UNIVERSIDAD NACIONAL HERMILIO VALDIZAN

FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

CARRERA PROFESIONAL DE INGENIERIA DE SISTEMAS

"PROPUESTA DE DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NTP-ISO/IEC 27001 PARA LA DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO – HUÁNUCO"

TESIS PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

TESISTA:

Bach. SANDOVAL ALANIA, Jose Carlos

ASESOR:

Ing. MEZA ORDOÑEZ, Luis

HUÁNUCO – PERÚ

2020

DEDICATORIA

A Dios por permitirme llegar a este momento tan especial, por los triunfos y momentos difíciles que me han enseñado a valorarlo cada día más. A mis familiares por ser las personas que me han acompañado durante todo mi trayecto estudiantil y de vida.

AGRADECIMIENTO

Mi más cordial reconocimiento y agradecimiento a todos y cada uno de los ingenieros de la facultad, porque de alguna manera supieron brindarme su gama de experiencia profesional.

Mi agradecimiento a mis asesores, por su colaboración y orientación en la realización del presente proyecto, ya que supieron guiarme de la mejor manera con su amplio conocimiento.

De igual modo al Dr. Miller Villanueva Santamaría, director de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco por permitirme realizar la investigación y el desarrollo del trabajo en la organización en mención, como a también a todo el personal por brindarme la información que requería para la realización del presente proyecto

RESUMEN

El presente proyecto inicia con la problemática de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco referente a la seguridad de su información. La organización no contempla entre sus procesos mecánicas, medidas o políticas que le ayuden a proteger sus activos de las amenazas y riesgos a los que están expuestos.

Para el desarrollo del Sistema de Gestión de Seguridad de la Información, se hizo uso de la Norma Técnica Peruana NTP – ISO/IEC 27001:2014 y la metodología MAGERIT en su versión 3 (v3) para el análisis y gestión de riesgos de los activos, partiendo desde la evaluación del estado inicial de la organización referente a la seguridad de la información para posteriormente empezar a planificar y diseñar el Sistema de Gestión de Seguridad de la Información, la aceptación que tendría este en la organización, definir sus alcance, sus políticas y su comité de seguridad para luego pasar al análisis y gestión de riesgos donde se determinó las amenazas y vulnerabilidades a las que están expuestos los activos de información. Una vez teniendo los resultados del análisis se realizó el tratamiento de riesgos para posteriormente elaborar los controles de seguridad y el diseño de la declaración de aplicabilidad de acuerdo al lineamiento de la Norma Técnica Peruana NTP – ISO/IEC 27001:2014.

El proyecto no solo logró determinar cuáles son los controles más adecuados para la organización y las que debería implementar para proteger sus activos de información, también acercó a la organización al tema de la seguridad de la información, y brindando la documentación necesaria para una posterior implementación de este SGSI en los procesos de la entidad.

PALABRAS CLAVE: Sistema de Gestión de Seguridad de la Información, Norma Técnica Peruana NTP – ISO/IEC 27001:2014, Seguridad de la Información.

SUMMARY

This project begins with the problem of the Regional Directorate of Labor and Employment Promotion - Huánuco regarding the security of your information. The organization does not consider among its mechanical processes, measures or policies that help it to protect its assets from the threats and risks to which they are exposed.

For the development of the Information Security Management System, the Peruvian Technical Standard NTP - ISO / IEC 27001:2014 and the MAGERIT in its version 3 (v3) methodology were used for the analysis and risk management of assets, starting from the evaluation of the initial state of the organization regarding information security to later begin to plan and design the Information Security Management System, the acceptance that it should be in the organization, define its scope, its policies and its security committee and then move on to the analysis and risk management where the threats and vulnerabilities to which information assets are exposed were determined. Once the results of the analysis were obtained, the risk treatment was carried out to later elaborate the security controls and the design of the declaration of applicability according to the guidelines of the Peruvian Technical Standard NTP - ISO / IEC 27001:2014.

The project will not only seek to determine the most appropriate controls for the organization and those that should be implemented to protect its information assets, it also brought the organization closer to the issue of information security, and providing the necessary documentation for a subsequent implementation of this. ISMS in the entity's processes.

KEY WORDS: Information Security Management System, Peruvian Technical Standard NTP - ISO / IEC 27001:2014, Information Security.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

INTRODUCCIÓN

Desde hace ya algunos años se viene tratando la importancia de la seguridad de la información en las organizaciones, las cuales invierten en sistemas y dispositivos de seguridad, sin embargo, esto no es suficiente para decir que un sistema es seguro. De allí que estos mecanismos requieren de un plan de gestión de seguridad que pueda integrar a las políticas de la empresa considerando a la organización como un todo. Este plan permite maximizar los esfuerzos que se desarrollan en todos los niveles, apoya el cumplimiento del marco legal, aporta una metodología para el desarrollo del análisis y gestión de riesgos y garantiza la implementación de medidas de seguridad consistente, eficiente y apropiada al valor de la información protegida.

El presente proyecto busca establecer los controles con las cuales la organización pueda implementar el Sistema de Gestión de Seguridad de la Información en su organización a fin de tener un plan de gestión de seguridad que pueda beneficiar a la entidad en la protección de sus activos; a su vez concientizar y capacitar a los trabajadores de la organización en el tema de seguridad de la información.

Para el presente proyecto se revisaron 17 tesis los cuales aportaron a esta investigación en cuanto a resultados obtenidos y conclusiones a los que llegaron sus autores; en varias de estas tesis la problemática es muy similar a la del presente proyecto, y nos da a entender que el tema de seguridad está poco aplicado en las organizaciones.

Las limitaciones más resaltantes que se tuvieron en el presente proyecto fueron: la burocracia en las entidades públicas y el tiempo de la culminación del curso hicieron que se llegue hasta la fase de diseño y la situación en la que se encuentra el país por la pandemia del COVID 19 hizo que se trabajara con la información recabada hasta antes de la pandemia.

I. PLANTEAMIENTO DEL PROBLEMA

1.1. Antecedentes y fundamentación del problema

La seguridad informática es uno de los temas que genera polémica y preocupación dado la cantidad de ciberataques que suceden a nivel mundial; dado que actualmente hay muchos datos sensibles que se procesan mediante diversos dispositivos y es imposible que pase de ser percibido.

Diversas investigaciones que se hicieron a nivel mundial arrojaron que países son más ciberseguros y menos ciberseguros; los resultados arrojados hacen referencia a que países ponen a la ciberseguridad en una posición estratégica dentro de sus políticas por medio de las legislaciones dándose estos en el sector público, en el sector privado se refleja la utilización de sus recursos disponibles para resguardar la protección de su información.

Si hacemos una vista a años atrás, podemos decir que la seguridad informática era algo casi inexistente e infravalorado en las agendas y reuniones de trabajo de las organizaciones, pero en estos tiempos está muy presente en el contexto mundial, esto sucede gracias a que surgieron hechos noticiosos dados a raíz de infiltraciones de piratas y crackers informáticos en entidades que hasta ese momento parecían impenetrables en el aspecto de seguridad física e informática, basta con mencionar 2 ejemplos como son: El caso de Sony Pictures, y el escándalo de las filtraciones de Wikileaks. Estos casos hicieron que cuando se haga mención a la seguridad informática no se haga referencia a un valor agregado, sino a una necesidad que tienen todas las organizaciones.

Pasando a nivel nacional, un estudio revelo que el Perú es el segundo país de América Latina con menos seguridad informática o ciberseguridad. Esto luego

de que se dio a conocer que es el país con mayor número de ataques de spyware sufridos después de Brasil y México. Y en la posición mundial ocupamos el puesto 39.

Se sabe que, en el país, el aumento de la infiltración en el internet es una fuerte ventaja competitiva para las empresas, pero a su vez también formula un riesgo para la ciberseguridad y el país todavía no está listo para afrontarlo, aunque se sabe que hay avances legislativos y ejecutivos con respecto a la gestión de la seguridad informática en el Perú como lo son: leyes que se aplican al campo de la ciberseguridad, la propuesta de un viceministerio de tecnología de la información y comunicación, la división de delitos de alta tecnología como parte de la policía nacional. Muy aparte, las empresas y organizaciones pueden adoptar medidas de seguridad relevantes como las que establece la Norma Técnica Peruana sobre la Tecnología de la Información.

A nivel regional, la seguridad informática es casi inexistente, puesto que se ve el poco interés de las organizaciones tanto públicas como privadas sobre la protección de su información, pese a que hay normativas que les pueden ayudar a mejorar la integridad y confidencialidad de su recurso más importante, también a la poca promoción que hace el gobierno regional referente a este tema. Esta situación refleja la poca conciencia que se tiene referente a nuestra seguridad.

Después de realizar una investigación previa al proyecto y la problemática que este engloba, se dividió los problemas encontrados en los siguientes indicadores:

En el aspecto tecnológico se vio problemáticas como la no realización de un adecuado control en cuanto al hardware y software en los equipos informáticos,

así como la no existencia de mantenimientos preventivos a estos, también que no existen iniciativas de aseguramiento de la información.

En el aspecto normativo se encontró que la aplicación de un SGSI es limitada y se refleja en planes de seguridad básicos, generalmente realizado por similitud con otras entidades y no especifica al entorno real de la organización, a su vez no existen políticas de seguridad para el resguardo de los activos de información y no realizan la aplicación o estándares de seguridad sobre los activos de información.

En el aspecto del conocimiento, el personal que labora en la organización no tiene el conocimiento sobre el tema de seguridad de la información dado que todo está a responsabilidad de las áreas directiva – administrativa, así como se pudo apreciar que los trabajadores de la organización se apoyan generalmente en las herramientas cualitativas como el juicio de expertos por una falta de políticas de seguridad de la información.

En el aspecto de los procesos, la investigación previa muestra que hay una preocupación de los usuarios a riesgos o pérdidas de información, ya que hoy en día no necesariamente siguen una normativa, también que la organización siente preocupación en los cambios tecnológicos y los riesgos en Tecnologías de Información y Comunicación (TIC’s), así como la gestión de la seguridad de la información constituye un tema fundamental, el cual recién está siendo implantado en el medio profesional y en las entidades públicas de manera obligatoria, los sistemas de gestión de la seguridad abarcan un conjunto de tratamientos de riesgos como por ejemplo poco personal fiable, falta de experiencia en gestión, problemas de personal, problemas con la tecnología, cambio de normativas de

gobierno, y se debe puntualizar cada riesgo, lo cual ayudará a entender mejor y permitir identificar el control más adecuado para el tratamiento de este.

De acuerdo a lo mencionado anteriormente vemos que hoy en día los sistemas de información que se utilizan para almacenar, procesar y trasmitir información están en toda clase de organizaciones de diferentes rubros y la información se ha convertido en un activo que al igual que otros activos importantes de las entidades públicas tiene un valor significativo. Es así que existe una cantidad cada vez mayor de personas que tienen acceso a información que podría ser crítica para las diferentes entidades en la que trabajan.

De forma adicional a este riesgo interno, se tiene presente el riesgo que supone la fuga de información sensible ya sea por medio de personas que cuentan con acceso a dicha información, como por terceros que han accedido a ella mediante mecanismo de ataque. Libremente de la forma que tome la información o el medio por el que se distribuya, debe de protegerse.

La Dirección Regional de Trabajo y Promoción del Empleo – Huánuco no se encuentra distante a lo descrito con anterioridad y actualmente esta entidad no cuenta con ningún sistema de gestión de la seguridad y mucho menos con iniciativa de planes de desarrollo, pese a que hoy en día se cuenta con una serie de normas y estándares internacionales publicadas por la Organización Internacional de Normalización (ISO), en el Perú han sido definidas leyes alineadas a estos para que puedan ser aplicadas al contexto de las entidades existentes en el país en cuestión a la gestión de la información utilizada por las entidades públicas. La Resolución Ministerial RM-004-2016-PCM 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 la Seguridad de la Información. Requisitos 2ª Edición"; la Resolución Ministerial RM-129-2012-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP – ISO/IEC 27001:2008 EDI TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistema de Gestión de la Seguridad de la Información. Requisitos", en todas las entidades integrantes del Sistema Nacional de Informática; la Resolución Ministerial RM-197-2011-PCM, establecen fecha límite para que diversas entidades en la administración pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana "NTP – ISO/IEC 17799:2007 EDI. TECNOLOGÍA DE LA INFORMACIÓN. Código de buenas prácticas para la Gestión de la Seguridad de la Información"; además del Decreto Supremo DS-050-2018-PCM que tiene por objetivo ESTABLECER LA DEFINICIÓN DE SEGURIDAD DIGITAL DEL ÁMBITO NACIONAL, publicadas por la Secretaría de Gobierno Digital.

Es por esto que las entidades públicas tienen la necesidad de contar con un análisis que les permita realizar el diseño de un Sistema de Gestión de la Seguridad de la Información, en conjunto con los controles correspondientes al mismo como respuesta a la exigencia establecida por las normas mencionadas con anterioridad, lo que en conjunto forman la problemática que el proyecto intenta resolver siguiendo las buenas prácticas y estándares correspondientes que permitan realizar una identificación de la información crítica con la que trabaja la entidad y en consecuencia, definir los riesgos a los que se encuentra expuesto, así como los controles que deberían ser implementados para garantizar su seguridad.

Esta es la descripción de la realidad problemática que atraviesa actualmente la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco,

se observa que se presenta dificultades en el manejo de información y la seguridad de esta; estos problemas deben de tener un tratamiento de manera rápida.

Para que esto sea posible, la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco debe tomar en consideración la importancia de la seguridad de la información y los riesgos a los que están expuesto, con el objetivo de impulsar de una manera conjunta y coherente los diferentes elementos que ayudarán en su desarrollo institucional y tecnológico, de esta manera dar un tratamiento adecuado a los riesgos de información presentes en los procesos más importantes de la institución pública.

1.2. Formulación del problema

Problema general

¿De qué manera la propuesta de un Sistema de Gestión de Seguridad de la Información basado en la NTP – ISO/IEC 27001:2014, lograría mejorar la seguridad de la información de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco?

Problemas específicos

- ¿Qué requisitos de la NTP – ISO/IEC 27001:2014 aplicar para determinar el nivel y situación actual de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco?
- ¿Qué documentos exige la NTP – ISO/IEC 27001:2014 para diseñar un Sistema de Gestión de Seguridad de la Información?
- ¿Qué metodología usar para el análisis y gestión de riesgos en la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco?

- ¿Qué documento es utilizado para registrar los controles de seguridad aplicables a la Dirección Regional de Trabajo y Promoción del Empleo - Huánuco?

1.3. Objetivos: General y Específicos

Objetivo general

Proponer el diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP – ISO/IEC 27001:2014, para mejorar la seguridad de la información de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco.

Objetivos específicos

- Aplicar los requisitos 4 y 5 de la NTP – ISO/IEC 27001:2014 para diagnosticar el nivel y situación actual de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco.
- Elaborar los documentos exigidos por la NTP – ISO/IEC 27001 para diseñar un Sistema de Gestión de Seguridad de la Información.
- Aplicar la metodología MAGERIT v3 para analizar y gestionar los riesgos de los activos de información en la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco.
- Elaborar la Declaración de Aplicabilidad (SoA) para registrar los controles de seguridad aplicables a la Dirección Regional de Trabajo y Promoción del Empleo - Huánuco.

1.4. Hipótesis

Para el presente proyecto investigación no se realizará una formulación de hipótesis dado que tiene un alcance de estudio exploratorio, puesto que se tiene

como objetivo examinar el problema de investigación planteado y a su vez un enfoque cualitativo dado que se evalúa el desarrollo natural de los sucesos, sin manipulación ni estimulación con respecto a la realidad. Al finalizar el presente proyecto de investigación no se afirmará o refutará nada, sólo se presentará una solución al problema encontrado.

1.5. Variables y dimensiones

Variable independiente

Sistema de Gestión de Seguridad de la Información basado en la NTP – ISO/IEC 27001:2014. Sus dimensiones son: Confidencialidad, Integridad y Disponibilidad.

Variable Dependiente

Seguridad de la información de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco. Sus dimensiones son: Confidencialidad, Integridad y Disponibilidad.

1.6. Definición operacional de: Variables y Dimensiones

Tabla 1: Operacionalización de variables

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES
VARIABLE INDEPENDIENTE: Sistema de Gestión de Seguridad de la Información basado en la NTP – ISO/IEC 27001:2014	Es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos	Confidencialidad Integridad Disponibilidad	• Alcance • Evaluación de riesgos • Declaración de aplicabilidad

	comerciales y/o de servicio.	
VARIABLE DEPENDIENTE: Seguridad de la Información de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco.	Conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información	Confidencialidad Integridad Disponibilidad

Nota. Fuente: Elaboración Propia

La matriz de consistencia de la operacionalización de variables completa se muestra en el **ANEXO A**.

1.7. Justificación e importancia

La importancia de la Seguridad de la Información se viene tratando desde hace algunos años en las organizaciones, las cuales hacen grandes inversiones en sistemas y dispositivos de seguridad como: firewalls, antivirus, sistemas de respaldo, entre otros; sin embargo, esto no es suficiente para considerar que un sistema es seguro en relación a la integridad, la disponibilidad y la confidencialidad de la información que se maneja. De allí que los mecanismos de seguridad necesitan de un Plan de Gestión de Seguridad que integre a las políticas generales de la empresa, considerando a la organización como un todo.

Un plan de Gestión de Seguridad de la Información permite maximizar los esfuerzos desarrollados para asegurar la organización en todos sus niveles, apoya el cumplimiento del marco legal, aporta una metodología para el análisis y gestión del riesgo y garantiza la implantación de medidas de seguridad consistente, eficiente y apropiada al valor de la información protegida.

Es así como la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco se beneficiará con el diseño de un Sistema de Gestión de Seguridad de la Información, porque este permitirá establecer políticas, procedimientos, objetivos y procesos claros para que permitan determinar y proponer controles de seguridad que ayuden a tratar los riesgos en la seguridad de la información, comprometido en espacios físicos, procesos automáticos y manuales, gestión del personal, usuarios de los sistemas y equipos para optimizar la gestión de los incidentes que se detecten y generar resultados en concordancia con las políticas y objetivos generales de la organización.

1.8. Limitaciones

Limitación interna

Como limitación interna se tiene a la restricción a cierta información de la organización por ser de carácter personal.

Limitación Externa

- La burocracia en las entidades públicas y el tiempo para la culminación del curso hicieron que el proyecto sea elaborado hasta la fase de diseño.
- El desarrollo del presente proyecto y la comunicación con la organización se vio disminuida por la pandemia del COVID – 19, por lo que se trabajó en base a la información recaudada hasta antes de la pandemia.

II. MARCO TEÓRICO

2.1. Revisión de estudios realizados

Antecedentes internacionales

“Diseño de un Sistema de Gestión de Seguridad de la Información – SGSI basado en la norma ISO 27001 para el colegio Pro – colombiano de la

ciudad de Bogotá, que incluye: asesoría, planeación”. Jerzon Alvarez Riaño, autor del proyecto, luego del desarrollo y presentación de sus resultados, llegó a las siguientes conclusiones: Se requiere de una urgente implementación de un SGSI en la institución debido a las vulnerabilidades y amenazas que tiene; la institución no tiene definidas normas, políticas o procedimientos legales que protejan sus activos de información; la directiva de la institución al tomar la decisión de implementar el SGSI cumplirán con los objetivos de afianzar su compromiso en el sentido de proteger sus activos de información. (Alvarez Riaño, 2016)

“Diseño de un Sistema de Gestión de la Seguridad Informática – SGSI, para empresas del área textil en las ciudades de Itagüí, Medellín, Bogotá D.C. a través de la auditoría”. Alexánder Guzmán García y Carlos Taborda Bedoya, autores del proyecto, presentaron los siguientes resultados luego de su investigación: Con los resultados obtenidos se pueden dimensionar herramientas de software, protocolos, procedimientos que mitiguen el riesgo en las empresas Color Shop y Guille Sport; el riesgo informático es un factor que puede determinar la permanencia en el mercado o desaparición gradual de las empresas; herramientas como auditoría permiten visualizar el grado de protección en que se encuentran los activos de información en las organizaciones; se evidencian similitudes entre las empresas en cuanto al desconocimiento de metodologías y procesos para gestionar la seguridad informática; las PYMES no dimensionan en un alto grado lo importante que es hoy mantener segura la información y los activos que se interrelacionan con esta; los cambios constantes y las dinámicas del negocio hacen que se generen nuevas amenazas y vulnerabilidades, por ende

deben mantener capacitaciones constantes. (Guzmán García & Taborda Bedoya, 2015)

"Sistema de Gestión de Seguridad de la Información (SGSI) para el área de contabilidad de la E.S.E hospital local de Río de Oro Cesar". Aura Casadiegos Santana, Marcela Quintero Jiménez y Mileidy Toro Rueda, autoras de la tesis, luego de la elaboración y la contrastación de resultados llegaron a las siguientes conclusiones: La auditoría administrativa y de sistemas de información realizada logró identificar las falencias y vulnerabilidades que fomentan el riesgo de pérdida, daño o mal funcionamiento de la información física y lógica del área; se tomó como base la norma ISO/IEC 27001 que fue preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI y la NTC – ISO/IEC 27002 que es referido a buenas prácticas para salvaguardar la información; la política de seguridad establecida se realizó bajo los términos de las características de área. (Casadiegos Santana, Quintero Jiménez, & Toro Rueda, 2014)

Antecedentes Nacionales

"Diseño de un Sistema de Gestión de Seguridad de Información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013". Zuly Justino Salinas, autora de la tesis, después del desarrollo y presentación de sus resultados, llegó a las siguientes conclusiones: Es necesario establecer roles y responsabilidades dentro de la organización para garantizar el cumplimiento de las políticas de seguridad de información. Según su análisis de riesgo, el nivel de la seguridad en la organización es bajo, debido a que hay riesgos que se consideran no aceptables y al no contar con una regulación específica que exija tomar un modelo de seguridad de información, la organización trabajará en el

aspecto cultural de seguridad a todo nivel para concientizar al personal y llevar a cabo el SGSI. (Justino Salinas, Diseño de un Sistema de Gestión de Seguridad de la Información para una empresa inmoviliaria alineado a la norma ISO/IEC 27001: 2013, 2015)

“Desarrollo de un Sistema de Gestión de Seguridad de la Información para minimizar riesgos en los activos de información en la sub gerencia de informática y telecomunicaciones de la municipalidad distrital de Independencia 2016”. Angelica Armas Huamán y Alberto Medina Villacorta, autores de la tesis, después del desarrollo y presentación de resultados, llegaron a las siguientes conclusiones: El proyecto será un gran aporte como punto de partida a la minimización de riesgos existentes; los activos, en su mayoría, están entre un estado intolerable y un riesgo extremo, por lo que sería oportuno implementar las medidas correctivas. (Armas Huamán & Perez Romero, 2018)

“Diseño de un Sistema de Gestión de Seguridad de la Información para servicios postales del Perú S.A”. David Aguirre Mollehuanca, autor de la tesis, después del desarrollo y presentación de sus resultados, llegó a las siguientes conclusiones: La alta dirección jugó un papel importante en el sistema de gestión ya que ayudó a los jefes de las áreas a entender que el SGSI busca proteger toda la información crítica del negocio; otra conclusión del proyecto fue que es necesario difundir las normas de seguridad en la organización por ende se precisa establecer charlas y capacitaciones a toda la organización y finalmente es necesario contratar un personal especializado para dar soporte a los procesos involucrados en el SGSI, como también mejorar la comunicación con el área logística quien es la encargada de la adquisición de los activos que ayudaron en el tratamiento de riesgos detectados. (Aguirre Mollehuanca, 2014)

“Sistema de Gestión de Seguridad de Información (SGSI) basado en la Norma ISO/IEC 27001 para mejorar la seguridad del área de operaciones y tecnología de Global BPO Center Allu Chiclayo – 2015”. Cinthia Rojas Viera y Tefhany Zavaleta Verona, autoras de la tesis, después del desarrollo y presentación de sus resultados, llegaron a las siguientes conclusiones. La evaluación de riesgos se inició con criticidad alta, los cuales se usaron para un tratamiento de riesgos, así como, los controles seleccionados de la Norma ISO/IEC 27001 para su implementación fueron 13, los cuales se eligieron para mitigar los riesgos más críticos del área en mención. (Rojas Viera & Zavaleta Verona, 2019)

“Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015”. Ronal Leiva Peña, el autor de la tesis, después del desarrollo y presentación de sus resultados, llegaron a las siguientes conclusiones: La evaluación de los riesgos aplicando la norma inició con una criticidad alta, un total de 75; los controles seleccionados para su implementación fueron un total de 20, los cuales fueron elegidos para mitigar los riesgos más críticos del proceso de suministro de medicamentos. (Leiva Peña, 2016)

“Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la empresa agroindustrial POMALCA S.A.A – 2016”. César Villegas Rivera y Germán Zamora Li, autores de la tesis, después del desarrollo y presentación de sus resultados, llegaron a las siguientes conclusiones: El proyecto permitió conocer mediante la aplicación del estándar internacional que la organización no cumple con la mayoría de objetivos

de control y controles de seguridad, ya que se refleja la carencia de documentación correspondiente al estándar ISO, así como tampoco el empleo de mecanismos de seguridad en la transmisión y tratamiento de la información. (Villegas Rivera & Zamora Li, 2018)

"Implementación de un Sistema de Gestión de Seguridad de la Información – Norma ISO 27001 para la fábrica Radiadores Fortaleza". César Benites Duran, autor de la tesis, después del desarrollo y presentación de sus resultados, llego a la siguiente conclusión: La generación de controles informáticos generó un buen impacto en el resguardo de los activos de información, las pruebas de ello se demuestran en el presente escrito. El resultado fue satisfactorio, se redujo considerablemente los incidentes técnicos, así como la reducción de tiempo de respuesta en el usuario y el responsable de TI, gracias a esto se afianzó la seguridad y confianza usuario – área TI. (Benites Durand, 2019)

"Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001 para la Dirección de Salud Virgen de Cocharcas – Chincheros". Diego Escalante Coronel, autor de la tesis, después del desarrollo y presentación de sus resultados, llego a la siguiente conclusión: "Con el apoyo de la alta dirección y el compromiso de los trabajadores de la entidad, se logró implementar el diseño bajo el enfoque de la NTP – ISO/IEC 27001 para la Dirección de Salud Virgen de Cocharcas – Chincheros". (Escalante Coronel, 2019)

"Diseño de un Sistema de Gestión de Seguridad de la Información para los procesos académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001". Iván Vegas Varona, autor de la tesis, después del desarrollo y presentación de sus resultados, llego a las siguientes conclusiones: "Se encontró

un bajo porcentaje de cumplimiento del 39% que evidencia un descuido con respecto a la seguridad de la información dentro de la institución"; el modelo de los procesos puso en evidencia que hay 50 activos de información importantes para la organización, como también se vio que hay controles básicos para la seguridad de la información en la organización, pero estos no tienen una documentación y tampoco son conocidos por el personal. (Vega Varona, 2019)

"Diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP – ISO/IEC 27001: 2014 para la Dirección General de Informática y Estadística de la Universidad Nacional Daniel Alcides Carrión". Elmer Atencio Bazán, autor de la tesis, después del desarrollo y presentación de sus resultados, llego a las siguientes conclusiones: La problemática de la inseguridad de la información no puede resolverse solo con identificar los servicios a proteger, las herramientas o las operaciones, sino que trasciende más allá de eso, es algo más complejo, involucra un trabajo en conjunto de toda la organización; algunas decisiones respecto al cumplimiento de las políticas del SGSI deben ser de la alta dirección, siendo lo primero para adaptarse al cambio dentro de la Universidad; un SGSI no se puede implantar por simple requisito, sino se debe buscar objetivos que le den un valor agregado a la Universidad, pues toda nueva implementación es para mejorar y debe ser acompañado con los esfuerzos, pero hay poco interés de la organización por conocer los riesgos a los que están expuestos; dentro del análisis se pudo evidenciar que uno de los factores que afectan a la disponibilidad e integridad de la información son por fallas del personal, ya que en gran parte la manipulación de la información no está dada por sistemas operativos óptimos, lo cual general errores de configuración, de transacciones mal ejecutadas y saltos de información. (Atencio Bazan, 2019)

“Diseño de un Sistema de Gestión de Seguridad de la Información bajo la NTP – ISO/IEC 27001: 2014 para la Municipalidad de Huamanga, 2016”. Mercedes Ccesa Quincho, autora de la tesis, después del desarrollo y presentación de sus resultados, llego a la siguiente conclusión: Se determinó como características esenciales del diseño del SGSI para la Municipalidad Provincial de Huamanga, el compromiso y apoyo de la alta dirección, el conocimiento de la organización, la adecuada identificación del alcance del SGSI, la evaluación de riesgos y la mejora continua. (Ccsa Quincho, 2017)

“Propuesta de un Sistema de Gestión de Seguridad de la Información, aplicando la metodología MAGERIT para el gobierno regional de Puno caso: Proyecto especial Camélidos Sudamericanos – PECSA, 2017”. William Yana Viveros, autor de la tesis, después del desarrollo y presentación de sus resultados, llego a las siguientes conclusiones: Se realizó la propuesta del SGSI, con el diagnóstico inicial de la organización, entrevistando al personal, dando luego como resultado respuestas negativas, poniendo en evidencia que el PECSA, no contaba con un SGSI; el uso de la herramienta PILAR fue importante para los controles del SGSI, pues con ellos se determinaron los activos con alta criticidad. (Yana Viveros, 2018)

Antecedentes locales

“Propuesta de un Sistema de Gestión de Seguridad de la 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”. Eduardo Argüezo Ramírez, autor de esta tesis, después del desarrollo y presentación de sus resultados, llegó a las siguientes conclusiones: El desarrollo de las políticas de seguridad es de gran utilidad para la protección de los activos

de información, con la investigación se identificó y evaluó los riesgos a los que están expuestos los activos de la información realizando la matriz de amenazas y el plan de tratamiento de riesgos para estos, para asegurarse la protección de los activos de información. (Argüero Ramirez, 2019)

"Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa GEOSURVEY de la ciudad de Lima". Ehytel Vilca Mosquera, autor de la tesis, después del desarrollo y presentación de sus resultados, llegó a las siguientes conclusiones: La intervención en la empresa GEOSURVEY resultó en una mejora del sistema de gestión de la seguridad de la información en el área de recursos humanos, optimizando los procesos de capacitación y formación de la seguridad en cuanto al uso de la información y de los equipos de la empresa. (Vilca Mosquera, 2017)

2.2. Principales leyes, definiciones y conceptos fundamentales

- **Resolución Ministerial N° 004 – 2016 – PCM:** Aprueban el uso obligatorio de la Norma Técnica Peruana "ISO NTP/ IEC 27001:2014. Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática. (…) Que la actual Política Nacional de Gobierno Electrónico 2013 – 2017, aprobada mediante el Decreto Supremo N° 081 – 2013 – PCM, prevé determinados Lineamientos Estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información, el mismo que busca velar por la integridad, seguridad y disponibilidad de los datos debiendo establecer lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible al ciudadano. (Gob.pe, 2016)

- **Resolución Ministerial N° 129 – 2012 – PCM:** Aprueban el uso obligatorio de la Norma Técnica Peruana “NTP – ISO/IEC 27001:2008. EDI Tecnología de la Información. Técnicas de Seguridad. Sistema de gestión de seguridad de la información”. (Gob.pe, 2012)
- **Resolución Ministerial N° 197 – 2011 – PCM:** Establece fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana “NTP – ISO/IEC 17799: 2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”. (Gob.pe, 2011)
- **Norma Técnica Peruana NTP – ISO/IEC 27001:** En el Perú se cuenta con esta norma para garantizar la confidencialidad como la integridad de la información, y a su vez, los sistemas que lo tratan. Esta norma para los Sistemas de Gestión de Seguridad de la Información hace posible que las organizaciones evalúen el riesgo y apliquen los controles para su mitigación o total eliminación; esta norma permite que las organizaciones se diferencien del resto de las entidades que compiten en el mismo mercado a su vez que aumenta su reputación. (ISOTools Excellence, s.f.)
- **ISO 27001**: Es una norma internacional emitida por la Organización Internacional de Normalización (ISO); proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada, esto significa que una entidad de certificación independiente conforma que la seguridad de la información ha sido implementada en esa organización en cumplimiento de la norma.

  El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto se logra investigando

cuales son los potenciales problemas que podrían afectar la información y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan.

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma:

1) Cumplir con los requerimientos legales: Cada vez hay más leyes, normativas y requerimientos relacionados con la seguridad de la información.
2) Obtener ventaja comercial: Si una empresa obtiene su certificación y sus competidores no, es posible que se obtenga una ventaja sobre ellos ante los ojos de los clientes.
3) Menores costos: La filosofía principal del ISO 27001 es evitar que se produzcan incidentes de seguridad, por lo tanto, evitándolos, su empresa va a ahorrar mucho dinero.
4) Una mejor organización: La implementación del ISO 27001 ayuda a resolver las situaciones donde la empresa no tiene tiempo para hacer una pausa y definir sus procesos y procedimientos; la norma alienta a las empresas a escribir sus principales procesos, lo que les permite reducir el tiempo perdido de sus empleados. (Segovia, sf.)

- **MAGERIT**: Es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Puntualmente MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas

que pueden afectar a la compañía y las vulnerabilidades que puedan ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

Lo interesante de esta metodología es que presenta una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgos.

Esta metodología es muy útil para aquellas empresas que inicien con la gestión de la seguridad de la información, pues permite enfocar los esfuerzos en los riesgos que pueden resultar más críticos para la empresa. Lo interesante es que al estar alineado con los estándares ISO, su implementación se convierte en el punto de partida para una certificación o mejorar los sistemas de gestión. (Amaya Gutiérrez, 2013)

- **Sistema de Gestión de Seguridad de la Información (SGSI)**: Se puede definir como una herramienta que nos va a permitir conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en nuestra empresa.

  Cada día surgen nuevas formas de delito informático que pueden afectarnos. Por ello, la legislación se ha desarrollado para proteger a todos los actores que utilizamos las nuevas tecnologías ante el aumento de estos delitos.

  Hay que tener en cuenta que desarrollar en nuestra organización este proceso de seguridad va a mejorar la imagen y confianza proyectada entre clientes, proveedores y socios.

  A la hora de implantar en nuestra organización este sistema de seguridad debemos tomarlo como una decisión estratégica que involucre a toda la organización y que sea apoyada y dirigida desde la dirección.

  Su diseño dependerá de los objetivos y necesidades de la empresa, así de como de su estructura. Estos elementos son los que van a definir el alcance

de la implantación del sistema, es decir, las áreas que van a verse involucradas en el cambio. Hay que tener presente, la solución más sencilla de implantar y mantener suele ser la más acertada. (CIC, 2019)

2.3. Marco situacional

La Dirección Regional de Trabajo y Promoción del Empleo – Huánuco es una entidad pública la cual antes del proyecto presentaba un escenario desconocido referente a la seguridad de la información. No se hacía un adecuado uso de la infraestructura tecnológica, la no existencia de políticas de seguridad, el poco interés de la alta dirección en la inversión de dispositivos de seguridad para la organización, el desconocimiento del personal referente al tema de seguridad de la información. La organización se enfocaba en cumplir sus metas y funciones sin tener en consideración los puntos de seguridad, lo que le generó inconvenientes en varias oportunidades, pese a esto la organización seguía con sus actividades hasta la presentación del presente proyecto a la alta dirección y la aceptación por parte de esta.

2.4. Conceptualización de términos

- **Activo:** Los activos son los componentes indispensables para el funcionamiento de un sistema informático. Se clasifican en: Hardware, Software y Datos o Información. (Fundación Carlos Jlim, s.f.)
- **Alcance:** Describe la extensión y los límites del SGSI, por lo que puede estar definido en términos de los activos de información, la ubicación física, las unidades organizacionales, actividades o procesos de mayor importancia para la organización, es decir, se trata de la selección de los elementos críticos a proteger. (Mendoza, Welivesecurity, 2018)

- **Amenaza:** Son las situaciones que desencadenan en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información. (SGSI, 2015)
- **Compromiso de la Dirección:** Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. (ISO27000.ES, 2005)
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (ISO27000.ES, 2005)
- **Control:** Medida por la que se modifica el riesgo. (ISO27000.ES, 2005)
- **Declaración de aplicabilidad:** Documento que enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001. (Mendoza, Welivesecurity, 2015)
- **Degradación de datos (degradación):** Deterioro gradual que sufre un medio de almacenamiento digital con el paso del tiempo. (GuíasPracticas.COM, 2017)
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (ISO27000.ES, 2005)
- **Estimación de riesgos:** Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable. (ISO27000.ES, 2005)
- **Evaluación de riesgos:** Proceso global de identificación, análisis y estimación de riesgos. (ISO27000.ES, 2005)

- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (ISO27000.ES, 2005)
- **Identificación de riesgos:** Proceso de encontrar, reconocer y describir riesgos. (ISO27000.ES, 2005)
- **Impacto:** El coste para la empresa de un incidente – de la escala que sea -, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc. (ISO27000.ES, 2005)
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (ISO27000.ES, 2005)
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud. (ISO27000.ES, 2005)
- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesitan por tanto ser protegidos de potenciales riesgos. (ISO27000.ES, 2005)
- **Monitoreo:** Determinar el estado de un sistema, un proceso o una actividad. Para determinar el estado, puede ser necesario verificar, supervisar u observar críticamente. (ISO27000.ES, 2005)
- **Nivel de riesgo:** Magnitud de un riesgo expresado en relación a la combinación de consecuencias y su probabilidad. (ISO27000.ES, 2005)

- **Parte interesada:** Persona u organización que puede afectar, ser afectada o percibirse a sí misma como afectada por una decisión o actividad. (ISO27000.ES, 2005)
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO27000.ES, 2005)
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO27000.ES, 2005)
- **Proceso de gestión de riesgo:** Aplicación sistemática de políticas de gestión, procedimientos y prácticas a las actividades de comunicación, consultoría, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, monitoreo y revisión de riesgos. (ISO27000.ES, 2005)
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. (ISO27000.ES, 2005)
- **Sistema de gestión:** Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas y objetivos y procesos para alcanzar esos objetivos. (ISO27000.ES, 2005)
- **Sistema de información:** Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información. (ISO27000.ES, 2005)
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO27000.ES, 2005)

III. MARCO TEÓRICO

3.1. Tipo de investigación

El presente proyecto de investigación es de tipo aplicada, porque busca la aplicación práctica de los conocimientos existentes a una realidad concreta. No se aspira a probar una hipótesis, pero si contribuir a la solución del problema que presenta la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco, mediante la propuesta de diseño del Sistema de Gestión de Seguridad de la Información.

3.2. Diseño de investigación

El diseño del presente proyecto investigación fue no experimental - transversal. No experimental porque se observó los fenómenos tal y como se dieron en su contexto natural, sin manipular deliberadamente las variables. Transversal porque se recolectaron los datos en un solo momento.

3.3. Determinación del Universo / Población

La población para el presente proyecto de investigación vino a ser todos los activos de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco, dado que la aplicación de la seguridad de la información es importante en toda la organización.

3.4. Selección de muestra

Para el presente proyecto, la muestra vino a ser la misma cantidad de activos de información que la de la población, porque la organización está conformada sub áreas en la que los activos de información de cada área son igual de importante y no puede y no puede quedar desprotegida ninguna.

3.5. Técnicas e instrumentos de recolección de datos

La técnica para la realización del presente proyecto fue la observación no experimental porque se recolecta los datos en el contexto natural y no controlado por el investigador.

Los instrumentos utilizados para la recolección de datos fueron: una guía de observación (**ver ANEXO B**) y un cuestionario para identificar los activos de información, dado que los trabajadores de la organización pueden no reconocer todos los activos que pueden estar a su cargo, estos instrumentos ayudaran a que ningún activo quede fuera del análisis en la organización.

3.6. Procesamiento y presentación de datos

Luego de recolectar los datos sobre los activos de información se procedió a llevarlos a Excel y organizarlo por tipos según lo especificado por la metodología MAGERIT, a partir de aquí se construyeron tablas, las cuales ayudaron a realizar el análisis de los activos, y conocer la situación de la organización en cuanto a su seguridad informática. La información resultante del análisis ayudó a diseñar la declaración de aplicabilidad y las políticas de seguridad de la información para la organización.

IV. RESULTADOS

Fase I: Diagnóstico de la situación actual de la organización

En esta fase se van a presentar las actividades que se realizan para conocer la situación de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco (DRTPE) frente a la seguridad de la información y el diseño del SGSI.

- **Evaluación del estado inicial de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco con respecto a los requisitos de la NTP – ISO/IEC 27001**

Para evaluar el estado inicial de la organización con respecto a los requisitos de la ISO/IEC 27001, se ha definido dos formas de presentar los resultados: una descriptiva y otra cuantificable (**ver tabla 2**). Esta técnica se basa en calificar el estado de los requerimientos en función a una escala de Likert aplicando cinco opciones que van de menor a mayor.

Tabla 2: Criterio para evaluar el estado actual de la DRTPE

CRITERIO DE CALIFICACÓN	VALORACIÓN
No diseñado: Las actividades/métodos demuestran que no se tiene el requisito y/o no se ha bosquejado su implementación.	0%
Parcialmente diseñado: Las actividades/métodos demuestran que se tiene el requisito definido, pero no es del todo conforme con el requisito de la NTP – ISO/IEC 27001.	25%
Diseñado: Los métodos son conformes con el requisito de la NTP – ISO/IEC 27001, pero sin evidencias de aplicación.	50%
Parcialmente Implementado: Las actividades/métodos son conformes con el requisito de la NTP – ISO/IEC 27001, pero con pocas evidencias de aplicación.	75%
Completamente Implementado: Las actividades/métodos son conformes con el requisito de la NTP – ISO/IEC 27001, y se cuenta con evidencias de aplicación permanentes.	100%

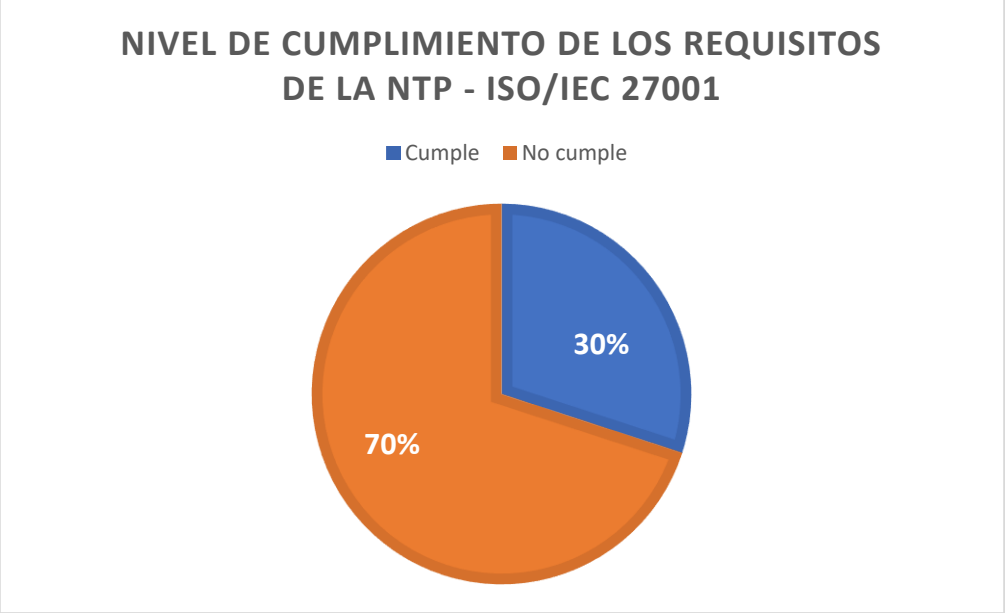
Nota. Fuente: *"Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001 para la Dirección de Salud Virgen de Cocharcas – Chicheros" (tesis), Escalante Coronel, Diego, 2019, p.26.*

El punto de partida fue elaborado con los capítulos y requerimientos de la norma; la evaluación fue realizada de la siguiente manera:

- Se realizó la calificación de cada requisito.

- Según el puntaje obtenido se colocó la evidencia / sugerencia para el cumplimiento de la NTP – ISO/IEC 27001.
- Para el porcentaje del capítulo, se sacó el promedio de los requisitos de este.

Ilustración 1: Nivel de cumplimiento de los requisitos de la NTP - ISO/IEC 27001



Por medio de este análisis diferencial es posible determinar que la organización comprende la importancia y beneficios de un SGSI y posee el liderazgo que se requiere para poder realizarlo; sin embargo, aún no se ha establecido adecuadamente una metodología de análisis y evaluación de riesgos informáticos y su tratamiento, como tampoco ninguna documentación requerida por la NTP – ISO/IEC 27001.

El resultado que se obtuvo de la evaluación inicial de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco respecto a los requisitos de la NTP – ISO/IEC 27001 se muestra en el **ANEXO C**.

- **Resultado de la evaluación del estado inicial de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco con respecto a los requisitos de la NTP – ISO/IEC 27001**

  Según la evaluación realizada, de un total de 100% de los requisitos de la NTP – ISO/IEC 27001 que se deben cumplir, la organización obtuvo un puntaje total de 5%, por lo que se puede decir que la DRTPE se encuentra en una etapa básica del cumplimiento de la norma (no diseñado).

  El resultado obtenido también muestra que la seguridad de la información dentro de la organización no es gestionada, que el diseño y posterior implementación del SGSI implicará un mayor esfuerzo, dependerá del compromiso y disponibilidad del personal de la organización.

Fase II: Elaboración de la documentación requerida por la NTP – ISO/IEC 27001:2014 para el diseño de un SGSI

Los objetivos de esta fase fueron: definir el alcance del SGSI, elaborar las políticas y objetivos de seguridad, identificar los requisitos legales (aplicables al SGSI) y proponer el comité de seguridad de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco. Estos objetivos se consiguieron tras analizar los contextos externos e internos de la organización y comprender las necesidades y expectativas de las partes interesadas en el SGSI.

- **Contexto de la organización**

  La NTP – ISO/IEC 27001 hace referencia en el capítulo 4: Contexto de la organización, la importancia de comprender la organización y su contexto, esto se refiere a que, los aspectos internos y externos que son relevantes para el establecimiento del SGSI, así mismo, comprender también las necesidades y expectativas de las partes interesadas y determinar el alcance del SGSI.

- **Contexto externo**

En el ítem se analizó los factores externos (relevantes) que afectan a la organización. En este aspecto por un lado tenemos influencias como el Estado, Gobierno Regional, las municipalidades, las empresas públicas y privadas, los sindicatos de trabajo, la sociedad, etc., y por otro tenemos la situación actual del país debido a la pandemia del COVID – 19; la organización tiene que afrontar los nuevos retos tecnológicos; en otras palabras tiene que re organizar sus procesos e incluir hacer uso de herramientas tecnológicas a fin de poder cumplir sus funciones y responsabilidades con la sociedad.

Para ello se utilizó la herramienta de análisis PEST (iniciales de factores Políticos – Legales, Económicos, Socio – Culturales y Tecnológicos)

El resultado del análisis se aprecia en la **tabla 3**.

Tabla 3: Análisis PEST

Político - Legal	○ Interés del estado y gobierno regional por la seguridad de la información en todas las entidades públicas. ○ Marco regulatorio sobre seguridad de la información. ○ Estandarización de procesos y sistemas de gestión.
Económico	○ Alto costo de consultores para establecer un SGSI.
Socio – Cultural	○ Sociedad peruana cada vez más tecnológica. ○ Sociedad peruana preocupada por la seguridad de su información.
Tecnológico	○ Aparición de necesidades de implementación tecnológica. ○ Nuevas necesidades de implementación tecnológica. ○ Vulnerabilidad en la seguridad de la información.

Nota. Fuente: Adaptado de *"Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001*

para la Dirección de Salud Virgen de Cocharcas – Chicheros" (tesis), Escalante Coronel, Diego, 2019, p.29.

La comprensión del contexto externo es muy importante para estar seguros que los objetivos e inquietudes de las partes externas se tienen en cuenta cuando se desarrollan los criterios de riesgo.

- **Contexto interno**

Como factores internos podemos citar algunos como: la resistencia al cambio, deficiencia en el mantenimiento de los recursos tecnológicos, uso inadecuado de los recursos tecnológicos, uso inadecuado por parte del personal concerniente a los permisos de trabajo, entre otros.

El SGSI debe alinearse con la cultura, los procesos, la estructura y la estrategia de la organización.

- **Naturaleza de la entidad**

La Dirección Regional de Trabajo y Promoción del Empleo – Huánuco como organismo público, es un órgano desconcentrado con dependencia técnica y normativa del Ministerio de Trabajo y Promoción del Empleo, pero presupuestalmente y administrativamente dependiente del Gobierno Regional de Huánuco comprendiendo el ámbito territorial de Huánuco; constituyéndose en el ente rector encargado de observar las políticas socio – laborales y promoción del empleo, cuyo personal se encuentra sujeto tanto al régimen de la actividad pública como al de la actividad privada.

- **Misión**

"Somos el ente rector en materia de desarrollo y evaluación de las políticas sociales de trabajo y promoción de la empleabilidad e inserción laboral, el autoempleo y trabajo decente a nivel regional, garantizando el cumplimiento de la normativa vigente, la prevención y solución de conflictos,

la mejora de las condiciones de trabajo y el respeto a los derechos fundamentales del trabajador para el progreso de nuestras empresas en beneficio del desarrollo socioeconómico de la región, en un marco democrático y de diálogo social".

- **Visión**

  Ser una institución pública moderna, líder en la promoción y generación de empleo productivo digno; en la administración del trabajo y de un ambiente socio – laboral justo y democrático. Promover la concertación y diálogo entre los actores sociales y el Estado para contribuir al mejoramiento de la calidad de vida de la población.

- **Objetivos**

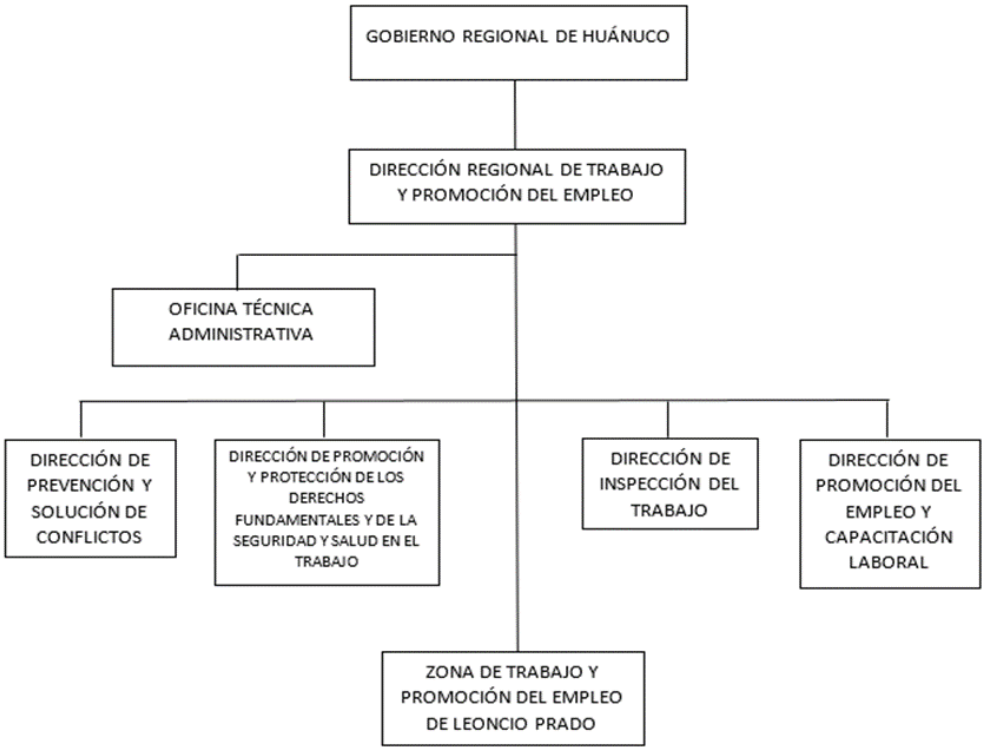
  - Promover el empleo y el mejoramiento de las condiciones de trabajo y calidad de vida del trabajador, el desarrollo socio – laboral; el fomento de las relaciones laborales, la promoción y previsión social, a través de la concertación y le diálogo con los trabajadores, empleadores y organizaciones sociales que correspondan.
  - Promover las condiciones que eliminen el desempleo y sub empleo, proteger y mejorar el ingreso real de los trabajadores, contribuir al incremento de la productividad, promover la seguridad y salud en el trabajo; fomentar la formación profesional y capacitación técnica y mejorar el bienestar y seguridad social del trabajador y su familia, sin discriminación alguna.
  - Extender la protección y campo de acción del derecho laboral de la administración del trabajo y promoción y previsión social a los pobladores y categoría socio – económica actualmente no protegidas.

- Fomentar el cumplimiento de las normas laborales de los regímenes privados y públicos, asegurando la conformidad de las normas y prácticas nacionales en materia laboral, a los estándares y normas establecidas por la Organización Internacional del Trabajo (OIT).

- **Estructura orgánica**

Aquí se muestra la estructura orgánica de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco. En este organigrama se ha designado a la dirección y la oficina técnica administrativa como responsables de la seguridad de la información dentro de la entidad.

Ilustración 2: Organigrama de la Dirección Regional de Trabajo y Promoción del Empleo - Huánuco.



Nota. Fuente: (Rios Rivera, Olivera Ruiz, Rios Rivera, & Ponce Guizabalo, 2013)

- **Aspectos técnicos**

La organización dispone en sus instalaciones 37 estaciones de trabajo, 3 switches, 1 router y una página institucional en Facebook (https://es-facebook.com/www.drtpehuanuco.gob.pe). Cada trabajador, de cada sub área almacena y gestiona la información en su propia PC, no hay una red propia de la entidad, no se cuenta con un servidor, las copias de seguridad lo hacen los mismos trabajadores con una unidad de almacenamiento externo.

Para la salida de los sistemas de información se cuenta con línea de fibra óptica.

Cabe hacer mención que en la institución el cableado de red está expuesto, revuelto en algunos casos y tendido por el suelo en algunas áreas, así también se puede decir que, todos los activos están expuestos a amenazas que afecten sus dimensiones de integridad, confidencialidad y disponibilidad.

- **Sistemas de información de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco**

  La organización cuenta con varios sistemas de información desarrollados por terceros dentro de los que se encuentran:

  - ✓ **Sistema Integrado de Gestión Administrativa (SIGA)**: Es una aplicación en el cual se ve plasmada toda la normatividad relacionada a las contrataciones del Estado y en cada una de las interfaces y opciones que tiene este sistema se puede apreciar todo el proceso logístico que va desde la generación de los pedidos, el proceso de selección y posteriormente se general ya sean los contratos, las órdenes de compra y servicio. (Cámara de comercio e industrias de Huánuco, s.f.)
  - ✓ **Sistema de Gestión Documentaria (SISGEDO)**: Es una aplicación web desarrollada por el Gobierno Regional de Huánuco para efectuar el registro, control y seguimiento detallado y estricto de todos los expedientes

que se procesan en la institución, tanto externos como internos. (Gobierno Regional de Huánuco, s.f.)

- ✓ **Sistema de Intermediación Laboral (SILNET)**: Es una herramienta informática que permite automatizar los procesos del Servicio de Intermediación Laboral de la red de los Centros de Empleo a nivel nacional, siendo éstos: Bolsa de Trabajo, Acercamiento Empresarial, Certificado Único Laboral y Asesoría en la Búsqueda de Empleo, así como el registro y publicación de vacantes públicas. (Vásques Colquehuanca, 2018)
- ✓ **Sistema de Registro Nacional de Trabajadores de Construcción Civil (RTCC)**: Tener un registro actualizado de trabajadores del régimen de construcción civil, siendo fuente de información para la inspección del trabajo, permitiendo ofertas de empleo y la identificación de aquellas personas infiltradas en las obras de construcción que realizan actos delincuenciales, así como, coadyuvará a la capacitación, especialización y certificación de las competencias laborales de los trabajadores del rubro de Construcción Civil. (Dirección Regional de Trabajo y Promoción del Empleo - Apurimac, s.f.)

- ➢ **Comprender las necesidades y expectativas de las partes interesadas**

Conforme al requisito 4.2 (Comprender las necesidades y expectativas de las partes interesadas) de la norma. En este apartado se identificaron las partes interesadas externas e internas afectadas por el diseño y posterior implementación del SGSI.

- ❖ **Partes interesadas externas**
  - **Gobierno (ONGEI – PCM)**

La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), es el Órgano Técnico Especializado que depende directamente del Despacho

de la Presidencia del Consejo de Ministros (PCM), ONGEI, es en su calidad de Ente Rector de Sistema Nacional de Informática, se encarga de liderar los proyectos, la normatividad y las diversas actividades que en materia de Gobierno Electrónico realiza el Estado. Entre sus actividades permanentes se encuentran las vinculadas a la normatividad informática, la seguridad de la información, el desarrollo de proyectos emblemáticos en Tecnologías de la Información y Comunicación (TIC), brindar asesoría técnica e informática a las entidades públicas, así como, ofrecer capacitación y difusión en temas de Gobierno Electrónico y la modernización y descentralización del Estado. (ONGEI, s.f.)

- **Contraloría General de la República**

  Es la máxima autoridad del Sistema Nacional de Control. Supervisa, vigila y verifica la correcta aplicación de las políticas públicas y el uso de los recursos y bienes del Estado. Para realizar con eficiencia sus funciones, cuenta con autonomía administrativa, funcional, económica y financiera. (La Contraloría General de la República del Perú, s.f.)

- **Los usuarios**

  Corresponde a la sociedad huanuqueña, a las personas naturales, los trabajadores de construcción civil, estudiantes, micro empresas, etc.

❖ **Partes interesadas internas**

- **Alta dirección**

  Debe demostrar liderazgo y compromiso con respecto al SGSI, asegurando que los objetivos que se establecen sean compatibles con la planeación estratégica de la organización y estableciendo una política de seguridad de la información.

- **Responsable de informática**

Es el responsable de la seguridad de la información y continuidad tecnológica de la entidad.

- **Responsable administrativo**

Responsable del SI antes, durante y después de la vinculación de los funcionarios y trabajadores.

- **Trabajadores de la organización**

Responsables de velar por la seguridad de los activos de información de la organización, cumplir a cabalidad con las normas y políticas de seguridad establecidas en la entidad.

Tabla 4: Requisitos de las partes interesadas

PARTES INTERESADAS	REQUISITOS
Alta dirección	✓ Supervisar las actividades y proyectos del responsable de informática en temas de seguridad de la información. ✓ Debe demostrar liderazgo y compromiso con la seguridad de la información.
Responsable de informática	✓ Levantamiento de no conformidades respecto a la seguridad de la información. ✓ Capacitar a los trabajadores en temas de seguridad de la información.
Responsable administrativo	✓ Verificar la seguridad de la información antes, durante y después de la vinculación de los trabajadores.
Trabajadores de la DRTPE	✓ Conocer las normas y políticas en temas de seguridad de la información. ✓ Velar por los activos de información de la DRTPE. ✓ Protección de su información personal. ✓ Capacitación en temas de seguridad de la información.

Nota. Fuente: Adaptado de *"Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001 para la*

Dirección de Salud Virgen de Cocharcas – Chicheros" (tesis), Escalante Coronel, Diego, 2019, p.35.

- **Comité de seguridad de la información**

De acuerdo al requisito 5.3 Roles, responsabilidades y autoridades organizacionales de la NTP ISO/IEC 27001:2014 la alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.

De igual manera, la RM – 004 – 2016 – PCM en su artículo 5, establece la creación del comité de gestión de seguridad de la información para dar cumplimiento al requisito 5.3 de la NTP ISO/IEC 27001:2014. Este comité de gestión de seguridad de la información, estará conformado por:

1. El director
2. El administrador
3. El responsable de informática
4. El responsable de asesoría jurídica
5. El oficial de seguridad de la información

A continuación, se describirán los roles y responsabilidades de cada uno:

- **El director**
  - ✓ Aprobar la política de seguridad de la información y comunicarla a todos los trabajadores de la entidad.
  - ✓ Definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.
  - ✓ Promover una cultura de seguridad de la información en la entidad.
- **El administrador**
  - ✓ Proponer al director la política de seguridad de la información para la entidad.

- ✓ Hacer cumplir la política de seguridad de la información dentro de la entidad.
- ✓ Revisar la política de seguridad de la información en intervalos planificados o cuando se produzcan cambios significativos en la normatividad de seguridad.
- ✓ Controlar el avance de seguridad de la información dentro de la DRTPE.

El responsable de informática

- ✓ Garantiza la disponibilidad y operatividad de los SI, de los equipos informáticos de la entidad.
- ✓ Establecer los mecanismos adecuados para la gestión y administración de riesgos, seguridad de la información, velar por la capacitación del personal de la entidad en lo referente a estos temas.
- ✓ Informar al administrador y director sobre los aspectos relacionados con el SGSI.
- ✓ Asegurar la existencia de metodologías para el tratamiento de riesgos y oportunidades, políticas de SI, así como la existencia de los documentos exigidos por la NTP – ISO/IEC 27001:2014.
- ✓ Asegurar el cumplimiento de las políticas y requerimientos de seguridad establecidos para la adquisición, diseño, desarrollo, operación, administración y mantenimiento de infraestructura tecnológica de la entidad.
- ✓ Asignar las funciones, roles y responsabilidades de seguridad, a los trabajadores a su cargo para la operación y administración de la infraestructura tecnológica de la entidad.

El responsable de asesoría jurídica

- ✓ Conocer e interpretar las leyes y normatividad vigente relacionada con la seguridad de la información bajo el contexto de la entidad.
- ✓ Evaluar el cumplimiento de las leyes y normatividad vigente en temas de seguridad de la información de la entidad.

- ✓ Mantener actualizado un archivo de normas legas relacionadas con la seguridad de la información.

- **El oficial de seguridad de la información**
  - ✓ Diseñar y coordinar la implementación de las políticas, normas y procedimientos de SI, con la participación activa de las dependencias de la entidad.
  - ✓ Identificar los riesgos a los que se encuentran expuestos los activos de información de la DRTPE.
  - ✓ Definir los controles asociados al SGSI y evaluarlos.
  - ✓ Definir los controles asociados al SGSI y evaluarlos.
  - ✓ Desarrollar charlas de capacitación y concientización en temas de seguridad de información para el personal de la entidad.
  - ✓ Atender auditorías internas y externas de aspectos asociados a la seguridad de la información.
  - ✓ Reportar al responsable de informática los incidentes de SI, los resultados de las auditorías, la revisión y supervisión del SGSI.

- **Política de seguridad de la información**

La política de seguridad de información está formada por un conjunto de principios que la organización debe seguir para asegurar la confiabilidad de sus sistemas informáticos. Por si misma, no constituye una garantía para la seguridad de información, se convertirá en una cuando responda a los interesas y necesidades de la empresa. (Justino Salinas, Diseño de un Sistema de Gestión de Seguridad de la Información para una empresa inmoviliaria alineado a la norma ISO/IEC 27001: 2013, 2015)

En este apartado, se definió la política de seguridad de la información de la organización (acorde al requisito 5.2 de la NTP – ISO/IEC 27001:2014).

La política de seguridad deberá ser aprobada por la alta dirección y revisada anualmente, dado que, puede surgir cambios organizacionales relevantes, como el despido y contratación de nuevo personal, cambio en la infraestructura tecnológica de la organización, el desarrollo de nuevos servicios, etc.

Una vez aprobada la política de seguridad, la institución comunicará esta política a todos los trabajadores de la organización en él. La política de seguridad de información se encuentra en el **ANEXO D**.

- **Alcance del SGSI**

En este apartado se define el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) para la organización.

Ilustración 3: Alcance del Sistema de Gestión de Seguridad de la Información

1. **Propósito, alcance y usuarios**
   El propósito de este documento es definir claramente cuáles son los límites del Sistema de Gestión de Seguridad de la Información (SGSI) de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco y es aplicable a toda la documentación perteneciente al SGSI.
   Los únicos usuarios autorizados a este documento son los miembros del comité de seguridad de la información y el personal autorizado del área de dirección y área administrativa de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco.

2. **Alcance del SGSI**
   El alcance del Sistema de Gestión de Seguridad de la Información aplica solo para los procesos de gestión de activos de información y gestión de riesgos de seguridad de la información, sub procesos de la gestión integral de la seguridad de la información y relativos a la planeación del SGSI.

Fuente: Adaptado de *"Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001 para la Dirección*

- **Objetivos del SGSI**

Estas políticas se desarrollaron para que se establezcan los bases en cuanto a la administración de la información de la organización, y que con ella se pueda lograr

garantizar la seguridad de los sistemas y procesos al igual que se pueda mantener la integridad de la información que manejan, como también lograr reducir el impacto de las vulnerabilidades e incidentes de seguridad.

Los objetivos del SGSI se muestran en la siguiente ilustración:

Ilustración 4: Objetivos de Sistema de Gestión de Seguridad de la Información

- Asegurar la confidencialidad de la información almacenados en los sistemas de información, del personal de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco.
- Asegurar la confidencialidad, integridad y disponibilidad de la información sensible de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco.
- Garantizar que nuestras operaciones, procesos actuales y futuros cumplan con la legislación y normatividad vigente en materia de seguridad de la información.
- Reducir los riesgos de seguridad de la información a un nivel aceptable para la DRTPE.
- Difundir la política de seguridad a través de cada uno de los responsables del área.
- Evaluar la efectividad del SGSI y llevar a cabo la mejora continua.

Fuente: *Adaptado de "Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001 para la Dirección de Salud Virgen de Cocharcas – Chicheros" (tesis), Escalante Coronel, Diego, 2019, p.37.*

Fase III: Diseño del Sistema de Gestión de Seguridad de la Información

En esta fase se llevó a cabo las actividades para tratar los riesgos y asegurar que el diseño del SGSI alcance los objetivos: evaluar los riesgos de seguridad de la información de la organización y elaborar la lista de controles de seguridad para mitigar los riesgos identificados.

- **Evaluación de riesgos**

De acuerdo a la metodología de análisis y gestión adoptada (MAGERIT); se definió la siguiente clasificación de activos:

Tabla 5: Clasificación de los activos de información

TIPO DE ACTIVO	DESCRIPCIÓN
Dato / Información	Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información o será transferido de un lugar a otro por medios de transmisión de datos.
Servicios	Función que satisface una necesidad de los usuarios (del servicio).
Aplicaciones informáticas / Software	Se refiere a las tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la presentación de los servicios.
Equipamiento informático (Hardware)	Dícese de los medios materiales, físicos destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o transmisión de datos.
Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
Soporte de información	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.
Equipamiento auxiliar	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con los datos.
Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones.
Personal	Personas relacionadas con los sistemas de información.

Nota. Fuente*:* ***Fuente especificada no válida.***

Para identificar los activos de información de la organización se utilizó el formato del **ANEXO E**. Cuestionario para identificar los activos de la organización. En el **ANEXO F** se muestra el inventario de activos obtenido con el cuestionario del anexo anterior.

- **Valoración de activos**

Para valorar los activos de información se consideró dos aspectos: el legal y la imagen, que pueden afectar a los activos en sus dimensiones de confidencialidad, integridad y disponibilidad.

El criterio que se siguió para valorar los activos de información se muestra en la **tabla 6**.

Tabla 6: Criterio para la valoración de activos

ASPECTOS	CRITERIOS DE CALIFICACIÓN	VALORACIÓN
[L] **Legal** Incumplimiento de leyes y normas	Probablemente cause un incumplimiento excepcionalmente grave de ley o regulación.	10
	Probablemente cause un incumplimiento grave de ley o regulación.	9
	Probablemente sea causa de incumplimiento de una ley o regulación.	6 – 8
	Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación.	3 – 5
	Pudiera causar el incumplimiento leve o técnico de una ley o regulación.	1 – 2
[IMG] **Imagen** Afecta a la imagen de la DRTPE	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones con otras organizaciones.	10
	Probablemente causaría una publicidad negativa generalizada por afectar	9

	gravemente a las relaciones con otras organizaciones.	
	Probablemente causaría una publicidad negativa y afecte las relaciones con otras organizaciones.	6 – 8
	Probablemente afecte negativamente a las relaciones internas de la organización.	3 – 5
	Pudiera causar una pérdida menor de la confianza dentro de la organización.	1 – 2
Nota. Fuente: *Adaptado de "Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001 para la Dirección de Salud Virgen de Cocharcas – Chicheros" (tesis), Escalante Coronel, Diego, 2019, p.43.*		

De igual forma, se estableció preguntas para determinar la criticidad del activo de información. Estas preguntas se muestran en la **tabla 7**.

Tabla 7: Preguntas para determinar la criticidad de un activo

PARÁMETRO	ASPECTO	PREGUNTA
[C] Confidencialidad	Legal	¿Si el activo o la información que se gestiona a través de él es divulgado sin autorización puede afectar el cumplimiento de leyes o normas impartidas por entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él es divulgado sin autorización puede afectar la imagen de la entidad?
[I] Integridad	Legal	¿Si el activo o la información que se gestiona a través de él es alterado sin autorización puede generar sanciones de entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él es alterado sin autorización puede afectar la imagen de la entidad?

[D] Disponibilidad	Legal	¿Si el activo o la información que se gestiona a través de él no está disponible pueden generar sanciones legales de entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él no está disponible puede afectar la imagen de la entidad?

Nota. Fuente: *Adaptado de "Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001*

Por último, para determinar el nivel de criticidad del activo valorado, se usó el criterio de la **tabla 8**. De esta manera se determinó la importancia de los activos de información dentro del proceso: gestión de la infraestructura tecnológica.

Tabla 8: Niveles de criticidad de los activos de información

CRITERIO DE EVALUACIÓN	VALOR	NIVEL
El activo de información compromete un nivel alto de integridad y/o confidencialidad y/o disponibilidad de la información.	$7 < VF \leq 10$	Alto
El activo de información compromete un nivel medio de integridad y/o confidencialidad y/o disponibilidad de la información.	$4 < VF \leq 7$	Medio
El activo de información compromete un nivel bajo de integridad y/o confidencialidad y/o disponibilidad de la información.	$0 < VF \leq 4$	Bajo

Nota. Fuente: *Adaptado de "Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001 para la Dirección de Salud Virgen de Cocharcas – Chicheros" (tesis), Escalante Coronel, Diego, 2019, p.45.*

En el **ANEXO G** se encuentra el resultado de la valoración de activos y su nivel de criticidad. De esta valoración se puede decir que: El valor de la columna VFC (Valor Final de Confidencialidad), corresponde al valor promedio de los aspectos legal e imagen, que afectan a la seguridad del activo en su dimensión de confidencialidad. Este mismo criterio se siguió para obtener los valores de VFI (Valor Final de

Integridad) y VFD (Valor Final de Disponibilidad) cada uno dentro de la dimensión que le corresponde.

El valor VF (Valor Final del activo de información), es el valor promedio de VFC, VFI y VFD.

Al terminar la valoración de los activos de información, se seleccionaron aquellos con un nivel de criticidad **alto** y **medio**.

- **Identificación y valoración de amenazas**

En esta etapa, se identifican las amenazas que afectan a los activos de información, la lista de amenazas elaborada se encuentra en el ANEXO G.

Para determinar la probabilidad de que estas se materialicen se estableció el criterio mostrado en la **tabla 9**.

Tabla 9: Probabilidad de ocurrencia de amenazas

CRITERIO	VALOR
Prácticamente segura	5
Probable	4
Posible	3
Improbable	2
Muy raro	1

Nota. Fuente: *Elaboración propia*

En el **ANEXO H** de este documento se encuentra el catálogo de amenazas que pueden afectar a cada tipo de activo y la(as) dimensiones en las que pueden ser afectados.

El **ANEXO I** de este documento contiene la tabla general de identificación de amenazas: la relación de activos con un nivel de criticidad alto y medio, sus amenazas identificadas y la probabilidad de materialización de esas amenazas.

Como no todas las amenazas afectan a todos los activos, sino que hay una relación entre el tipo de activo y lo que le podría ocurrir, se clasificó las amenazas por activo de información.

Al final se valoró la degradación de los activos bajo el criterio de la **tabla 10**.

Tabla 10: Criterio para valorar la degradación de un activo

CRITERIO	VALOR	
Muy alto	90%	100%
Alto	70%	80%
Medio	40%	60%
Bajo	20%	30%
Despreciable	0%	10%

Nota. Fuente: *Elaboración propia*

Para el presente proyecto se evaluó la degradación en 3 activos que están en un nivel de criticidad alto y medio, estos activos sufren un deterioro gradual con el tiempo: Equipo medio (Sistema de cámaras de seguridad – DVR), Informática personal (PCs y laptops) y dispositivos de almacenamiento externo.

El **ANEXO J** muestra los activos seleccionados, la probabilidad de materialización de la amenaza y la degradación en cada uno de sus dimensiones (confidencialidad, integridad y disponibilidad)

- **Cálculo del impacto**

En este ítem, se calculó el impacto que viene dado en función al valor del activo y la degradación que produciría la amenaza en caso de materializarse. Para ello se estableció el criterio y valoración en la **tabla 11** y la **tabla 12**.

Tabla 11: Criterios para calcular el impacto en un activo

VALOR DEL IMPACTO			IMPACTO		
VALOR		CRITERIO	VALOR		CRITERIO
10		Muy alto	9	10	Desastroso
7	9	Alto	7	8	Mayor

4	6	Medio	4	6	Moderado
1	3	Bajo	2	3	Menor
0		Despreciable	0	1	Insignificante

Nota. Fuente: Elaboración propia

Tabla 12: Matriz de evaluación del impacto

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

Nota. Fuente: *Elaboración Propia.*

Es conveniente decir que esta valoración fue calculada sin considerar las posibles medidas de seguridad que actualmente se está aplicando. De esta manera se trata de calcular el máximo riesgo para cada uno de los activos.

En la **tabla 13** se muestra el resultado del impacto en los activos de información.

Tabla 13: Resultado del impacto en los activos

ACTIVO	PROB	DIMENSIONES

		C	I	D
Equipo medio (Sistema de cámaras de seguridad - DVR)	3	7	7	8
Informática personal (PCs, laptops)	3	6	7	8
Dispositivos de almacenamiento externo	3	6	7	4

Nota. Fuente: Elaboración propia

En el **ANEXO K** se muestra el cuadro completo de la valoración del impacto en los activos: equipo medio, informática personal y dispositivos de almacenamiento externo.

- **Cálculo de riesgos**

El cálculo de riesgos está en función del impacto que se producirá sobre el activo en caso de materializarse y de la probabilidad de materialización de la amenaza.

Con base en esta comparación, se puede considerar la necesidad de tratamiento, además las decisiones que se deben tomar de acuerdo a los requisitos legales, reglamentos y otros.

La evaluación de riesgos también puede tener como resultado la decisión de no tratar el riesgo de ninguna manera diferente a los controles que puedan existir en la organización. Para el presente proyecto se elaboró el siguiente criterio para la evaluación del nivel de riesgo de los activos.

Tabla 14: Criterio para calcular el nivel de riesgo

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

Nota. Fuente: Elaboración Propia

Estos niveles se ven reflejados en la matriz:

Tabla 15: Matriz de evaluación de riesgos

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

Nota. Fuente: *Elaboración Propia*

En la **tabla 16** vemos el resultado de los riesgos en los activos.

Tabla 16: Resultado de los riesgos en los activos

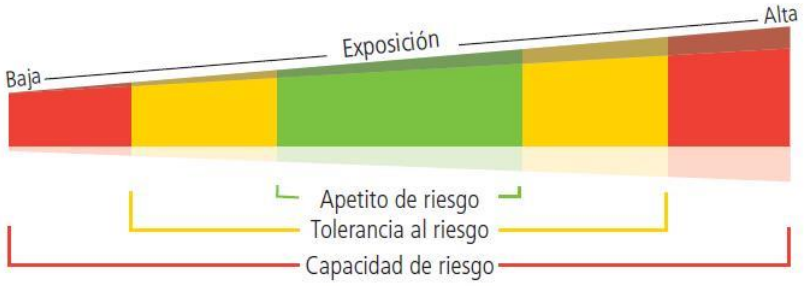
ACTIVO	**PROB**	**DIMENSIONES**		
		C	**I**	**D**
Equipo medio (Sistema de cámaras de seguridad - DVR)	3	21	21	24
Informática personal (PCs, laptops)	3	20	22	24
Dispositivos de almacenamiento externo	3	19	20	13

Nota. Fuente: Elaboración propia

En el **ANEXO K** se muestra el cuadrado completo de la valoración de riesgo para los activos equipo medio (Sistema de cámaras de seguridad – DVR), informática personal (PCs, laptops) y dispositivos de almacenamiento interno.

La organización, en la actualidad, no tiene establecido el apetito de riesgo, es decir que, no se tiene definido hasta que nivel de riesgo podría ser tomado como aceptable. Dado esta situación se propuso: Como se sabe la organización en la que se está desarrollando el proyecto, tiene una calificación de gran empresa, el apetito de riesgo que estaría dispuesta a aceptar serían los riesgos aceptables y tolerables, los riesgos intolerables deberían ser monitoreados y controlados constantemente. Para finalizar, no se puede aceptar bajo ninguna circunstancia los riesgos extremos, estos deberían ser monitoreados y controlados de inmediato.

Ilustración 5: Apetito de riesgo para el tratamiento de riesgos



Nota. Fuente: (Rodriguez, 2016)

- **Propietarios del riesgo**

En esta etapa se identificó al propietario del riesgo, este es el responsable de aprobar los riesgos excedentes y los planes de tratamiento de riesgos (para reducir los riesgos a un nivel aceptable). Para el presente proyecto se determinó que los únicos propietarios del riesgo son el área administrativa de la organización, conformada por la dirección y la oficina técnica administrativa.

- **Tratamiento de riesgos**

En concordancia con la naturaleza del riesgo, las opciones para tratarlos pueden ser: reducir, compartir o transferir, eliminar y aceptar el riesgo.

Tabla 17: Opciones de mitigación en el tratamiento de riesgos

TRATAMIENTO	DESCRIPCIÓN
Reducir	Se trata de implantar las medidas preventivas o correctivas necesarias con el fin de reducir la posibilidad de ocurrencia o el impacto de riesgo.
Transferir	Esta opción está relacionada con la contratación de algún tipo de seguro que compense las consecuencias económicas de una pérdida o deterioro de la información.
Eliminar	Si el riesgo es muy crítico, hasta el punto de que pueda poner en peligro la propia continuidad de la organización, ésta debe poner todos los medios para tratar de eliminarlo, de manera que haya una posibilidad cero de que la amenaza se llegue realmente a producir.
Aceptar	Cuando las acciones necesarias para eliminar un riesgo, tienen un coste demasiado alto – superior a las consecuencias previstas de la ocurrencia del incidente, conviene pensar en la posibilidad de convivir con el riesgo, y minimizar su impacto.

Nota. Fuente: Elaboración propia.

En el presente proyecto, con los valores y niveles de riesgo obtenidos, se estableció como máximo riesgo asumible los que están en un nivel tolerable; para todos los riesgos que tienen niveles intolerables o extremos se aplicaron los controles que ayudaron a reducir los riesgos producidos por las amenazas a un nivel aceptable en las dimensiones afectadas.

Se priorizó el tratamiento de los riesgos de nivel intolerable y extremo, a ellos se les aplicó todas las medidas de seguridad. De igual manera, es resaltable mencionar que los riesgos de nivel tolerable fueron monitoreados para evitar que su impacto y probabilidad crezcan con el tiempo.

Tabla 18: Plan de tratamiento de riesgos

IDENTIFICACIÓN DE RIESGOS		EVALUACIÓN DE RIESGOS			TRATAMIENTO DEL RIESGO					
		Nivel de riesgo								
Nombre del activo	**Amenaza**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Estrategia de respuesta**	**Plan de contingencia**	**Tipo de control**	**Cláusula del control ISO/IEC 27001**	**Control ISO/IEC 27001**	**Responsable**
[mid] Equipo medio (Sistema de cámaras de seguridad – DVR)	Fuego	-	-	Extremo	Reducir	Designar fondos a las metas designadas para el cuidado de las instalaciones físicas de la organización y adquisidores de equipos.	Correctivo	11. Seguridad física y ambiental	11.1.1	Director de la DRTPE/ Administrador de la DRTPE
	Avería de origen físico o lógico	-	-	Intolerable	Reducir	Contactar al proveedor del equipo tecnológico para un cambio o reparación según sea el caso.	Correctivo	11. Seguridad física y ambiental	11.2.2	Administrador de la DRTPE
	Corte de suministro eléctrico	-	-	Intolerable	Reducir	Realizar la adquisición y uso de un generador eléctrico en la organización	Preventivo	11. Seguridad física y ambiental	11.2.2	Administrador de la DRTPE
	Degradación de los soportes de	-	-	Extremo	Reducir	Renovar los dispositivos en un periodo determinado	Preventivo	11. Seguridad	11.2.4	Administrador de la DRTPE

	almacenamiento de la información					para evitar la degradación de datos necesarios e importantes		física y ambiental		
	Errores de los usuarios	Intolerable	Intolerable	Intolerable	Reducir	Considerar una sanción tomando en cuenta la gravedad, el impacto, si es deliberada o si existe repetición	Correctivo	7. Seguridad ligada a los recursos humanos	7.2.3	Administrador de la DRTPE
	Errores de configuración	-	Intolerable	-	Reducir	Elaborar el manual de configuración del sistema de información	Preventivo	12. Seguridad en la operativa	12.4.1 12.4.3	Director de la DRTPE / Administrador de la DRTPE
	Errores de mantenimiento / actualización de equipos (Hw)	-	Intolerable	-	Transferir	Elaborar un plan de mantenimiento del hardware junto al proveedor / administrador del equipo informático	Preventivo	11. Seguridad física y ambiental	11.2.4	Administrador de la DRTPE
	Robo	Extremo	-	Extremo	Reducir	Realizar la autenticación y monitorización de los visitantes, la identificación y revisión de los permisos del personal.	Preventivo	11. Seguridad física y ambiental	11.1.2	Dirección de la DRTPE
	Fuego	-	-	Extremo	Reducir	Designar fondos a las metas designadas	Correctivo	11. Seguridad	11.1.1	Director de la DRTPE/

						para el cuidado de las instalaciones físicas de la organización y adquisidores de equipos.		física y ambiental		Administrador de la DRTPE
	Avería de origen físico o lógico	-	-	Intolerable	Reducir	Contactar al proveedor del equipo tecnológico para un cambio o reparación según sea el caso.	Correctivo	11. Seguridad física y ambiental	11.2.2	Administrador de la DRTPE
	Corte de suministro eléctrico	-	-	Intolerable	Reducir	Realizar la adquisición y uso de un generador eléctrico en la organización	Preventivo	11. Seguridad física y ambiental	11.2.2	Administrador de la DRTPE
[pc] Informática personal (PCs, laptops)	Degradación de los soportes de almacenamiento de la información	-	-	Extremo	Reducir	Renovar los dispositivos en un periodo determinado para evitar la degradación de datos necesarios e importantes	Preventivo	11. Seguridad física y ambiental	11.2.4	Administrador de la DRTPE
	Errores de los usuarios	Intolerable	Intolerable	Intolerable	Reducir	Considerar una sanción tomando en cuenta la gravedad, el impacto, si es deliberada o si existe repetición	Correctivo	7. Seguridad ligada a los recursos humanos	7.2.3	Administrador de la DRTPE
	Difusión de software dañino	Tolerable	Extremo	Extremo	Reducir	Establecer un procedimiento de seguridad dirigido a los usuarios respecto	Preventivo	12. Seguridad en la operativa	12.2.1	Administrador de la DRTPE

						a la seguridad de la información y así evitar que abran archivos adjuntos sin asegurarse de que no sean maliciosos, no hagan clic en enlaces en correos electrónicos ni visiten sitios web que puedan cargar virus, troyanos, etc.				
	Alteración accidental de la información	-	Intolerable	-	Reducir	Realizar procedimientos de copias de seguridad para la protección de la información y considerar una sanción tomando en cuenta la gravedad, el impacto, si es deliberada o si existe repetición	Preventivo	8. Gestión de activos. 7. Seguridad ligada a los recursos humanos	8.2.3 7.2.3	Director de la DRTPE / Administrador de la DRTPE
	Fugas de información	Intolerable	-	-	Reducir	Asignar los permisos de acceso limitados solamente a la información necesaria para hacer un trabajo, tanto a nivel físico, como lógico y considerar una sanción tomando en	Preventivo	9. Control de accesos 7. Seguridad ligada a los recursos humanos	9.1.1 7.2.3	Directo de la DRTPE / Administrador de la DRTPE

						cuenta la gravedad, el impacto, si es deliberada o si existe repetición				
	Errores de mantenimiento / actualización de programas (SW)	-	Intolerable	Intolerable	Transferir	Elaborar un plan de actualización de las aplicaciones junto al área informática del GOREHCO	Preventivo	11. Seguridad física y ambiental	11.2.4	Administrador de la DRTPE
	Errores de mantenimiento / actualización de equipos (HW)	-	-	Intolerable	Transferir	Elaborar un plan de mantenimiento de los equipos informáticos junto al área de informática del GOREHCO	Preventivo	11. Seguridad física y ambiental	11.2.4	Administrador de la DRTPE
	Uso no previsto	Tolerable	Tolerable	Intolerable	Reducir	Documentar el uso apropiado de la información y equipos informáticos, describiendo los requisitos de seguridad de la información de los activos, etc. Y comunicar a los trabajadores para evitar su uso indebido.	Correctivo	8. Gestión de activos	8.1.3	Administrador de la DRTPE

	Acceso no autorizado	Intolerable	Intolerable	-	Reducir	Asignar la menor cantidad de privilegios posibles para llevar a cabo una tarea dentro de un sistema de información, y asignar una identificación y autenticación a cada trabajador.	Preventivo	9. Control de accesos	9.1.1 9.2.2	Administrador de la DRTPE
	Manipulación de programas	Intolerable	Intolerable	Intolerable	Reducir	Establecer una planificación para los cambios a realizar en equipos, sistemas software, etc., realizando al final un registro de lo que se hizo.	Preventivo	12. Seguridad en la operativa	12.1.2	Administrador de la DRTPE
	Robo	Extremo	-	Extremo	Reducir	Realizar la autenticación y monitorización de los visitantes, la identificación y revisión de los permisos del personal.	Preventivo	11. Seguridad física y ambiental	11.1.2	Dirección de la DRTPE
[dae] Dispositivos de almacenamiento externo	Fuego	-	-	Extremo	Reducir	Designar fondos a las metas designadas para el cuidado de las instalaciones físicas de la organización y adquisidores de equipos.	Correctivo	11. Seguridad física y ambiental	11.1.1	Director de la DRTPE/ Administrador de la DRTPE

	Degradación de los soportes de almacenamiento de la información	-	-	Extremo	Reducir	Renovar los dispositivos en un periodo determinado para evitar la degradación de datos necesarios e importantes	Preventivo	11. Seguridad física y ambiental	11.2.4	Administrador de la DRTPE
	Errores de los usuarios	Intolerable	Intolerable	Extremo	Reducir	Considerar una sanción tomando en cuenta la gravedad, el impacto, si es deliberada o si existe repetición	Correctivo	7. Seguridad ligada a los recursos humanos	7.2.3	Administrador de la DRTPE
	Difusión de software dañino	Tolerable	Extremo	Extremo	Reducir	Establecer un procedimiento de seguridad dirigido a los usuarios respecto a la seguridad de la información y así evitar que abran archivos adjuntos sin asegurarse de que no sean maliciosos, no hagan clic en enlaces en correos electrónicos ni visiten sitios web que puedan cargar virus, troyanos, etc.	Preventivo	12. Seguridad en la operativa	12.2.1	Administrador de la DRTPE
	Alteración accidental	-	Intolerable	-	Reducir	Realizar procedimientos de copias de seguridad	Preventivo	8. Gestión de activos.	8.2.3 7.2.3	Director de la DRTPE /

	de la información					para la protección de la información y considerar una sanción tomando en cuenta la gravedad, el impacto, si es deliberada o si existe repetición		7. Seguridad ligada a los recursos humanos		Administrador de la DRTPE
	Fugas de información	Intolerable	-	-	Reducir	Asignar los permisos de acceso limitados solamente a la información necesaria para hacer un trabajo, tanto a nivel físico, como lógico y considerar una sanción tomando en cuenta la gravedad, el impacto, si es deliberada o si existe repetición.	Preventivo	9. Control de accesos 7. Seguridad ligada a los recursos humanos	9.1.1 7.2.3	Directo de la DRTPE / Administrador de la DRTPE
	Pérdida de equipos	Intolerable	-	Extremo	Reducir	Establecer un control específico para gestionar el uso de estos soportes extraíbles y considerar una sanción tomando en cuenta la gravedad, el impacto, si es deliberada o si existe repetición.	Preventivo	7. Seguridad ligada a los recursos humanos	7.2.2 7.2.3	Administrador de la DRTPE

	Uso no previsto	Intolerable	Intolerable	Intolerable	Reducir	Documentar el uso apropiado de la información y equipos informáticos, describiendo los requisitos de seguridad de la información de los activos, etc. Y comunicar a los trabajadores para evitar su uso indebido.	Correctivo	8. Gestión de activos	8.1.3	Administrador de la DRTPE
	Acceso no autorizado	Intolerable	Intolerable	-	Reducir	Asignar la menor cantidad de privilegios posibles para llevar a cabo una tarea dentro de un sistema de información, y asignar una identificación y autenticación a cada trabajador.	Preventivo	9. Control de accesos	9.1.1 9.2.2	Administrador de la DRTPE
	Robo	Extremo	-	Extremo	Reducir	Realizar la autenticación y monitorización de los visitantes, la identificación y revisión de los permisos del personal.	Preventivo	11. Seguridad física y ambiental	11.1.2	Dirección de la DRTPE

- **Identificación de controles según la NTP – ISO/IEC 2001**

La selección de controles depende de las decisiones de la empresa, basadas en el criterio de aceptación del riesgo, las opciones de tratamiento del riesgo, el enfoque general para la gestión del riesgo en la empresa, así como las regulaciones y legislaciones nacionales e internacionales. (Giménez Albacete, 2014)

Es así que, luego de realizar la evaluación de los riesgos, únicamente se tomarán aquellos que se encuentren fuera del apetito, es decir, aquellos que se consideran como riesgo aceptable, a los que se les asignará uno o más controles para su tratamiento. Esto, en conjunto, constituye el plan de tratamiento de riesgos.

En el **ANEXO L**, se presenta una explicación de cada cláusula de los controles que según la ISO 270001:2013 se pueden implementar dentro de cualquier organización. Algunos de los controles en esta norma serán considerados como principios para la gestión de seguridad de la información y se aplicarán a los riesgos identificados en la organización.

- **Declaración de aplicabilidad**

Después de realizar la identificación de los controles para todos los riesgos con un nivel intolerante y extremo para la organización, se procederá a detallar cuales se aplican o no al contexto de la dirección. El documento en el que se especifican los controles que aplican dentro del sistema de gestión, está denominado como declaración de aplicabilidad.

La declaración de aplicabilidad contempla la siguiente información:

- **Cláusula:** Está dado por el título de los dominios de la ISO/IEC 27001:2013.
- **Sección:** Contiene el identificador de sección de los controles propuestos.
- **Objetivos de control:** Es el nombre del control propuesto por la norma y hace referencia a un tema en específico al que un riesgo puede estar relacionado.

- **Estado:** Menciona el estado de control dentro de la DRTPE, es decir si está aplicado se va a aplicar o no.
- **Justificación:** Es dado por la justificación de aplicabilidad o no aplicabilidad del control mencionado.

Tabla 19: Declaración de aplicabilidad

ISO 27001: 2013 CONTROLES DE SEGURIDAD			¿ES APLICABLE A LA ORGANIZACIÓN?	JUSTIFICACIÓN DE APLICABILIDAD
Cláusula	**Sección**	**Objetivo de control**	**Estado**	
5. Políticas de seguridad	5.1	Directrices de la dirección en seguridad de la información		
	5.1.1	Conjunto de políticas para la seguridad de la información	Aplica	Es necesario el establecimiento de una política de seguridad de información, este servirá de base para iniciar la gestión de seguridad de la información.
	5.1.2	Revisión de las políticas para la seguridad de la información	Aplica	En la organización no hay ninguna política de seguridad de la información actualizada y aprobada. Es necesario que las políticas de seguridad de información sean revisadas antes de ser aprobadas.
6. Aspectos organizativos de la seguridad de la información	6.1	Organización interna		
	6.1.1	Asignación de responsabilidades para la seguridad de la información	Aplica	No hay roles de seguridad de información propiamente dichas, el que asumen esa responsabilidad es el especialista en logística. Por ello es necesario definir roles de seguridad de información dentro de la organización, para evitar sobrecarga de actividades
	6.1.2	Segregación de tareas	Aplica	Actualmente, el rol del especialista en logística está sobrecargado de responsabilidades. Es necesario segregar funciones entre los roles de la organización, de esta manera evitar la sobrecarga de tareas y la ineficiente ejecución de los procesos.
	6.1.3	Contacto con las autoridades	No aplica	No hay una entidad que exija a la organización a implementar un SGSI
	6.1.4	Contacto con grupos de interés especial		No hay una entidad que exija a la organización a implementar un SGSI

	6.1.5	Seguridad de la información en la gestión de proyectos	Aplica	En la organización, no existe una metodología de riesgos definida para poder realizar el análisis de riesgos de seguridad en los proyectos. Es necesario incluir a la seguridad de información e identificar controles necesarios en la gestión de proyectos.
	6.2	Dispositivos para movilidad de trabajo		
	6.2.1	Políticas de uso de dispositivos para movilidad	Aplica	No hay documentación actualizada sobre políticas del uso de dispositivos móviles.
	6.2.6	Teletrabajo	No aplica	En la organización el trabajo a distancia o teletrabajo no es usado. El trabajo se realiza dentro de las oficinas de la organización.
7. Seguridad ligada a los recursos humanos	7.1	Antes de la contratación		
	7.1.1	Investigación de antecedentes	Aplica	En el área de capital humano, y como parte del proceso de selección y reclutamiento se revisan los antecedentes penales y policiales de cada uno de los candidatos a un puesto laboral. Sin embargo, es necesario realizar una búsqueda o investigación más exhaustiva si el puesto laboral tiene un mayor rango.
	7.1.2	Términos y condiciones de contratación	Aplica	Como parte de las cláusulas del contrato firmado por los colaboradores se establece la confidencialidad hacia la organización; sin embargo, no se establece la confidencialidad respectiva a los datos personales del trabajador, es por ello que es necesario incluir ciertas cláusulas que cumplan con la ley de protección de datos personales.
	7.2	Durante la contratación		
	7.2.1	Responsabilidades de gestión	Aplica	Es necesario hacer que los trabajadores apliquen la seguridad con relación a las políticas y procedimientos de la organización.
	7.2.2	Concientización, educación y capacitación en seguridad de la información	Aplica	En la actualidad, no se toma en cuanta algunos aspectos de seguridad de información en la cultura organizacional, es por ello que es necesario que todos los trabajadores de la organización deben recibir una adecuada concientización, entrenamiento y

				actualizaciones regulares en los procesos y políticas organizacionales, como acciones relevantes de su función laboral.
	7.2.3	Proceso disciplinario	Aplica	Es necesario que haya sanciones para aquellos trabajadores que cometan una violación a la seguridad o que haya incumplido con la política aprobada.
	7.3	Cese o cambio de puesto		
	7.3.1	Cese o cambio de puesto de trabajo	Aplica	Al finalizar el contrato del trabajador, las responsabilidades de seguridad de la información y funciones deben seguir vigentes después del término o cambio de empleo. De igual forma, estás responsabilidades deben ser definidas y comunicadas al trabajador o contratista.
8. Gestión de activos	8.1	Responsabilidad sobre los activos		
	8.1.1	Inventario de activos	Aplica	Es necesario realizar una lista de activos de información de la organización, con el fin de hacer seguimiento y monitorearlos. Como parte del diseño del SGSI se ha realizado un inventario de activos de información en el proceso de alcance.
	8.1.2	Propiedad de los activos	Aplica	Es necesario realizar una lista de activos de información de la organización, con el fin de hacer seguimiento y monitorearlos. Como parte del diseño del SGSI se ha realizado un inventario de activos de información en el proceso de alcance, también se especifican las propiedades de cada uno.
	8.1.3	Uso aceptable de los activos	Aplica	Si bien el reglamento interno de trabajo se menciona acerca del adecuado uso de los activos de la empresa, no ha sido difundido correctamente
	8.1.4	Devolución de activos	Aplica	Se debe definir en un procedimiento, las actividades que se realizan para la devolución de los activos de la organización que están en posesión de algún colaborador cuando termine su contrato.
	8.2	Clasificación de los activos		

	8.2.1	Directrices de clasificación	Aplica	De acuerdo al inventario de activos de información, se debe clasificar en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.
	8.2.2	Etiquetado y manipulado de la información	Aplica	Actualmente no se ha definido un procedimiento para etiquetar o clasificar la información. De igual manera, se debe definir un esquema de clasificación de activos para la organización.
	8.2.3	Manipulación de los activos	Aplica	Actualmente no se ha definido un procedimiento para etiquetar o clasificar la información. De igual manera, se debe definir un esquema de clasificación de activos para la organización.
	8.3	Manejo de los soportes de almacenamiento		
	8.3.1	Gestión de soportes extraíbles	Aplica	El uso de laptop para realizar charlas, seminarios, talleres, etc., fuera de la sede central requiere que este tipo de activos sean protegidos.
	8.3.2	Eliminación de soportes	Aplica	El uso de laptop para realizar charlas, seminarios, talleres, etc., fuera de la sede central requiere que este tipo de activos sean protegidos.
	8.3.3	Soportes físicos en transito	Aplica	El uso de laptop para realizar charlas, seminarios, talleres, etc., fuera de la sede central requiere que este tipo de activos sean protegidos.
9. Control de accesos	9.1	Requisitos del negocio para el control de accesos		
	9.1.1	Política de control de accesos	Aplica	No hay políticas actualizadas con respecto al control de acceso.
	9.1.2	Control de acceso a las redes y servicios asociados	Aplica	No hay políticas actualizadas con respecto al uso de servicios red.
	9.2	Gestión de acceso de usuario		
	9.2.1	Gestión de altas/bajas en el registro de usuarios	Aplica	De acuerdo al análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de acceso actualizado, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad.

	9.2.2	Gestión de los derechos de acceso asignados a los usuarios	Aplica	No hay un procedimiento en el que se abastezcan de usuarios de acceso.
	9.2.3	Gestión de los derechos de acceso con privilegios especiales	Aplica	Es necesario realizar un procedimiento documentado, en el cual se indique que cada director de sub dirección, debe solicitar permisos adecuados para cada colaborador que se le autorice.
	9.2.4	Gestión de información confidencial de autenticación de usuarios	Aplica	Es necesario establecer lineamientos para la adecuada gestión de autenticación de usuarios.
	9.2.5	Revisión de los derechos de acceso de los usuarios	Aplica	De acuerdo al análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de acceso actualizada, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad.
	9.2.6	Retirada o adaptación de los derechos de acceso	Aplica	De acuerdo al análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de acceso actualizada, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad.
	9.3	Responsabilidades del usuario		
	9.3.1	Uso de información confidencial para la autenticación	Aplica	No hay cultura de seguridad en los trabajadores de la organización, esto hace que las vulnerabilidades se vean expuestas. Es por ello que es necesario que cada trabajador sea responsable de su usuario y contraseña.
	9.4	Control de acceso a sistemas y aplicaciones		
	9.4.1	Restricción del acceso a la información	Aplica	La ausencia de una matriz de perfiles de acceso actualizada dificulta la ejecución de algunos procesos, por ello es necesario establecer controles de acceso.
	9.4.2	Procedimientos seguros de inicio de sesión	Aplica	Es necesario establecer lineamientos para establecer una conexión segura al acceder a los sistemas y aplicaciones.
	9.4.3	Gestión de contraseñas de usuario	Aplica	Debe actualizarse el documento que contenga las políticas de uso de contraseñas, de igual manera, debe documentarse las actividades necesarias para la creación de contraseñas a nuevos

				usuarios, adicionalmente se debe solicitar a los usuarios que firmen un compromiso para no compartir su contraseña con otros usuarios.
	9.4.4	Uso de herramientas de administración de sistemas	Aplica	Es necesario realizar un procedimiento documentado, en el cual se indique que cada director de sub dirección, debe solicitar los permisos adecuados para cada trabajador bajo su supervisión.
	9.4.5	Control de acceso al código fuente de los programas	Aplica	De acuerdo al análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de acceso actualizada, lo que ha ocasionado que la información se exponga a varios riesgos de seguridad.
10. Cifrado	10.1	Controles criptográficos		
	10.1.1	Política de uso de los controles criptográficos	No aplica	En el alcance del SGSI para la organización no se incluye esta cláusula.
	10.1.2	Gestión de claves	No aplica	En el alcance del SGSI para la organización no se incluye esta cláusula.
11. Seguridad física y ambiental	11.1	Áreas seguras		
	11.1.1	Perímetro de seguridad física	No aplica	Existe un personal designado al resguardo de la seguridad de la infraestructura de la organización.
	11.1.2	Controles físicos de entrada	No aplica	Existen controles y un personal designado al resguardo de la seguridad de la organización.
	11.1.3	Seguridad de oficinas. Despachos y recursos	Aplica	Se deben establecer controles y políticas para las oficinas.
	11.1.4	Protección contra las amenazas externas y ambientales	Aplica	Establecer políticas para la protección física ante desastres naturales y ambientales.
	11.1.5	El trabajo en áreas seguras	Aplica	Se deben establecer controles y políticas en los espacios de trabajo en áreas seguras.
	11.1.6	Áreas de acceso público, carga y descarga	No aplica	Existen un personal designado al resguardo de la seguridad de la infraestructura de la organización.

	11.2	Seguridad de los equipos		
	11.2.1	Emplazamiento y protección de equipos	No aplica	Existen metas en el presupuesto para mantener una infraestructura segura.
	11.2.2	Instalaciones de suministro	No aplica	Existen acuerdos y contratos con suministradores.
	11.2.3	Seguridad del cableado	Aplica	Es necesario establecer lineamientos para mantener un cableado seguro.
	11.2.4	Mantenimiento de los equipos	Aplica	Es necesario establecer lineamientos para realizar regularmente el mantenimiento de los equipos informáticos.
	11.2.5	Salida de activos fuera de las dependencias de la empresa	No aplica	Existen políticas que especifican que los equipos de información no deben ser retirados fuera de la organización sin previa autorización.
	11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	No aplica	Existen políticas que especifican que los equipos, información y otras aplicaciones no deben utilizar candados de seguridad.
	11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	No aplica	Existen políticas que especifican que los equipos, información y otras aplicaciones no deben utilizar candados de seguridad.
	11.2.8	Equipo informático de usuario desatendido	No aplica	Existen políticas que especifican que los equipos, información y otras aplicaciones no deben utilizar candados de seguridad.
	11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	Aplica	Es necesario establecer lineamientos para mantener un escritorio limpio y pantalla limpia.
12. Seguridad operativa	12.1	Responsabilidades y procedimientos de operación		
	12.1.1	Documentación de procedimientos de operación	Aplica	Establecer lineamientos para garantizar que la información esté disponible. Realizar regularmente el mantenimiento de los equipos informáticos.
	12.1.2	Gestión de cambios	No aplica	No aplica al alcance del SGSI

	12.1.3	Gestión de capacidades	Aplica	Establecer lineamientos para garantizar que la información esté disponible. Realizar regularmente el mantenimiento de los equipos informáticos.
	12.1.4	Separación de entornos de desarrollo, prueba y producción	No aplica	No aplica al alcance del SGSI
	12.2	Protección contra código malicioso		
	12.2.1	Controles contra el código malicioso	Aplica	Establecer políticas de seguridad con respecto al uso del correo electrónico, respecto a las páginas de internet de contenido dudoso.
	12.3	Copias de seguridad		
	12.3.1	Copias de seguridad de la información	Aplica	Establecer políticas de respaldo de información, realizar backups.
	12.4	Registro de actividad y supervisión		
	12.4.1	Registro y gestión de eventos de actividad	No aplica	No aplica al alcance del SGSI
	12.4.2	Protección de los registros de información	No aplica	No aplica al alcance del SGSI
	12.4.3	Registros de actividad del administrador y operador del sistema	No aplica	No aplica al alcance del SGSI
	12.4.4	Sincronización de relojes	No aplica	No aplica al alcance del SGSI
	12.5	Control de software en explotación		
	12.5.1	Instalación del software en sistemas en producción	No aplica	No aplica al alcance del SGSI
	12.6	Gestión de la vulnerabilidad técnica		
	12.6.1	Gestión de las vulnerabilidades técnicas	Aplica	Establecer políticas de seguridad para cumplir con la ley de protección de datos personales.
	12.6.2	Restricciones en la instalación de software	No aplica	Existen políticas de restricción de software para personal no autorizado, solo el usuario administrador puede instalar aplicaciones al equipo.

	12.7	Consideraciones de las auditorías de los sistemas de información		
	12.7.1	Controles de auditoría de los sistemas de información	No aplica	No aplica al alcance del SGSI
13. Seguridad en las telecomunicaciones	13.1	Gestión de la seguridad en las redes		
	13.1.1	Controles de red	Aplica	Se debe establecer políticas y segregar grupos de servicios en las redes, para evitar la congestión de las mismas.
	13.1.2	Mecanismos de seguridad asociados a servicios en red	Aplica	Se debe establecer políticas y segregar grupos de servicios en las redes, para evitar la congestión de las mismas.
	13.1.3	Segregación de redes	Aplica	Se debe establecer políticas y segregar grupos de servicios en las redes, para evitar la congestión de las mismas.
	13.2	Intercambio de información con partes externas		
	13.2.1	Políticas y procedimientos de intercambio de información	Aplica	Es necesario establecer políticas sobre la transferencia de información, así como monitorear y hacer seguimiento a las operaciones del sistema.
	13.2.2	Acuerdos de intercambio	Aplica	Es necesario establecer políticas sobre la transferencia de información, así como monitorear y hacer seguimiento a las operaciones del sistema.
	13.2.3	Mensajería electrónica	Aplica	Es necesario establecer políticas sobre la transferencia de información, así como monitorear y hacer seguimiento a las operaciones del sistema y servidor de correos.
	13.2.4	Acuerdos de confidencialidad y secreto	No aplica	Existen políticas de confidencialidad de información en la organización.
14. Adquisición. Desarrollo y mantenimiento de	14.1	Requisitos de seguridad de los sistemas de información		
	14.1.1	Análisis y especificación de los requisitos de seguridad	Aplica	El sistema debe contar con especificaciones técnicas de seguridad para evitar la intrusión del malware.

los sistemas de información	14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	Aplica	El sistema debe contar con especificaciones técnicas de seguridad para evitar la intrusión del malware.
	14.1.3	Protección de las transacciones por redes telemáticas	No aplica	En el alcance del SGSI para la organización no se ha incluido el desarrollo de sistemas.
	14.2	Seguridad en los procesos de desarrollo y soporte		
	14.2.1	Política de desarrollo seguro de software	No aplica	En el alcance del SGSI para la organización no se ha incluido el desarrollo de sistemas.
	14.2.2	Procedimientos de control de cambios en los sistemas	No aplica	En el alcance del SGSI para la organización no se ha incluido el desarrollo de sistemas.
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	No aplica	En el alcance del SGSI para la organización no se ha incluido el desarrollo de sistemas.
	14.2.4	Restricciones a los cambios en los paquetes de software	No aplica	En el alcance del SGSI para la organización no se ha incluido el desarrollo de sistemas.
	14.2.5	Uso de principios de ingeniería en protección de sistemas	No aplica	En el alcance del SGSI para la organización no se ha incluido el desarrollo de sistemas.
	14.2.6	Seguridad en entornos de desarrollo	No aplica	En el alcance del SGSI para la organización no se ha incluido el desarrollo de sistemas.
	14.2.7	Externalización del desarrollo de software	No aplica	En el alcance del SGSI para la organización no se ha incluido el desarrollo de sistemas.
	14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	No aplica	En el alcance del SGSI para la organización no se ha incluido el desarrollo de sistemas.

	14.2.9	Pruebas de aceptación	No aplica	En el alcance del SGSI para la organización no se ha incluido el desarrollo de sistemas.
	14.3	Datos de prueba		
	14.3.1	Protección de los usuarios utilizados en pruebas	No aplica	En el alcance del SGSI para la organización no se ha incluido el desarrollo de sistemas.
15. Relaciones con suministradores	15.1	Seguridad de la información en las relaciones con suministradores		
	15.1.1	Política de seguridad de la información para suministradores	Aplica	Establecer condiciones en caso de incumplimiento del servicio.
	15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	Aplica	Establecer condiciones en caso de incumplimiento del servicio.
	15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	No aplica	No se ha definido en el alcance del SGSI
	15.2	Gestión de la prestación del servicio por suministradores		
	15.2.1	Supervisión y revisión de los servicios prestados por terceros	Aplica	Establecer condiciones en caso de incumplimiento del servicio.
	15.2.2	Gestión de cambios en los servicios prestados por terceros	Aplica	Establecer condiciones en caso de incumplimiento del servicio.
16. Gestión de incidentes en la seguridad de la información	16.1	Gestión de incidentes de seguridad de la información y mejoras		
	16.1.1	Responsabilidades y procedimientos	Aplica	Se debe mantener evidencia de cada incidencia de seguridad, para generar un historial de eventos o incidentes, que luego se tomará como retroalimentación. De igual manera, se debe mantener los procesos actualizados.

	16.1.2	Notificación de los eventos de seguridad de la información	Aplica	Se debe mantener evidencia de cada incidencia de seguridad, para generar un historial de eventos o incidentes, que luego se tomará como retroalimentación. De igual manera, se debe mantener los procesos actualizados.
	16.1.3	Notificación de puntos débiles de la seguridad	Aplica	Se debe mantener evidencia de cada incidencia de seguridad, para generar un historial de eventos o incidentes, que luego se tomará como retroalimentación. De igual manera, se debe mantener los procesos actualizados.
	16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	Aplica	Se debe mantener evidencia de cada incidencia de seguridad, para generar un historial de eventos o incidentes, que luego se tomará como retroalimentación. De igual manera, se debe mantener los procesos actualizados.
	16.1.5	Respuesta a los incidentes de seguridad	Aplica	Se debe mantener evidencia de cada incidencia de seguridad, para generar un historial de eventos o incidentes, que luego se tomará como retroalimentación. De igual manera, se debe mantener los procesos actualizados.
	16.1.6	Aprendizaje de los incidentes de seguridad de la información	Aplica	Se debe mantener evidencia de cada incidencia de seguridad, para generar un historial de eventos o incidentes, que luego se tomará como retroalimentación. De igual manera, se debe mantener los procesos actualizados.
	16.1.7	Recopilación de evidencias	Aplica	Se debe mantener evidencia de cada incidencia de seguridad, para generar un historial de eventos o incidentes, que luego se tomará como retroalimentación. De igual manera, se debe mantener los procesos actualizados.
17. Aspectos de seguridad de la información en la gestión de la	17.1	Continuidad de la seguridad de la información		
	17.1.1	Planificación de la continuidad de la seguridad de la información	Aplica	Necesario para identificar puntos débiles en cuanto a la continuidad de las operaciones.

continuidad del negocio	17.1.2	Implantación de la continuidad de la seguridad de la información	Aplica	Necesario para garantizar la continuidad de los servicios.
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Aplica	Necesario para verificar la adecuación a los planes y de mejora continua.
	17.2	Redundancias		
	17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	No aplica	Por el momento se considera que no es necesario debido a que el coste supera los beneficios obtenidos.
18. Cumplimiento	18.1	Cumplimiento de los requisitos legales y contractuales		
	18.1.1	Identificación de la legislación aplicable	Aplica	Establecer políticas de seguridad para cumplir con la ley de protección de datos personales.
	18.1.2	Derechos de propiedad intelectual (PDI)	Aplica	Establecer políticas de seguridad para cumplir con la ley de protección de datos personales.
	18.1.3	Protección de los registros de la organización	Aplica	Establecer políticas de seguridad para cumplir con la ley de protección de documentación clasificada.
	18.1.4	Protección de datos de privacidad de la información personal	Aplica	Establecer políticas de seguridad para cumplir con la ley de protección de datos personales.
	18.1.5	Regulación de los controles criptográficos	No aplica	No se aplica esta regulación en la organización.
	18.2	Revisiones de la seguridad de la información		
	18.2.1	Revisión independiente de la seguridad de la información	Aplica	Se debe revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la

				información) y gestión de la seguridad de la información, planificar las revisiones.
	18.2.2	Cumplimiento de las políticas y normas de seguridad	Aplica	En las auditorías se verificará el cumplimiento de políticas, procedimientos y normas
	18.2.3	Comprobación del cumplimiento	Aplica	Establecer un plan de revisión de los SI y verificar si cumplen con las políticas y normas de seguridad dispuesta por la organización.

V. DISCUSIÓN DE RESULTADOS

Para la realización del presente proyecto fue indispensable hacer una revisión de tesis y/o proyectos realizados anteriormente con similitudes al tema abordado en esta investigación, y analizar los enfoques tomados por los autores y al resultado que deseaban llegar; algunos lo abordaron desde una perspectiva de auditoría, otros lo tomaron como un proyecto informático y algunos otros como un tema de investigación como tal, pero en muchos puntos este proyecto no dista mucho al de los autores revisados, puesto que se llega al mismo resultado que es la presentación de las políticas de información y la declaración de aplicabilidad para la organización.

Algunos autores iniciaron su punto de partida desde la realización del análisis de los activos informáticos una vez recogido los datos para sus investigaciones. Para el presente proyecto se inició siguiendo los lineamientos de la NTP – ISO/IEC 27001 que especifica el punto de partida en la evaluación inicial de la organización referente al tema de seguridad de la información. De esta manera se puede determinar el nivel de aceptación que tendrá el SGSI en la organización.

El siguiente paso fue el inicio de los preparativos del Sistema de Gestión de Seguridad de la Información, realizando un análisis del contexto tanto interno como externo de la organización, definiendo el alcance del SGSI, elaborando las políticas, los objetivos y el comité de seguridad según lo especifica la NTP – ISO/IEC 27001.

En tercer lugar, continuando con la planificación del SGSI, se realizó la evaluación de riesgos; muchos autores revisados optaron por utilizar la metodología MAGERIT para este apartado, en algunos casos algunos usaron la metodología OCTAVE; para el presente proyecto se usó la metodología MAGERIT porque ofrece una visión más

estructurada para la realización del proceso de análisis y gestión de riesgos hasta llegar al tratamiento de los riesgos encontrados.

En el paso final, se realizó el diseño de los controles y la declaración de aplicabilidad según el requisito de la NTP – ISO/IEC 27001, si bien es el resultado al que llegaron la mayoría de autores, algunos otros lo implementaron en la empresa, este resultado es variable porque cada organización o entidad es diferente de otra, aunque esté sea del mismo rubro.

Si bien el presente proyecto puede tener la limitación de que está desarrollado hasta la fase de diseño y no fue implementado, sienta las bases para este último, aparte de estar alineado a la Norma Técnica Peruana NTP – ISO/IEC 27001, se le brinda a la organización una documentación en la cual señala las amenazas en cuanto a seguridad de la información que tiene y así pueda gestionarlas de manera eficaz.

El resultado obtenido con el presente desarrollo del proyecto, acerca a la organización al tema de la seguridad de la información, si bien es un tema que es muy hablado, no es aplicado en el contexto de la organización. Luego del desarrollo y la presentación de resultados a la organización, se espera que está introduzca entre sus procesos las buenas prácticas de seguridad a fin de proteger sus activos más importantes ante amenazas y riesgos que estos pueden estar expuestos.

CONCLUSIONES

Se concluye en primer lugar que, según la aplicación de los requisitos 4 (Contexto de la Organización) y 5 (Liderazgo) de la NTP – ISO/IEC 27001:2014, la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco se encontraba en un nivel básico de la aplicación de la norma (no diseñado) con un 30% del cumplimiento de los requisitos de la NTP – ISO/IEC 27001:2014 y en una situación actual en la cual la organización

comprendía la importancia y los beneficios que tiene un SGSI y posee el liderazgo para poder realizarlo, pero no se había establecido estrategias o metodologías para la evaluación de los riesgos informáticos y su tratamiento, al igual que ninguna documentación requerida por la NTP – ISO/IEC 27001:2014.

En segundo lugar, se concluye que, la elaboración de la documentación exigida por la NTP – ISO/IEC 27001, permitió comprender a la organización y su contexto tanto interno como externo, identificar las necesidades y expectativas de sus partes interesadas, formar el comité de seguridad de la información, establecer las políticas de seguridad de información y determinar el alcance que tendrá el Sistema de Gestión de Seguridad de la Información y los objetivos de este antes de realizar el diseño. Todo esto ayudó a tener una visión enriquecida de la organización y establecer las bases diseño del Sistema de Gestión de Seguridad de la Información para la organización.

Se concluye en tercer lugar que, la aplicación de la metodología MAGERIT para el análisis y gestión de riesgos permitió observar las amenazas internas y externas a las que está expuesta la organización, su impacto y los riesgos que lleva consigo. Según el análisis realizado, la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco se encontraba en un nivel intolerable, dado que, la mayor cantidad de sus activos estaban fuera del apetito de riesgo. Al finalizar el análisis se definió a los propietarios de los riesgos encontrados; para el presente proyecto se definió al único propietario del riesgo que vino a ser el área administrativa de la DRTPE – Huánuco.

Finalmente se concluye que, el desarrollo del plan de tratamiento de riesgos ayudó a la organización a establecer los controles y acciones para mitigar los riesgos de las amenazas identificadas en los activos anteriormente, y junto a este se realizó el desarrollo de la declaración de aplicabilidad que permitió llevar el registro de los controles de seguridad que fueron aplicables y si estos se encuentran operando o todavía no.

RECOMENDACIONES

Se recomienda al personal responsable del área de Tecnologías de Información de las entidades públicas hacer parte de su organización los lineamientos propuestos por la NTP – ISO/IEC 27001, por ser de carácter obligatorio.

Durante el desarrollo del presente proyecto, se observó la necesidad que tiene la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco de realizar la implantación del SGSI y de tener la documentación de gestión referente a la seguridad de la información. Para que sea posible una implementación exitosa del Sistema de Gestión de Seguridad de la Información en la organización, es recomendable en primer lugar contratar los servicios de un consultor que guíe a la organización, luego asignar presupuesto para la implantación del SGSI; también se debe seguir con estos factores para lograr el éxito; en primer lugar, se debe tener el apoyo de la alta dirección, después, seguir con el diseño del SGSI, el cual fue desarrollado a lo largo de este proyecto; luego, concientizar a todos los trabajadores de la organización. Puede que este aspecto no se consiga inmediatamente, debido a que, muchas personas se mostrarán en contra del cambio, lo cual, puede generar inconvenientes en la implementación del SGSI.

Es conveniente realizar charlas y capacitaciones permanentes a los trabajadores antes de la implementación del SGSI, y explicarles dentro de estas, la situación actual en la que la organización se encuentra referente a la seguridad de la información y los roles y responsabilidades que tendrán cada persona concerniente a la seguridad de la información, así mismo, resolver las inquietudes que tengan los trabajadores de esta forma generaremos una cultura de seguridad dentro de la organización.

Es recomendable crear el rol de Oficial de Seguridad de Información conocido también como CISO que son sus siglas en inglés, quien será el encargado responsable

de planificar, presupuestar y verificar el rendimiento de los componentes de la seguridad de la información, así como de realizar una correcta gestión de riesgos para la toma de decisiones, y que, junto con los demás responsables del sistema de información ayuden a los trabajadores en un futuro proceso de implementación.

Por último y como opción para futuros trabajos, el diseño del presente proyecto puede ser ampliado y abarcar también a la sucursal de Tingo María e integrar a ambos en el mismo SGSI.

BIBLIOGRAFÍA

Aguirre Mollehuanca, D. A. (2014). *Diseño de un Sistema de Gestión de Seguridad de la Información para servicios postales del Perú S.A.* Pontifica Universidad Católica, Lima. Lima: s.e. Recuperado el 11 de Marzo de 2020, de http://hdl.handle.net/20.500.12404/5677

Alvarez Riaño, J. H. (2016). *Diseño de un Sistema de Gestión de Seguridad de la Información - SGSI basado en la norma ISO 27001 para el colegio Pro - colombiano de la ciudad de Bogota, que incluye: asesoría, planeación.* Universidad Nacional Abierta y Distancia, Escuela de ciencias básicas, tecnología e ingeniería. Bogotá: s.e. Recuperado el 1 de Septiembre de 2020, de https://repository.unad.edu.co/handle/10596/3448

Amaya Gutiérrez, C. (14 de Mayo de 2013). Recuperado el 12 de Marzo de 2020, de Welivesecurity: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Argüero Ramirez, E. D. (2019). *Propuesta de un Sistema de Gestión de Seguridad de la 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.*

Universidad de Huánuco, Huánuco. Huánuco: s.e. Recuperado el 11 de Marzo de 2020, de http://repositorio.udh.edu.pe/123456789/2084

Armas Huamán, A. M., & Perez Romero, F. R. (2018). *Desarrollo de un Sistema de Gestión de Seguridad de la Información para minimizar riesgos en los activos de información en la sub gerencia de informática y telecomunicaciones de la Municipalidad Distrital de Independencia 2016.* Universidad Nacional Santiago Antúnez de Mayolo, Huaraz. Huaraz: s.e. Recuperado el 11 de Marzo de 2020, de http://repositorio.unasam.edu.pe/handle/UNASAM/2208

Atencio Bazan, E. L. (2019). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP - ISO/IEC 27001: 2014 para la Dirección General de Informática y Estadística de la Universidad Nacional Daniel Alcides Carrión Pasco Perú.* Universidad Nacional Daniel Alcides Carrión, Pasco. Cerro de Pasco: s.e. Recuperado el 11 de Marzo de 2020, de http://repositorio.undac.edu.pe/handle/undac/1474

Benites Durand, C. A. (2019). *Implementación de un Sistema de Gestión de Seguridad de la Información - Norma ISO 27001 para la fábrica Radiadores Fortaleza.* Universidad Tecnológica del Perú, Lima. Lima: s.e. Recuperado el 11 de Marzo de 2020, de http://repositorio.utp.edu.pe/handle/UTP/1933

Cámara de comercio e industrias de Huánuco. (s.f. de s.f. de s.f.). *Cámara de comercio e industrias de Huánuco*. Recuperado el 08 de Agosto de 2020, de https://camarahuanuco.org.pe/seminario-de-actualizacion-sistema-integrado-de-gestion-administrativa/

Casadiegos Santana, A. L., Quintero Jiménez, M., & Toro Rueda, M. (2014). *Sistema de Gestión de Seguridad de la Información (SGSI) para el área de contabilidad de la*

E.S.E. Hospital local de Río de Oro Cesar. Universidad Francisco de Paula Santander Ocaña, Facultad de Ingenierías. Bogotá: s.e. Recuperado el 01 de Septiembre de 2020, de http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/327/1/25098.pdf

Ccsa Quincho, M. (2017). *Diseño de un Sistema de Gestión de Seguridad de la Información bajo la NTP ISO/IEC 27001: 2014 para la Municipalidad Provincial de Huamanga, 2016.* Universidad Nacional de San Cristobal de Huamanga, Ayacucho. Huamanga: s.e. Recuperado el 11 de Marzo de 2020, de http://repositorio.unsch.edu.pe/handle/UNSCH/1751

CIC. (15 de Mayo de 2019). Recuperado el 12 de Marzo de 2020, de Consulting Informático: https://www.cic.es/que-es-un-sgsi/

Dirección Regional de Trabajo y Promoción del Empleo - Apurimac. (s.f. de s.f. de s.f.). *Dirección Regional de Trabajo y Promoción del Empleo - Apurimac*. Recuperado el 20 de Agosto de 2020, de https://trabajoapurimac.gob.pe/index.php/noticiass/88-registro-de-construccion-civil-retcc

Escalante Coronel, D. M. (2019). *Diseño de un Sistema de Gestión de Seguridad de la Información bajo en enfoque de la NTP ISO/IEC 27001 para la Dirección de Salud Virgen de Cocharcas - Chincheros.* Universidad Nacional José María Argueras, Apurímac. Andahuaylas: s.e. Recuperado el 11 de Marzo de 2020, de http://repositorio.unajma.edu.pe/handle/123456789/504

Fundación Carlos Jlim. (s.f. de s.f. de s.f.). *Capacítate para el empleo.* Recuperado el 2 de Junio de 2020, de https://capacitateparaelempleo.org/assets/yog3nc0.pdf

Giménez Albacete, J. F. (2014). *Seguridad en equipos informáticos* (Primera ed.). Antequera, Málaga, España: IC Editorial. Recuperado el 11 de Junio de 2020, de https://books.google.com.pe/books?id=Fa7KCQAAQBAJ&pg=PT148&lpg=PT148&dq=La+selecci%C3%B3n+de+controles+depende+de+las+decisiones+de+la+organizaci%C3%B3n+basada+en+los+criterios+de+aceptaci%C3%B3n+de+riesgos,+las+opciones+de+tratamiento+de+riesgo&source=bl

Gob.pe. (21 de Junio de 2011). Recuperado el 12 de Marzo de 2020, de Plataforma digital única del Estado Peruano: https://www.gob.pe/institucion/pcm/normas-legales/292550-197-2011-pcm

Gob.pe. (23 de Mayo de 2012). Recuperado el 12 de Marzo de 2020, de Plataforma digital única del Estado Peruano: https://www.gob.pe/institucion/midis/normas-legales/270075-129-2012-pcm

Gob.pe. (8 de Enero de 2016). Recuperado el 12 de Marzo de 2020, de Plataforma digital única del Estado Peruano: https://www.gob.pe/institucion/pcm/normas-legales/292578-004-2016-pcm

Gobierno Regional de Huánuco. (s.f.). *Manual de Usuario Sistema de Gestión Documentaria SisGeDo 1.5.0.* Huánuco: s.e. Recuperado el 15 de Agosto de 2020

GuíasPracticas.COM. (19 de Junio de 2017). Recuperado el 12 de Junio de 2020, de http://www.guiaspracticas.com/recuperacion-de-datos/degradacion-de-datos

Guzmán García, A., & Taborda Bedoya, C. A. (2015). *Diseño de un Sistema de Gestión de la Seguridad Informática - SGSI, para empresas del área textíl en las ciudades de Itagüi, Medellín y Bogotá D.C. a través de la auditoría.* Universidad Nacional Abierta y Distancia, Escuela de ciencias básicas, tecnología e ingeniería. Bogotá:

s.e. Recuperado el 01 de Septiembre de 2020, de https://repository.unad.edu.co/handle/10596/3448

ISO27000.ES. (s.f. de s.f. de 2005). Obtenido de https://www.iso27000.es/glosario.html

ISOTools Excellence. (s.f. de s.f. de s.f.). *Acerca de nosotros: ISOTools Excellence*. Recuperado el 02 de Septiembre de 2020, de ISOTools Excellence: https://www.isotools.pe/normas/ntp-iso-27001/

Justino Salinas, Z. I. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para una empresa inmoviliaria alineado a la norma ISO/IEC 27001: 2013.* Pontifica Universidad Católica del Perú, Lima. Lima: s.e. Recuperado el 11 de Marzo de 2020, de http://hdl.handle.net/20.500.12404/6045

Justino Salinas, Z. I. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para una empresa inmoviliaria alineado a la norma ISO/IEC 27001: 2013.* Pontifica Universidad Católica del Perú, Lima. Lima: s.e. Recuperado el 11 de Marzo de 2020, de http://hdl.handle.net/20.500.12404/6045

La Contraloría General de la República del Perú. (s.f. de s.f. de s.f.). *La Contraloría General de la República del Perú*. Recuperado el 18 de Septiembre de 2020, de https://www.contraloria.gob.pe/wps/wcm/connect/CGRNew/as_contraloria/as_portal/Conoce_la_contraloria/conoceContraloria/QuienesSomos/

Leiva Peña, R. (2016). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque.* Universidad Nacional Pedro Ruiz Gallo, Chiclayo. Lambayeque: s.e. Recuperado el 11 de Marzo de 2020, de http://repositorio.unprg.edu.pe/handle/UNPRG/1019

Mendoza, M. Á. (1 de Abril de 2015). *Welivesecurity*. Recuperado el 12 de Junio de 2020, de https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

Mendoza, M. Á. (9 de Enero de 2018). *Welivesecurity*. Recuperado el 12 de Junio de 2020, de https://www.welivesecurity.com/la-es/2018/01/09/definir-alcance-sgsi/

ONGEI. (s.f. de s.f. de s.f.). Recuperado el 18 de Septiembre de 2020, de https://sites.google.com/site/ongeiwiki/

Rios Rivera, C. A., Olivera Ruiz, G., Rios Rivera, L. M., & Ponce Guizabalo, S. V. (2013). *Informe del trabajo final.* Universidad Nacional Hermilio Valdizan, Escuela de Post Grado. Tingo María: s.e. Recuperado el 3 de Julio de 2020, de https://es.slideshare.net/carlo2086/informe-26785245

Rodriguez, B. (4 de Noviembre de 2016). *Linked in*. Recuperado el 12 de Junio de 2020, de https://www.linkedin.com/pulse/apetito-de-riesgo-una-asunto-gobierno-corporativo-y-bismark?trk=mp-author-card

Rojas Viera, C. K., & Zavaleta Verona, T. L. (2019). *Sistema de Gestión de Seguridad de Información (SGSI). Basado en la Norma ISO/IEC 27001 para mejorar la Seguridad del área de operaciones y tecnología de global BPO Center Allus Chiclayo - 2015.* Universidad Nacional Pedro Ruiz Gallo, Chiclayo. Lambayeque: s.e. Recuperado el 11 de Marzo de 2020, de http://repositorio.unprg.edu.pe/handle/UNPRG/5865

Segovia, A. J. (sf. de sf. de sf.). Recuperado el 12 de Marzo de 2020, de Advisera: https://advisera.com/27001academy/es/que-es-iso-27001/

SGSI. (6 de Abril de 2015). Recuperado el 12 de Junio de 2020, de Blog especializado en Sistemas de Gestión de Seguridad de la Información: https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

Vásques Colquehuanca, A. J. (2018). *Implementación de la aplicación informática para el centro de empleo administrado por el Ministerio de Trabajo y Promoción del Empleo.* Lima: s.e. Recuperado el 17 de Agosto de 2020, de http://repositorio.usil.edu.pe/handle/USIL/8403

Vega Varona, I. A. (2019). *Diseño de un Sistema de Gestión de Seguridad de la Información para los procesos académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001.* Universidad Nacional de Piura, Piura. Piura: s.e. Recuperado el 11 de Marzo de 2020, de http://repositorio.unp.edu.pe/handle/UNP/1875

Vilca Mosquera, E. C. (2017). *Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa GEOSURVEY de la ciudad de Lima.* Universidad de Huánuco. Huánuco: s.e. Recuperado el 11 de Marzo de 2020, de http://repositorio.udh.edu.pe/123456789/809

Villegas Rivera, C. A., & Zamora Li, G. S. (2018). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001: 2013 para la empresa agroindustrial POMALCA S.A.A - 2016.* Universidad Nacional Pedro Ruiz Gallo, Chiclayo. Lambayeque: s.e. Recuperado el 11 de Marzo de 2020, de http://repositorio.unprg.edu.pe/handle/UNPRG/2440

Yana Viveros, W. (2018). *Propuesta de un Sistema de Gestión de Seguridad de la Información, aplicando la metodología MAGERIT para el Gobierno Regional de*

Puno caso: Proyecto Especial Camélidos Sudamericanos - PECSA, 2017. Universidad Privada TELESUP, Lima. Lima: s.e. Recuperado el 11 de Marzo de 2020, de https://repositorio.utelesup.edu.pe/handle/UTELESUP/336

ANEXOS

ANEXO A: Matriz de consistencia

<table>
<tr><th>TÍTULO</th><th>FORMULACION DEL PROBLEMA</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th>VARIABLES</th><th>DIMENSIONES</th><th>DISEÑO DE LA INVESTIGACIÓN</th></tr>
<tr><td>Propuesta de diseño de un Sistema de Gestión de la Seguridad de la Información basado en la NTP-ISO/IEC 27001 para la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco</td><td>¿De qué manera un Sistema de Gestión de Seguridad de la Información basado en la NTP-ISO/IEC 27001 lograría mejorar la seguridad de la información la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco?</td><td>OBJETIVO GENERAL

Proponer el diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP – ISO/IEC 27001, para mejorar la seguridad de la información de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco</td><td rowspan="5">Para la presente investigación no se realizará una formulación de hipótesis dado que tiene un alcance de estudio exploratorio, y a su vez un enfoque cualitativo. Al finalizar el presente proyecto no se afirmará o refutará nada, se presentará una solución al problema encontrado.</td><td>VARIABLE INDEPENDIENTE

Sistema de Gestión de la Seguridad de la Información basado en la NTP-ISO/IEC 27001</td><td>Confidencialidad

Disponibilidad

Integridad</td><td rowspan="5">Investigación no experimental – transeccional.</td></tr>
<tr><td colspan="2">PROBLEMAS ESPECÍFICOS</td><td>OBJETIVOS ESPECÍFICOS</td><td></td><td></td></tr>
<tr><td colspan="2">1. ¿Qué requisitos de la NTP – ISO/IEC 27001: 2014 aplicar para diagnosticar el nivel y la situación actual de la DRTPE – Huánuco?</td><td>1. Aplicar los requisitos 4 y 5 de la NTP – ISO/IEC 27001: 2014 para diagnosticar el nivel y situación actual de la DRTPE - Huánuco</td><td></td><td></td></tr>
<tr><td colspan="2">2. ¿Qué documentos te exige la NTP – ISO/IEC 27001: 2014, para diseñar el Sistema de Gestión de Seguridad de la Información en la DRTPE – Huánuco?</td><td>2. Elaborar los documentos exigidos por la NTP – ISO/IEC 27001 para el diseño del SGSI en la DRTPE - Huánuco.</td><td>VARIABLE DEPENDIENTE

Seguridad de la Información de la Dirección Regional de Trabajo y Promoción del Empleo - Huánuco</td><td>Confidencialidad

Disponibilidad

Integridad</td></tr>
<tr><td colspan="2">3. ¿Qué metodología usar para el análisis y gestión de riesgos en la DRTPE – Huánuco?</td><td>3. Aplicar la metodología MAGERIT para analizar y gestionar los riesgos de los activos de información en la DRTPE – Huánuco.</td></tr>
<tr><td colspan="2">4. ¿Qué documento es utilizado para registrar los controles aplicables a la DRTPE – Huánuco?</td><td>4. Elaborar la declaración de aplicabilidad para registrar los controles aplicables a la DRTPE – Huánuco</td></tr>
</table>

ANEXO B: Instrumentos – Guía de observación

GUÍA DE OBSERVACIÓN

OBJETIVO: El propósito de esta guía es recolectar información sobre los activos de la organización.

DATOS DEL TRABAJADOR	
NOMBRE	
CARGO	
ÁREA	
DIRECCIÓN A LA QUE PERTENECE	

EQUIPOS INFORMÁTICOS A SU CARGO	CANTIDAD

APLICATIVOS QUE USA	PROGRAMAS QUE UTILIZA

DOCUMENTOS QUE ELABORA	DOCUMENTOS QUE RECIBE

TIPO DE INFORMACIÓN DIGITAL QUE UTILIZA

ANEXO C: Situación actual de la organización

SECCIÓN	REQUISITOS DE LA NTP ISO/IEC 27001: 2014	ESTADO	EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE? / ¿QUÉ SE TENDRÍA QUE HACER?)	VALORACIÓN
4	**CONTEXTO DE LA ORGANIZACIÓN**	No diseñado	Se sugiere realizar el análisis del contexto de la DRTPE para comprender tanto los aspectos externos como internos, las partes interesadas y relevantes al SGSI.	**6%**
4.1	**Comprender la organización y su contexto** La organización debe determinar los aspectos externos e internos que son relevantes para el propósito y afectan su capacidad de lograr el(los) resultado(s) deseados de este sistema de gestión de seguridad de la información.	Parcialmente diseñado	La DRTPE posee documentos visibles de su misión, visión, Manual de Organización y Funciones (MOF), Reglamento de Organización y Funciones (ROF). Pero no contempla de forma clara los ítems de seguridad de la información. **Sugerencia:** Establecer objetivos de seguridad de la información que estén alineados con los objetivos estratégicos.	25%
4.2	**Comprender las necesidades y expectativas de las partes interesadas** La organización debe determinar las partes interesadas y los requisitos de las mismas relevantes a la seguridad de la información.	No diseñado	**Sugerencia:** Determinar las partes interesadas y comprender las necesidades y expectativas de estas, referentes a la seguridad de la información.	0%
4.3	**Determinar el alcance del sistema de gestión de seguridad de la información** La organización debe determinar los límites y la aplicabilidad del SGSI para establecer el alcance.	No diseñado	**Sugerencia:** Determinar el alcance del SGSI, teniendo en consideración los aspectos referidos, documentarlo y ponerlo a disposición de las partes interesadas.	0%
4.4	**Sistema de Gestión de Seguridad de la Información** La organización debe establecer, implementar, mantener y mejorar continuamente un SGSI, en conformidad con los requisitos de este Proyecto de Norma Técnica Peruana.	No diseñado	**Sugerencia:** Establecer un plan para la mejora continua del SGSI conforme a la NTP vigente.	0%

5	**LIDERAZGO**	No diseñado	El titular de la entidad, debe mostrar liderazgo y compromiso con respecto al SGSI. Entonces, debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas. Por lo tanto, es necesario establecer políticas de seguridad de la información y los objetivos de estos, acorde al propósito de la organización.	**3%**
5.1	**Liderazgo y compromiso** La alta dirección debe demostrar liderazgo y compromiso respecto del SGSI.	No diseñado	El titular de la entidad debe mostrar liderazgo y compromiso.	10%
5.2	**Política** La alta dirección debe establecer una política de seguridad de la información.	No diseñado	Establecer la política de seguridad de la información acorde al propósito de la organización, incluir los objetivos de la seguridad de la información, mantener disponible y comunicada a toda la organización.	0%
5.3	**Roles, autoridad y responsabilidades organizacionales**	No diseñado	La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.	0%
PUNTAJE TOTAL DE LA EVALUACIÓN DE REQUISITOS DE LA NTP ISO/IEC 27001: 2014				**5%**

ANEXO D: Política de Seguridad de Información

POLÍTICA DE SEGURIDAD DE INFORMACIÓN

1. INTRODUCCIÓN

Para la Dirección Regional de Trabajo y Promoción del Empleo - Huánuco, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

2. OBJETIVO

Establecer la política que contemple las directivas y normas, para la protección de los activos de información, basada en la confidencialidad, integridad y disponibilidad que la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco requiere.

3. ALCANCE

Esta política abarca a todos los trabajadores de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco y terceros con acceso a los activos de información.

4. POLÍTICA DE SEGURIDAD DE INFORMACIÓN

La Dirección Regional de Trabajo y Promoción del Empleo - Huánuco, tiene la necesidad de proteger los servicios y activos de la información, lo que implica que toda información obtenida, utilizada, procesada, almacenada y distribuida debe ser rigurosamente asegurada. Apoyándose en los principios fundamentales para preservar la información, como son la confidencialidad, integridad y disponibilidad de la información.

5. OBJETIVOS DE LA SEGURIDAD DE INFORMACIÓN

- Minimizar el riesgo en las funciones más importantes de la entidad.

- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Proteger los activos tecnológicos.
- Establecer políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en trabajadores y terceros de la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco.
- Garantizar la continuidad del negocio frente a incidentes.

6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, terceros.
- La Dirección Regional de Trabajo y Promoción del Empleo – Huánuco protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos autorizados a terceros o como resultado de un servicio interno en subcontratación.
- La Dirección Regional de Trabajo y Promoción del Empleo – Huánuco protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o custodia.
- La Dirección Regional de Trabajo y Promoción del Empleo – Huánuco protegerá su información de las amenazas originadas por parte del personal.
- La Dirección Regional de Trabajo y Promoción del Empleo – Huánuco protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- La Dirección Regional de Trabajo y Promoción del Empleo – Huánuco controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Dirección Regional de Trabajo y Promoción del Empleo – Huánuco garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Dirección Regional de Trabajo y Promoción del Empleo – Huánuco garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La Dirección Regional de Trabajo y Promoción del Empleo – Huánuco garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

7. ROLES Y RESPONSABILIDADES

Todo el personal de la Dirección Regional de Trabajo y Promoción del Empleo - Huánuco y terceros, que interactúan de una manera habitual u ocasional con los activos de información, son responsables de informarse del contenido de la Política de Seguridad de Información y cumplirlo en el desarrollo de sus tareas habituales.

La siguiente es una lista de roles y responsabilidades de la seguridad de la información a alto nivel:

Plana General:

- Conocer y difundir la política de seguridad de la información a todos los trabajadores de la organización.
- Estar comprometidos con el SGSI.

Comité de Seguridad de Información:

- Comunicar la importancia de los objetivos de la seguridad de la información y la necesidad de mantener una mejora continua.
- Estar informados de las recientes actualidades del negocio y de los cambios dados en los procesos pertenecientes al alcance del SGSI.
- Facilitar y dar seguimiento a la asignación de recursos relacionados al SGSI.

Oficial de Seguridad de la Información:

- Diseñar, implementar, monitorear y mejorar el SGSI en la empresa.
- Elaborar y ejecutar planes de capacitación para el personal involucrado con el alcance del SGSI.
- Seleccionar y capacitar al personal adecuado para la auditoría interna del SGSI.

Personal de la organización

- Conocer e identificar aquellos activos de información de los cuales son dueños.
- Asegurar que los activos de información que poseen son manejados y administrados correctamente.
- Reportar al oficial de seguridad de la información sobre cualquier vulnerabilidad que afecte sus activos de información.

Proveedores de bienes y servicios:

- Comprometerse por escrito a la adhesión a la presente política.
- Cumplir con lo indicado en el marco regulatorio del SGSI de la institución, en lo que respecta a su relación de terceros.

8. SANCIONES

El incumplimiento de la Política de Seguridad de Información de la Dirección Regional de Trabajo y Promoción del Empleo - Huánuco, tendrá como resultado la aplicación de la respectiva sanción, conforme a la magnitud y característica del aspecto incumplido.

9. REVISION DE LA POLÍTICA

La revisión de la política del SGSI deberá realizarse una vez al año con la presencia de los miembros del comité de seguridad de la información y la del oficial de seguridad de la información en la empresa.

10. REVISIÓN DEL ALCANCE DEL SGSI

La revisión del alcance del SGSI, se deberá realizar una vez al año o cuando existan cambios importantes en los procesos pertenecientes al alcance actual del SGSI u otros relacionados a los mismos.

ANEXO E: Cuestionario para identificar los activos informáticos

RELACIÓN DE ACTIVOS – EN CADA TABLA SELECCIONAR (X) LOS ACTIVOS CON LOS QUE CUENTA LA DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO – HUÁNUCO

TABLA DE RELACIÓN DE ACTIVOS DE TIPO DATO / INFORMACIÓN
( ) Ficheros o bases de datos
( ) Copias de respaldo
( ) Datos de configuración de los sistemas de información
( ) Datos de gestión interna
( ) Credenciales (Ejm. Contraseñas)
( ) Datos de validación de credenciales
( ) Datos de control de acceso
( ) Registro de actividad o de los sistemas de información
( ) Código fuente de los sistemas de información
( ) Código ejecutable de los sistemas de información
( ) Datos de prueba para la implementación de los sistemas de información

TABLA DE RELACIÓN DE ACTIVOS DE TIPO SERVICIO
( ) Anónimo (sin requerir identificación del usuario)
( ) Al público en general (sin relación contractual)
( ) A usuarios externos (bajo una relación contractual)
( ) Interno (a usuarios de la propia organización)
( ) Internet
( ) Acceso remoto a cuenta local
( ) Correo electrónico
( ) Almacenamiento de ficheros (File Server)
( ) Transferencia de ficheros (FTP)
( ) Intercambio electrónico de datos (EDI)
( ) Servicios de directorio
( ) Gestión de identidades (Servicios que permiten altas y bajas de usuarios a los sistemas)

TABLA DE RELACIÓN DE ACTIVOS DE TIPO SOFTWARE / APLICACIONES INFORMÁTICAS
( ) Software de desarrollo propio
( ) Software a medida (subcontratado)
( )Página web
( ) Intranet
( ) Servidor de aplicaciones
( ) ERP (Enterprise Resource Planing – Planificación de Recursos Empresariales)
( ) Correo electrónico

( ) Sistema de gestión de bases de datos
( ) Ofimática
( ) Antivirus
( ) Sistema operativo
( ) Gestor de máquinas virtuales
( ) Servidor de terminales
( ) Sistema de backup

TABLA DE RELACIÓN DE ACTIVOS DE TIPO EQUIPOS INFORMÁTICOS

( ) PCs
( ) Servidor
( ) Equipamiento de respaldo
( ) Medios de impresión (Impresoras y servidores de impresión
( ) Escáneres
( ) Módems
( ) Conmutadores (Swich)
( ) Encaminadores (Router)
( ) Cortafuegos (Firewall)
( ) Punto de acceso inalámbrico
( ) Teléfono IP
( ) Otros: ……..

TABLA DE RELACIÓN DE ACTIVOS DE TIPO REDES DE COMUNICACIONES

( ) Red telefónica
( ) Comunicaciones radio
( ) Red Inalámbrica
( ) Telefonía móvil
( ) Red local
( ) Internet

TABLA DE RELACIÓN DE ACTIVOS DE TIPO SOPORTE DE INFORMACIÓN

( ) Discos duros
( ) Discos virtuales
( ) Almacenamiento en red
( ) Disquetes
( ) Cederrón (CD-ROM)
( ) Memorias USB
( ) DVD
( ) Cinta magnética
( ) Tarjetas de memoria
( ) Tarjetas inteligentes

( ) Material impreso
( ) Cinta de papel
( ) Otros: ……..

TABLA DE RELACIÓN DE ACTIVOS DE EQUIPAMIENTO AUXILIAR
( ) Fuentes de alimentación
( ) Generadores eléctricos
( ) Cable eléctrico
( ) Fibra óptica
( ) Equipos de destrucción de soportes de información
( ) Suministros esenciales
( ) Mobiliario, armarios, etc.
( ) Otros: ……..

ANEXO F: Inventario de activos

N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	TIPO DE ACTIVO	UBICACIÓN
1	Datos vitales	Datos que almacenan los diferentes sistemas de información esenciales para el funcionamiento de la DRTPE.	Datos/Información	PC / Archivo físico (estantería)
2	Archivos personales	Documentos personales de los trabajadores de la DRTPE.	Datos/Información	PC / Dispositivos de almacenamiento externo
3	Copias de respaldo	Copias de respaldo de datos/información que manejan los distintos sistemas de la DRTPE.	Datos/Información	PC / Dispositivos de almacenamiento externo
4	Datos de configuración de los sistemas de información	Correspondiente a los documentos, manuales y procedimientos relacionados a la administración de los diferentes sistemas de información.	Datos/Información	Archivo físico (estantería)
5	Datos de gestión interna	Corresponde a los documentos de la DRTPE	Datos/Información	PC
6	Datos de control de acceso	Corresponde a los datos de los usuarios internos que utilizan los sistemas de información y/o aplicaciones.	Datos/Información	PC
7	Al público general	Servicios brindados por los sistemas de información a la comunidad huanuqueña.	Servicios	PC / Archivo físico (estantería)
9	Página web	Página web de la organización.	Servicios	VPS
10	Acceso remoto a cuenta local	Acceso a SIGA y SISGEDO del Gobierno regional de Huánuco	Servicios	Servidor de GOREHCO
11	Correo electrónico	Correo electrónico de la organización.	Servicios	correo electrónico GMAIL

12	Navegador web	Aplicación que permite el acceso a la web.	Aplicaciones informáticas / Software	PC
13	Ofimática (Microsoft Office)	Conjunto de programas informáticos que se aplican al trabajo en oficina.	Aplicaciones informáticas / Software	PC
14	Antivirus (Kaspersky)	Programa cuyo objetivo es detectar y eliminar virus informáticos.	Aplicaciones informáticas / Software	PC
15	Sistema operativo (Windows)	Conjunto de programas que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas.	Aplicaciones informáticas / Software	PC
16	Sistema Integrado de Gestión Administrativa (SIGA)	Es una herramienta informática que simplifica y automatiza los procesos administrativos en una entidad del Estado.	Aplicaciones informáticas / Software	VPS
17	Sistema de Gestión documentaria (SISGEDO)	Es un sistema informático desarrollado por el gobierno regional de Huánuco para efectuar el registro, control y seguimiento detallado y estricto de todos los expedientes que se procesan en la institución, tanto externos como internos.	Aplicaciones informáticas / Software	VPS
18	Sistema de Intermediación Laboral (SILNET)	Sistema web desarrollado para la inscripción a las personas en bolsas de trabajo.	Aplicaciones informáticas / Software	VPS
19	Sistema de Registro Nacional de Trabajadores de Construcción Civil (RTCC)	Sistema web diseñado para la inscripción de trabajadores de construcción civil.	Aplicaciones informáticas / Software	VPS
20	Aplicación de diseño gráfico (Corel Draw X8)	Software informático desarrollado para facilitar la creación de logotipos e ilustraciones digitales.	Aplicaciones informáticas / Software	PC

21	Editor de gráficos (Adobe Photoshop CC)	Software informático desarrollado para retoques de fotografías y gráficos.	Aplicaciones informáticas / Software	PC
22	Editor de gráficos (Adobe Illustrator CC)	Software informático desarrollado para editar y modificar imágenes vectoriales.	Aplicaciones informáticas / Software	PC
23	Editor de gráficos (Adobe Ligthroom CC)	Software informático desarrollado para trabajar con imágenes digitales.	Aplicaciones informáticas / Software	PC
24	Aplicación de producción de discos (Nero 7)	Software desarrollado para grabar discos ópticos.	Aplicaciones informáticas / Software	PC
25	Equipo medio (Cámaras de seguridad)	Dispositivo diseñado para supervisar una diversidad de ambientes, de costo medio tanto en su adquisición como mantenimiento.	Equipos informáticos (hardware)	Oficina
26	Informática personal (PCs, laptops)	Computadoras utilizadas por los trabajadores de la organización.	Equipos informáticos (hardware)	Oficina
27	Medios de impresión	Impresoras y fotocopiadoras de la organización.	Equipos informáticos (hardware)	Oficina
28	Escáneres	Usado para pasar un documento físico a digital.	Equipos informáticos (hardware)	Oficina
29	Red telefónica	Red de comunicación usada dentro de la organización.	Redes de comunicaciones	Red local
30	Internet	Red utilizada para acceder a servicios web.	Redes de comunicaciones	Red local
31	Dispositivo de almacenamiento externo	CD, DVD, USB, etc.	Soporte de información	Archivo físico y estante
32	Fuentes de alimentación	Pieza de hardware que se utiliza para convertir la energía suministrada desde la toma de corriente en energía utilizable para las muchas partes dentro de la carcasa del ordenador.	Equipamiento auxiliar	Oficina

33	Cableado	Sistema de cables, conectores, canalizaciones y dispositivos que permiten establecer una infraestructura de telecomunicaciones en un edificio.	Equipamiento auxiliar	Oficina
34	Suministros esenciales	Suministros esenciales en la organización.	Equipamiento auxiliar	Oficina
35	Mobiliario (armarios, etc.)	Muebles donde se encuentran los equipos informáticos.	Equipamiento auxiliar	Oficina
36	Oficinas	Lugar donde se encuentran los equipos informáticos.	Instalaciones	Edificio de la DRTPE
37	Usuarios internos	Directores de cada área.	Personal	Oficinas de la DRTPE
38	Subcontratas	Personal contratado.	Personal	Oficinas de la DRTPE
39	Proveedores	Personal externo que trabaja directamente con la organización.	Personal	Usuarios externos

ANEXO G: Valoración de activos

	N°	CAPA	CÓDIGO	ACTIVO	CONFIDENCIALIDAD		INTEGRIDAD		DISPONIBILIDAD		VFC	VFI	VFD	VF	NIVEL DE CRITICIDAD
					L	IMG	L	IMG	L	IMG					
ACTIVOS ESENCIALES	AE01	[D] Datos / Información	[vr]	Datos vitales (registros de la organización)	10	9	10	9	10	9	10	10	10	8	Alto
	AE02		[per]	Datos de carácter personal	9	8	9	5	8	5	9	7	7	6	Medio
	AE03		[backup]	Copias de respaldo	10	9	10	9	10	9	10	10	10	8	Alto
	AE04		[conf]	Datos de configuración de los sistemas de información	8	5	9	5	8	5	7	7	7	5	Medio
	AE05		[int]	Datos de gestión interna	10	9	10	9	10	9	10	10	10	8	Alto
	AE06		[acl]	Datos de control de acceso	9	5	8	5	9	5	7	7	7	5	Medio
	AE07	[S] Servicios	[pub]	Al público general	8	9	8	8	8	9	9	8	9	7	Medio
	AE08		[www]	Página web	8	9	8	8	8	8	9	8	8	6	Medio
	AE09		[telnet]	Acceso remoto a cuenta local	8	8	9	8	9	8	8	9	9	7	Medio
	AE10		[email]	Correo electrónico	9	9	9	9	2	5	9	9	4	6	Medio
	EI01		[browser]	Navegador web	4	4	4	4	2	4	4	4	3	3	Bajo
	EI02		[office]	Ofimática (Microsoft Office)	9	9	9	9	2	5	9	9	4	6	Medio

EQUIPAMIENTO INFORMÁTICO	EI03	[SW] Aplicaciones Informáticas / Software	[av]	Antivirus (Kaspersky)	2	2	5	2	2	5	2	4	4	3	Bajo
	EI04		[os]	Sistema operativo (Windows)	5	2	2	2	5	2	4	2	4	3	Bajo
	EI05		[siga]	Sistema Integrado de Gestión Administrativa (SIGA)	9	8	9	9	5	2	9	9	4	6	Medio
	EI06		[sisgedo]	Sistema de Gestión documentaria (SISGEDO)	9	8	9	9	5	2	9	9	4	6	Medio
	EI07		[silnet]	Sistema de Intermediación Laboral (SILNET)	9	8	9	9	5	2	9	9	4	6	Medio
	EI08		[rtcc]	Sistema de Registro Nacional de Trabajadores de Construcción Civil (RTCC)	9	8	9	9	5	2	9	9	4	6	Medio
	EI09		[cd]	Aplicación de diseño gráfico (Corel Draw X8)	2	2	2	2	2	2	2	2	2	2	Bajo
	EI10		[ap]	Editor de gráficos (Adobe Photoshop CC)	2	2	2	2	2	2	2	2	2	2	Bajo

	EI11		[ai]	Editor de gráficos (Adobe Illustrator CC)	2	2	2	2	2	2	2	2	2	2	Bajo
	EI12		[al]	Editor de gráficos (Adobe Ligthroom CC)	2	2	2	2	2	2	2	2	2	2	Bajo
	EI13		[nero]	Aplicación de producción de discos (Nero 7)	2	2	2	2	2	2	2	2	2	2	Bajo
	EI14	[HW] Equipos Informáticos	[mid]	Equipo medio (Sistema de cámaras de seguridad - DVR)	10	9	10	9	10	9	10	10	10	8	Alto
	EI15		[pc]	Informática personal (PCs, laptops)	10	9	10	9	10	9	10	10	10	8	Alto
	EI16		[print]	Medios de impresión	5	2	2	2	2	5	4	2	4	3	Bajo
	EI17		[scan]	Escáneres	5	2	2	2	2	5	4	2	4	3	Bajo
	EI18	[COM] Redes de Comunicaciones	[PSTN]	Red telefónica	9	6	3	3	2	3	8	3	3	4	Bajo
	EI19		[Internet]	Internet	9	6	3	3	2	3	8	3	3	4	Bajo

	EI20	[MEDIA] Soporte de Información	[dae]	Dispositivos de almacenamiento externo	8	9	8	9	5	5	9	9	5	6	Medio
ENTORNO	E01	AUX] Equipamiento	[power]	Fuentes de alimentación	2	2	2	2	2	2	2	2	2	2	Bajo
	E02		[cabling]	Cableado	2	2	2	2	2	2	2	2	2	2	Bajo
	E03		[supply]	Suministros esenciales	5	2	5	2	2	5	4	4	4	3	Bajo
	E04		[furniture]	Mobiliario (armarios, etc.)	6	5	6	5	5	5	6	6	5	4	Bajo
INSTALACIONES FISICAS	IF01	[L] Instalaciones	[local]	Oficinas	8	8	8	8	5	5	8	8	5	5	Medio
PERSONAL	P01	[P] Personal	[ui]	Usuarios internos	8	8	8	8	5	5	8	8	5	5	Medio
	P02		[sub]	Subcontratas	8	8	8	8	5	5	8	8	5	5	Medio
	P03		[prov]	Proveedores	6	5	6	5	5	5	6	6	5	4	Bajo

ANEXO H: Lista de amenazas

[I.1] FUEGO	
TIPO DE ACTIVOS	DIMENSIONES
[Hw] Equipos informáticos (Hardware) [Media] Soporte de información [Aux] Equipamiento auxiliar [L] Instalaciones	[D] Disponibilidad
Descripción: Incendios: Posibilidad de que el fuego acabe con los recursos del sistema	
Origen: Entorno (Accidental) Humano (Accidental y deliberado)	
[N.2] DAÑOS POR AGUA	
TIPO DE ACTIVOS	DIMENSIONES
[HW] Equipos informáticos (Hardware) [Media] Soporte de información [Aux] Equipamiento auxiliar [L] Instalaciones	[D] Disponibilidad
Descripción: Inundaciones: Posibilidad de que el agua acabe con los recursos del sistema	
Origen: Entorno (Accidental) Humano (Accidental y deliberado)	
[N.*] DESASTRES NATURALES	
TIPO DE ACTIVOS	DIMENSIONES
[HW] Equipos informáticos (Hardware) [Media] Soporte de información [Aux] Equipamiento auxiliar [L] Instalaciones	[D] Disponibilidad
Descripción: Otros incidentes debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, etc.	
Origen: Entorno (Accidental) Humano (Accidental y deliberado)	
[I.3] CONTAMINACIÓN MECÁNICA	
TIPOS DE ACTIVOS	DIMENSIONES

[HW] Equipos informáticos (Hardware) [Media] Soporte de información [Aux] Equipamiento auxiliar	[D] Disponibilidad
Descripción: Vibraciones, polvo, suciedad, etc.	
Origen: Entorno (Accidental) Humano (Accidental y deliberado)	
[I.4] CONTAMINACIÓN ELÉCTRICA	
TIPOS DE ACTIVOS	DIMENSIONES
[HW] Equipos informáticos (Hardware) [Media] Soporte de información [Aux] Equipamiento auxiliar	[D] Disponibilidad
Descripción: Interferencias de radio, campos magnéticos, luz ultravioleta, etc.	
Origen: Entorno (Accidental) Humano (Accidental y deliberado)	
[I.5] AVERIA DE ORIGEN FÍSICO O LÓGICO	
TIPO DE ACTIVOS	DIMENSIONES
[SW] Aplicaciones (software) [HW] Equipos informáticos (Hardware) [Media] Soporte de información [Aux] Equipamiento auxiliar	[D] Disponibilidad
Descripción: Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.	
Origen: Entorno (Accidental) Humano (Accidental y deliberado)	
[I.6] CORTE DEL SUMINISTRO ELECTRICO	
TIPOS DE ACTIVOS	DIMENSIONES
[HW] Equipos informáticos (Hardware) [Media] Soportes de información (eléctricos) [Aux] Equipamiento auxiliar	[Disponibilidad]
Descripción: Cese de la alimentación de potencia	

Origen: Entorno (Accidental) Humano (Accidental y deliberado)	
[I.7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	
TIPOS DE ACTIVOS	DIMENSIONES
[HW] Equipos informáticos (Hardware) [Media] Soportes de información [Aux] Equipamiento auxiliar	[D] Disponibilidad
Descripción:	
Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.	
Origen: Entorno (Accidental) Humano (Accidental y deliberado)	
[I.8] FALLOS DE SERVICIOS DE COMUNICACIONES	
TIPOS DE ACTIVOS	DIMENSIONES
[COM] Redes de comunicaciones	[D] Disponibilidad
Descripción: Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad de atender al tráfico presente.	
Origen: Entorno (Accidental) Humano (Accidental y deliberado)	
[I.9] INTERRUPCIÓN DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES	
TIPOS DE ACTIVOS	DIMENSIONES
[Aux] Equipamiento auxiliar	[D] Disponibilidad
Descripción: Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante, etc.	
Origen: Entorno (Accidental) Humano (Accidental y deliberado)	
[I.10] DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN	
TIPO DE ACTIVOS	DIMENSIONES
[Media] Soportes de información	[D] Disponibilidad

Descripción: Como consecuencia del paso del tiempo	
Origen: Entorno (Accidental) Humano (Accidental y deliberado)	
[I.11] EMANACIONES ELECTROMAGNÉTICAS	
TIPO DE ACTIVOS	DIMENSIONES
[HW] Equipos informáticos (Hardware) [Media] Media [Aux] Equipamiento auxiliar [L] Instalaciones	[C] Confidencialidad
Descripción:	
Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque	
Origen: Entorno (Accidental) Humano (Accidental y deliberado)	
[E.1] ERRORES DE LOS USUARIOS	
TIPOS DE ACTIVOS	DIMENSIONES
[D] Datos / Información [S] Servicios [SW] Aplicaciones (software) [Media] Soportes de información	[I] Integridad [C] Confidencialidad [D] Disponibilidad
Descripción: Equivocaciones de las personas cuando usan los servicios, datos, etc.	
[E.2] ERRORES DE ADMINISTRADOR	
TIPOS DE ACTIVOS	DIMENSIONES
[D] Datos / Información [S] Servicios [SW] Aplicaciones (software) [HW] Equipos informáticos (Hardware) [COM] Redes de comunicaciones [Media] Soportes de información	[D] Disponibilidad [I] Integridad [C] Confidencialidad
Descripción: Equivocaciones de personas con responsabilidades de instalación y operación	
[E.3] ERRORES DE MONITORIZACIÓN (LOG)	
TIPOS DE ACTIVOS	DIMENSIONES
[D.log] Registros de actividad	[I] Integridad (trazabilidad)
Descripción: Inadecuado registro de actividades: falta de registros, registros incompletos, etc.	

[E.4] ERRORES DE CONFIGURACIÓN	
TIPOS DE ACTIVOS	DIMENSIONES
[D.conf] Datos de configuración	[I] Integridad
Descripción: Introducción de datos de configuración erróneos	
[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	
TIPO DE ACTIVOS	DIMENSIONES
[SW] Aplicaciones (software)	[D] Disponibilidad [I] Integridad [C] Confidencialidad
Descripción: Propagación inocente de virus (spyware), gusanos, troyanos, etc.	
[E.9] ERRORES DE [RE-] ENCAMINAMIENTO	
TIPO DE ACTIVOS	DIMENSIONES
[S] Servicios	[C] Confidencialidad
[SW] Aplicaciones (software) [COM] Redes de comunicaciones	
Descripción: Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera	
[E.10] ERRORES DE SECUENCIA	
TIPO DE ACTIVOS	DIMENSIONES
[S] Servicios [SW] Aplicaciones (software) [COM] Redes de comunicaciones	[I] Integridad
Descripción: Alteración accidental del orden de los mensajes transmitidos	
[E.15] ALTERACIÓN ACCIDENTAL DE LA INFORMACIÓN	
TIPOS DE ACTIVOS	DIMENSIONES
[D] Datos / Información [S] Servicios [SW] Aplicaciones (software) [COM] Redes de comunicaciones [Media] Soportes de información [L] Instalaciones	[I] Integridad
Descripción: Alteración accidental de la información	
[E.18] PÉRDIDA DE LA INFORMACIÓN	
TIPO DE ACTIVOS	DIMENSIONES

[D] Datos / Información [S] Servicios [SW] Aplicaciones (software) [COM] Redes de comunicaciones [Media] Soporte de información [L] Instalaciones	[D] Disponibilidad
Descripción: Pérdida accidental de la información	
[E.19] FUGAS DE INFORMACIÓN	
TIPO DE ACTIVOS	DIMENSIONES
[D] Datos / Información [S] Servicios [SW] Aplicaciones (software) [COM] Redes de comunicaciones [Media] Soporte de información [L] Instalaciones	[C] Confidencialidad
Descripción: Revelación por indiscreción; incontinencia verbal, medios electrónicos, etc.	
[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	
TIPOS DE ACTIVOS	DIMENSIONES
[SW] Aplicaciones (software)	[I] Integridad [D] Disponibilidad [C] Confidencialidad
Descripción: Defectos en el código que da pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar	
[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACION DE PROGRAMAS (SOFTWARE)	
TIPOS DE ACTIVOS	DIMENSIONES
[SW] Aplicaciones (software)	[I] Integridad [D] Disponibilidad
Descripción: Defectos de los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por fabricante	
[E.23] ERRORES DE MANTENIMIENTO / ACTUALIZACION DE EQUIPOS (HW)	
TIPO DE ACTIVOS	DIMENSIONES
[HW] Equipos informáticos (Hardware) [Media] Soportes electrónicos	[D] Disponibilidad

[Aux] Equipamiento auxiliar	
Descripción: Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso	
[E.24] CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	
TIPO DE ACTIVOS	DIMENSIONES
[S] Servicios [HW] Equipos informáticos (Hardware) [COM] Redes de comunicaciones	[D] Disponibilidad
Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	
[E.25] PÉRDIDA DE EQUIPOS	
TIPO DE ACTIVOS	DIMENSIONES
[HW] Equipos informáticos (Hardware) [Media] Soporte de información [Aux] Equipamiento auxiliar	[D] Disponibilidad [C] Confidencialidad
Descripción: La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir la indisponibilidad. Se puede perder todo el equipamiento, siendo la perdida de equipos y soportes de información los más habituales	
[E.28] INDISPONIBILIDAD DEL PERSONAL	
TIPO DE ACTIVOS	DIMENSIONES
[P] Personal Interno	[D] Disponibilidad
Descripción: Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, etc.	
[A.3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD (LOG)	
TIPO DE ACTIVOS	DIMENSIONES
[D.log] Registros de actividad	[I] Integridad (trazabilidad)
[A.4] MANIPULACION DE LA CONFIGURACIÓN	
TIPO DE ACTIVOS	DIMENSIONES
[D.log] Registros de actividad	[I]Integridad [C] Confidencialidad [D] Disponibilidad

Descripción: Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujo de actividades, registro de actividad, etc.	
[A.5] SUPLANTACION DE LA IDENTIDAD DEL USUARIO	
TIPO DE ACTIVOS	DIMENSIONES
[D] Datos / Información [S] Servicios [SW] Aplicaciones (software) [COM] Redes de comunicaciones	[C] Confidencialidad [A] Autenticidad [I] Integridad
Descripción: Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para fines propios, esta amenaza puede ser realizada por un personal interno, personas fuera de la organización o personal contratado temporalmente	
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	
TIPO DE ACTIVOS	DIMENSIONES
[D] Datos / Información [S] Servicios [SW] Aplicaciones (software) [HW] Equipos informáticos (Hardware) [COM] Redes de comunicaciones	[C] Confidencialidad [I] Integridad [D] Disponibilidad
Descripción: Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia surge problemas	
[A.7] USO NO PREVISTO	
TIPO DE ACTIVOS	DIMENSIONES
[S] Servicios [SW] Aplicaciones (software) [HW] Equipos informáticos (Hardware) [COM] Redes de comunicaciones [Media] Soportes de información [Aux] Equipamiento auxiliar [L] Instalaciones	[D] Disponibilidad [C] Confidencialidad [I] Integridad
Descripción: Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en internet, programas personales, etc.	
[A.8] DIFUSION DE SOFTWARE DAÑINO	

TIPO DE ACTIVOS	DIMENSIONES
[SW] Aplicaciones (software)	[D] Disponibilidad [I] Integridad [C] Confidencialidad
Descripción: Propagación intencionada de virus, espías (spyware), gusanos, troyanos, etc.	
[A.9] [RE-] ENCAMINAMIENTO DE MENSAJES	
TIPOS DE ACTIVOS	DIMENSIONES
[S] Servicios [SW] Aplicaciones (software) [COM] Redes de comunicaciones	[C] Confidencialidad
Descripción: Envió de información a un destino incorrecto a través de un sistema o red, que llevan la información a donde o por donde no es debido	
[A.10] ALTERACION DE SECUENCIA	
TIPO DE ACTIVOS	DIMENSIONES
[S] Servicios [SW] Aplicaciones (software) [COM] Redes de comunicaciones	[I] Integridad
Descripción: Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado	
[A.11] ACCESO NO AUTORIZADO	
TIPO DE ACTIVOS	DIMENSIONES
[D] Datos / Información [S] Servicios [SW] Aplicaciones (software) [HW] Equipos informáticos (Hardware) [COM] Redes de comunicaciones [Media] Soportes de información [Aux] Equipamiento auxiliar [L] Instalaciones	[C] Confidencialidad [I] Integridad
Descripción:	
El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización	
[A.12] ANÁLISIS DE TRÁFICO	
TIPOS DE ACTIVOS	DIMENSIONES
[COM] Redes de comunicaciones	[C] Confidencialidad

Descripción: El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis de origen, destino, volumen y frecuencia de los intercambios	
[A.13] REPUDIO	
TIPOS DE ACTIVOS	DIMENSIONES
[S] Servicios [D.log] Registros de actividad	[I] Integridad (trazabilidad)
Descripción: Negación de actuaciones o compromisos adquiridos en el pasado; repudio de origen, de recepción y de entrega	
[A.14] INTERCEPTACION DE INFORMACIÓN (ESCUCHA)	
TIPO DE ACTIVOS	DIMENSIONES
[COM] Redes de comunicaciones	[C] Confidencialidad
Descripción: El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada	
[A.15] MODIFICACIÓN DELIBERADA DE LA INFORMACIÓN	
TIPOS DE ACTIVOS	DIMENSIONES
[D] Datos / Información [S] Servicios (acceso) [SW] Aplicaciones (software) [COM] Redes de comunicaciones (tránsito) [Media] Soportes de información [L] Instalaciones	[I] Integridad
Descripción: Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio	
[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	
TIPO DE ACTIVOS	DIMENSIONES
[D] Datos / Información [S] Servicios (acceso) [SW] Aplicaciones (software) [Media] Soportes de información [L] Instalaciones	[D] Disponibilidad
Descripción: Eliminación intencional de información, con ánimo de obtener un beneficio o causar algún perjuicio	
[A.19] DIVULGACIÓN DE INFORMACIÓN	
TIPOS DE ACTIVOS	DIMENSIONES

[D] Datos / Información [S] Servicios (acceso) [SW] Aplicaciones (software) [COM] Redes de comunicaciones (tránsito) [Media] Soportes de información [L] Instalaciones	[C] Confidencialidad
Descripción: Revelación de información	
[A.22] MANIPULACIÓN DE PROGRAMAS	
TIPOS DE ACTIVOS	DIMENSIONES
[SW] Aplicaciones (software)	[C] Confidencialidad [I] Integridad [D] Disponibilidad
Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza	
[A.23] MANIPULACIÓN DE LOS EQUIPOS	
TIPOS DE ACTIVOS	DIMENSIONES
[HW] Equipos informáticos (Hardware) [Media] Soportes de información [Aux] Equipamiento auxiliar	[C] Confidencialidad [D] Disponibilidad
Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza	
[A.24] DENEGACIÓN DE SERVICIO	
TIPOS DE ACTIVOS	DIMENSIONES
[S] Servicios [HW] Equipos informáticos (Hardware) [COM] Redes de comunicaciones	[D] Disponibilidad
Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	
[A.25] ROBO	
TIPOS DE ACTIVOS	DIMENSIONES
[HW] Equipos informáticos (Hardware) [Media] Soportes de información [Aux] Equipamiento auxiliar	[D] Disponibilidad [C] Confidencialidad

Descripción: La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad	
[A.26] ATAQUE DESTRUCTIVO	
TIPOS DE ACTIVOS	DIMENSIONES
[HW] Equipos informáticos (Hardware) [Media] Soportes de información [Aux] Equipamiento auxiliar [L] Instalaciones	[D] Disponibilidad
Descripción: Vandalismo, terrorismo, acción militar, etc.	
[A.27] OCUPACIÓN ENEMIGA	
TIPOS DE ACTIVOS	DIMENSIONES
[L] Instalaciones	[D] Disponibilidad [C] Confidencialidad
Descripción: Cuando los locales han sido inválidos y se carece de control sobre los propios medios de trabajo	
[A.28] INDISPONIBILIDAD DEL PERSONAL	
TIPOS DE ACTIVOS	DIMENSIONES
[P] Personal Interno	[D] Disponibilidad
Descripción: Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueos de los accesos, etc.	
[A.29] EXTORSIÓN	
TIPOS DE ACTIVOS	DIMENSIONES
[P] Personal Interno	[C] Confidencialidad [I] Integridad [D] Disponibilidad
Descripción: Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido	
[A.30] INGENIERÍA SOCIAL (PICARESA)	
TIPOS DE ACTIVOS	DIMENSIONES
[P] Personal Interno	[C] Confidencialidad [I] Integridad [D] Disponibilidad
Descripción: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero	

ANEXO I: Identificación de amenazas en los activos

N°	CÓDIGO	ACTIVO	PROB
AE01	**[vr]**	**Datos vitales (registros de la organización)**	**4**
	[E.1]	Errores de los usuarios	4
	[E.2]	Errores de administrador	3
	[E.15]	Alteración accidental de la información	4
	[E.18]	Pérdida de información	3
	[E.19]	Fuga de información	4
AE02	**[per]**	**Datos de carácter personal**	**3**
	[E.18]	Pérdida de información	3
AE03	**[backup]**	**Copias de respaldo**	**4**
	[E.18]	Pérdida de información	3
	[E.19]	Fuga de información	4
AE04	**[conf]**	**Datos de configuración de los sistemas de información**	**2**
	[E.4]	Errores de configuración	2
	[E.18]	Pérdida de la información	2
AE05	**[int]**	**Datos de gestión interna**	**4**
	[E.1]	Errores de los usuarios	4
	[E.2]	Errores de administrador	3
	[E.15]	Alteración accidental de la información	4
	[E.18]	Pérdida de información	3
AE06	**[acl]**	**Datos de control de acceso**	**4**
	[E.2]	Errores de los usuarios	4
AE07	**[pub]**	**Al público en general**	**3**
	[E.2]	Errores de administrador	3
	[E.15]	Alteración accidental de la información	3
AE08	**[www]**	**Página web**	**3**
	[E.2]	Errores de administrador	3
	[E.15]	Alteración accidental de la información	3
AE09	**[email]**	**Correo electrónico**	**3**
	[E.2]	Errores de administrador	3
	[E.15]	Alteración accidental de la información	3
EI02	**[office]**	**Ofimática (Microsoft Office)**	**5**
	[E.1]	Errores de los usuarios	5
	[E.15]	Alteración accidental de la información	4
EI05	**[siga]**	**Sistema Integrado de Gestión Administrativa (SIGA)**	**4**
	[E.1]	Errores de los usuarios	4
	[E.15]	Alteración accidental de la información	4
EI06	**[sisgedo]**	**Sistema de Gestión Documentaria (SISGEDO)**	**4**
	[E.1]	Errores de los usuarios	4
	[E.15]	Alteración accidental de la información	4
EI07	**[silnet]**	**Sistema de Intermediación Laboral (SILNET)**	**4**

	[E.1]	Errores de los usuarios	4
	[E.15]	Alteración accidental de la información	4
EI08	**[rtcc]**	**Sistema de Registro Nacional de Trabajadores de Construcción Civil**	**4**
	[E.1]	Errores de los usuarios	4
	[E.15]	Alteración accidental de la información	4
EI14	**[mid]**	**Equipo medio (Sistema de cámaras de seguridad – DVR)**	**3**
	[I.1]	Fuego	1
	[I.3]	Contaminación mecánica	5
	[I.5]	Avería de origen físico o lógico	2
	[I.6]	Corte de suministro eléctrico	2
	[I.10]	Degradación de los soportes de almacenamiento de la información	3
	[E.23]	Errores de mantenimiento / actualización de equipos	3
	[A.25]	Robo	2
EI15	**[pc]**	**Informática personal (PCs, laptops)**	**3**
	[I.1]	Fuego	1
	[I.3]	Contaminación mecánica	5
	[I.5]	Avería de origen físico o lógico	3
	[I.6]	Corte de suministro eléctrico	2
	[I.10]	Degradación de los soportes de almacenamiento de la información	3
	[E.23]	Errores de mantenimiento / actualización de equipos	3
	[A.25]	Robo	1
EI20	**[dae]**	**Dispositivos de almacenamiento externo**	**3**
	[I.1]	Fuego	1
	[1.3]	Contaminación mecánica	3
	[I.5]	Avería de origen físico o lógico	3
	[I.10]	Degradación de los soportes de almacenamiento de la información	2
	[E.18]	Pérdida de la información	3
	[E.25]	Pérdida de equipos	3
	[A.7]	Uso no previsto	5
	[A.25]	Robo	2
IF01	**[local]**	**Oficinas**	**4**
	[E.15]	Alteración accidental de la información	5
	[E.18]	Pérdida de información	3
	[E.19]	Fuga de información	4
P01	**[ui]**	**Usuarios internos**	**4**
	[E.28]	Indisponibilidad del personal	4
P02	**[sub]**	**Subcontratas**	**4**
	[E.28]	Indisponibilidad del personal	4

ANEXO J: Degradación de los activos

CODIGO		ACTIVO	PROB	DIMENSIONES		
				C	I	D
EI14	**[mid]**	**Equipo medio (Sistema de cámaras de seguridad - DVR)**	**3**	**70%**	**70%**	**80%**
	[I.1]	Fuego	1	-	-	100%
	[I.3]	Contaminación mecánica	5	-	-	50%
	[I.5]	Avería de origen físico o lógico	3	-	-	70%
	[I.6]	Corte de suministro eléctrico	3	-	-	70%
	[I.10]	Degradación de los soportes de almacenamiento de la información	5	-	-	90%
	[E.1]	Errores de los usuarios	4	70%	70%	80%
	[E.4]	Errores de configuración	3	-	70%	-
	[E.23]	Errores de mantenimiento / actualización de equipos (Hw)	4	-	-	80%
	[A.25]	Robo	2	-	-	100%
EI15	**[pc]**	**Informática personal (PCs, laptops)**	**3**	**68%**	**73%**	**79%**
	[I.1]	Fuego	1	-	-	100%
	[I.3]	Contaminación mecánica	5	-	-	60%
	[I.5]	Avería de origen físico o lógico	3	-	-	70%
	[I.6]	Corte de suministro eléctrico	3	-	-	70%
	[I.10]	Degradación de los soportes de almacenamiento de la información	5	-	-	90%
	[E.1]	Errores de los usuarios	4	70%	80%	80%
	[E.8]	Difusión de software dañino	4	50%	90%	90%
	[E.15]	Alteración accidental de la información	5	-	70%	-
	[E.19]	Fuga de información	4	80%	-	-
	[E.21]	Errores de mantenimiento / actualización de programas	4	-	80%	80%
	[E.23]	(SW)	4	-	-	80%
	[A.6]	Errores de mantenimiento / actualización de equipos (HW)	3	40%	60%	60%
	[A.7]	Abuso de privilegios de acceso	5	60%	60%	70%
	[A.11]	Uso no previsto	2	70%	70%	-
	[A.22]	Acceso no autorizado	2	70%	70%	80%
	[A.25]	Manipulación de programas	1	100%	-	100%
		Robo				
EI20	**[dae]**	**Dispositivos de almacenamiento externo**	**3**	**71%**	**73%**	**88%**

	[I.1]	Fuego	1	-	-	100%
	[I.10]	Degradación de los soportes de almacenamiento de la información	5	-	-	90%
	[E.1]	Errores de los usuarios	3	70%	70%	90%
	[E.8]	Difusión de software dañino	4	50%	90%	90%
	[E.15]	Alteración accidental de la información	4	-	70%	-
	[E.19]	Fuga de información	3	80%	-	-
	[E.25]	Pérdida de equipos	4	80%	-	100%
	[A.6]	Abuso de privilegios de acceso	3	40%	60%	60%
	[A.7]	Uso no previsto	5	70%	70%	70%
	[A.11]	Acceso no autorizado	3	80%	80%	-
	[A.25]	Robo	2	100%	-	100%

ANEXO K: Valoración de riesgos

CÓDIGO	AMENAZA	PROBABILIDAD	DEGRADACIÓN			IMPACTO			ESTIMACIÓN DEL RIESGO		
			CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
EI14	**EQUIPO MEDIO (Sistema de cámaras de seguridad - DVR)**	**3**	**70%**	**70%**	**80%**	**7**	**7**	**8**	**21**	**21**	**24**
[I.1]	Fuego	1	-	-	100%	-	-	Desastroso	-	-	Extremo
[I.3]	Contaminación mecánica	5	-	-	50%	-	-	Moderado	-	-	Tolerable
[I.5]	Avería de origen físico o lógico	3	-	-	70%	-	-	Mayor	-	-	Intolerable
[I.6]	Corte de suministro eléctrico	3	-	-	70%	-	-	Mayor	-	-	Intolerable
[I.10]	Degradación de los soportes de almacenamiento de la información	5	-	-	90%	-	-	Desastroso	-	-	Extremo
[E.1]	Errores de los usuarios	4	70%	70%	80%	Mayor	Mayor	Mayor	Intolerable	Intolerable	Intolerable
[E.4]	Errores de configuración	3	-	70%	-	-	Mayor	-	-	Intolerable	-
[E.23]	Errores de mantenimiento / actualización de equipos (Hw)	4	-	-	80%	-	-	Mayor	-	Intolerable	-
[A.25]	Robo	2	-	-	100%	Desastroso	-	Desastroso	Extremo	-	Extremo
[pc]	**INFORMÁTICA PERSONAL (PCs, laptops)**	**3**	**68%**	**73%**	**79%**	**7**	**7**	**8**	**20**	**22**	**24**
[I.1]	Fuego	1	-	-	100%	-	-	Desastroso	-	-	Extremo

[I.3]	Contaminación mecánica	5	-	-	60%	-	-	Moderado	-	-	Tolerable
[I.5]	Avería de origen físico o lógico	3	-	-	70%	-	-	Mayor	-	-	Intolerable
[I.6]	Corte de suministro eléctrico	3	-	-	70%	-	-	Mayor	-	-	Intolerable
[I.10]	Degradación de los soportes de almacenamiento de la información	5	-	-	90%	-	-	Desastroso	-	-	Extremo
[E.1]	Errores de los usuarios	4	70%	80%	80%	Mayor	Mayor	Mayor	Intolerable	Intolerable	Intolerable
[E.8]	Difusión de software dañino	4	50%	90%	90%	Moderado	Desastroso	Desastroso	Tolerable	Extremo	Extremo
[E.15]	Alteración accidental de la información	5	-	70%	-	-	Mayor	-	-	Intolerable	-
[E.19]	Fuga de información	4	80%	-	-	Mayor	-	-	Intolerable	-	-
[E.21]	Errores de mantenimiento / actualización de programas (SW)	4	-	80%	80%	-	Mayor	Mayor	-	Intolerable	Intolerable
[E.23]	Errores de mantenimiento / actualización de equipos (HW)	4	-	-	80%	-	-	Mayor	-	-	Intolerable
[A.6]	Abuso de privilegios de acceso	2	40%	60%	60%	Moderado	Moderado	Moderado	Tolerable	Tolerable	Tolerable
[A.7]	Uso no previsto	5	60%	60%	70%	Moderado	Moderado	Mayor	Tolerable	Tolerable	Intolerable
[A.11]	Acceso no autorizado	2	70%	70%	-	Mayor	Mayor	-	Intolerable	Intolerable	-
[A.22]	Manipulación de programas	2	70%	70%	80%	Mayor	Mayor	Mayor	Intolerable	Intolerable	Intolerable
[A.25]	Robo	1	100%	-	100%	Desastroso	-	Desastroso	Extremo	-	Extremo
[dae]	**DISPOSITIVOS DE ALMACENAMIENTO EXTERNO**	**3**	**71%**	**73%**	**88%**	**6**	**7**	**4**	**19**	**20**	**13**
[I.1]	Fuego	1	-	-	100%	-	-	Desastroso	-	-	Extremo
[I.10]	Degradación de los soportes de almacenamiento de la información	5	-	-	90%	-	-	Desastroso	-	-	Extremo

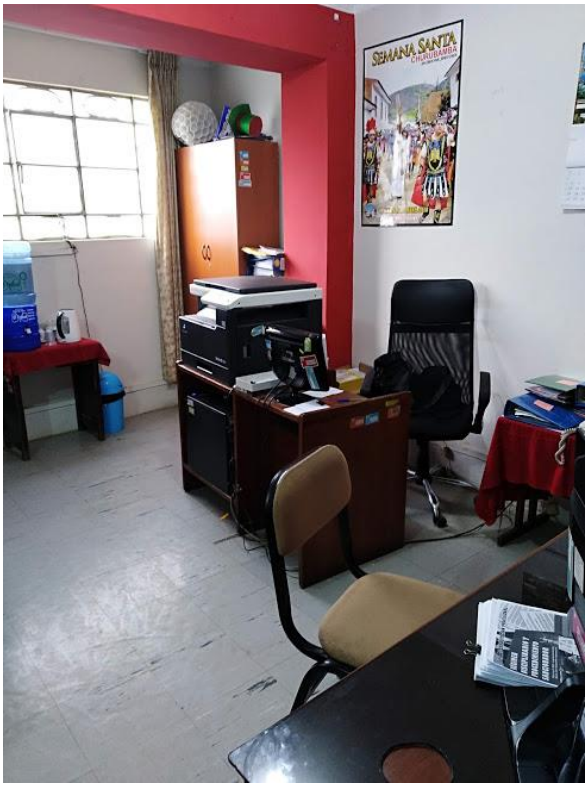
[E.1]	Errores de los usuarios	3	70%	70%	90%	Mayor	Mayor	Desastroso	Intolerable	Intolerable	Extremo
[E.8]	Difusión de software dañino	4	50%	90%	90%	Moderado	Desastroso	Desastroso	Tolerable	Extremo	Extremo
[E.15]	Alteración accidental de la información	4	-	70%	-	-	Mayor	-	-	Intolerable	-
[E.19]	Fuga de información	3	80%	-	-	Mayor	-	-	Intolerable	-	-
[E.25]	Pérdida de equipos	4	80%	-	100%	Mayor	-	Desastroso	Intolerable	-	Extremo
[A.6]	Abuso de privilegios de acceso	3	40%	60%	60%	Moderado	Moderado	Moderado	Tolerable	Tolerable	Tolerable
[A.7]	Uso no previsto	5	70%	70%	70%	Mayor	Mayor	Mayor	Intolerable	Intolerable	Intolerable
[A.11]	Acceso no autorizado	3	80%	80%	-	Mayor	Mayor	-	Intolerable	Intolerable	-
[A.25]	Robo	2	100%	-	100%	Desastroso	-	Desastroso	Extremo	-	Extremo

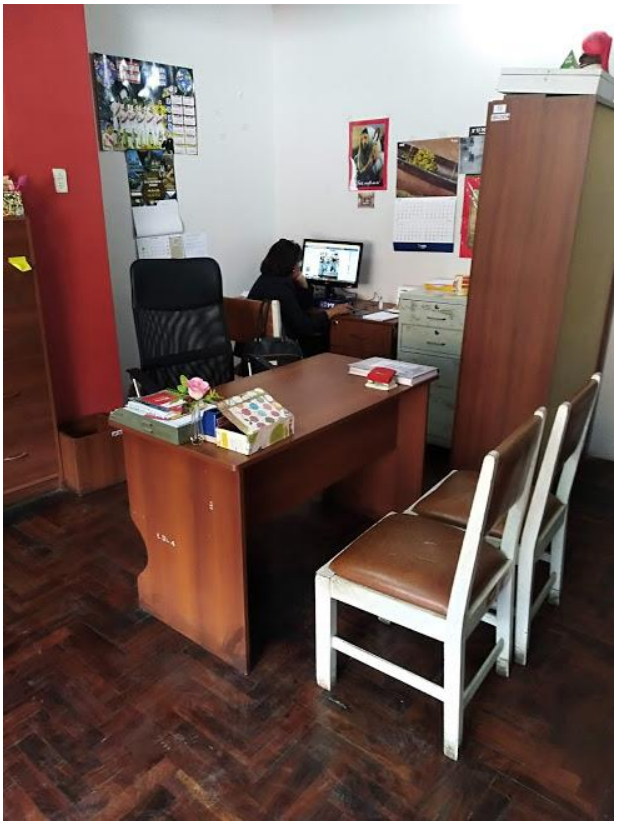
ANEXO L: Controles de la NTP – ISO/IEC 27001

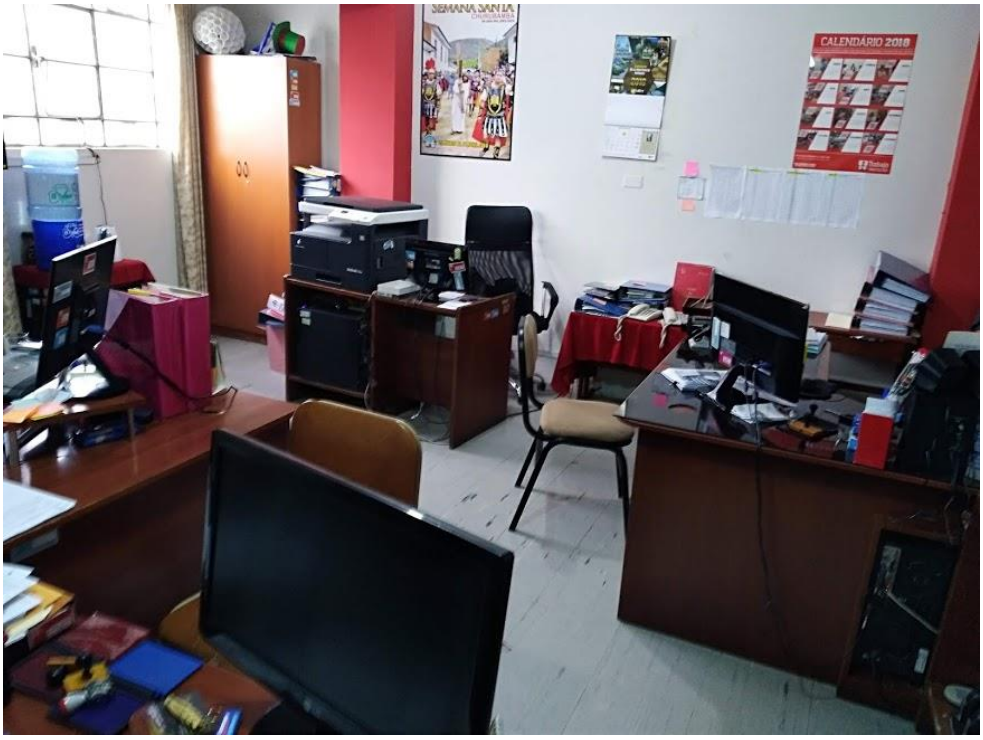
CLÁUSULA DE LOS CONTROLES ISO/IEC 27001:2013	DESCRIPCIÓN DE OBJETIVO
5. POLÍTICAS DE SEGURIDAD	Proporcionar orientación y apoyo de la dirección para la seguridad de la información de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Establecer un marco de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización. Garantizar la seguridad del teletrabajo y del uso de dispositivos móviles
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	Asegurar que los empleados y contratistas entiendan sus responsabilidades y que sean aptos para los roles para los cuales están siendo considerados. Así mismo, sean conscientes y cumplan con las responsabilidades de seguridad de la información. Para finalizar, se debe proteger los intereses de la organización como parte del proceso del cambio o terminación del empleo.
8. GESTIÓN DE ACTIVOS	Identificar los activos y definir las responsabilidades de protección adecuadas. Asegurar que la información recibe el nivel de protección adecuado de acuerdo con su importancia en la organización. Para finalizar, evitar la divulgación no autorizada, modificación, eliminación de la información almacenada en los medios de comunicación.
9. CONTROL DE ACCESO	Primeramente, se debe limitar el acceso a la información y a las instalaciones de procesamiento de información. Así mismo, asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios de información. Y para finalizar se debe hacer a los usuarios responsables de salvaguardar su información de autenticación.
10. CRIPTOGRAFÍA	Garantizar el uso adecuado y eficaz del cifrado para proteger la confidencialidad, autenticidad y/o integridad de la información.
11. SEGURIDAD FÍSICA DEL ENTORNO.	Prevenir el acceso físico no autorizado, daños e interferencia a la información de la organización y a las instalaciones de procesamiento de información. También, evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las operaciones de la organización.
12. SEGURIDAD EN LAS OPERACIONES	Asegurar que las operaciones sean correctas y seguras en las instalaciones de procesamiento de información. Asegurar que estas instalaciones y la información estén protegidas contra el malware. Evitar la pérdida de datos. Registrar eventos y generar

	evidencia. Garantizar la integridad de los sistemas operativos. Evitar la explotación de vulnerabilidades técnicas. Y minimizar el impacto de las actividades auditada en los sistemas operativos.
13. SEGURIDAD EN LAS COMUNICACIONES	Garantizar la protección de la información en las redes y las instalaciones de procesamiento de información. Mantener la seguridad de la información transferida desde la organización con cualquier entidad externa.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcional los servicios a través de redes públicas. Para finalizar, garantizar la protección de los datos utilizados para pruebas.
15. RELACIONES CON SUMINISTRADORES	Garantizar la protección de los activos de la organización que sea accesible por lo proveedores. Mantener un nivel de seguridad de la información y de prestación de servicios alineado con los acuerdos con los proveedores.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluidos los de comunicación de los eventos de seguridad y los puntos débiles.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	La continuidad de la seguridad de información se incluirá dentro de los sistemas de gestión de continuidad de negocio de la organización. Garantizar la disponibilidad de las instalaciones de procesamiento de información.
18. CUMPLIMIENTO	Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas a la seguridad de la información y a los requisitos de seguridad. Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.

ANEXO M: Fotos






CALENDARIO 2018


CALENDARIO 2018
SEMANA SANTA

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 08 Días del mes de enero de 2021, siendo las 08 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. 48º al 52º, se procedió a la evaluación de la sustentación de la tesis virtual, titulado**: "PROPUESTA DE DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÍON BASADO EN LA NTPISO/IEC 27001 PARA LA DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO – HUÁNUCO",** presentado por (el) (la) la Bachiller en Ingeniería de Sistemas: **JOSE CARLOS SANDOVAL ALANIA**. 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:

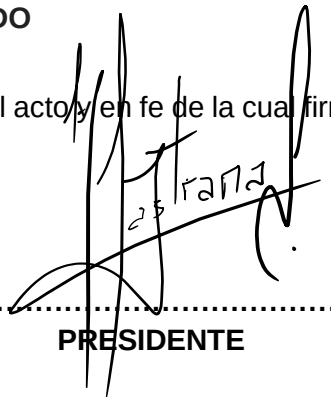
PRESIDENTE: Dra. NÉRIDA DEL CARMEN PASTRANA DÍAZ

SECRETARIO: Mg. ELMER CHUQUIYAURI SALDIVAR

VOCAL: Dra. INES JESUS TOLENTINO

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 el siguiente resultado: **Nota: 17** equivalente a la calificación de **Muy Bueno** Quedando (el) (la) Bachiller en Ingeniería de Sistemas: **JOSE CARLOS SANDOVAL ALANIA 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

AUTORIZACIÓN PARA PUBLICACIÓN DE TESIS ELECTRÓNICAS DE PREGRADO

IDENTIFICACIÓN PERSONAL (especificar los datos de los autores de la tesis)

Apellidos y Nombres Sandoval Alania Jose Carlos

DNI 72107721 Correo Electrónico jcarlosalania05@gmail.com

Teléfono Casa 062 405362 Celular 983769593 Oficina _____

Apellidos y Nombres _____

DNI _____ Correo Electrónico _____

Teléfono Casa _____ Celular _____ Oficina _____

Apellidos y Nombres _____

DNI _____ Correo Electrónico _____

Teléfono Casa _____ Celular _____ 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:

Propuesta de diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001 para la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco.

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 cuando 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 periodo de tiempo en que la tesis tendría el tipo de acceso restringido:

( ) 1 año

( ) 2 años

( ) 3 años

( ) 4 años

Luego del periodo señalado por usted (es), automáticamente la tesis pasara a ser de acceso público

Fecha de firma: 04 de mayo del 2021

Firma del autor y/o autores