pasará a ser de acceso público.

Fecha de firma: 03 de marzo del 2022

Firma del autor y/o autores:

RIVERA ANASTACIO, DANIEL KEVIN

VALDIVIA ESCOBAR, JHONATHAN HAROLD