ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN
DIRECCIÓN PÚBLICA

Propuesta de mejora en el diseño de gestión de seguridad de la información bajo la norma ISO 27001:2013, para las actividades operativas y administrativas de la división de apoyo técnico judicial de la Dirección Antidrogas de la Policía Nacional del Perú

Trabajo de Investigación
para optar el Grado a Nombre de la Nación de:

Maestro en
Dirección Pública

Autores:
Bach. Torres Graneros, Hebert Serjino

Docente Guía:
Mtra. Barriga Andrade, Yesica Yanira

TACNA – PERÚ

2022

Dedicatoria

El presente está dedicado al personal de la División de Apoyo técnico judicial de la Dirección Antidrogas de la Policía Nacional del Perú, para que resulte como material de consulta en una futura implementación del ISO-27001.

Agradecimiento

En especial a mi familia, tutores, compañeros y amigos; que colaboraron en la formulación del presente trabajo de investigación.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INDICE DE ANEXOS

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

RESUMEN

El División de Apoyo Técnico Judicial de la Dirección Antidrogas de la Policía Nacional del Perú, es un área especializada que gestiona el sistema legal de interceptación de las comunicaciones, técnica especial de investigación que es utilizada como herramienta eficaz para la lucha del tráfico ilícito de drogas, terrorismo y crimen organizado; mediante la ejecución de un mandatos judiciales de los órganos jurisdiccionales, de su aplicación se obtiene información sensible que es almacenada mediante grabación, para su posterior registro, custodia y transcripción, siendo necesario la aplicación de un diseño de un Sistema de Gestión de la Seguridad de la Información dentro de los estándares de la Norma ISO 27001.

La necesidad de obtener el reconocimiento de seguridad de la información obtenida legalmente y respaldado sobre la hipótesis fiscal en un proceso penal en la etapa investigación intermedia, la autoridad fiscal no solo contaría con el reconocimiento de la plena labor que realiza la División de Apoyo Técnico Judicial (DIVATJ), sino que este al obtener el ISO 27001 tiene la certeza que la información que se maneja es completamente certera sin posibilidad de ser adulterada durante el proceso, siendo necesario capacitar al personal de Analistas tácticos en temas relacionados en Seguridad de la información y en técnicas para la protección de datos y seguridad de la información. Además, las capacitaciones deben estar enfocadas a la aplicación de herramientas para la protección de datos y seguridad de la información.

Mediante un estudio no experimetal el presente trabajo de investigación intenta demostrar las características y cualidades del área de tecnología de la

información y comunicación, asimismo de las áreas encargadas de la recolección de la información digital que será objeto de estudio en el periodo 2022.

El ISO 27001, es un estándar internacional para la gestión de la seguridad de la información, que proporciona un marco sistemático para proteger la información sensible que se obtiene de la interceptación legal de la comunicación. La DIVATJ necesita del ISO 27001, para mejorar la eficacia y eficiencia de los sistemas de seguridad de la información, al seguir un enfoque basado en procesos que aseguren que los riesgos sean identificados, analizados y gestionados adecuadamente, lo que es necesario el uso del método MAGERIT: Metodología de Análisis y Gestión de Riesgos de los sistemas de Información como herramienta pilar la cual soporta el análisis y gestión de los riesgos es usado como fuente para determinar las brechas en seguridad de la información. Asimismo, demuestra a los clientes, Ministerio Público y Grupo Operativo Policial, que se toma en serio la seguridad de la información y está comprometida con la protección de datos secretos, reservados y confidenciales. Implica que la División de Apoyo Técnico Judicial cumple con los requisitos legales y reglamentos relativos a la privacidad y protección de datos.

En síntesis, la División de Apoyo Técnico Judicial necesita del ISO 27001 para proteger su información obtenida de la interceptación legal de las comunicaciones, al ser observado como una entidad competente y atractiva, que cumple con la ley y reglamentos.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

ABSTRACT

The Judicial Technical Support Division of the Anti-Drug Directorate of the National Police of Peru is a specialized area that manages the legal system of interception of communications, a special investigative technique that is used as an effective tool in the fight against illicit drug trafficking, terrorism and organized crime; Through the execution of judicial mandates of the jurisdictional bodies, sensitive information is obtained from its application, which is stored by recording, for its subsequent registration, custody and transcription, being necessary the application of a design of an Information Security Management System within the standards of the ISO 27001 Standard.

The need to obtain the recognition of information security legally obtained and supported on the prosecutorial hypothesis in a criminal process in the intermediate investigation stage, the prosecutorial authority would not only have the recognition of the full work done by the Judicial Technical Support Division (DIVATJ), but this by obtaining the ISO 27001 has the certainty that the information handled is completely accurate without the possibility of being adulterated during the process, being necessary to train the staff of tactical analysts on issues related to information security and techniques for data protection and information security. In addition, training should be focused on the application of tools for data protection and information security.

Through a non-experimental study, this research work attempts to demonstrate the characteristics and qualities of the area of information technology and

communication, as well as the areas responsible for the collection of digital information that will be the subject of study in the period 2022.

ISO 27001 is an international standard for information security management, which provides a systematic framework for protecting sensitive information obtained from lawful interception of communication. DIVATJ needs ISO 27001 to improve the effectiveness and efficiency of information security systems by following a process-based approach to ensure that risks are properly identified, analyzed and managed, which requires the use of the MAGERIT method: Methodology of Analysis and Risk Management of Information Systems as a pillar tool that supports the analysis and management of risks used as a source to determine the gaps in information security. It also demonstrates to clients, the Public Prosecutor's Office and the Police Task Force that it takes information security seriously and is committed to protecting secret, reserved and confidential data. It implies that the Technical Judicial Support Division complies with legal requirements and regulations regarding privacy and data protection.

In summary, the Judicial Technical Support Division needs ISO 27001 to protect its information obtained from lawful interception of communications by being seen as a competent and attractive entity that complies with the law and regulations.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

INTRODUCCIÓN

Durante la última década, las organizaciones criminales han intensificado sus actividades en el Perú y el mundo, con el surgimiento de nuevas tecnologías que les permiten beneficiarse en contra del Estado, dado el enorme poder económico obtenido principalmente a través de actividades ilícitas vienen realizando actividades delictivas a nivel nacional e internacional como son el tráfico ilegal de drogas, el terrorismo y otras actividades delictivas relacionadas al crimen organizado. (Frías, L. 2022)

Ante estos acontecimientos que resquebrajan la percepción de seguridad que se tiene el país, los operadores de justicia desde el 2009 vienen combatiendo de manera anónima, en la institución policial se rige del mandato jurídico-constitucional enmarcado en la Constitución política del Perú (1993) Artículo 166º: "…previene, investiga y combate la delincuencia…"; el División de apoyo Técnico Judicial de la Dirección Antidrogas de la Policía Nacional del Perú, a partir de ahora denominado DIVATJ, depende de administraba y operativamente de la Dirección Antidrogas de la Policía Nacional del Perú y realiza su labor en coordinación con las Fiscalías Especializadas en Crimen Organizado, y ejecutan las Resoluciones Judiciales en amparo a la restricción al derecho fundamental del secreto y la inviolabilidad de las comunicaciones privadas, contenidas en el artículo 2°, inciso 10° de la Constitución Política del Perú; ejecutando con profesionalismo, diligencia, discreción, legalidad, y en principio de la confiabilidad; direccionado su actuar en los términos establecidos por el Código Procesal Penal, establecido en el Subcapítulo II La intervención de comunicaciones y

telecomunicaciones establecido en el artículo 230° sobre la intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles.

La función de prevenir, investigar y combatir la criminalidad organizada el estado peruano dicta normas valor específico que faculta al Ministerio Publico y a la Policía Nacional del Perú utilizar herramientas jurídicas y técnicas, estas se establecen en la Ley Nº 30077 en su Capitulo segundo, Técnicas especiales de investigación; que mediante su resultado sea idóneo, necesario e indispensable y existan los suficientes elementos de convicción acerca de la comisión de un hecho delictivo que se ejecuta en tiempo real y es vinculante a una organización criminal; y durante la investigación se respete los principios de necesidad, razonabilidad y proporcionalidad, es cuanto la ejecución de la medida establecida en el artículo 10° Intervención de las comunicaciones, la medida se ejecuta mediante la grabación, registro, custodia, transcripción de comunicaciones de alto valor de confidencialidad por su naturaleza, la que es manejada por un selecto personal policial y la autoridad Fiscal que lleva el caso.

En tal sentido de lo expresado, se debe tener conciencia de la labor delicada del grupo humano que realiza una labor cautelosa y anónima en la lucha con el crimen organizado; es por esta razón que el tipo de información que se almacena y los procedimientos de emisión de los registros en una base de datos deben contar con la seguridad debida y en una mejor medida contar con un estándar de calidad internacional.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

La norma ISO 27001, es de gran importancia en el ámbito de la seguridad de la información, esta define las buenas prácticas asociadas a la gestión de la seguridad de la información y proporciona un marco para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad (SGSI). Como objetivo principal del ISO 27001 es garantizar la confidencialidad, integridad y disponibilidad de la información, protegiéndola contra posibles amenazas y vulnerabilidades. Aunque no es obligatorio certificar un SGSI, es altamente recomendable hacerlo. La certificación ISO 27001 es un reconocimiento formal que garantiza que la organización ha implementado un SGSI alineado con los requisitos de la norma. Además, la certificación puede ser una ventaja competitiva para la entidad, ya que mejora la confianza de los clientes, en este caso del Ministerio Público y los grupos operativos de la Policía nacional del Perú, que se encuentran interesados en la capacidad de la DIVATJ en mantener protegida la información obtenida por la interceptación de legal de las comunicaciones, siendo el objetivo principal de su implementación la gestión de los riesgos.

Implementar el ISO 27001, SGSI, permite a la DIVATJ identificar y evaluar los riesgos de seguridad de la información y establecer medidas para minimizarlas y tratarlas adecuadamente, lo que proporciona un marco garantista de seguridad de la información y protegerla contra posibles amenazas y vulnerabilidades.

En la actualidad el DIVATJ, cuenta con una Certificación ISO 9001-2015 Norma internacional de Sistema de la gestión de la Calidad, lo que garantiza la mejor

satisfacción, y demuestra ser una entidad pública confiable, a los servicios brindados al Ministerio Público y grupos de investigación de la Policía Nacional del Perú.

Las entidades públicas actualmente deben tener un compromiso mayor en la era de la información y comunicación; por el tipo de activos que se cuenta en el DEPATJ, y ser reconocida como una entidad proyección a la excelencia, se ve por necesario seguir innovando es por ello que se propone la Aplicación de un Sistema de Gestión de la Seguridad de la Información bajo la norma ISO 27001:2013, para las actividades operativas y administrativas; importancia radica que las informaciones que se almacenan deben protegerse como lo más importante de la organización a fin de evitar riesgos de ataques, vulnerabilidades de factores internos y externos basados en principios de disponibilidad, integridad y confidencialidad. Pues a falta de apoyo y tiempo no pueden ser excusa para no avanzar a un desarrollo del sistema de gestión de seguridad, puesto que en términos económicos es costosa; sin embargo, la inseguridad puede serlo mucho más. (Ladino, M., Villa, P., y López, A. 2011, pp 334).

Como se ha expresado en los párrafos anteriores el producto obtenido por intervención legal de las comunicaciones, es un bien físico que será utilizado para esclarecer un hecho delictivo por lo cual su uso en materia judicial tiene un valor de prueba material que sumado a otras técnicas de investigación, son indispensable al Juez para optar por una sanción adecuada y ejemplarizadora; por lo tanto, es determinante en una sanción de privativa de libertad; tener una certificación ISO 27001 que garantice un archivo de texto y audio sin vulneraciones, evita cuestionamientos por

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

que garantiza una información basada en principios de confidencial, disponibilidad e integridad.

Para su mejor apreciación en el presente trabajo de investigación está compuesto por el Capítulo I Antecedentes de Estudio, Capitulo II Marco Teórico, Capitulo III Marco Referencial, Capitulo IV Resultados y concluyendo con el Capitulo V Sugerencias y Recomendaciones; donde se presentará los argumentos adecuados y contundentes para mejorar la calidad de los servicios y ser una entidad de excelencia.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

1 CAPITULO I: ANTECEDENTES DE ESTUDIO

1.1 Título del Tema

PROPUESTA DE MEJORA EN EL DISEÑO DE GESTION DE SEGURIDAD DE LA INFORMACIÓN NORMA ISO 27001:2013, PARA LAS ACTIVIDADES OPERATIVAS Y ADMINISTRATIVAS DE LA DIVISIÓN DE APOYO TÉCNICO JUDICIAL DE LA DIRECCIÓN ANTIDROGAS DE LA POLICÍA NACIONAL DEL PERÚ.

1.2 Planteamiento del Problema

El División de Apoyo Técnico Judicial de la Dirección Antidrogas de la Policía Nacional del Perú (DEPATJ), es unidad que pertenece a la Dirección Antidrogas de la Policía Nacional del Perú (DIRANDRO), que se encarga de realizar la interceptación legal de las comunicaciones en tiempo real brindando apoyo en la materia funcional al Ministerio Público y a Grupos Operativos de investigación, Divisiones de Investigación de Alta Complejidad y a las Divisiones de Investigación Criminal, que se encuentran a nivel nacional, sus integrantes son funcionarios con un alto nivel confiabilidad, discreción, profesional y comprometido en realizar actividades que conllevan a la manipulación de información sensible.

Considerando el servicio que brinda la DIVATJ, produce productos físicos, pueden ser vulnerados desde su obtención por parte de los analistas que puedan obtener un beneficio el cual por su naturaleza puede poner en riesgo las operaciones policiales donde se esté utilizando la herramienta de investigación lo que generaría un déficit de intervenciones aumentando la criminalidad; por otro lado, le brinda seguridad al Representante del Ministerio Público que la información obtenida durante el

desarrollo de la actividad de escuchas legales, esta no va ser modificada y llegue de forma veras y autentica al despacho fiscal; en tal sentido este trabajo permitirá aceptar que el activo más importante para toda organización es la información que posee, por tal razón se debe de garantizar la integridad, confidencialidad y disponibilidad (Lema, R., & Donoso, D., 2018), de la información que se almacena en los activos (Hardware – Software) de la Oficina de Sistemas de la DIVATJ, Según (Calder, 2017) afirma que “el ciber riesgo se ha convertido en un problema empresarial serio, con la alta gerencia cada vez más bajo presión, por parte de clientes, reguladores y socios, para garantizar que su organización puede defenderse, responder y recuperarse de un ciberataque.”(p. 9)

La DIVATJ, planifica y monitorea sus actividades, sin embargo, ciertas deficiencias son observados en procesos y procedimientos (en los cuales el público exige que la información requerida por los despachos judiciales y de investigación no sean vulneradas por agentes internos o externos). En este sentido, Calder, A. (2017) indica que “la seguridad de la información es ahora también claramente un problema de gestión y una responsabilidad de la gobernanza.” (p. 10)

Un sistema de gestión de Seguridad de la información (SGSI), permite que la empresa e instituciones conozcan los riesgos a los que se encuentra expuesto sus activos informáticos lo que permite realizar normativa interna establecidos en directivas. Estos documentos se encuentran disponibles para los integrantes de la dirección y los colaboradores, quienes constantemente deben ser expuestos a mejoras continuas. (Monzó, 2020).

A nivel metodológico, la investigación se reviste de importancia por que en ella se

evidencia el fiel cumplimiento de los procesos científicos para el desarrollo de una investigación, el cual servirá como guía para otros estudios a realizar sobre la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), en el instituto policial.

El presente trabajo de investigación procura que se forme una doctrina actualizada en el cual sea materia de consulta, evaluación y futura implementación de una cultura de seguridad de la información en la División de Apoyo Técnico Judicial.

1.3 Objetivos de la Investigación

Objetivo General

Elaborar un diseño de mejora de Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma del ISO/IEC 27001: 2013, que será implementado para el control físico y digital de información y documentación que contenga información sensible, con finalidad de proponer un modelo de mejora en la administración de la información sensible que se custodia para el año 2022 con proyección al 2023.

Objetivos Específicos

- Realizar un análisis de brechas (GAP o Análisis de Necesidades) basados en norma ISO/IEC 27001:2013.
- Definir una metodología para la identificación, clasificación y valorización de los activos de información propensos a ser vulnerados.
- Establecer procesos de control físico y digital de documentos físicos y virtuales de los productos obtenidos durante el monitoreo de las escuchas

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

legales, así como identificar los riesgos asociados al control físico y digital de documentos.

- Generar políticas, protocolos y directivas internas necesaria para el mantenimiento del Sistema de Gestión de Seguridad de la Información, durante y después de las actividades control de las comunicaciones.
- Realizar un cronograma de capacitación en seguridad de la información.

1.4 Metodología

Se aplicará una metodología tipo no experimental en el presente trabajo de investigación debido a que se observara como la información obtenida de la interceptación legal de las comunicaciones, es convertida en los productos físicos, Actas, y en productos digitales, Archivos de Audio. Asimismo, se aplicará un diseño transversal, debido a que se observará a los analistas en todas las etapas durante la herramienta especial de investigación se encuentre activa, en el cual se estudiará durante el periodo 2022.

1.5 Población de Muestra

El estudio estará direccionado al personal que labora en el DIPATJ-DIRAND; la población es de doscientos tres (203) integrantes funcionarios, siendo repartido en tres grupos, la Dirección y el área administrativa conformados por 03 funcionarios, los jefes de área conformados por 16 funcionarios y el personal de Analistas Tácticos conformados por 184 funcionarios; debido que tienen acceso directo a la información sensible.

Para la obtener los mejores resultados se trabajará mediante encuesta se

realizará mediante la fórmula para el cálculo de la muestra en poblaciones finitas (Sánchez, M 2015), donde la muestra “N” será calculada mediante la siguiente formula:

$$N = \frac{N * (Z_{\alpha})^2 * p*q}{d^2 * (N-1) + (Z_{\alpha})^2 * p*q}$$

Donde:

- “N” es el Total de la población, para este caso equivale a doscientos tres (203) analistas tácticos.
- “Z_{α}” es el coeficiente de seguridad, del cual se aplicaría al 1.96, si la seguridad es del 95%.

  Según diferentes seguridades el coeficiente de “Z_{α}” varia:

  • Si la seguridad Zα fuese del 90% el coeficiente sería 1.645

  • Si la seguridad Zα fuese del 95% el coeficiente sería 1.96

  • Si la seguridad Zα fuese del 97.5% el coeficiente sería 2.24

  • Si la seguridad Zα fuese del 99% el coeficiente sería 2.576
- “P” equivale a la proporción esperada, en este caso 5% o 0.05.
- “q” equivale a la Unidad menos la proporción esperada. (1-p en este caso 1-0.05= 0.95)
- “d” equivale a la precisión, por lo que en esta investigación se hará uso del 5%.

En la aplicación de las variables en la formula antes descrita se obtiene que:

$$N = \frac{203 * (1.96)^2 * 0.05 * 0.95}{(0.05)^2 * (203-1) + (1.96)^2 * 0.05 * 0.95} = 53.84 \text{ analistas.}$$

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

La muestra equivale a cincuenta y tres punto ochenta y cuatro Analistas Tácticos, mediante un redondeo a cincuenta y cuatro (54) Analistas Tácticos a quienes se les aplicara la encuesta, lo que corresponde a 26.6% de la población de la División de Apoyo Técnico Judicial de la Dirección Antidrogas.

1.6 Técnica o Instrumento

La obtención de datos será obtenida mediante encuesta dirigida a cincuenta y cuatro (54) Analistas Tácticos que hacen uso el equipo de interceptación legal de las comunicaciones en las áreas de Oficina de Salas de Intervenciones y Oficina de Tecnología de la Información y comunicación.

Molano Espinel (2017) presenta un modelo de encuesta basada en tres categorías, siendo la primera el Conocimiento en Seguridad de la Información, las técnicas de protección de datos y seguridad de la información, y aplicación de herramientas para la protección de datos y seguridad de la información; en la cual busca identificar los riesgos y vulnerabilidades de una empresa, puesto que hoy en día el avance de la tecnología en el hardware, software, base de datos y redes se encuentran en constante evolución.

La encuesta está basada en la escala de Likert, el cual establecerá una evaluación objetiva de las reacciones, actitudes y comportamientos de los Analistas Tácticos, en el cual se utilizará la evaluación de cada pregunta en una escala del 1 al 5, siendo uno Totalmente Insatisfecho y siete totalmente satisfecho. siguiente escala:

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Figura 1

Escala de Likert – Grado de satisfacción

Grado de Satisfacción	Niveles
Excelente	5
Bueno	4
No Tiene Conocimiento	3
Muy deficiente	2
Regular	1

Fuente: Elaboración propia.

En tal sentido es necesario aplicar una encuesta que pueda esclarecer los tres parámetros de la seguridad de la información cuales son la integridad, confidencialidad y disponibilidad.

1.7 Justificación

El proyecto de mejora propuesta de mejora en el Diseño de Gestión de Seguridad de la Información bajo la norma ISO 27001:2013, para las actividades operativas y administrativas del División de Apoyo Técnico Judicial de la Dirección Antidrogas de la Policía Nacional, es de gran relevancia para que se implemente mecanismos adecuados para identificar riesgos a medida que sean observados por los miembros de la entidad y se garantice un nivel de protección de datos en términos de confidencialidad, integridad y disponibilidad (Nieves, 2017).

Con la investigación y el análisis relacionado se busca conocer las debilidades de las tecnologías de la información, se plantea detectar de manera temprana vulnerabilidades en el sistema DIVATJ; lo que reduce riesgos de un posible ataque

cibernético en su infraestructura digital, siendo necesario desarrollar un plan de contingencia por medio de políticas de seguridad de la información; además, desarrollar nuevas doctrinas de seguridad entre los integrantes de la División de apoyo técnico judicial.

El aporte social del presente proyecto de mejora se relaciona en generar la creación de ideas, políticas y principios básicos de la Seguridad de la Información para los integrantes del DIVATJ-DIRANDRO.

En la Escuela de Postgrado NEWMAN, adquiere información relevante y precedente de un trabajo de investigación nuevo e interesante; que se enfoca en una función no explorada por ser el DIVATJ parte de un grupo especial y con altos estándares de confidencialidad. Conteniendo el presente una base teórica nueva y original.

En tal sentido, la implementar un Sistema de Gestión de Seguridad de la Información, basado en el ISO/IEC 27001:2013; proporcionará las condiciones necesarias que respalde y amplie los objetivos estratégicos de la entidad, y garantice una gestión operativa y administrativa de la División de Apoyo Técnico Judicial. (Nieves, 2017)

Asimismo, obtenida la información se podrá enfocar cuales son los riesgos y debilidades actuales; a fin de contribuir en brindar un mejor servicio al Ministerio Público y grupos operativos diversos que hacen uso de la técnica especial de investigación, interceptación legal de las comunicaciones.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

1.8 Principales definiciones

Se presenta las definiciones más resaltantes relacionadas al tema de investigación:

1.8.1 Seguridad de la información

Según Valencia, F. y Orozco, M. (2017) indica que la seguridad de la información se enfoca en la tecnología misma dentro de la infraestructura tecnológica utilizada para administrar la información dentro de una organización y como una herramienta estratégica para tomar decisiones empresariales acertadas en las organizaciones actuales.

1.8.2 Seguridad informática

En palabras de Valencia, F. y Orozco, M. (2017) menciona que la seguridad de la información en sí misma es el activo estratégico de la organización, y su función se encuentra sobre los elementos de las tecnologías de la información y comunicación.

1.8.3 Sistema de gestión de la seguridad de la información SGSI

La gestión de la seguridad de la información, según (López, s.f.), consiste en preservar su confidencialidad, integridad y disponibilidad, de los documentos digitales y físicos dentro de una organización. En este sentido los tres términos constituyen la base que sedimenta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se proporcionará ni divulgará información a personas, organizaciones o procesos no autorizados.
- Integridad: es el mantenimiento de la exactitud e integridad de la información y su

procesamiento.

- Disponibilidad: acceso y uso de la información, así como los sistemas de procesamiento y utilizarla cuando sea necesario.

1.8.4 ISO 27001

El estándar internacional publicado por la Organización Internacional para la Estandarización (ISO) describe la gestión de la seguridad de la información dentro de una empresa. La revisión más reciente de esta norma se publicó en 2013 y su nombre completo ahora es ISO/IEC 27001:2013.

La primera evaluación se publicó en 2005 y se desarrolló sobre la base de BS 7799-2. El ISO 27001 se puede implementar en cualquier tipo de regulación, en entidades privadas o públicas, que propone una metodología para implementar la gestión de la seguridad de la información en una organización. Su aplicación permite a la entidad pueda obtener un certificado; significando que un organismo de certificación independiente confirma que la seguridad de la información se ha implementado en esta organización de acuerdo con el estándar ISO 27001.

1.8.5 Análisis de Riesgo

Es el proceso cuantitativo o cualitativo que ayuda a evaluar el riesgo. El primer paso en el análisis es decidir qué activos deben protegerse o valorarse. La evaluación de riesgos es comparar el nivel de riesgo que se descubrió durante el proceso de análisis con estándares de riesgo previos. La función de evaluación incluye un nivel razonable de consenso sobre los objetos mencionados anteriormente y para garantizar el nivel mínimo para ayudar a desarrollar indicadores operativos de medidas y

evaluación. Los resultados obtenidos del análisis permitirán la aplicación del tratamiento de riesgos más adecuado donde se ve incluida la identificación y evaluación de opciones que existen para abordar los riesgos y la preparación e implementación de un plan para tratar los riesgos.

En el tema del análisis de riesgos, se reflejan los cinco conceptos importantes como la probabilidad, amenaza, vulnerabilidad, activo e influencia (Nieves, 2017).

1.8.6 MAGERIT

Es una metodología creada por el Centro Nacional de Inteligencia, corresponde a un Procedimiento Informático Lógico para el Análisis de Riesgos esta es una herramienta desarrollada para el análisis y la gestión de riesgos del sistema de información. Se basa en analizar las siguientes dimensiones (Molina, 2017):

- Confiabilidad
- Integridad
- Disponibilidad
- Autenticidad
- Trazabilidad

1.8.7 Ciclo de mejora continua en la Norma ISO/IEC 27001:2013

La mejora continua de las organizaciones, entidad pública, se desarrollan procesos orientados a maximizar la calidad de bienes o el servicio, debiendo existir un nexo durante todo el desarrollo de la ejecución, por ello es necesario la aplicación de la cultura de calidad de Kaizen en el cual es necesario aplicar el ciclo PDCA (Plan, Do-Hacer, Check-Controlar, Act- Actuar). (Yenque, 2002)

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

1.8.8 Activo

Es definido como: cualquier bien que tienen valor para la organización, es decir estos activos relacionados con sistemas de información. Se ejemplifican en los datos, el hardware, el software, servicios, documentos, edificios y recursos humanos.

1.8.9 Impactos

Las consecuencias de la ocurrencia de las distintas amenazas son siempre negativas. Las pérdidas generadas pueden ser financieras, no financieras, de corto plazo o de largo plazo.

1.8.10 Amenazas

Las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc.

1.8.11 Gestión del riesgo

Actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

1.8.12 Vulnerabilidad

Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades son propensas a aparecer en cualquier elemento de hardware o software. (Emilio, 2015)

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

1.9 Alcances y limitaciones

El alcance estará dirigido a los funcionarios que integran el DIVATJ-DIRANDRO.

Para el presente trabajo de investigación se estableció los siguientes factores como limitantes a su desarrollo:

1.9.1 Factor económico

El trabajo de investigación será solventado por el propio maestrante debido a que la información que será recogida y evaluada pertenece a una organización pública donde se desempeña laboralmente.

1.9.2 Factor Tiempo

El trabajo de investigación al ser ejecutada por el maestrante cuenta con un límite de tiempo por ser reducido aproximadamente 06 meses para todo el proceso.

La información recogida será limitada al factor tiempo respecto a que para solicitar la esta debe presentar formalmente a la gerencia y esta será evaluada para recién obtener la autorización de datos.

1.9.3 Factor Éticos Morales

Los Analistas del DIVATJ-DIRANDRO, cuentan con altos estándares de confiabilidad y discreción, y por el manejo de la información sensible que cada uno de los integrantes obtiene no es posible la publicación de nombres de los encuestados que han participado en la investigación.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

1.10 Cronograma

Figura 2

Cronograma de actividades - Trabajo de investigación

Fuente: elaboración propia.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

2 CAPITULO II: MARCO TEÓRICO

2.1 Bases teóricas de las variables y/o tópicos

2.1.1 Seguridad de la información.

En la actualidad la tecnología de la información se encuentra en un punto de avance, se vive la etapa en la que la humanidad ha alcanzado un desarrollo imprevisible; cada día son mayores las diferencias sociales, políticas y económicas (Quiroga, 2002). Se aprecia que actualmente el activo más valioso de una empresa, institución pública es la información almacenada en su sistema de almacenamiento.

En palabras de Valencia, F. y Orozco, M. (2017) menciona que la seguridad informática, hace referencia a la seguridad de la información, se relaciona con la información en sí misma, como activo estratégico de la organización, y su función se encuentra sobre los elementos técnicos que hacen parte de las tecnologías de la información y comunicación.

Por otro lado, Areitoi, J. (2008) menciona que la seguridad de los datos clasificados del gobierno en el ámbito militar o diplomáticos, al tener una dimensión inimaginables y crecientes que incluye varios ámbitos y en especial la información personal e inteligencia, por ello, es imprescindible que las necesidades de seguridad potenciales sean tenidas en cuenta. En ese sentido la seguridad abarca el desarrollo, la integración, la operación, la administración, el mantenimiento y la evolución de los sistemas y aplicaciones, es todo el ciclo de vida de los productos o unidades de negocio.

Entonces, Areitoi, J. (2008, p.2) concluye que la seguridad de los sistemas de información es una disciplina la cual su meta primigenia en una organización cumpla

con todos sus objetivos relacionados con la misión de la entidad, implementando sistemas que tengan especial cuidado y consideración hacia los riesgos relativos a las tecnologías de la información y comunicación.

Ahora es necesario definir el termino Información; a través de la revisión del estudio según Fernandez & Piattini (2012) indica que información consiste en el conjunto de datos organizados en poder de una organización que poseen valor para la misma, independientemente de la forma en la que se guarde o retrasmita su origen o fecha de elaboración. Es por ello, que la implementación de mecanismos administrativos adecuados es necesaria para su tratamiento brinde al público interno y externo la confianza que la información adquirida no sea vulnerada.

Según Melo, V., & Hernando, A. (2008 p. 336), menciona que la información en la actualidad no solo es un activo valioso, por lo contrario, es un bien estratégico en las organizaciones, la misma que debe ser protegida de muchas maneras, como la encriptación que otorga a estos atributos de confidencialidad, integridad y autenticidad. Asimismo, en esta deben intervenir diferentes disciplinas como la informática, la gerencial, la logística, la matemática y la jurídica.

2.1.2 Política de seguridad de la información.

Para dar inicio la gestión de la seguridad de la información dentro de una organización, se debe formular políticas de seguridad, que como objetivo es brindar apoyo y orientación a la alta dirección respecto a la seguridad de la información los cuales deben estar ligados a los reglamentos y leyes vigentes. (Melo, V. & Hernando, A. 2008).

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

2.1.3 Sistema de Gestión de Seguridad de la Información (SGSI).

A fin de comprender que es el SGSI, es necesario entender que las tecnologías de la información y comunicación son recursos necesarios y primordiales para la productividad y competitividad de las organizaciones, y como otros recursos están sujetos a múltiples amenazas que se materializan en riesgos con múltiples consecuencias. (Valencia, J. y Orozco, M. 2017).

Una definición actual de la SGSI explicada por Hamdi, Z., Anir Norman, A., Nuha Abdul Molok, N. & Hassandoust, F. (2019), determinan que es un conjunto de políticas y métodos que utiliza la administración para proteger la seguridad de la información en sus actividades diarias de la organización. Y está basada en una correcta evaluación de los riesgos y vulnerabilidades, además en su estructura más sencilla se planifica mediante el ciclo PDCA

Plan: diseño de SGSI

Hacer: Implementar y Operar SGSI

Comprobar: Seguimiento y revisión del SGSI

Actuar: Mantener y mejorar el SGSI.

Para Blumsztein, E. C. (2007), la SGSI se encarga de controlar, difundir y evaluar en forma continua el avance de las actividades necesarias para su implementación estableciendo cuatro dimensiones: la primera enfocada al cronograma de proyecto de seguridad de información, la segunda enfocada al cronograma de desarrollo de procedimiento de seguridad corporativa, la tercera debe cumplirse el plan

de auditoría de sistema de información y por ultimo determinar los indicadores de tiempo de respuesta y cantidad de consultas de seguridad de información.

El SGSI es una actividad, según Montaño, V. (2010) que tienen por propósito no exactamente asegurar la seguridad debido a que esta no es absoluta, pero si reducir los riesgos con la finalidad que estos sean conocidos, asumidos, gestionados y minimizados por la institución. La documentación de la actividad debe ser registrada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías.

2.2 Metodología para la Implementación de un Sistema de Gestión de Seguridad de la Información.

Según, Valencia, J. y Orozco, M. (2017), explica que existen diversas formas de realizar la implementación de un SGSI en una organización y para ello se debe realizar en forma sistemática para cumplir con los elementos necesarios e indispensables; esta metodología contempla cinco fases secuenciales, los cuales a partir de un proyecto donde se incorporan personas, recursos y tiempo con autorización de la alta dirección de la organización; siendo este requisito indispensable para cumplir con los requisitos exigidos para cumplir el objetivo.

2.2.1 Fase 1: Aprobación de la Dirección para iniciar el proyecto.

En palabras de Ladino, M. I., Villa, P. A., & López, A. M. (2011), es la primera y tal vez la más importante, es el conocimiento de los Altos Directivos e informar cuales serían los escenarios de riesgo que puede suceder si no se implementa el Sistema de Gestión de seguridad de la información y cuáles serían las pérdidas económicas y

otras. Además, de que esta tarea sea supervisada por el jefe del área de sistemas de la organización.

Para cumplir este propósito es necesario subdividir en otras actividades como:

- Establecimiento de las prioridades de la organización para desarrollar un SGSI.
- Definir el alcance preliminar del SGSI
- Creación del plan del proyecto para ser aprobado por la Dirección.

2.2.2 Fase 2: Definir el alcance, los límites y la política del SGSI

Definición del alcance: La importancia que tiene el establecimiento del alcance está fundamentada en que permite delimitar el proceso de gestión de riesgos y, por ende, pone foco a todo el proceso de implementación del SGSI. (Ladino, M. I., Villa, P. A., & López, A. M. 2011)

Definición de la política y objetivos de seguridad: De acuerdo con Diaz (2010) la política de seguridad refleja lo que la organización quiere hacer con respecto a la seguridad de la información, los objetivos que pretende conseguir, contemplando los requisitos legales y reglamentarios aplicables y teniendo en cuenta el compromiso de la Dirección para conseguirlos.

Aprobación de la Dirección: Una de las formas de demostrar el apoyo de la Dirección de manera inicial, es la aprobación que ella da a las políticas y objetivos del SGSI dentro del alcance Valencia, J. y Orozco, M. (2017)

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

2.2.3 Fase 3: Análisis de los requisitos de seguridad de la información

De lo expuesto por Valencia, J. y Orozco, M. (2017) y de acuerdo con lo establecido en la norma ISO 27003, para establecer estos requisitos es necesario cumplir con el desarrollo de los cinco elementos:

1. Identificar los activos de información importantes.
2. La visión de la organización y sus efectos sobre los requisitos futuros de procesamiento de información.
3. Las formas actuales de procesamiento de información (aplicaciones, redes, la ubicación de las actividades y recursos de TI).
4. Requisitos legales, reglamentarios, obligaciones contractuales, normas de la industria, acuerdos con clientes y proveedores, condiciones de pólizas de seguros, etc.;
5. El nivel de toma de conciencia sobre seguridad de la información y los requisitos de formación y educación en seguridad.

2.2.4 Fase 4: Valoración de riesgos y planificar el tratamiento de riesgos

Al respecto se deben tener en cuenta las siguientes sub-fases, las mismas que propone Valencia, J. y Orozco, M. (2017).

Establecimiento de contexto, en esta fase se considera los elementos que se requiere en el en el proceso SGSI, partiendo del contexto, alcance, políticas, objetivos y parámetros de evaluación de riesgo.

- Parámetros de probabilidad, estos deben establecer la frecuencia de la

posible ocurrencia de las amenazas, con los niveles requeridos por la organización.

- Parámetros de impacto, la amenaza no solo se mide respecto al monto económico sino a los diferentes eventos que surgen en la organización y pueden llegar a afectarla en su conjunto.

Determinación de la vulnerabilidad Valencia, J. y Orozco, M. (2017), establecen que para determinar qué tan importante es el riesgo deben establecer una medida para estimar el impacto. La vulnerabilidad se mire en términos matemáticos porcentuales y en función a las variables de probabilidad e impacto, y para ello se utiliza la siguiente formula: VX = (P × I)/ max (P × I); Donde VX es la vulnerabilidad del escenario de riesgo X, P es la probabilidad de ocurrencia e I es el impacto.

Criterios de aceptabilidad del riesgo, La mayor dificultad que existe para determinar las condiciones de seguridad de una organización, se fundamenta en el hecho de establecer los parámetros de aceptabilidad del riesgo, debido a la coincidencia de múltiples intereses, así como la evaluación hecha por personas con diferentes niveles de conocimientos, experiencia y “emotividad”, lo que genera diversas percepciones sobre el mismo (Duque, 2017).Explicado por Vanegas, A., y Pardo, C. J. (2014), determinar los riesgos en forma coherente es una actividad que está a cargo del equipo SGSI y la Alta Dirección de la organización.

Valoración del riesgo, en concordancia con lo que establece la norma ISO/IEC 27005:2009 contempla tres fases: identificación de los escenarios de riesgo, estimación del riesgo y evaluación del riesgo.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

- Identificación de escenarios de riesgo: la intención de identificar los riesgos es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida (ICONTEC, 2009).
- Estimación del riesgo: Para estimar el riesgo, se pueden llevar a cabo análisis cualitativo, semicuantitativo o cuantitativo, o bien, una combinación de los tres (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016).
- Evaluación del riesgo, la evaluación de riesgos implica comparar las vulnerabilidades creadas por cada riesgo y compararlas con la aceptación del riesgo. (Vanegas, A., y Pardo, C. J. 2014)
- Tratamiento del riesgo, La fase de tratamiento de riesgos identifica las acciones que es necesario desarrollar utilizando los controles propuestos para lograr un nivel de riesgo aceptable para la organización. Para ello, se debe priorizar el resto de los riesgos. Según criterios de aceptabilidad, priorizando aquellos con mayor nivel de vulnerabilidad. Es importante recordar que la elaboración de un plan de gestión de riesgos requiere de un análisis de costo – beneficio de los controles a realizar y del presupuesto asignado para su elaboración, por lo que es importante para la organización.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

2.2.5 Fase 5: Diseñar el Sistema de Gestión de Seguridad de la Información (SGSI)

Según Valencia, J. y Orozco, M. (2017), refieren que el diseño del SGSI considera tres componentes: La documentación que debe tener el sistema, la implementación de los controles previstos en el plan de tratamiento de riesgos y el monitoreo constante de la seguridad de la información.

Documentación del sistema: La información documentada que debe tener un SGSI comprende los requisitos contemplados en la norma ISO/IEC 27001, los cuales surgen a partir de la implementación de sus diferentes fases.

Implementar el plan de tratamiento de riesgos: La aplicación del plan de tratamiento de riesgos debe ser autorizado por la alta dirección con los recursos asignados para tal fin, y el mantenimiento de los controles existentes, es lo que permite garantizar niveles aceptables de seguridad de la información en la organización; pues es alli donde inicia el control de los ecesanios de riesgos.

Monitoreo de la seguridad de la información: lo establece la norma ISO/IEC 27001:2013, la evaluación del desempeño del SGSI se realiza a través de la supervisión, medición, análisis y evaluación del sistema; las auditorías periódicas y la revisión por la Dirección. (Nieves, A. C. 2017).

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

2.3 Proceso de certificación

Al termino de la implementacion de un SGSI en una institucion, esta solicita la auditotia a la empresa certificadora según lo expuesto por Ladino, M. I., Villa, P. A., & López, A. M. (2011), que a su vez de desarrollaran cuatro fases:

- Pre-autoria, la cual es opcional, sin embargo ayuda a recoger información sobre el estado de organización, a fin de ser utilizado en la auditoria real.
- Fase 1, Auditoria, en esta etapa se desarrolla el analisis de la documentación obtenida y estará a cargo del Auditor Jefe e inicia la preparación del Informe de la documentación básica de SGSI de la entidad solicitante. Para la siguiente etapa debe transcurrir seis meses.
- Fase 2, Auditoria, en esta fase se revisa las políticas, la implementación de controles de seguridad y la eficacia de los controles en su conjunto. Se realiza una revisón de las exclusiones según ña declaracion de aplicabilidad, hallados en la Fase 1, el resultado es el informe de la auditoria.
- Certificación, si durante la auditoria se observase anomalias graves, la institución debera implementar acciones correctivas o una vez verificado la implementación y no haberse constatado inconformidades, el auditor emite el informe favorable y el SGSI de la organización sera certificado según ISO 27001.

2.3.1 Organización Internacional de Normalización (ISO)

Las siglas ISO (INTERNTIONAL ORGANIZATION FOR STARDARDIZATION) es la Organización Internacional de Normalización es una norma técnica internacional que contribuye a que el desarrollo de la producción y el suministro de

bienes y servicios sean más eficaces (FUNDIBEQ, s.f.) ; esta contribución genera que las entidades tengan altos estándares de calidad reflejados en los productos y servicios que brinda.

Según lo indicado en Montaño, V. (2010) el ISO es un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información, presentando una relación de los tipos de ISO, los cuales son:

ISO 27000: Contiene términos y definiciones que se emplean en toda la serie 27000.

ISO 27001: Contiene la estructura y requerimientos para la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

ISO 27002: Establece y describe los objetivos de control y controles recomendables a tener en cuenta para la construcción de un adecuado SGSI.

ISO 27003: Contiene una guía de implementación de SGSI acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.

ISO 27004: Especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y efectividad de la implantación de un SGSI y de los controles relacionados.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

ISO 27005: Consiste en una guía para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI.

ISO 27006: Especifica el proceso de acreditación de entidades de certificación y el registro de SGSI.

En tanto, los ISO, expuestos son de relación directa con el ISO 27001, a fin de su implementación enfocado con objetivo del control de la Tecnología de la información de alto nivel donde las tareas estén dentro de los dominios: Planificar y Organizar, Adquirir e Implementar, Entrega y soporte, y Monitoreo y Evaluación; en el cual Montaño, V. (2010) aplica la versión COBIT 4.1 distribuidos en los dominios expuestos, dentro de estos se encuentran distribuidos 34 procesos que contiene 310 actividades de control.

2.3.2 ISO 27001

La norma ISO 27001 ofrece los requisitos básicos para implementar un Sistema de Gestión de Seguridad de la Información. Debe entenderse que la seguridad de la información consiste en la preservación de la confidencialidad, integridad y disponibilidad de los datos como el activo más importante, según Coello, R. R., y Pico, L. M. (2018). Además, los sistemas que se encuentren implicados en su tratamiento, dentro de la institución cual lo custodia.

Según lo expone Ladino, M. I., Villa, P. A., & López, A. M. (2011), la norma ISO 27000 es certificable, esto indica que una empresa o institución puede solicitar la

auditoria a fin de obtener un certificado para lo cual debe contar con un sistema de gestión de seguridad de información implementado.

Lo mencionado para Hamdi, Z., Anir Norman, A., Nuha Abdul Molok, N. & Hassandoust, F. (2019), que esta norma de la serie ISO 27000 se aplica en varios países e industrias, debido a que es un estándar de gestión y evaluación de procesos y consta de dos partes importantes, la primera proporciona los requisitos necesarios para la implementación del SGSI: mantenimiento y mejora; mientas una segunda parte direccionado a los objetivos de control, así como a los controles de seguridad. Como dato adicional en la última encuesta del 2017, por el Foro Internacional de Acreditación, la certificación del ISO 27001 a aumentado en un 7.9% a nivel mundial.

Para la implementación de la norma ISO 27001, Coello, R. R., y Pico, L. M., recomiendan que se debe seguir las siguientes recomendaciones:

- Mantener la sencillez y restringir el alcance; dentro de la institución las áreas involucradas deben dar alcances de forma gradual en las diferentes fases de planear-hacer-verificar y actuar.
- Comprender los detalles que tiene el proceso de implementación; realizar consultas a especialistas a fin de adquirir experiencias y adquirir formación para su implementación y sostenimiento.
- Gestionar el proyecto fijando los diferentes objetivos y posibles resultados.
- La autoridad y el compromiso de la dirección, con la implementación de una nueva filosofía organizacional de la seguridad de la información fundamental de la norma ISO 27001.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

- La certificación como objetivo; la visión de la obtención del certificado fortalece al equipo con un objetivo claro y tangible del trabajo elaborado.
- No inventarse nada, los datos utilizados en el desarrollo de la actividad de búsqueda de certificación deben ser reales expresados en las actividades propias de la institución.
- Pueden ser otros sistemas de gestión también implementado como ISO 9001, ISO 14001, etc. La implementación de otros ISO puede resultar útil puesto que implica que se tiene un conocimiento de como implementar de manera adecuada el ISO 27001.
- Reservar la dedicación necesaria al día o a la semana; el equipo de trabajo se involucra en el proyecto y realiza un trabajo en sinergia.
- Registrar las evidencias, el tiempo adecuado para observar los avances de la actividad de obtención de certificación se evidencia en los tres siguientes meses antes de la realización de la auditoria. Lo que demuestra que el el Sistema de Gestión de Seguridad de la Información funciona de forma óptima.
- Mantener y mejorar de forma continua, Es necesario considerar el mantenimiento y la mejora del Sistema de Gestión de Seguridad de la Información.

2.3.3 Dominios del Ciclo de la Seguridad para la Norma ISO 27001

Para Melo, V., & Hernando, A. (2008), expone que para pretender establecer un ciclo de seguridad lo más completo posible lo cual propone diez dominios que serían necesarios para su realización siendo estos:

1. Política de Seguridad de la Información.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

2. Organización de la Seguridad de la Información.

3. Gestión de Activos.

4. Seguridad de Recursos Humanos.

5. Seguridad Física y del Entorno.

6. Gestión de Comunicaciones y Operaciones.

7. Control de Acceso.

8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

9. Gestión de Incidentes de la Seguridad de la Información.

10. Cumplimiento.

Y estos dominios deben estar compuestos por subdominios y sus correspondientes controles dentro de un modelo PHVA (Planificar-Actuar-Verificar y Actuar).

2.4 Análisis comparativo de las bases teóricas

Es preciso mencionar que al instalar un Sistema de Gestión de seguridad de la información en las organizaciones se ha vuelto necesario debido a que los riesgos de la tecnología de la información; sea esta información durante mucho tiempo se considera importante y valioso, por la facilidad de la toma de decisiones de la Alta Dirección. Mantener esta seguridad debe contar con protección física y lógica de los sistemas y equipos es indispensable que se cuente con métodos reconocidos. (Molina, M. 2017)

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Para la aplicación de la un método idóneo a utilizar en el análisis y gestión de riesgos de la seguridad de información, en bases de mecanismos de identificación de activos, vulnerabilidades, en función de probabilidades, variable de medición de riesgo y calculo basándose en las ISO 27001, 27002 y 27005; se propone realizar una comparación entre la Metodología de Análisis y Gestión de Riesgos de los sistemas de información (MAGERIT) y la Metodología para el análisis y la gestión de riesgos **(**Risk Analysis and Management Method - CRAMM). (Cordero, K. 2015).

2.4.1 El riesgo, la gestión de riesgo y el análisis y evaluación de riesgo

Según, Lema, R. & Donoso, G . (2018 p. 10), define el riesgo como una conbinacion de las conseceuncias que se presentarían despues de un evento indeseado; por otro lado, la gestion de riesgos es el requisito principal para una correcta implementacion del un SGSI, en esta etapa se construye el modelo de seguridad donde se presentan los activos y su jerarquia; y tambien todo aquello que pueda ocurrir y tenga impacto sobre ello y la organización. Por ultimo, el análisis y evaluacion del riesgo permite determinar el valor de los activos información, en este punto se identicica la amenza y vulneabidad latente, controles existentes y sus defectos en el riesgo, se determina las concecuencias potenciales, se prioriza los riresgos y se clasifica frente a criterios de evaluación.

A continuación, se explicará brevemente las metodologías de mayor relevancia en para un proceso de análisis en la gestión de riesgos.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

2.4.2 MAGERIT: Metodología de Análisis y Gestión de Riesgos de los sistemas de Información.

MAGERIT es una metodología española para implementar un sistema de gestión de riesgos derivados del uso de tecnologías de la información, como parte del gobierno de las Tecnologías de la información. (Magerit, 2012).

MAGERIT es una metodología más utilizada que permite el análisis de riesgos de los sistemas de información, esta fue desarrollada por el Consejo Superior de Administración Electrónica para minimizar riesgos de la implantación y uso de tecnologías de la información; asimismo, proporciona principios básicos y los requisitos mínimos para la protección de la información. (Molina, M. 2017).

Según, Molina, M. (2017), presenta que este método se puede resumir en:

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio o coste supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Para Cordero, K. (2015 p. 24) el cálculo del riesgo en MAGERIT es la media del daño probable sobre un sistema en el cual conociendo el impacto sobre el activo y determinando su frecuencia es posible determinar si se tiene un riesgo acumulado o un riesgo repercutido.

El riesgo acumulado se calcula para un activo teniendo en cuenta sobre un activo debido a una amenaza y la frecuencia de la amenaza.

El riesgo repercutido, es el cálculo sobre cada uno de los activos, por cada amenaza y cada dimensión de valorización, teniendo como función del valor propio, la degradación causada y la frecuencia de la amenaza.

La fórmula considerada para determinar el riesgo se determina por:

RIESGO = VALOR DEL ACTIVO X VULNERABILIDAD X IMPACTO

MAGERIT, al basarse en el dominio de administración de recursos de la norma ISO 27001, se debe formular un inventario del software y hardware; así como las redes internas y externas de la organización. (Cordero, K. 2015)

2.4.3 Ciclo de Deming.

Implementar un SGSI implica más que simplemente instalar equipos de seguridad o contratar una empresa especializada para implementar controles y monitorearlos. ISMS integra varias estrategias, estructuras organizacionales, procesos, reglas, registros y más. Juntos, forman un sistema que se mejora continuamente para lograr el mejor nivel de protección de la información. (Robles & Rodriguez de Roa, 2016).

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Por ello, es que las normativas relacionadas a la seguridad de la información, como son la familia de normas ISO/IEC 2700x, contemplan un marco de referencia conocido como Modelo del PDCA (Planificar-Hacer-Evaluar-Corregir); modelo popularizado por W. Edwards Deming, como el “Ciclo Deming”, con el propósito de lograr este objetivo. Es un modelo relacionado a la gestión de la calidad ISO 9001 (Robles & Rodriguez de Roa, 2016).

Como se puede apreciar la metodología MAGERIT, es una actividad formal para el análisis y gestión de riesgo, creada con el fin de sensibilizar a todos los responsables de los sistemas de información de una organización sobre los riesgos y la necesidad de prevenir situaciones adversas.

2.4.4 CRAMM: (Risk Analysis and Management Method) Metodología para el análisis y la gestión de riesgos.

Esta metodología de análisis de riesgo fue desarrollada por el Centro de Informática y la Agencia Nacional de Telecomunicaciones del Gobierno del Reino Unido en 1987. La versión vigente es la 5.2. (Huerta, A. 2012)

Según Huerta, A. (2012) la metodología CRAMM se direcciona al análisis y gestión del riesgo orientado a salvaguardar la confidencialidad, integridad y disponibilidad de un sistema además de sus activos.

Como mecanismo de identificación de activos CRAMM, permite identificar los componentes del sistema de información como el hardware, software, datos y activos de localización. Por otro lado, la valorización de los activos físicos se determina por su costo de reemplazo, datos y activos de software en términos del impacto que sufre la

información si fuese disponible a cualquiera, destruida, divulgada o modificada. (Cordero, K. 2015).

2.5 Identificación de vulnerabilidades

Cordero, K. (2015), para determinar la identificación de vulnerabilidades se puede utilizar dos métodos el cualitativo y cuantitativo, el primero referido a las ideas, entrevistas con expertos, foros y debates con los involucrados, mientras el segundo asignando valores de probabilidad de ocurrencia.

2.5.1 Variable de medición de riesgo

Las variables que usa CRAMM para realizar la medición de los riesgos son la magnitud del daño y la probabilidad de las amenazas (Cordero, K. 2015).

2.5.2 Cálculo del Riesgo

Se basa en una evaluación activa y una combinación de los niveles de amenaza y vulnerabilidad obtenidos durante la identificación de la vulnerabilidad y la amenaza. Los cálculos de riesgo se realizan en una escala del 1 al 7, donde 1 es la línea de seguridad más baja y 7 la línea de seguridad más alta. (Huerta, A. 2012)

2.5.3 Alineación con el estándar ISO 27001

CRAMM al igual que el estándar antes mencionado realiza un inventario de activos de la información, sean estos software, hardware e infraestructura física que brinda soporte a las tecnologías de información y comunicación. Estos activos son claramente definidos y clasificados según sea por el sentido de su valor, la sensibilidad y criticidad a la organización (Huerta, A. 2012).

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Se puede concluir la metodología permite definir el marco de gestión de riesgo e identificarlo, así como a los propietarios de los riesgos, así como identificar respuestas adecuadas al riesgo e implementar respuestas a fin de obtener garantías de efectividad, monitorizar y revisar. Adicional a ello, se alinea con las normas ISO, tomando lo relevante de cada una de ellas.

2.6 Análisis crítico de las bases teóricas

El ISO 27001 ofrece un marco de gestión de la seguridad de la información en la organización, sin embargo, la información propia del conocimiento y experiencia de los involucrados debe ser tratado por diferentes medios como reuniones de trabajo; además no se debe centrar la atención en los sistemas informáticos ya que se podría dejar de atender y dejar sin protección otras actividades de la organización.

Cano, J y Almanza, A. (2020) indican que los cambios que se realizan en una organización que se relacionan a la seguridad de la información da inició con la toma de decisiones del área de tecnología de información respaldado por las Alta dirección, donde se asegura un referente técnico y operacional, y evoluciona con el tiempo, a una táctica y de riesgos clave, que le permite a la empresa comprender la exposición ante los riesgos.

En materia de la seguridad de la información los datos obtenidos de las personas naturales o jurídicas y son utilizadas por las organizaciones privadas y publicas deben contar con un sistema de gestión de la seguridad de la información cumpliendo con una norma ISO 27001, a fin de que no sean vulnerados, aplicados en principios de confidencialidad, integridad, disponibilidad y no repudio.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

La información es un recurso que se encuentra en el mismo nivel que los recursos financieros, materiales y humanos, ejes en los que había girado el mundo de las instituciones y organizaciones, sin embargo, su importancia en la actualidad se mantiene al mismo nivel de los clásicos elementos primarios como el capital, la tierra y el trabajo; siendo la información un cuarto recurso a gestionar. (Muñoz, A. 2003).

La versión COBIT 4.1 dispone de cuatro dominios: Planificar y organizar, Adquirir e implantar, Entrega y soporte, y Monitorear y evaluar; deben estar presentes durante todo el proceso de implementación ISO 27001 donde lo importante es que los riesgos se analicen y se gestionen, que la seguridad se planifique, se implemente y, sobre todo, se revise, se corrija y mejore. (Montaño, V. 2010)

Figura 3

Dominios de la norma ISO 27001

Fuente: Montaño, V. (2010)

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

En relación con los modelos de metodológicos de evaluación de la Gestión de Riesgos MAGERIT y CRAMM.

En palabras de Cordero, G. (2015), en una evaluación de las bondades que ofrece los modelos metodológicos en los cuales el objetivo principal es la gestión y análisis de riego en mayor beneficio destaca MAGERIT, puesto que al no solo contra con el idioma inglés dispone de manera gratuita; además presenta un enfoque más practico que concuerda correctamente con el ISO 27002, 27005.

Adicional a lo antes mencionado, CRAMM identifica los riesgos primigenios y luego estima la frecuencia; sin embargo, MAGERIT inicia con una identificación de activos de información, para luego identificar las amenazas lógicas y su entorno, estimando las frecuencias y el impacto. Y por último de lo expresado tomando en cuenta la su aplicación directa en el desarrollo para certificación ISO 27001 se determina que la de mejor aplicación es la metodología MAGERIT.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

3 CAPITULO III: MARCO REFERENCIAL

3.1 Reseña histórica

La División de Apoyo Técnico Judicial órgano técnico que gestiona el programa de la interceptación legal de las comunicaciones, fue implementado en la Dirección Antidrogas con equipamiento otorgado por el Gobierno Americano, iniciando sus actividades el 19 de mayo de 2009, en sus inicios denominado Oficina de Apoyo Técnico Judicial cambia a denominarse División según la Resolución Directoral N° 46-2014-DIRGEN/EMG-PNP del 28ENE2014, por ser una unidad de apoyo dentro de la estructura orgánica sería considerado como una Unidad de Línea dentro de la estructura orgánica de la Dirección Antidrogas de la Policía Nacional del Perú.

El programa inició con una sala de interceptación legal de comunicaciones y personal especializado y seleccionado por rigurosos exámenes como: entrevista, toxicológico, psicológico, audiometría y de polígrafo, que aseguren el alto nivel de confiabilidad respecto a la información sensible, constituyéndose hoy en día como una importante técnica especial de investigación en concordancia con la Ley N° 30077 Ley Contra el Crimen Organizado.

La actividad de intervención legal de las comunicaciones en tiempo real se realiza en apoyo de la investigación del delito conducido por el Ministerio Público y otras unidades operativas tales como la Dirección Antidrogas y Direcciones de Investigación de la Policía Nacional del Perú; la capacidad operativa al principio a sus inicios era limitada sin embargo con el pasar del tiempo y con la adquisición de nueva tecnología se produjo la ampliación de la capacidad y especio laboral.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

En marzo de 2015 luego de los acuerdos con funcionarios de la Administración de Control de Drogas (Drug Enforcement Administration-DEA) y la Agencia Nacional contra el Crimen del Reino Unido (National Crime Agency-NCA), se inició la implementación de salas adicionales de escuchas legales en el local central de la Dirección Antidrogas culminando los trabajos en enero de 2016; lo que nos permitió ampliar su cobertura de servicio nuevas estaciones de trabajo implementando la sala de escucha de unidades externas, que serían utilizadas para los representantes del Ministerio Publico; ese mismo año la incorporaron 50% de efectivos policiales duplicando la cantidad del personal existente género contribuir a la investigación del crimen organizado y otros delitos. (DEPATJ, 2020)

Consecuentes con la evolución tecnológica actualmente se encuentra en proceso de continuidad y desarrollo puesto que el Sistema Nacional de Intervenciones Legal de las Comunicaciones ofrece una cobertura y servicios a nivel nacional.

3.2 Filosofía organizacional

3.2.1 Misión

El División de apoyo técnico judicial, DIVATJ, tiene por misión gestionar el Sistema de Intervención y control de las Comunicaciones de la Policía Nacional del Perú con mandato judicial en el ámbito nacional con la conducción del Ministerio Público en la investigación de la criminalidad organizada y otros delitos conexos, el cual se desarrolla en el marco normativo peruano. (DEPATJ, 2020)

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

3.2.2 Visión

El División de apoyo técnico judicial, DIVATJ, es una entidad pública, que se desarrolla sus funciones bajo el mando de la Dirección Antidrogas de la Policía Nacional del Perú (DIRANDRO), con la finalidad de cumplir los mandatos judiciales relacionados a la interceptación legal de comunicaciones. (DEPATJ, 2020)

El DIVATJ-DIRANDRO, es una entidad pública con Certificación ISO 9001-2015 Sistema de la Gestión de la Calidad, que tiene la exclusividad la intervención legal de las comunicaciones que cuente con los más altos estándares de calidad en busca de la mejora continua basados en los principios de legalidad, confiabilidad y atención al cliente; apoyando al Ministerio Público y unidades policiales de investigación en la investigación de la criminalidad organizada.

La Visión es ser una gran unidad, que brinde su servicio policial oportuno, eficaz, de calidad inspirando confianza; orientado al cumplimiento de las expectativas nacionales, teniendo los estándares con certificación de calidad a la norma ISO 9001. (DEPATJ, 2019)

3.2.3 Políticas de calidad del Ministerio del interior y la Policía Nacional del Perú

El Ministerio del Interior tiene como finalidad diseñar, establecer, promover, ejecutar, supervisar y evaluar políticas públicas, planes sectoriales y programas en materia de orden interno, orden público y seguridad ciudadana con el objeto de garantizar el cumplimiento de la ley; respecto a los derechos y libertades

fundamentales de los ciudadanos y así como mantener el orden y la seguridad en todo el territorio nacional. (MININTER, 2020)

- Brindar un servicio que atienda los requerimientos que demanden los ciudadanos y partes interesadas, con el fin de lograr su satisfacción, en el marco de confianza, tranquilidad y pasa social.
- Mejorar continuamente el sistema de gestión de calidad y los procesos del MININTER, cumpliendo con la legislación aplicable.
- Gestionar los riesgos que puedan afectar la calidad de los servicios que brinda el MININTER.
- Promover, entre los colaboradores, los principios éticos de integridad, transparencia, honestidad y responsabilidad.

3.2.4 Objetivos de Calidad del Ministerio del interior y la Policía Nacional del Perú

- Mejorar la satisfacción de los ciudadanos con respecto a los servicios brindados por el MINITER y PNP.
- Atender los requerimientos de los ciudadanos y partes interesadas dentro del Plazo establecido.
- Identificar, abordar y mitigar los riesgos en los procesos que pudieran afectar la calidad de los servicios del MININTER y PNP.
- Desarrollar acciones de mejora eficaces en los procesos del Sistema de Gestión de Calidad (SGC).
- Fortalecer las fortalezas del talento humano y su desarrollo integral, a través del

cumplimiento del Plan de Desarrollo de Personas, alineado al Plan estratégico Institucional. (MININTER, 2020)

3.2.5 Funciones de la División de apoyo técnico policial de la Dirección antidrogas de la PNP.

La División de Apoyo Técnico Judicial de la DIRANDRO (PNP, 2021), tiene las siguientes funciones:

- Ejecutar los mandatos judiciales de levantamiento de secreto de comunicaciones; los cuales son emitidos por la autoridad judicial competente que inicia la medida.
- Efectuar el análisis del contenido de las Comunicaciones interceptadas, transmitiendo a las autoridades que intervienen directamente en la ejecución de la medida.
- Grabar en soporte magnético, en el cual se archiva las comunicaciones relevantes de información confidencial para su posterior entrega a la autoridad judicial y fiscal; formalizando los informes de actas de recolección y control de las comunicaciones segmentadas.
- Realizar coordinaciones frecuentes con los operadores policiales y del Ministerio Público.
- Mantener el compartimentaje para garantizar la seguridad y reserva de la información sensible.
- Gestionar el mantenimiento, soporte actualización y renovación de la tecnología licencias, servicios, capacidades, conocimientos y otras.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

3.3 Diseño organizacional

3.3.1 Dirección Antidrogas

Es una organización a organización sistémica y especializada de la PNP, encargada de planear, organizar, coordinar y ejecutar las operaciones policiales a nivel nacional e internacional para prevenir, investigar, denunciar y combatir el tráfico ilícito de drogas y sus delitos conexos, protegiendo a la persona humana y a la sociedad en su conjunto del drogadicción, la violencia y la criminalidad, coadyuvando al desarrollo social y económico del país, cumpliendo para tal n un servicio de excelencia con personal profesional especializado. (DIRANDRO, 2022)

3.3.2 División de Apoyo Técnico Judicial

Es una cedula de apoyo de investigación que ejecuta las resoluciones judiciales de levantamiento legal de las comunicaciones en tiempo real, se ejecuta mediante los principios de Legalidad, confiabilidad y atención, valiéndose de las técnicas especiales de investigación contra el Crimen organizado y entre otros delitos. (DEPATJ, 2020)

3.3.3 Secretaria

Órgano de apoyo que asesora a la jefatura en temas administrativos, además comunica y ejecuta las disposiciones emitidas ejerciendo autoridad al alcance de su función (PNP, 2021). Tiene como función:

- Administrar la documentación pasiva y activa.
- Administrar el archivo físico y magnético.
- Llevar la estadística de ingreso, tramitación y control de la documentación recibida.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

- Cumplir otras actividades que se deriven de las actividades del servicio.

3.3.4 Jefatura Administración

Es el órgano de apoyo encargado de administrar de forma permanente los recursos humanos, logísticos y los servicios de seguridad interna; vela por la disciplina del personal, así como por el mantenimiento y conservación de la infraestructura y equipamiento asignado.

Como órgano de apoyo, asesora a la jefatura en materia de su competencia y brinda información actualizada de la documentación activa, asimismo, formula las cartas funcionales del personal policial asignados a la División de Apoyo Técnico Judicial. (PNP, 2021)

3.3.5 Moral y Disciplina

Es el área de personal que mantiene control de la disciplina de la División de apoyo técnico policial, demostrando el cabal cumplimiento de sus funciones lo que permite alcanzar la integridad del personal que labora en la unidad policial. (DEPATJ, 2019)

3.3.6 Bienestar

Es el área que brinda reconocimiento a los integrantes de la organización mediante actos públicos y privados a fin de fortalecer los vínculos de camarería y hermandad institucional, a fin de obtener mayor compromiso y lealtad con los objetivos de la división. (PNP, 2021)

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

3.3.7 Oficina de Recepción Documentaria

Es la jefatura que se encarga de recibir, registrar, clasificar y distribuir la documentación dirigida a la División de Apoyo Técnico Judicial, verificando su correcto foliado y destinatario; asimismo, realizar el seguimiento del trámite documentario derivando sus funciones a la Mesa de Partes y Sección de Asignación de Casos. (PNP, 2021)

3.3.8 Mesa de Partes

Oficina que se encarga de administrar el Sistema de Gestión de expedientes de la División de Apoyo Técnico Judicial, realiza copias de los expedientes atendidos para ser derivados al área de Sección de Asignación de Casos.

3.3.9 Sección de Asignación de Casos

Oficina que ejerce la función proactiva de revisión y derivación de Resoluciones Judiciales, derivando al Área de Operación de Sistema, para acceso al sistema de interceptación legal de las comunicaciones.

3.3.10 Oficina de Seguridad

Es el área encargada de la seguridad interna y externa, así como la atención al público extremando las medidas de seguridad, orientados a brindar de manera inmediata a los requerimientos exigidos por la jefatura.

3.3.11 Auxiliar de Seguridad

Es el efectivo policial encargado de vigilar, prevenir, alertar e impedir todo tipo de riesgos contra el personal, vehículos e instalaciones, no podrá alejarse de su puesto

toda vez que está a cargo de identificar a los visitantes. Para la óptima función durante toda su facción de servicio, estando prohibido portar instrumento, objeto y/o equipo electrónico (teléfono, radio, tv, tablet, periódicos, libros, etc.), que distraiga a los auxiliares de seguridad.

Entre otra función, tiene de transmitir las consignas recibidas por la jefatura de la Oficina de Seguridad, así como coordinar el ingreso de Fiscales e integrantes de los grupos de investigación. (PNP, 2021)

3.3.12 Oficina de Recursos Humanos.

Es el área encargada de asignar el personal en los distintos cargos de la unidad, en función a su especialidad y necesidad; asimismo lleva los registros del personal respecto a permisos, comisiones, vacaciones, licencias, descansos médicos y aptitud psicosomática.

Entre otras actividades tiene por función:

- Generar políticas de estímulo para levantar el desempeño.
- Adoptar medidas preventivas orientadas al mantenimiento de la disciplina, ética, servicio e imagen institucional.

3.3.13 Oficina de Logística.

Es el área encargada de velar por el mantenimiento y conservación de las instalaciones, operatividad de los vehículos, equipos de cómputo y proponer los recursos necesarios para el funcionamiento de las oficinas atendiendo los requerimientos supervisando su uso y empleo.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Adicionalmente, la Unidad de Tecnología de la Información y comunicación, administra los equipos informática, disponiendo su mantenimiento preventivo del primer escalón y coordina la actualización de la base de datos y software; además, supervisa la operatividad de los equipos de telecomunicaciones. (PNP, 2021)

Por otro lado, se encarga de la correcta administración de vehículos y contrataciones de Ración orgánico único diario.

3.3.14 Oficina de tecnología de Información y Comunicación

Es el órgano de apoyo encargada de planificar, implementar, almacenar y gestionar el sistema de interceptación legal de las comunicaciones, garantizando las actualizaciones del sistema; coordinando con la jefatura principal para las disposiciones en manejo de la información importante. (PNP, 2021)

3.3.14.1 Área de Operación de Sistema

Es una subárea encargada de la verificación de acceso al sistema de interceptación y de asignación de casos; así como el control y superación de objetivos.

3.3.14.2 Área de cadena de Custodia

Es una subárea encargada de ejecutar la entrega de información histórica mediante el protocolo de actuación conjunta entre el Ministerio Público y la Policía Nacional del Perú

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

3.3.15 Oficina Sala de Intervención

Es el área encargada de ejecutar las resoluciones judiciales, personificando la tarea por el Analista Táctico, en principios de legalidad y confiabilidad; teniendo por función las siguientes actividades. (PNP, 2021)

3.4 Productos y/o servicios (según corresponda)

3.4.1 Informes de comunicación Escrito

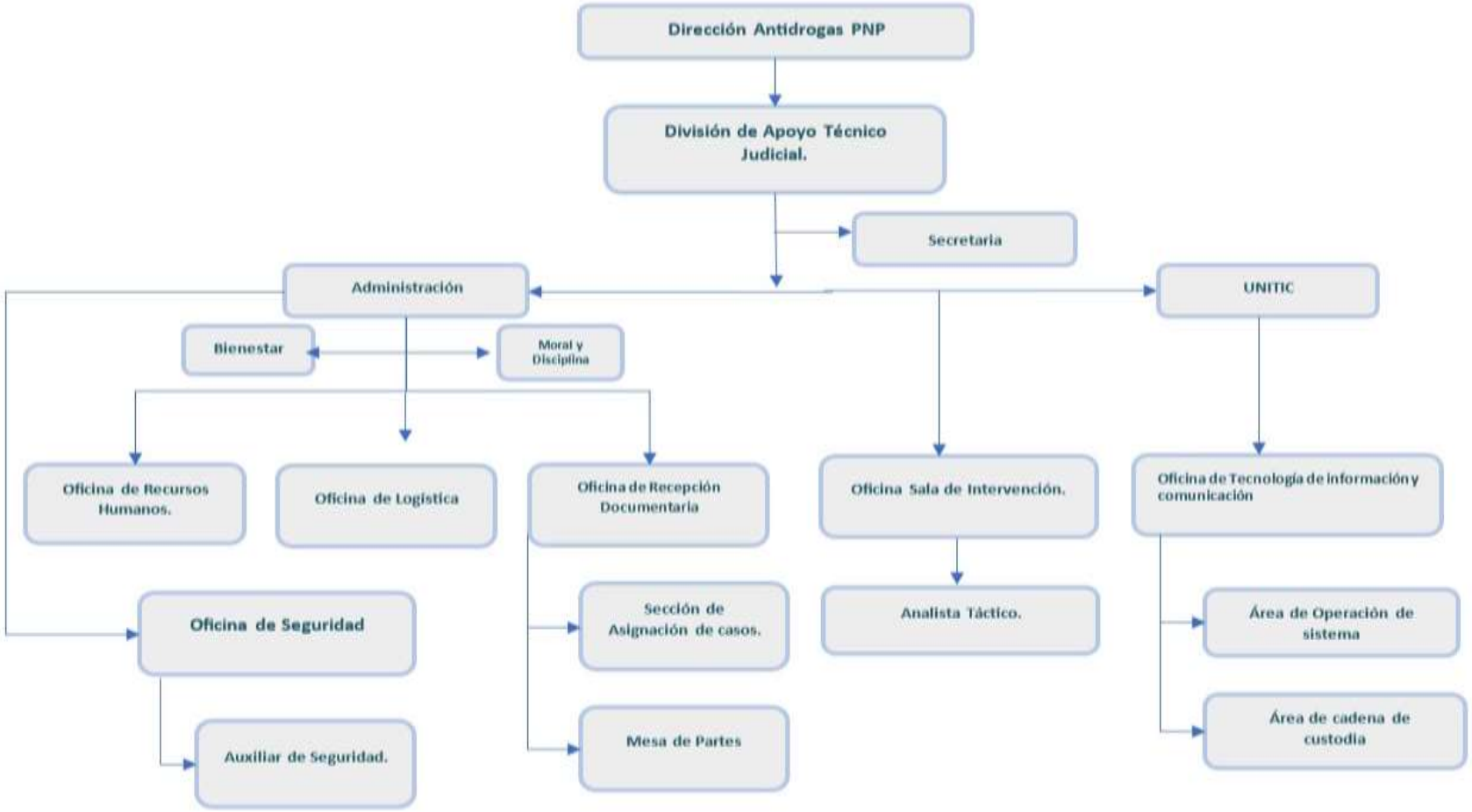
Se materializa en el Acta de recolección y control, elemento físico donde se consigna los datos técnicos y el análisis/síntesis de la comunicación de la información relevante o texto trascrito conforme a la conversación asignada en el sistema de interceptación legal de las comunicaciones. (PJ, 2014)

3.4.2 Informes de comunicación Verbal

Se materializa mediante el servicio de comunicación verbal referente a las actividades realizadas por el objetivo que es informado en tiempo real al representante del Ministerio Público que tiene la carga de la investigación.

Es el acto y servicio primordial del proceso debido a su importancia fundamental en la investigación y prevención del delito; asimismo se encuentra amparado en el principio de la confiabilidad, legalidad, objetividad y proporcionalidad. (PJ, 2014)

Figura 4 *Estructura Orgánica de la División de Apoyo Técnico Judicial*



Fuente: Elaboración Propia.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

3.5 Diagnóstico organizacional

El análisis de fortalezas, oportunidades, debilidades y amenazas tiene por propósito realizar un análisis fundamental a fin de potenciar las fortalezas de la corporación, y aprovechar las oportunidades que se presentan y prevenir y hacer frente las amenazas existentes que pongan en riesgo la sostenibilidad de la organización y su desarrollo. (DEPATJ, 2019)

Se revisará el seguimiento y revisión de la información de la cuestiones internas y eternas una vez al año durante la revisión por la dirección o cuando la alta dirección lo requiera. (DEPATJ, 2019)

3.5.1 Fortalezas

3.5.1.1 Marco legal establecido.

La actividad de la intervención legal de las comunicaciones (DEPATJ, 2019), es una actividad que constituye la restricción al derecho fundamental del secreto y la inviolabilidad de las comunicaciones privadas, contenido en el artículo 2, inciso 10 de la Constitución Política del Perú. La medida adoptada se fundamenta en la normativa peruana vigente tal como:

- Ley N° 27697, Ley que faculta al fiscal para la intervención y control de las comunicaciones y documentos privados.
- Ley N° 30077 Ley contra el crimen organizado.
- Ley N° 29733 Ley de Protección de Datos Personales.
- Decreto Legislativo N° 957 Código Procesal Penal
- Resolución Ministerial 1217-2014IN Protocolo de Actuación Conjunta entre la

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Policía Nacional del Perú, Ministerio Publico y los órganos Jurisdiccionales Poder Judicial en la Lucha Eficaz Contra la Delincuencia y el Crimen Organizado.

3.5.1.2 Proceso de selección de personal.

El personal asignado en el sistema de intervención legal de las comunicaciones es estrictamente seleccionado, denominado Analista Táctico, el cual es seleccionado a través de un procedimiento que incluye entrevista, examen toxicológico, examen psicológico, examen médico y prueba de polígrafo.

3.5.1.3 Capacitación constante.

Los integrantes de la actividad de interceptación legal de las comunicaciones reciben de cursos de especializaciones y capacitaciones permanentes, asegurando de esta manera la idoneidad y confiabilidad del personal lo que establece un trato y uso correcto de la información.

3.5.1.4 Excelente Clima Laboral.

EL personal se rige a las normas establecidas entre el personal de armas de la Policía Nacional del Perú.

3.5.1.5 Adecuado equipamiento y apoyo logístico.

Con la aparición de nuevas tecnologías la institución policial cuanta con equipos modernos que facilitan la labor de los operadores de justicia.

3.5.1.6 Aceptación laboral (Excelente Imagen).

La División de interceptación legal de las comunicaciones de la Dirección antidrogas, por la excelente labor y función basados en principios de legalidad,

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

confiabilidad y atención al cliente, tiene una imagen de confianza de los operadores de justicia y viene cumpliendo las expectativas de los usuarios.

Controles de seguridad del personal en el proceso de selección.

Uno de los pilares de la División, puesto que existen diferentes niveles de seguridad desde el ingreso como primer eslabón, posteriormente el segundo nivel referido al uso de usuario y contraseña individual y el tercer nivel referido a los usuarios externos.

3.5.1.7 Manejo de Datos masivos (BIG-DATA).

El área de Unidad de Tecnología de Información y Comunicación cuenta con una capacidad basta de almacenamiento de datos histórico para el posterior solicito de la autoridad competente.

3.5.2 Oportunidades

3.5.2.1 Apoyo de instituciones internacionales y nacionales.

Para combatir la criminalidad organizada la institución policial cuenta con aliado estratégico a la Administración para el Control de Drogas de los Estados Unidos de América (DEA), así como diversas instituciones públicas, privadas y personas.

Buenas relaciones institucionales con el Estado y Ministerio Público.

La intervención legal de las comunicaciones como instrumento procesal penal se establece el protocolo de actuación conjunta entre el Ministerio Publico, Poder Judicial, Ministerio de Justicia y Derechos Humanos, a partir del tratamiento legal con un conjunto de Mejoras Tecnológicas en el rubro de las comunicaciones.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

3.5.3 Debilidades

3.5.3.1 Requerimiento de personal con perfil especifico.

El personal perteneciente a la División al ser seleccionado de la misma institución debe pasar por filtros adecuados lo que genera una demora en su asignación.

3.5.3.2 No contar con Área de Asesoría Jurídica.

Dentro de la administración no cuenta con un área de Asesoría Jurídica propia; sin embargo, las relaciones laborales con el Ministerio Público aplican la disminución de esta necesidad.

3.5.3.3 Recursos limitados para la cantidad de demanda de casos.

La demanda de casos se incrementa anualmente, lo que ocasionaría que la carga laboral para los analistas sea de mayor demanda.

Acceso compartido a las instalaciones (no se cuenta acceso directo).

A partir de la seguridad interna de las instalaciones el único sujeto que puede vulnerarla es el personal de analistas.

3.5.3.4 Personal se considera autosuficiente por la experiencia ganada.

El personal de la división aún debe continuar con los cursos capacitación y especialización que propicia un mejor resultado de la investigación.

No se aplica la política de reconocimiento e incentivos por objetivos logrados.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

3.5.3.5 Mínimos conocimientos en Seguridad de la Información.

El personal de la División de apoyo técnico judicial no cuenta con conocimientos claros sobre la gestión de riesgos de seguridad de la información, lo que significa que ante hechos que puedan ocurrir no sería atendidos de manera inmediata.

Por lo que es necesario establecer programas de capacitación adecuados para su formación.

3.5.4 Amenazas

3.5.4.1 Exceso de demandas por caso.

Las comunicaciones que realizan los objetivos son densas lo que implica que la demanda de comunicaciones deba ser atendidas de manera simultánea.

Información mal intencionada del servicio brindado.

Durante el desarrollo de la comunicación se puede dar por error o a intención información errada que represente un retraso a las investigaciones.

Constante cambio de normativa.

El cambio de la legislación en relación con el ámbito penal por la constante actualización de la legislación.

3.5.4.2 Inestabilidad Política.

El cambio de autoridades políticas repercute en el funcionamiento de los eslabones menores por el cambio de disposiciones a niveles estratégicos.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

3.5.4.3 Rotación de Personal.

La renovación de cuadros es esencial para la continuidad de la organización, sin embargo, la salida de personal calificado reduce la capacidad operativa.

Personal Receptor de la Información no capacitado en el manejo de información confidencial.

Los reportes de comunicación realizados en forma verbal son entregados a los clientes, Ministerio Público o personal asignado al caso, los cuales se desconoce sobre su nivel de confiabilidad.

3.5.4.4 Uso inadecuado e inseguro de la información proporcionada.

El riesgo latente que la información que se transmite al Ministerio Publico, sea utilizado con fines delincuenciales y favorezcan a las organizaciones criminales.

Figura 5

Análisis FODA

Fortaleza	Debilidades
1. Marco legal establecido. 2. Proceso de selección de personal. 3. Capacitación constate. 4. Excelente Clima Laboral. 5. Adecuado equipamiento y apoyo logístico. 6. Aceptación laboral (Excelente Imagen). 7. Controles de seguridad del personal en el proceso de selección. 8. Manejo de Datos masivos (BIG-DATA).	1. Requerimiento de personal con perfil especifico. 2. No contar con Área de Asesoría Jurídica. 3. Recursos limitados para la cantidad de demanda de casos. 4. Acceso compartido a las instalaciones (no se cuenta acceso directo). 5. Personal se considera autosuficiente por la experiencia ganada. 6. No se aplica la política de reconocimiento e incentivos por objetivos logrados.
Oportunidades	**Amenazas**
1. Apoyo de instituciones internacionales y nacionales. 2. Buenas relaciones institucionales con el Estado y Ministerio Público. 3. Mejoras Tecnológicas en el rubro de las comunicaciones.	1. Exceso de demandas por caso. 2. Información mal intencionada del servicio brindado. 3. Constante cambio de normativa. 4. Inestabilidad Política. 5. Rotación de Personal. 6. Personal Receptor de la Información no capacitado en el manejo de información confidencial. 7. Uso inadecuado e inseguro de la información proporcionada.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Fuente: Elaboración Propia

3.6 Análisis del FODA del DIVATJ-DIRANDRO

Mediante el análisis de la matriz FODA, para analizar las Fortalezas, Oportunidades, Debilidades y Amenazas, que se presenta para la División de Apoyo Técnico Judicial fueron recolectados con la intención de obtener los puntos necesarios para una evaluación objetiva durante la encuesta a los analistas tácticos.

Mediante la aplicación del instrumento (encuesta), aplicada a la población de muestra, que es objeto de estudio de la División de Apoyo Técnico Judicial, esto nos permitirá medir el nivel de conocimiento en seguridad de la información, en técnicas para la protección de datos y seguridad de la información, y en la aplicación de herramientas para la protección de datos y seguridad de la información.

Para mejores opciones que exige el estándar ISO 27001 se toma en cuenta la Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, para implementar un sistema de Gestión de seguridad de la información. Asimismo, Ciclo de mejora continua en la Norma ISO/IEC 27001:2013 que es utilizado para desarrollar procesos orientados a mejorar la calidad de los servicios brindados por la División de Apoyo Técnico Judicial

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

4 CAPÍTULO IV: RESULTADOS

4.1 Diagnóstico.

4.1.1 Modelo de análisis de riesgo

Según la Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT V3.0), los pasos a continuación para realizar un análisis de riesgo metódico para identificar riesgos:

- Determinar cuáles son los activos más relevantes para la organización.
- Determinar que amenazas afectan a los activos informáticos.
- Determinar qué medidas de seguridad existen y que tan efectivas son contra los riesgos.
- Riesgo pronosticado, definido como el impacto ponderado por frecuencia del peligro.

4.1.2 Técnica e instrumento de recolección de datos.

El método para la recopilación de información se realizó por intermedio de la encuentras realizada a la población de muestra de la División de Apoyo Técnico Judiar, con la finalidad de comprender e identificar tres puntos importantes para una identificación clara u oportuna respecto a los conocimientos sobre la seguridad de la información, la aplicación de herramientas y técnicas de protección de datos. Asimismo, se realiza un trabajo de campo para buscar información histórica con la finalidad de evaluar la toma de ciertas decisiones sobre las tareas de método desarrollado, en caso de ser necesario, para justificar la función y modelo operativo.

A. La encuesta, se utilizaron métodos de encuestas en el proceso de

evaluación del modelo SGSI.

B. Revisión bibliográfica y documental, analizar informes y otros documentos sobre gestión de seguridad de la información y gestión de riesgos de tecnología de la información y desarrollar estudios teóricos.

C. La observación directa, el trabajo in situ se realiza mediante observación directa para analizar el funcionamiento del dispositivo y describir el estado actual del sistema de gestión de seguridad de la información.

D. Confección de Fichas de Técnicas de procedimientos.

4.1.3 Metodología para construcción de un sistema de gestión de seguridad de la información.

El estándar ISO/IEC 2700X y el método Magerit, se utilizan como pautas para la creación de un modelo de sistema de gestión de seguridad de la información; del cual se presentan los siguientes componentes:

- Componente 1: Alcance del sistema de la gestión de la seguridad de la información.
- Componente 2: Estructura del sistema de la gestión de la seguridad de la información.
- Componente 3: Evaluación de Riesgos.
- Componente 4: Tratamiento de Riesgos.
- Componente 5: Declaratoria de aplicación.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

4.1.4 Construcción del componente 1: Alcance del sistema de la gestión de la seguridad de la información. (SGSI)

La norma ISO 27001, determina que el alcance de un SGSI se toma como referencia el contexto y entorno de la organización, se considera su estructura, procesos, activos, tecnologías y otros.

Identificar los activos de tecnología e información se considera en la evaluación de riesgos, las tareas consideradas en esta fase son las siguiente:

a. Identificar de procesos: se realiza el mapeo de los procesos de seguridad mediante los protocolos internos denominados directivas.
b. Definir el catálogo de activos de tecnología de información: realiza un inventario de los activos software y hardware.

Formulación del catálogo de inventario según al siguiente formato:

Denominación del activo de Tecnología de Información (TI)

- Categoría del activo de Tecnología de la Información, para la categoría de los activos se utilizan las siguientes nominaciones:

1. Información,
2. Software,
3. Hardware,
4. Servicios y
5. Analistas Tácticos.

- Clasificación. Para la clasificación de los activos de Tecnología de Información (TI), se utiliza un criterio de accesibilidad, de la siguiente manera:

1. Confidencial,

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

2. Uso Interno y
3. Público

- Frecuencia de uso. Para determinar la frecuencia de uso y explotación del activo de Tecnología de Información, se utilizó la siguiente nominación:

1. Diario,
2. Mensual,
3. Anual y
4. Otro

- Ubicación del activo. Dependiente del tipo de activo, la ubicación puede ser física o lógica.
- Usuario responsable del uso o explotación del activo de Tecnología de Información.
- Responsable de la custodia del activo de Tecnología de Información.
- Responsable del activo de Tecnología de Información.
- Criticidad del activo. Para valorar de la criticidad o importancia de los activos de Tecnología de Información. (TI), se utilizó la escala:

1. Alto,
2. Medio o
3. Bajo.

- Procesos relacionados. Se identificaron los procesos que están relacionados con cada activo de Tecnología de Información (TI).

4.1.5 Procedimiento para la construcción del componente 2: estructura del sistema de la gestión de la seguridad de la información.

En base a las necesidades de seguridad de información y la identificación de

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

las partes interesadas, se definieron los siguientes aspectos en este componente:

- Política de seguridad, basados en conocimiento en temas relacionados a la seguridad de la información.
- Objetivos de la seguridad, relacionado a la protección de datos y seguridad de la información.
- Organización de la seguridad, basado en herramientas para la protección de datos y seguridad de la información.

4.1.6 Procedimiento para la construcción del componente 3: la evaluación de riesgo.

Para construir este componente, se consultó principalmente el método de identificación de componentes de Magerit.

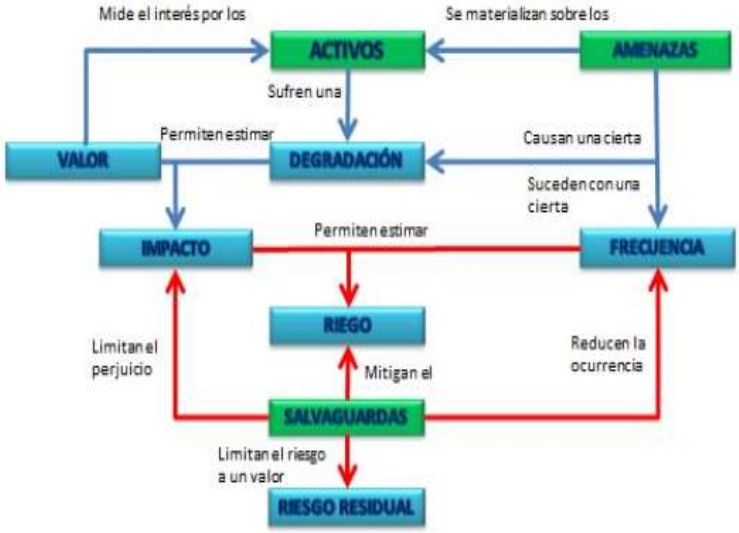
En la gráfica siguiente se aprecia que los elementos de un modelo de gestión de riesgos de Tecnología de Información, según la metodología Magerit, son:

- Los activos de Tecnología de Información.
- La estimación de la criticidad de los activos de Tecnología de Información.
- Las amenazas que pueden afectar los activos de Tecnología de Información.
- El impacto en el negocio debido a la ejecución de una amenaza.
- La frecuencia de una amenaza

Figura 6

Elemento de la Gestión de Riesgos de Tecnología de la Información.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.



Fuente: (Magerit – Libro 1 2012)

En base al modelo de gestión de riesgos de tecnología de información se definieron las siguientes tareas:

4.1.6.1 Inventario de activos

Se analizará el proceso de asignación de casos y de líneas de los sistemas de gestión de la seguridad de información. El inventario de activos se considera las categorías propuesto en la metodología Magerit.

Tabla 2

Tabla de referencia para la tipificación de activos de Tecnología de la Información.

TIPO	CODIGO	DETALLE
Activo de Información (L)	L1	Manejo de Información Electronica
	L2	Manejo de Información Escrita
	L3	Manejo de Documentos Fisicos (Actas - Informes)
	L4	Manejo de Documentos Dijitales (Audios)
Activo de Software (S)	S1	SISTEMA OPERATIVO
	S2	Aplicaición de intervencion de comunicación.
	S3	Sistema de Almacenamiento
Actio de Hardware (H)	H1	Equipos de procesamiento de escuchas
	H2	Equipos de Almacenamiento de escuchas
	H3	Medios de Almacenamiento
	H4	Mobiliario y Equipo
	H5	Otros Equipos
Servicios de Terceros (T)	T1	Procesamiento de la Información
	T2	Servicios de mantenimiento
	T3	Otros Servicios

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Fuente: Elaboración propia, adaptado de Magerit.

Asimismo, la siguiente información debe ser registrada para cada activo:

- Clasificación: Reservado, Secreto y Confidencial
- Frecuencia de uso de los activos
- Ubicación física y lógica.
- Responsable del uso
- Responsable del activo
- Proceso donde se usa el activo.
- Valor del activo.

Mediante la clasificación de activos se procede a realizar un programa de mantenimiento para el sistema de la Gestión de la seguridad de la información para la disminución de actos que contravengan la seguridad de la información, es propio establecer que los actos de su aplicación derivan de la aplicación propia mediante recursos de la unidad ejecutora de la Dirección antidrogas. Véase el Anexo N° 5.

4.1.6.2 Conocimiento doctrinario de la seguridad de la Información.

Mediante la encuesta realizada se determina realizar las afirmaciones que se relacionan directamente con el Conocimiento en la seguridad de la Información relacionados con los activos de Información de código “L”, que establece si el analista táctico presenta conocimientos relacionados a los apartados:

- Posee conocimientos con respecto a la seguridad de la información.
- Tiene conocimientos sobre las normas que establecen la seguridad de la información.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

- Adquiere conocimiento a través de las capacitaciones realizadas en la seguridad de la información por parte del DIVATJ.
- Se tiene conocimiento sobre Normas ISO 27001.
- Tiene conocimiento sobre la Ley de Protección de Datos Personales Ley N° 29733.
- Tiene conocimiento sobre la Ley Contra el Crimen Organizado Ley N° 30077.

En la encuesta realizada se formuló las siguientes afirmaciones las cuales fueron contestadas mediante la escala de 1 a 5, siendo el nivel

1 de satisfacción Regular, el nivel 2 de satisfacción Muy deficiente, el nivel 3 de satisfacción Bueno, y el nivel 5 de satisfacción Excelente; mediante los criterios dentro de la escala de Likert, se evaluará cual es el nivel de satisfacción que observan lo analistas tácticos lo que representa el nivel de impacto en relación al conocimiento sobre la seguridad de la información.

Tabla 2

Resultado de Conocimiento en la seguridad de la información.

N°	Descripción	%
1.1	Posee conocimientos con respecto a la seguridad de la información.	27%
1.2	Tiene conocimientos sobre las normas que establecen la seguridad de la información.	50%
1.3	Adquiere conocimiento a travéz de las capacitaciones realizadas en la seguridad de la información por parte del DIVATJ.	67%
1.4	Se tiene conocimiento sobre Normas ISO 27001.	60%
1.5	Tiene conocimiento sobre la Ley de Protección de Datos Personales Ley N° 29733.	91%
1.6	Tiene conocimiento sobre la Ley Contra el Crimen Organizado Ley N° 30077.	100%

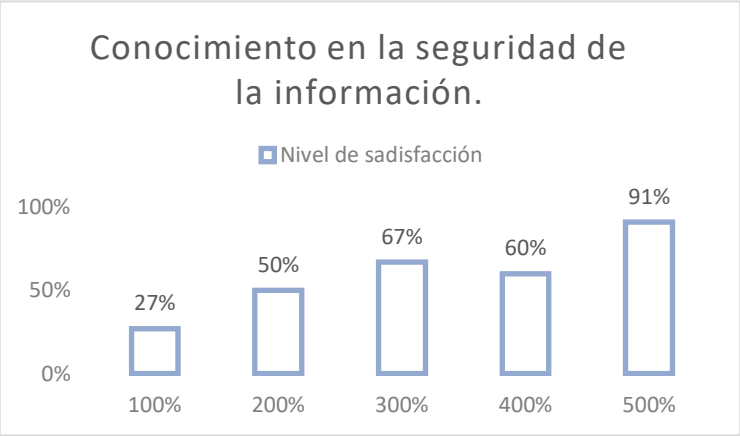
Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Fuente: Elaboración Propia, resultado de Encuesta Anexo 1

Mediante la obtención de los resultados de la encuesta de cincuenta y cuatro (54) Analistas tácticos se puede observar sobre las debilidades observadas:

Figura 7

Debilidades en el Conocimiento en la seguridad de la información.



Fuente: Elaboración Propia, resultado de Encuesta Anexo 1

4.1.6.3 Determinación de criticidad de los activos de la Tecnología de Información.

Para determinar el nivel de criticidad de las instalaciones de almacenamiento, se analizaron y evaluaron características de seguridad de la información tomadas de la norma ISO 27001, como: la confidencialidad, integridad y disponibilidad.

Se utiliza en la encuesta en el apartado de Técnicas para la protección de Datos y Seguridad de la Información mediante la escala de 1 a 5, siendo el nivel 1 de satisfacción Regular, el nivel 2 de satisfacción Muy deficiente, el nivel 3 de satisfacción Bueno, y el nivel 5 de satisfacción Excelente; mediante los criterios dentro de la escala de Likert, se evaluara cual es el nivel de satisfacción que

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

observan lo analistas tácticos lo que representa el nivel de impacto de seguridad, los apartados evaluados se ve afectada negativamente por un incidente o incidentes de seguridad.

Tabla 3

Escala de Valores para criterios de seguridad de la información.

CRITERIO	VALOR EN ESCALA	DESCRIPCIÓN
DISPONIBILIDAD	1 AL 5	El medio donde se alojan los backup de los servidores en ¿qué estado se encuentra?
	1 AL 5	Los hardware que utiliza ¿qué estado se encuentra?
INTEGRIDAD	1 AL 5	Los datos que se verifican despues de realizadas las copias de seguridad se cataloga como:
	1 AL 5	El servicio prestado por el operador alterno en caso de que el principal falle lo podemos resolver.
	1 AL 5	En que estado se encuenta el servidor alterno.
CONFIDENCIALIDAD	1 AL 5	El sistema de control para el ingreso a esta área se define como:
	1 AL 5	Como se define las pistas dejadas al ingresar a esta a las Oficina de Sala de Intervenciones y Oficina de Tecnologia de Informaición.
	1 AL 5	Como se definen los controles que se ejerce a los usuarios de la Oficina de Sala de Intervenciones y Oficina de Tecnologia de Informaición.

Fuente: Elaboración Propia, tomando como referencia la tabla basada en las escalas de valoración de la metodología Magerit.

Mediante la encuesta realizada a los cincuenta y cuatro (54) analistas tácticos se obtiene el total de satisfacción cuando se alcanza el puntaje de doscientos setenta (270) que implica el 100% de satisfacción:

Tabla 4

Técnicas para la protección de Datos y Seguridad de la información.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

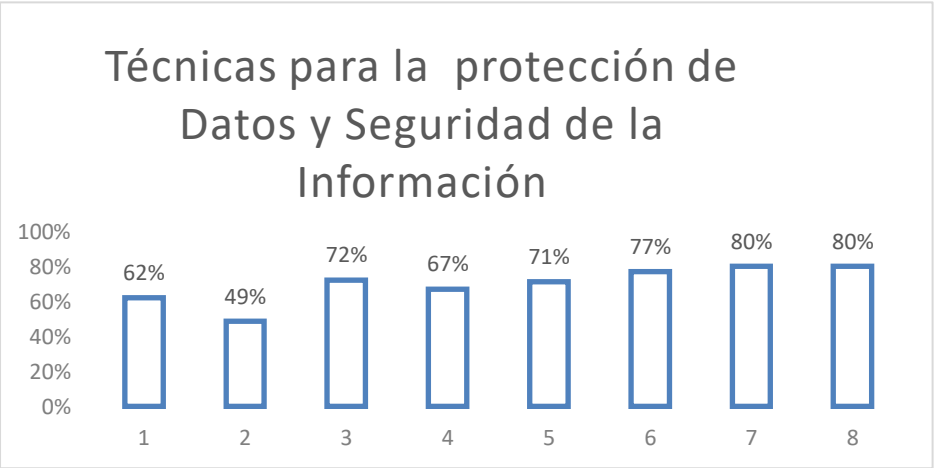
N°	Descripción	%
2.1	El medio donde se alojan los backup de los servidores en ¿qué estado se encuentra?	62%
2.2	ıcuentra?	49%
2.3	Los datos que se verifican despues de realizadas las copias de seguridad se cataloga como:	72%
2.4	El servicio prestado por el operador alterno en caso de que el principal falle lo podemos resolver.	67%
2.5	no.	71%
2.6	El sistema de control para el ingreso a esta área se define como optima.	77%
2.7	Como se define las pistas dejadas al ingresar a esta a las Oficina de Sala de Intervenciones y Oficina de Tecnologia de Informaición.	80%
2.8	Como se definen los controles que se ejerce a los usuarios de la Oficina de Sala de Intervenciones y Oficina de Tecnologia de Informaición.	80%

Fuente: Elaboración Propia, resultado de Encuesta Anexo 1

En la figura siguiente se puede evidenciar la debilidad que presenta el DIVATJ-DIRANDRO toda vez que se encuentran por debajo del 95%.

Figura 8

Técnicas para la protección de Datos y Seguridad de la información, vista de porcentaje menores de riesgo.



Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Fuente: Elaboración Propia, resultado de Encuesta Anexo 1

4.1.6.4 Aplicación de Herramientas para la protección de datos y la seguridad de la información.

En el DIVATJ-DIRANDRO, es importante determinar cuan necesario es establecer cuál es el riesgo de la información obtenida su no se obtiene los recursos adecuados para el mantenimiento físico y virtual de los equipos tecnológicos, en tal sentido se presentará los resultados obtenidos en la encuesta desarrollada por la muestra de Analistas Tácticos.

Por lo que se obtuvo los siguientes resultados:

Tabla 5

Herramientas para la protección de datos y la seguridad de la Información.

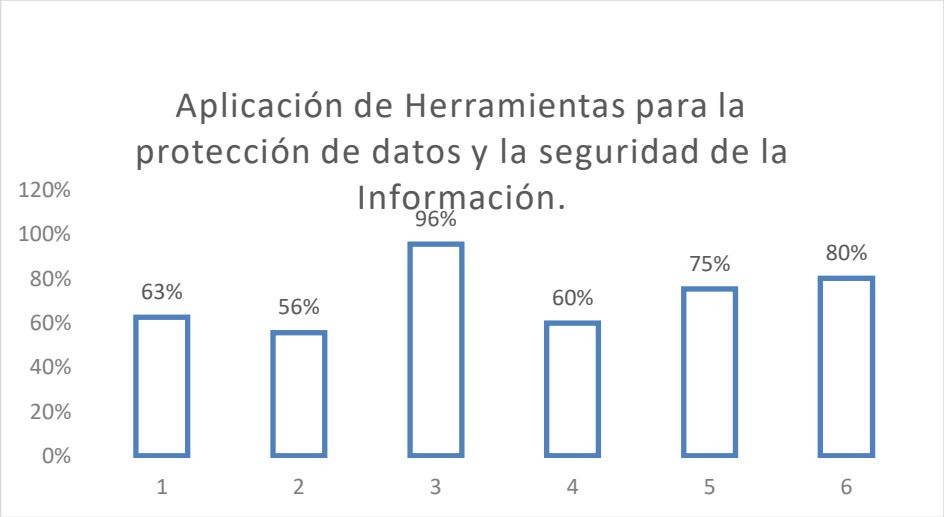
N°	Descripción	%
3.1	El antivirus instalado en los equipos de cómputo del DIVATJ se puede definir como adecuado.	63%
3.2	El nivel de protección brinda el antivirus instalado en los equipos de cómputo.	56%
3.3	Como se define las restricciones a paginas no permitidas en la DIVATJ.	96%
3.4	Los equipos de cómputo tienen licenciamiento vigente.	60%
3.5	Como define el password para el ingreso al sistema.	75%
3.6	El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema.	80%

Fuente: Elaboración Propia, resultado de Encuesta Anexo 1

Del cuadro anterior se puede observar que la deficiencia de la protección de datos y la seguridad de la información se puede observar lo siguiente:

Figura 9

Aplicación de Herramientas para la protección de datos y la seguridad de la Información.



Fuente: Elaboración Propia, resultado de Encuesta Anexo 1

4.1.6.5 Identificación de las amenazas y vulnerabilidades

Para identificar las amenazas que se consideran eventos que pueden causar hechos inesperados o pueden degradar los activos de TI, se utilizara como referencia el catálogo de amenazas propuesto por el método Magerit, mediante las siguientes categorías:

- Amenazas por su naturaleza (algún tipo de sismo, incendio natural, tormentas, etc.)
- Amenazas de tipo industrial (fuego, explosiones, corto circuito, sobrecalentamiento, etc.)
- Amenazas por origen humano (descuidos, mal intensiones, irresponsabilidades, incumplimiento de funciones, etc.)
- Amenaza tecnológica (fallas en la red, fallas en la BD, virus, hackeo, etc.)

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

- Amenaza operacional (mala logística, fallas en el proceso, obsolescencia, etc.)

4.1.6.6 Estimación del impacto

Se utilizará una escala de cinco puntos para evaluar el impacto del peligro. Los criterios de evaluación de estos escenarios de riesgo están tomados del método Magerit (Magerit - Volumen 1, 2012): En función de los objetivos de la investigación, elegir los siguientes:

- Continuidad o interrupción de los servicios

- Economía de la empresa e intereses comerciales

- Seguridad.

Tabla 6

Tabla de escala de valoración del impacto de una amenaza.

NIVEL DE IMPACTO	ONTINUIDAD DE LOS SERVICIOS	ECONOMIA DEL DIVATJ E INTERESES	SEGURIDAD
5: MUY ALTO	Ocaciona interrupciones serias en las actividades del DIVATJ, generando mala reputacion en los operadores de justicia. Ocaciona destruccion de los equipos o en las instalaciones.	Ocaciona pérdidas econimicas elevadas. Ocaciona imcumplimiento graves a las responsabilidades y obligaciones	Causan incidentes muy graves. No se puede realizar el debido seguimineto.
4: ALTO	Ocaciona interrupciones graves en las actividades del DIVATJ, paralizaciones en la prestacion de servicios. Ocaciona incidentes que demandan tiempo y costos considerables	Ocaciona pérdidas econimicas graves. Ocaciona imcumplimiento serios a las responsabilidades y obligaciones	Causan incidentes relacionados a la seguridad. Existe dificultad para realizar el seguimiento.
3: MEDIO	Ocaciona interrupciones en las actividades del DIVATJ, en la prestacion de servicios. Ocaciona condiciones negativas que aumentan la carga del trabajo.	Ocaciona pérdidas econimicas. Ocaciona imcumplimiento significativo con algunas obligaciones.	Causan incidentes relacionados a la seguridad. Se puede realizar seguimiento de los incidenyes
2:BAJO	Ocaciona interrupciones graves en las actividades del DIVATJ, genera alguna interferencia en los servicios, continua con procedimientos de emergencia.	Ocaciona ciertas mermas. Ocaciona imcumplimiento de responsabilidades y obligaciones	Causan indidentes relacionados a la seguridad con poca repercusión en los activos de información
1:MUY BAJO	Ocaciona interrupciones en las actividades de menor importancia.	Ocaciona ciertas mermas. Ocaciona imcumplimiento leves de responsabilidades y obligaciones	Causan indidentes de seguridad casi nula en perjuicio de la información.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Fuente: Elaboración propia, tomando como referencia la propuesta de la metodología Magerit

4.1.6.7 Estimación de la probabilidad de ocurrencia.

Para evaluar la probabilidad de que ocurra una amenaza, se realiza la consulta en la siguiente tabla, que muestra cinco niveles de evaluación:

Tabla 7

Tabla de escala de valoración para probabilidad de ocurrencia.

NIVEL	DESCRIPCIÓN DEL NIVEL
5: MUY ALTO	OCURRE DE MANERA DIARIA. LOS MECANISMOS DE SEGURIDAD IMPLANTADOS SON INEXISTENTES O INEFICIENTES.
4: ALTO	OCURRE DE MANERA SEMANAL. LOS MECANISMOS DE SEGURIDAD IMPLANTADOS POCO EFICIENTES.
3: MEDIO	OCURRE DE MANERA MENSUAL. LOS MECANISMOS DE SEGURIDADIMPLANTADOS A VECES PUEDEN IMPEDIR LA AMENAZA.
2:BAJO	OCURRE DE MANERA ANUAL. LOS MECANISMOS DE SEGURIDAD IMPLANTADOS SON EFICIENTES PARA IMPEDIR UNA AMENAZA.
1:MUY BAJO	OCURRE MÁS DE UNA VEZ AL AÑO. LOS MECANISMOS DE SEGURIDAD SON ALTAMENTE EFICIENTES QUE CASI SIEMPRE IMPIDEN UNA AMENAZA.

Fuente: Elaboración propia.

a. Estimación del nivel de exposición al riesgo.

Las estimaciones de los niveles de riesgo de Tecnología de Información se utilizan para determinar la exposición del DIVATJ en cada escenario de riesgo. El análisis debe tener en cuenta las vulnerabilidades y amenazas identificadas de cada activo de Tecnología de Información. (Serrano, et al 2019).

Se realiza este cálculo se utiliza las siguientes formulas:

Riesgo = Criticidad + (Probabilidad * Impacto)

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Criticidad del activo = C + I + D

C= confiabilidad.

I= Integridad.

D= Disponibilidad.

Se estableció una escala para determinar los niveles de tolerancia a los riesgos. Cada nivel corresponde a un rango de valores de los niveles de riesgo.

Tabla 8

*Escala para determinar el nivel de tolerancia a los riesgos**.***

NIVEL	DESCRIPCIÓN DEL NIVEL
TOLERABLE	**00 - 06**
REGULARMENTE TOLERABLE O ACEPTABLE	**07 - 13**
NO TOLERABLE - NO ACEPTABLE	**14 - 20**

Fuente: Elaboración propia

4.1.7 Procedimiento para la construcción del componente 4: Tratamiento y control del riesgo.

a. Identificación de mecanismos de seguridad para la mitigación de los riesgos no tolerables.

Este ejercicio identifica las medidas de seguridad que la organización implementará para reducir el riesgo. Estas medidas pueden ser tecnológicos o administrativas. Algunos escenarios de riesgo pueden implementarse con los mecanismos de seguridad existentes, pero otros escenarios de riesgo requieren

tecnología o elementos técnicos.

b. Definición de la estrategia de tratamiento de los mecanismos de seguridad y controles

Las estrategias para el tratamiento de los mecanismos de seguridad y controles han sido clasificadas de la siguiente manera:

1. Reducción del riesgo (R)

Esta estrategia se utiliza generalmente cuando la capacidad instalada requerida y la economía de implementar los mecanismos de seguridad y control son suficientes.

2. Aceptar el riesgo (A)

Esta estrategia es comúnmente utilizada cuando no se cuenta con la capacidad requerida (personal calificado, infraestructura y normativa) y los fondos para implementar mecanismos de seguridad y controles son insuficientes.

3. Transferencia del riesgo (T)

Esta estrategia generalmente se utiliza cuando no se cuenta con la capacidad instalada requerida (personal calificado, infraestructura y normatividad), pero se tienen ahorros significativos al implementar mecanismos y controles de seguridad, y delegar a terceros especializados.

4. Evitar el riesgo (E)

El riesgo se debe ser el mínimo puntaje obtenido en la formula del cálculo de exposición de riesgo toda vez que se puede cuantificar siendo lo ideal que se encuentre cercano a cero; este resultado nulo se alcanza cuando se implementan mecanismos y controles de seguridad.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Riego Residual = Criticidad + (Probabilidad * Impacto) = CERO (00), significa que no existe riesgo en la seguridad de la información.

4.1.8 Procedimiento para la construcción del componente 5: Declaratoria de aplicación.

a. Análisis de aplicabilidad de controles.

El procedimiento incluye determinar qué aspectos de la seguridad de la información están o no cubiertos actualmente y determinar el alcance de la aplicación.

Este análisis puede determinar qué controles se considerarán en el plan de gestión de riesgos e identificar las brechas de seguridad de la información existentes. Para analizar las brechas se utilizará un enfoque descriptivo entre la situación real de la seguridad de la información del DIVATJ y las buenas prácticas de seguridad o medidas de control propuestas en la norma ISO/IEC 2700x. Para este propósito, se ha desarrollado una lista de verificación para verificar si las herramientas cumplen con los criterios anteriores.

La aplicación de la lista de verificación para determinar las brechas de seguridad de la información con ámbitos el primero “Cumple” se relaciona directamente con la Valoración de la probabilidad de ocurrencia en sus cinco niveles.

Tabla 9

Lista de Verificación para la identificación de brechas de seguridad de la Información.

.

ÍTEM	DOMINIO	CUMPLE	NIVEL DE CUMPLIMIENTO
1	POLÍTICAS DE SEGURIDAD		
2	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
3	GESTIÓN DE ACTIVOS		
4	SEGURIDAD LIGADA A RECURSOS HUMANOS		

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

5	SEGURIDAD FISICA Y VIRTUAL
6	GESTION DE LAS COMUNICACIONES Y OPERACIONES
7	CONTROL DE ACCESOS
8	ADQUICISIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE
9	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMCIÓN
10	GESTIÓN DE LA CONTINUIDAD DEL DIVATJ
11	CONFORMIDAD

Fuente: Elaboración Propia, Adaptado de Anexo A de la ISO/IEC27001, este cuadro se desarrollará posteriormente.

b. Plan de Tratamiento de Riesgos.

Después de determinar la aplicabilidad del control, se crea una tabla que define un conjunto de actividades para implementar cada propuesta de control para ayudar a superar las vulnerabilidades encontradas en cada escenario de riesgo.

Figura 10

Mapa de Procesos DIVATJ para implementación ISO-27001

FUENTE: Elaboración propia del Mapeo de proceso del DIVATJ-DIRANDRO-PNP.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Procesos Operativos

- Recepción y asignación de Solicitudes
- Monitoreo y Registro de llamadas
- Formulación y entrega de informes

Procesos de apoyo

- Recursos Humanos
- Mantenimiento
- Logística
- Sistema

Mediante el subproceso del área de apoyo y de producción se presenta a continuación:

El subproceso de los procesos apoyo y procesos operativos se presenta la siguiente tabla:

Proceso de apoyo Sistemas

- Oficina de tecnología de Información
- Área de Operaciones de Sistema
- Área de cadena de Custodia

Procesos Operativos: Intervenidos y Control legal de las comunicaciones

- Recepción y asignación de solicitudes
- Monitoreo y Registro de Llamadas
- Formulación y entregas de Informe mediante cadena de custodia.

Figura 11

Mapeo del Subproceso de desarrollo entre el área de apoyo y operativo.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

FUENTE: Elaboración propia del Mapeo de proceso de apoyo del DIVATJ-DIRANDRO-PNP.

4.1.9 Capacitación en Seguridad de la Información.

Según los resultados obtenidos en la encuesta en el apartado de Conocimiento en la seguridad de la información, es el punto crítico debido a los resultados donde son observables la deficiencia:

Tabla 10

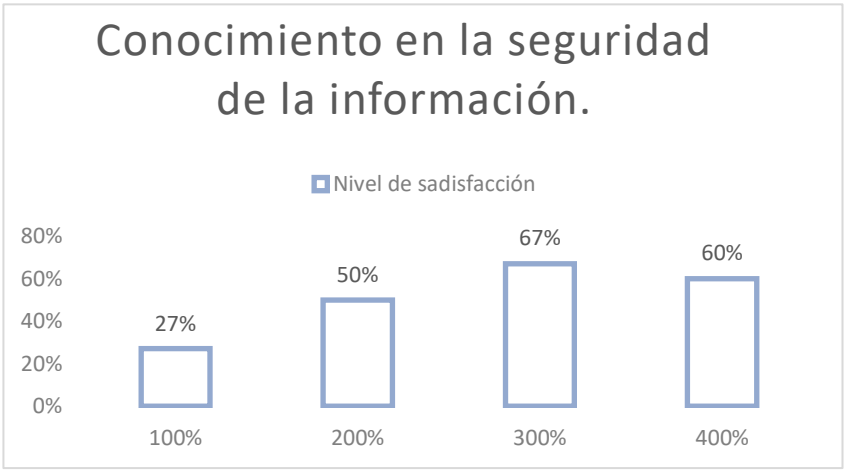
Conocimiento en la seguridad de información.

N°	Descripción	%
1.1	Posee conocimientos con respecto a la seguridad de la información.	27%
1.2	Tiene conocimientos sobre las normas que establecen la seguridad de la información.	50%
1.3	Adquiere conocimiento a travéz de las capacitaciones realizadas en la seguridad de la información por parte del DIVATJ.	67%
1.4	ɔnocimiento sobre Normas ISO 27001.	60%
1.5	Tiene conocimiento sobre la Ley de Protección de Datos Personales Ley N° 29733.	91%
1.6	Tiene conocimiento sobre la Ley Contra el Crimen Organizado Ley N° 30077.	100%

Fuente: Elaboración Propia, resultado de Encuesta Anexo 1

Figura 12

Conocimiento en la seguridad de información.



Fuente: Elaboración Propia, resultado de Encuesta Anexo 1

Es observable que es reducido el conocimiento que tiene la población de muestras de Analistas Tácticos, no cuenta con conocimientos concretos en seguridad de la información por lo que es necesario realizar capacitaciones para evitar riesgos. En tal sentido, a partir de las capacitaciones los analistas tácticos podrán, detectar y manejar correctamente cualquier contingencia que ponga en riesgo la información obtenida durante la ejecución de la intervención legal de las comunicaciones.

Para elevar los niveles de satisfacción en la capacitación de seguridad de la información se procede a realizar un plan de trabajo, en el cual se realice una ficha técnica de procedimientos en el cual se establezca las responsabilidades y establecer los procedimientos para la capacitación del personal. Véase la ficha en el Anexo N° 3.

Para su desarrollo se ejecuta la capacitación para el personal insidiando en los temas de Introducción en la Norma ISO 27001 y Seguridad de la Información,

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Gestión de Indicadores de Riesgo, Sistema de Intervención de Comunicaciones, Taller de Crimen Organizado, Recolección, Control y Análisis de Comunicaciones en el proceso de Intervención Legal, Formación de autores internos, Sistema de Soporte de Inteligencia para la vigilancia Electrónica, e Intervención y Análisis de Comunicaciones. El programa de Capacitación véase en el Anexo N° 4.

El programa de capacitación se establecerá para todo el personal comprometido en las actividades de control legal de las comunicaciones el cual es de asistencia obligatoria. Con la capacitación del personal desencadenaría una cultura de seguridad de la información lo que evitaría que la información obtenida durante la ejecución de la medida de levantamiento de seguridad de la información se sustraída y modificada.

4.1.10 Evaluación de datos.

Mediante la encuesta realizada a los analistas tácticos usuarios Sistema de Intervención de Líneas indicaron que respecto al conocimiento en seguridad de la información solo el 27% tiene un conocimiento es muy deficiente, el 50% tiene conocimientos en las normas de seguridad de la información lo cual es muy deficiente o en su defecto desconoce, el 67% de los analistas encuestados está de acuerdo que el conocimiento se adquiere mediante las capacitaciones; y por último, por medio de la función que realizan los analistas el conocimiento de la normativa vigente en temas de seguridad buena o excelente; existe una aplicación de los principios de confidencialidad e integridad de la información.

Los resultados de la primera parte de la encuesta dan como resultado que existe un 66% satisfacción en los resultados de los analistas, sin embargo, no indica

que sea optimizado los conocimientos de seguridad de la información por lo que es necesario realizar una capacitación adecuada al personal de analistas tácticos a fin de que se pueda superar la brecha de falta de conocimientos.

Respecto a las brechas de seguridad de la información, se puede asegurar que las Políticas de seguridad deben implementarse previa instrucción del personal de analistas, del cual se cumple con un 66%; adicional a ello, la organización de la seguridad de la información se ve limitada por el bajo conocimiento que cuentan los analistas tácticos.

En la segunda etapa de la encuesta realizada en la cual se determina las técnicas para la protección de datos y seguridad de la información, el 62% de los analistas desconocen donde se alojan los backup de los servidores, lo que genera que no cuentan con un conocimiento amplio y adecuado, el 49% de los analistas tiene un conocimiento muy deficiente del estado en que se encuentra el hardware que utiliza para realizar sus labores, en el siguiente ítem el resultado fue de un 72%; sin embargo, por el porcentaje obtenido aun la tendencia es de desconocimiento pero se aproxima a que existe un grupo de encuestados que cuenta con los conocimientos técnicos sobre los datos de copia de seguridad se catalogan como adecuados para su uso. El resultado obtenido en servicio prestado por el operador alterno en caso de que el principal falle se pueda resolver obtuvo como resultado que un 67% de los analistas no conoce los procedimientos ante la situación anómala que se pueda generar.

Respecto a el estado del servidor el resultado se acercó a un 71%, encontrándose en el dentro de los resultados donde el analista táctico desconoce, lo

que hace es una desventaja. El ingreso al área laboral en este sentido a la Sala donde se ejecuta las medidas especiales de investigación dio como resultado un 77%, este resultado si bien se encuentra dentro de los parámetros de desconocimiento tiende a una tendencia a ser buena u optima toda vez que existen medidas de seguridad propias de la función policial, que mantienen estable el desenvolvimiento de los analistas a sus áreas respectivas.

En relación con las pistas, tomando como pistas aquellas rutas perennizadas por la función o rastro de actividades ejecutadas por los analistas tácticos, y los controles que se ejecutan son de aceptación buena equivalente a un 80% lo cual determina que este punto fuerte en una técnica de protección de datos y seguridad de la información.

En este punto es atendible que la gestión de los activos si se cumple; sin embargo, deben ser atendidos de mejor manera procurando optimizar y actualizar las medidas de seguridad. La Seguridad ligada al personal de analistas tácticos como recurso humano primordial es de medio, debido a que es requerido establecer lineamientos adecuados para la ejecución de medidas; brecha que sería disminuida con la aplicación de capacitación acordes a la necesidad.

De lo anterior, mejorar la seguridad del entorno físico equivaliera a disminuir cualquier agente que pueda contravenir cualquier riesgo de seguridad de la información. La Gestión de la comunicación y las operaciones es una brecha que se encentra ligada a los encargados de brindar el servicio como los operadores alternos durante fallos en el operador principal; debido a que existen encargados de monitorear los servicios.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

El control de ingreso a las áreas estipulado como brecha el control de acceso es necesario implementar mayores tecnologías, sino educar a los analistas de cuál es el correcto uso y necesidad de ejecutar correctamente el ingreso y salida de la información de las áreas ejecutoras de la medida especial de investigación.

Por último, en la aplicación de herramientas para la protección de datos y la seguridad de la información, respecto a los antivirus instalados en los equipos de cómputo contesto un 63% que desconoce su eficiencia, respecto a este punto se precisó que los equipos cuentan con una red interna existe la prohibición de su uso para asuntos externos, sin embargo, la contaminación por software externos es de alto riesgo para la ejecución de las escuchas legales; asimismo, respecto a la protección los analistas tácticos mediante sus conocimientos prácticos determinaron en un 56% que es muy deficiente la protección que brinda los antivirus instalados. El ingreso a las páginas restringidas tiene una aprobación excelente al 96%, debido a su notoria aceptación.

En relación con los equipos de cómputo un 60% de los encuestados respondieron no cuentan con el conocimiento si estos se encuentran con las licencias actualizadas. Respecto a las contraseñas (password) el 75% de los analistas tiende a indicar que es bueno; sin embargo, por desconocimiento el resultado tiene una tendencia baja, lo cual debe ser elevado mediante la instrucción que se le pueda brindar a los analistas; lo que se ve reflejado en el nivel de seguridad reflejado al ingreso del sistema siendo aceptado con un 80% de los analistas.

Las brechas que se encuentran vinculadas a la adquisición, desarrollo y

mantenimiento, así como la gestión de incidentes de la seguridad de la información. Para la mejora continua del DIVATJ, es necesario que se realice una actuación por la dirección en mejorar cada una de las afirmaciones que se determinaron en la encuesta puestos que los resultados obtenidos en el Conocimiento en la seguridad de la información cuentan con un promedio del 66%, estableciendo que se encuentra dentro de los parámetros de los conocimientos en seguridad de la información aún son desconocidos para la población de analistas. Las Técnicas para la protección de datos y seguridad de la información cuenta con un promedio del 70%, que implica que le personal no cuenta con conocimientos plenos, con cierta tendencia a ser calificad como bueno; y por último, la aplicación de herramientas para la protección de datos y seguridad de la informó obtuvo un resultado promedio de 71%, como resultado de la encuesta se obtiene que el personal de analistas desconoce de los temas relacionados con las herramientas de protección de datos y seguridad, lo cual debe ser reducido con capacitaciones y aplicaciones que repotencien la protección de los datos y la seguridad de la información.

Para desarrollar mejoras en las brechas de seguridad de la información que se obtuvieron a partir de la encuesta para propuesta de mejora en el diseño de gestión de seguridad de la información bajo la Norma ISO 27001:2013, para las actividades operativas y administrativas del División de Apoyo Técnico Judicial de la Dirección Antidrogas de la Policía Nacional del Perú, es necesario implementar un diseño propio que se direccione a mejoras continuas.

4.1.10.1 Evaluación de Brechas

Mediante los resultados obtenidos en la encuesta realizada a los analistas

tácticos, se logra determinar cuáles fueron las brechas obtenidas, en tal sentido se desarrolla cuadro de brechas en el cual se observa cuales se deben cumplir para realizar mejoras en la Gestión de la Seguridad de la Información.

Las brechas por mejorar se relacionan directamente con lo evaluado en la encuesta por consiguiente la determinación e identificación de estas son observables, cada una de las brechas se cumplen; el nivel de cumplimiento no es el deseado puesto que los resultados de la encuesta los determinan.

Para enfocarse los ítems 1 y 2 se relacionan con los resultados de las preguntas 1.1 al 1.6, los cuales reflejan que un conocimiento mínimo en temas relacionados en seguridad de la información por parte de los analistas tácticos no es concreto, los cuales pueden relacionarse con niveles de impacto medio.

Los ítems 3 al 7 se ven reflejado en cuanto a las técnicas para la protección de datos y seguridad de la información en el cual un promedio porcentual del 70% en el cual se refleja que los analistas desconocen los temas relacionados a la protección de datos, existe una tendencia a cumplir con los objetivos de seguridad.

Asimismo, de los ítems 8 al 10, guardan relación a la aplicación de herramientas para la protección de datos y seguridad de la información, donde la dirección del DIVATJ, debe realizar las gestiones de adquisiciones de nuevas tecnologías que repotencien su aplicación, es por ello que se tiene en promedio que la encuesta desarrollada alcanza un 71%, lo que hace equivalente a que los analistas no cuentan con el conocimiento apropiado de estas; sin embargo, existe una tendencia al conocimiento empírico sobre el uso correcto de las herramientas de protección de datos y seguridad de la información. Por lo que es requerido un plan

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

de mantenimiento de los equipos utilizados por los analistas tacticos

Tabla 11

Cuadro de brechas, Resultado.

	DOMINIO	CUMPLE	NIVEL DE CUMPLIMIENTO
1	POLÍTICAS DE SEGURIDAD	SI	REGULARMENTE TOLERABLE O ACEPTABLE
2	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	SI	REGULARMENTE TOLERABLE O ACEPTABLE
3	GESTIÓN DE ACTIVOS	SI	REGULARMENTE TOLERABLE O ACEPTABLE
4	SEGURIDAD LIGADA A RECURSOS HUMANOS	SI	REGULARMENTE TOLERABLE O ACEPTABLE
5	SEGURIDAD FISICA Y VIRTUAL	SI	REGULARMENTE TOLERABLE O ACEPTABLE
6	GESTION DE LAS COMUNICACIONES Y OPERACIONES	SI	REGULARMENTE TOLERABLE O ACEPTABLE
7	CONTROL DE ACCESOS	SI	REGULARMENTE TOLERABLE O ACEPTABLE
8	ADQUICISIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE	SI	REGULARMENTE TOLERABLE O ACEPTABLE
9	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMCIÓN	SI	REGULARMENTE TOLERABLE O ACEPTABLE
10	GESTIÓN DE LA CONTINUIDAD DEL DIVATJ	SI	REGULARMENTE TOLERABLE O ACEPTABLE
11	CONFORMIDAD	SI	REGULARMENTE TOLERABLE O ACEPTABLE

Fuente: Elaboración Propia.

Los resultados obtenidos se dan en el contexto de cada brecha es evaluada según el riesgo

4.1.11 Diseño de la propuesta.

Para su diseño se expresará mediante la matriz en observancia de las debilidades, amenazas, oportunidades y fortaleza, que se direcciona mediante los principios de la Confidencialidad, integridad y disponibilidad.

Tabla 12

Cuadro de Diagnostico.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

ACTIVIDAD	FUENTE	DESCRIPCIÓN DE LA FUENTE	REQUISITO	DESCRIPCIÓN DEL RIESGO	CONSECUENCIA	CONTROL EXISTENTE
Asignación del caso medios de almacenamiento	Debilidad	Uso inadecuado de la información sensible acumulado en los servidores.	ANALISTA debe ejecutar acciones mediante los principios de legalidad y confiabilidad.	Que la información obtenida durante las escuchas legales pueda verse dañada.	Entorpecimiento de la investigación por conflicto de intereses.	Control de seguridad en la selección de personal. Supervisión de Jefe de Grupo. Fiscal tiene Acceso a las Comunicaciones
Monitoreo y registro de llamada en base de datos	Amenaza	Sustracción de copias de seguridad por agentes externos		Agentes externos de mantenimiento u otros que requieran acceder a la base de datos	Reducción en el rendimiento y la capacidad de escucha y análisis del analista.	Gestiones de seguridad de Jefe de Equipos
Monitoreo y registro de llamada por servicio de terceros	Debilidad	Requerimiento de personal idóneo que ejecute la medida	ANALISTA: se debe ejecutar mediante los principios de legalidad y confiabilidad.	Reasignación de casos por vínculos, pedidos del fiscal o razones técnicos o del personal	Demora del servicio, sobrecosto por uso de herramientas	Requiere autorización escrita del jefe de División.
Monitoreo y registro de llamada	Amenaza	Infraestructura de comunicaciones obsoleta en algunas locaciones del país.	ANALISTA: Ambiente adecuado y seguro de ingreso exclusivo	Fallas técnicas en los enlaces de comunicación con las empresas de comunicaciones	No registro las comunicaciones durante ese lapso tiempo.	Reporte inmediato a las empresas de comunicaciones.
Formulación y entrega de informes	Oportunidad	Mejora de tecnologías en el rubro de comunicaciones	AUTORIDADES: Cumplimiento estricto de la normativa que le aplica el protocolo de Actuación conjunta.	Implementación de sistema de video conferencia para realización de reuniones virtuales	Mayor participación de fiscales en reuniones iniciales y coordinación	Ninguno
Todas las Actividades	Fortaleza	Controles de seguridad del personal en el proceso de selección.	DIRECTORES: Principio de confidencialidad en el personal que realiza la intervención de las comunicaciones.	Daño o sabotaje en el Data center.	Perdida de información registrada en los servidores	Copia Bakup de la información de los servidores Sistemas de prevención y detección de riesgos.

Fuente: Elaboración propia.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

4.1.11.1 Desarrollo de protocolo de seguridad de información.

Para un buen funcionamiento de los protocolos de Seguridad de la Información de los productos generados por la División de Apoyo Técnico Judicial se procede a la formulación de una ficha de técnica de procedimientos el cual se establezcan mediante los pilares de confiabilidad, integridad y disponibilidad.

El desarrollo de un protocolo como objetivo es asegurar que las comunicaciones obtenidas durante la intervención legal de las comunicaciones como instrumento procesal legal bajo los principios de legalidad y confiabilidad.

El procedimiento se inicia con la recepción de la solicitud de intervención, durante el proceso de captación de las informaciones de las empresas proveedoras se almacena en una base de datos a cargo de la Oficina de Tecnología de la información y comunicación; asimismo, hace alcance al momento propio de la entrega de los productos resultantes tales como las actas y audios entregados bajo el protocolo de cadena custodia.

4.2 Mecanismos de control.

4.2.1 Mecanismo de control para entrega de Actas de Recolección y control.

Mediante la actividad de recolección de comunicaciones, escucha, analiza y difusión; como primer término se ejecutan las reuniones de la comunicación con las autoridades comprometidas tales como el Fiscal de Caso y Pesquisa de caso.

Posterior a la reunión de coordinación se estableces las estrategias de las informaciones relevantes los cuales solo son conocidos por los participantes.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

La ejecución de la seguridad de la información entregada mediante actas se establece como primer filtro el ingreso a las instalaciones ejecutado por el Oficina de Seguridad en paralelo ejerce un segundo anillo de seguridad lo ejecuta el Jefe de Grupo.

4.2.2 Mecanismo de control para entrega de Audios mediante cadena de Custodia.

Una vez que el Analista Táctico mediante la recolección de la comunicación durante la escucha, análisis y difusión; se separan las informaciones obtenidas, indicando su relevancia las cuales son separadas mediante filtro en una base de datos; posteriormente a la solicitud expresa del Fiscal de Caso, es entregado mediante cadena de custodia el Grabado de audios y datos en soporte magnético encriptado.

La ejecución de la entrega se realiza en las instalaciones del DIVATJ, mediante la Oficina de Seguridad, como primer anillo de seguridad, posterior mediante conocimiento de la Dirección y ejecutado por el jefe de la Oficina de Tecnología de Información y Comunicación, y Encargado de Cadena de Custodia.

4.2.3 Mecanismo de control durante la intervención legal de comunicaciones

Es el acto más importante ejecutado por el Analista Táctico que al recibir el código de asignación de caso por el Área de Operación de Sistemas, procede a verificar e iniciar la ejecución de la medida.

Una vez generada la medida el control de la ejecución y no se filtre la

información que sea relevante o no relevante para una investigación, es por ello que la selección del personal por el comité conformado por la Dirección, Jefe de Administración y Jefe de UNITIC, tienen la responsabilidad que el personal asignado en la DIVATJ tenga características dentro del principio de confiabilidad, con características de alta discreción y compartimentaje.

El control inmediato se transfiere al Jefe de Grupo, en el caso concreto de que es el funcionario que cuenta con el contacto directo con el analista.

4.2.4 Determinación de responsabilidades

La distribución de las responsabilidades para el control y supervisión de los mecanismos de seguridad se encuentran establecidos por la Dirección, Jefaturas y encargados de área; presentado en el siguiente detalle

- Control de seguridad en la selección de personal.
    - Dirección
    - Jefe Administración
    - Jefe de UNITIC.
    - Jefe de Oficina de Tecnología de Información y Comunicación
    - Jefe de Sala de Intervenciones
    - Jefe de Grupo.
- Acceso a las Comunicaciones
    - Fiscales de las Fiscalías Especializadas
    - Analista Táctico
    - Analistas de Grupo Operativo
    - Encargado de Área de Cadena de Custodia

- Requiere autorización escrita del jefe de División.
    - Salida de Informes
    - Entrega de Cadena de Custodia
- Requiere autorización de entrega de actas de recolección y control.
    - Jefe de Grupo
    - Analista Táctico
- Reporte inmediato a las empresas de comunicaciones.
    - Dirección
    - Jefe de UNITIC
    - Jefe de Oficina de Tecnología de Información y Comunicación
- Copia Bakup de la información de los servidores Sistemas de prevención y detección de riesgos.
    - Jefe de Oficina de Tecnología de Información y Comunicación
    - Encargado de Operación de Sistemas
    - Encargado de Cadena de Custodia
- Gestiones para diferentes servicios de apoyo interno.
    - Jefe de Administración
    - Encargado de Área de Recursos Humanos
    - Encargado de Área de Logística
    - Encargado de Área de Recepción Documentaria
- Gestiones para diferentes servicios de apoyo externo.
    - Jefe de Oficina de Seguridad.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

5 CAPÍTULO V: SUGERENCIAS

CONCLUSIONES

En base a la información recopilada y los datos detectados, se concluye que un sistema gestión de la seguridad de la información basado en el ISO 27001, se encuentra planificado y según los datos aplicados es posible su implementación de un diseño de mejora de un Sistema de Gestión de Seguridad de la Información implementando como primera medida relacionada a una capacitación en temas de Seguridad de la información, posterior a ello se realiza formulación de técnicas para la protección y seguridad de datos, e implementar herramientas adecuadas para la protección de datos y seguridad de la información.

La ejecución de un sistema de gestión de seguridad basado en el ISO 27001, es aplicable dentro de los procesos administrativos de recolección de comunicaciones, formulación de actas, entrega de audios en cadena de custodia, a los operadores de justicia.

La evaluación de cada área debe ser realizada mediante la presencia física de los responsables de área a fin de establecer correcciones que deben ser subsanadas y establecer nuevos procesos perfilando las anomalías. Mediante un método practico en la observancia de los procesos de entrega hasta el cliente final.

Mediante el un análisis de las brechas es posible detectar en qué estado actual nos encontramos y que puntos son de especial atención para mejora políticas de seguridad, la gestión de activos, seguridad física y del entorno, control de

accesos; asimismo en la adquisición, desarrollo y mantenimiento de sistemas de información y gestión de incidentes de seguridad de la información.

La División de Apoyo Técnico Judicial con el ISO 27001 garantiza la seguridad de las informaciones y los datos de un sistema mediante la identificación, clasificación y valorización de los activos de información a fin de desarrollar procesos que mediante el análisis de riesgo y políticas en cultura de seguridad en todos los niveles.

Los mecanismos de control del ISO 27001 garantizan que las políticas, protocolos y directivas internas sean desarrolladas la seguridad de la información en una organización. La implementación adecuada de estos controles ayuda a prevenir la perdida, el robo o sustracción de la información confidencial. Además, estos mecanismos de control ayudan a garantizar la confidencialidad, integridad y disponibilidad de la información, lo que es esencial para mantener la confianza de los clientes internos y externos, usuarios y partes interesadas. También son importantes para cumplir con las regulaciones y leyes de protección de datos, así como para evitar posibles responsabilidades y consecuencias legales.

La implementación de los mecanismos de control del ISO 27001 maneja su importancia en garantizar la seguridad y protección de la información en la DIVATJ para mantener su buen funcionamiento y cumplimiento de las políticas, directivas y normas internas.

La capacitación del ISO 27001 ayuda a los miembros del equipo de la empresa a entender como implementar correctamente estos controles de seguridad

y cómo manejar los incidentes de seguridad si ocurren. Además, la capacidad ayuda a mejorar la cultura de la empresa y fomenta un enfoque proactivo hacia la seguridad de la información en toda la organización.

Implementar un sistema de gestión de seguridad de la información, es para el DIVATJ de la Dirección Antidrogas es de suma importancia para protección y defensa de los datos obtenidos, siendo estos los activos más importantes para la organización.

SUGERENCIAS

La División de Apoyo Técnico Judicial mediante una estructura enfocado en un modelo de gestión de seguridad de la información se basa en los resultados del diagnóstico de seguridad de la información y el diseño teórico de este estudio se fundamenta la aplicabilidad de un ISO 27001, en los procesos de la gestión de entrega de los productos resultantes de la intervención legal de las comunicaciones.

Como primera medida es fundamental generar capacitaciones que se incluya temas de seguridad de la información, así como, técnicas de protección de datos y seguridad de la información; además, mediante las áreas correspondientes se implementen herramientas para la protección de datos y seguridad de la información.

La DIVATJ-DIRANDRO; coordina con las partes interesadas que tienen la necesidad de proteger los datos, fundamentar que desde el proceso de su obtención, recolección, análisis y difusión; debe establecer un protocolo enfocado en la calidad a fin de aseverar su intangibilidad, direccionado en las actas y recolección de audios; siendo participes la Oficina de Intervenciones y el Área de cadena de

Custodia. Por lo tanto, es necesario analizar los procesos en estas áreas para determinar los activos que deben protegerse. Para llevar a cabo esta tarea, se realizaron entrevistas a los actores de seguridad de la información, desde el primer eslabón de la cadena, hasta la Dirección que se encargan de la revisión de los documentos pertinentes.

Dado que la principal necesidad que tiene la DIVATJ-PNP, en establecer un sistema de gestión de seguridad se debe crear un grupo en seguridad de la información que establezca funciones y responsabilidades durante el proceso de la entrega de productos; y sentar las bases para la creación de nuevas políticas que sean útiles en resolver hechos que contravengan en la seguridad e la información.

Una correcta estructura de formalizada para la gestión de la seguridad de la información; lo que se sugiere que se debe establecer mediante tres categorías: Medidas organizativas que incluye la creación de una política de seguridad de la información, la gestión de los riesgos de seguridad, la forma de iniciar y tratar incidentes de seguridad, la asignación de responsabilidades y la formación de los empleados mediante la capacitación. También implica la reconciliación de los procedimientos de entrega de productos con los requisitos de seguridad de la información. La segunda categoría dirigida a los Controles de seguridad Físicos, los cuales protegen los activos físicos de la organización, como los servidores, los equipos de red y los datos en papel de seguridad rotulado. Algunos ejemplos de controles físicos son el control de acceso a las instalaciones, la vigilancia y la protección contra riesgos ambientales. Por último, establecer control de seguridad lógico, que protegen los activos digitales de la organización, como los datos

almacenados en servidores, bases de datos y aplicaciones. Algunos ejemplos de. Controles lógicos incluyen firewalls, sistemas de detección y prevención de instrucciones, antivirus y sistemas de autentificación.

Establecer la capacitación del ISO 27001 toda vez que es importante para la DIVATJ PNP pueda cumplir con los requerimientos de seguridad de la Información. El ISO 27001 establece un marco y un conjunto de controles de seguridad para proteger la información contra los riesgos de seguridad cibernética, como el robo de datos y la vulneración de la privacidad, en tal sentido en el Anexo N° 03 se presenta un cuadro tentativo de las capacitaciones para los analistas tácticos el cual mejora las capacidades de los analistas tácticos y personal encargado de las áreas responsables de la administración de la información sensible.

Para aplicación del ISO 27001, es importante utilizar métodos ágiles en la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI) para asegurar la eficacia y eficiencia en la gestión de los riesgos de seguridad de la información. Además, se recomienda evitar el uso de plantillas de políticas de seguridad, ya que cada organización tiene sus propios riesgos y necesidades de seguridad, por lo que es importante personalizar las políticas y procedimientos de seguridad de la información según las necesidades específicas de la organización. Asimismo, es necesario saber utilizar el software para evaluar los riesgos de seguridad de la información, ya que esto puede ayudar a identificar y tratar los riesgos potenciales de manera más eficiente. Además, se sugiere que la organización determine primero lo que necesita para que tenga los mayores beneficios ante una implantación de un SGSI según ISO 27001.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Aplicar la norma ISO 27001 de manera efectiva, se debe utilizar métodos ágiles, personalizar las políticas y procedimientos de seguridad de la información, saber utilizar el software para evaluar los riesgos de seguridad de la información y determinar primero lo que necesita la organización para obtener los mayores beneficios de la implantación del SGSI. Se sugiere que la organización determine primero lo que necesita para que tenga los mayores beneficios ante una implantación de un SGSI según ISO 27001.

BIBLIOGRAFÍA

Blumsztein, E. C. (2007). Implantación del sistema de gestión de seguridad de la información en una empresa compleja. *Memoria Investigaciones en Ingeniería*, (5), 77-87.

Calder, A. (2017). *Nueve pasos para el éxito: Una visión de conjunto para aplicación de la ISO 27001:2013.* Itgp.

Cano, J y Almanza, A. (2020). Estudio de la evolución de la Seguridad de la Información en Colombia: 2000-2018. *Revista Ibérica de Sistemas y Tecnologías de Información* , (E27), 470-483.

Coello, R. R., & Pico, L. M. (2018). *Análisis de las ventajas y desventajas del sistema de gestión de la seguridad de la información y su influencia en la competitividad de las empresas que utilizan Cloud Computing y Big Data en el Ecuador*.

Cordero Torres, K. G. (2015). *Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgos de seguridad de la información* (Bachelor's thesis, Universidad del Azuay).

DEPATJ. (2019). *Procesos Estrategicos.* Lima.

DEPATJ. (2020). *Memoria Anual Depatj Dirandro.* Lima.

DIRANDRO. (2022). *Direccion Antidrogas Trabajando por el Perú y el Mundo.* Lima: Dirección Antidrogas.

Diaz, A. (2010). *Sistema de Gestión de la Seguridad de la Información*. Revista Calidad, (IV), 18–20.

Duque, A. C. (2017). *Metodología para la gestión de riesgos. Como integrar la seguridad a los objetivos estratégicos de los negocios de una manera costo-beneficiosa*. Retrieved April 10, 2017, from http://www.ridsso.com/documentos/muro/207_1469148692_57916e1488c74.pdf

Emilio, C. M. H. (2015, 18 abril). *Identificación de vulnerabilidades de seguridad en el control de acceso al sistema de gestión documental, mediante pruebas de testeo de red en la empresa ingelec S.A.S*. 10596/3451. https://repository.unad.edu.co/handle/10596/3451

Gómez, L. y. (2012). *Guia de aplicacon de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes .* ESPAÑA: AENOR EDICIONES.

Hamdi, Z., Anir Norman, A., Nuha Abdul Molok, N. & Hassandoust, F. (2019, 1 diciembre). A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors. *Journal of Physics: Conference Series*, *1339*(1), 012103.

Huerta, A. (2012). *Introducción al análisis de riesgos - Metodologías (I)*. Security Art Work. Recuperado 17 de octubre de 2022, de https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

ICONTEC. (2009). *Norma Técnica Colombiana. NTC-ISO/IEC 27005. Tecnología de Información. Técnicas de Seguridad. Gestión del riesgo en la seguridad de la información.* Retrieved from https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27005.pdf.

Javier, A. (2008, 1 enero). *Seguridad de la información. Redes, informática y sistemas de información*. Paraninfo.

Ladino, M. I., Villa, P. A., & López, A. M. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia et technica*, *17*(47), 334-339.

Lema, R. & Donoso, G . (2018). *Implementación de un sistema de gestión de seguridad de información basado en la Norma ISO 27001:2013 para el control físico y digital de docuemntos aplicado a la empresa LOCKERS S.A.* Obtenido de Repositorio

López, A. (s.f.). *ISO27000.ES*. Obtenido de Serie 27K: https://www.iso27000.es/iso27000.html

Melo, V., & Hernando, A. (2008). El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001. *Revista de derecho*, (29), 333-366.

MININTER. (2020). *Plan Estrategico Institucional.* Lima: Ministerio Del Interior.

Molano-Espinel, R. A. (2017). *Estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma ISO 27001 en el área de TI para la empresa Market Mix*. Repositorio Institucional Universidad Católica de Colombia - RIUCaC. http://hdl.handle.net/10983/15240

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Molina-Miranda, M. F. (2017). Análisis de riesgos de centro de datos basado en la herramienta pilar de Magerit. *Espirales revista multidisciplinaria de investigación*, *1*(11).

Montaño Ardila, V. M. (2010). Beneficios para el gobierno empresarial: Articulando COBIT con ISO 27000 para la exitosa implantación de un gobierno de TI. *ECONÓMICAS CUC*.

Monzó, G. (2020). *Aplicación de la ISO 27001:2017 Tecnología de la Información.Tecnicas de Seguridad.Sistema de Gestión de Seguridad de la Información (SGSI). Requisitos*. Obtenido de Universidad Politécnica de Valencia: https://riunet.upv.es/handle/10251/133924

Muñoz, A. (2003). Sistemas de información en las empresas. *Hipertext. net*, *1*(10).

Nieves, A. C. (6 de junio de 2017). *Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013.* Obtenido de Politécnico Grancolombiano-Institución Universitaria: http://hdl.handle.net/10823/994

Nieves, A. C. (6 de junio de 2017). *Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013.* Obtenido de Politécnico Grancolombiano-Institución Universitaria: http://hdl.handle.net/10823/994

PJ, M. P. (2014). *Protocolo De Actuación Conjunta-Intervencion de Registro de las Comunicaciones.* Lima .

PNP. (2021). *Manual de Organización y Función DEPATJ.* LIMA.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Robles, R., & Rodriguez de Roa, Á. (2016). La gestión de la seguridad en la empresa. *Comite de Entidades de Certificación de la AEC*, 14-18.

Sanchez, M. (2015). El Análisis Matemático aplicado al CALCULO DE LA MUESTRA El tamaño de la muestra es (in)finito. *Ciencia UNEMI*, *2*(3), 40-45. https://doi.org/10.29076/issn.2528-7737vol2iss3.2009pp40-45p

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of Information Security Risk Assessment (ISRA). *Computers & Security*, *57*, 14–30. http://doi.org/http://dx.doi.org/10.1016/j.cose.2015.11.001

Serrano, J. E. R., Salazar, V. H., Ruiz, X. N., & Guillén, C. N. (2019). Gestión de Riesgos de TIC en hospitales públicos. Revista Ibérica de Sistemas e Tecnologias de Informação,(E20), 280-291.

Quiroga, L. (2002). *Gestión de información, gestión del conocimiento y gestión de la calidad en las organizaciones*. *ACIMED,* 10

Valencia-Duque, F. J.-A. (2017). *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000.* Obtenido de Revista lbérica de Sistemas y Tecnologías de Información: 10.17013/risti.22.73–88

Valencia, J. y Orozco, M. (2017). *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000.* Obtenido de Revista lbérica de Sistemas y Tecnologías de Información: 10.17013/risti.22.73–88

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Vanegas, A., & Pardo, C. J. (2014). Hacia un modelo para la gestión de riesgos de TI en MiPyMEs : MOGRIT. *Revista S&T*, *12*(30), 35–48.

Vinlasaca Lema, R. C. (2018). *Implementación de un sistema de gestión de seguridad de información basado en la Norma ISO 27001:2013 para el control físico y digital de docuemntos aplicado a la empresa LOCKERS S.A.* Obtenido de Repositorio Universidad de las Fuerzas Armadas: http://repositorio.espe.edu.ec/handle/21000/14397

Yenque, J. ,. (2002). KAIZEN 0 LA MEJORA CONTINUA. En J. Santana, *INDUSTRIA DATA* (págs. 62-65). Lima: https://d1wqtxts1xzle7.cloudfront.net/62229726/KAIZEN_0_LA_MEJORA_CONTINUA20200228-70564-9hpl3d-with-cover-page-v2.pdf?Expires=1661130051&Signature=d0w2XWaUhrx1npMaAF~svjNuSL9fURvyvPKtbpIK8vpkdLu6drpmQEAicxA3zgjIwmqG13eWpVnO6zpeOB5sFk2El07LmiOCHjya7knxIrW.

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Anexos 01: ENCUESTA

PROPUESTA DE MEJORA EN EL DISEÑO DE GESTION DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO 27001:2013, PARA LAS ACTIVIDADES OPERATIVAS Y ADMINISTRATIVAS DEL DIVISIÓN DE APOYO TÉCNICO JUDICIAL DE LA DIRECCIÓN ANTIDROGAS DE LA POLICÍA NACIONAL DEL PERÚ.

Objetivo: Determinar el nivel de seguridad de la información en la Oficina de Sala de Intervención y Oficina de tecnología de Información y Comunicación basada en la Norma ISO 27001 en la División de Apoyo Técnico Judicial de la Dirección Antidrogas, para seleccionar la mejor estrategia.

DATOS:
CARGO: _____ Antigüedad en la DIVPATJ-DIRANDRO: _____ Nivel de educación: Técnico:____ Tecnológico:____ Profesional: _____ Otros: _____

Marque con una “X” en las casillas correspondientes la opción que considere pertinente:

[E]excelente (5) [B] Bueno (4) [NT] No tiene Conocimiento (3) [MD] Muy deficiente (2) [NT] regular (1)

Datos cumplimiento de los indicadores					
CATEGORIAS / INDICADORES	E (5)	B (4)	NT (3)	MD (2)	R (1)
1. CONOCIMIENTO EN SEGURIDAD DE LA INFORMACIÓN					
LA DIVISIÓN DE APOYO TÉCNICO JUDICIAL A IMPARTIDO CAPACITACIONES ADECUADA EN CUANTO NORMAS DE SEGURIDAD DE LA INFORMACIÓN TENIENDO EN CUNETA LO SIGUIENTE:					

1.1	Posee conocimientos con respecto a la seguridad de la información.					
1.2	Tiene conocimientos sobre las normas que establecen la seguridad de la información.					
1.3	Adquiere conocimiento a través de las capacitaciones realizadas en la seguridad de la información por parte del DIVATJ.					
CONOCIMIENTO DE LA NORMATIVIDAD						
1.4	Se tiene conocimiento sobre Normas ISO 27001.					
1.5	Tiene conocimiento sobre la Ley de Protección de Datos Personales Ley N° 29733.					
1.6	Tiene conocimiento sobre la Ley Contra el Crimen Organizado Ley N° 30077.					
2. TÉCNICAS PARA LA PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN						
PARA LA PROTECCIÓN DE LA INFORMACION SE DEBE TENER EN CUENTA LO SIGUIENTE						
2.1	El medio donde se alojan los backup de los servidores en ¿qué estado se encuentra?					
2.2	Los hardware que utiliza ¿qué estado se encuentra?					
2.3	Los datos que se verifican después de realizadas las copias de seguridad se catalogan como:					
2.4	El servicio prestado por el operador alterno en caso de que el principal falle lo podemos resolver.					
2.5	En qué estado se encuentra el servidor alterno.					
ACCESO A EL AREA DE SERVIDORES O BACKUP						
2.4	El sistema de control para el ingreso a esta área se define como:					
2.5	Como se define las pistas dejadas al ingresar a esta a las Oficina de Sala de Intervenciones y Oficina de Tecnología de Información.					
2.6	Como se definen los controles que se ejerce a los usuarios de la Oficina de Sala de Intervenciones y Oficina de Tecnología de Información.					
3. APLICACIÓN DE HERRAMIENTAS PARA LA PROTECIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN.						
HERRAMIENTAS PARA LA PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN						
3.1	El antivirus instalado en los equipos de cómputo del DIVATJ se puede definir como adecuado.					

3.2	El nivel de protección brinda el antivirus instalado en los equipos de cómputo.					
3.3	Como se define las restricciones a paginas no permitidas en la DIVATJ.					
ESTRATEGIA PARA LA PROTECCIÓN DE LA INFORMACIÓN						
3.4	Los equipos de cómputo tienen licenciamiento vigente.					
3.5	Como define la contraseña para el ingreso al sistema.					
3.6	El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema.					

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Anexos 02: RESULTADO DE ENCUESTA DE SADISFACCIÓN.

Anexo B. Escala de Likert

ITEM \ ENCUESTADO	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
1. Conocimiento en la seguridad de la Información																																																							
Posee conocimientos con respecto a la seguridad de la información.	2	2	2	1	1	2	1	1	1	2	2	1	1	1	1	1	1	1	2	2	2	1	2	1	2	1	1	2	1	2	1	2	1	1	2	1	2	1	1	1	2	2	2	2	1	1	1	1	1	1	1	1	1	1
Tiene conocimientos sobre las normas que establecen la seguridad de la información.	3	3	2	3	3	3	3	3	2	2	3	2	2	3	3	3	3	2	2	2	3	3	3	3	3	3	3	2	2	3	2	3	3	3	2	2	2	2	3	3	2	2	2	2	2	2	3	2	3	2	3	2	2	2
Adquiere conocimiento a travez de las capacitaciones realizadas en la seguridad de la información por parte del DIVATJ.	4	3	3	3	4	4	3	3	3	3	3	4	4	4	3	3	3	3	4	3	3	4	3	4	4	4	4	3	3	3	3	3	4	3	3	3	4	3	3	4	3	4	4	4	3	3	3	3	3	3	4	4	3	3
Se tiene conocimiento sobre Normas ISO 27001.	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Tiene conocimiento sobre la Ley de Proteción de Datos Personales Ley N° 29733.	4	4	4	4	4	4	5	5	5	4	4	4	4	4	5	5	5	5	5	4	5	5	5	4	4	5	5	5	5	5	5	5	4	4	4	4	4	4	4	5	4	4	5	4	5	5	5	5	5	5	5	5	5	5
Tiene conocimiento sobre la Ley Contra el Crimen Organizado Ley N° 30077.	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
2. Tecnicas para la protecion de Datos y Seguridad de la Información																																																							
El medio donde se alojan los backup de los servidores en ¿qué estado se encuentra?	3	3	3	3	2	3	3	3	3	5	5	3	3	3	3	4	3	3	3	3	3	2	3	4	3	3	5	2	4	3	4	3	3	3	3	3	3	3	3	3	3	2	3	3	5	2	2	3	3	3	3	3	3	3
Los hardware que utiliza ¿qué estado se encuentra?	3	3	1	3	3	1	3	2	1	3	3	3	3	1	3	3	3	2	3	1	3	3	3	2	2	3	3	3	3	1	3	1	3	3	3	2	1	3	3	3	3	3	3	2	2	3	2	2	2	2	2	1	3	3
Los datos que se verifican despues de realizadas las copias de seguridad se cataloga como:	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3	5	4	5	3	3	5	5	3	5	4	3	3	5	3	3	4	4	4	5	5	5	3	3	3	3	3	4	5	3	4	4	4	4	3	4	3	3
El servicio prestado por el operador alterno en caso de que el principal falle lo podemos resolver.	3	3	3	3	4	3	3	5	3	3	3	3	4	3	3	3	3	3	3	3	5	5	3	3	3	3	5	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	5	3	3	3	3	5
En que estado se encuenta el servidor alterno.	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	5	3	3	3	4	5	4	3	3	4	5	5	3	3	3	3	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3	5	4
El sistema de control para el ingreso a esta área se define como:	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	3	3	4	4	4	4	4	4	4	4	4	3	4	4	3	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	3	4	4	4	4	3	4	4

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Como se define las pistas dejadas al ingresar a esta a las Oficina de Sala de Intervenciones y Oficina de Tecnologia de Informaición.	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
Como se definen los controles que se ejerce a los usuarios de la Oficina de Sala de Intervenciones y Oficina de Tecnologia de Informaición.	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
3. Aplicación de Herramientas para la protección de datos y la seguridad de la información.																																																						
El antivius instalado en los equipos de computo del DIVATJ se puede definir como adecuado.	2	5	3	3	3	3	4	3	3	2	3	3	4	5	3	3	3	4	3	2	3	3	3	4	3	2	4	3	3	2	2	3	2	3	3	4	3	3	5	3	3	3	5	4	2	3	3	3	5	3	2	2	3	3
El nivel de protección brinda el antivirus instalado en los equipos de computo.	3	3	3	3	2	2	3	3	3	3	2	3	3	3	3	3	2	3	2	3	3	3	3	2	3	3	3	3	3	2	3	3	3	2	2	3	3	3	3	3	3	3	3	3	3	3	2	3	2	3	3	2	3	3
Como se define las restricciones a paginas no permitidas en la DIVATJ.	5	5	5	4	5	5	5	5	5	5	4	4	5	5	5	4	5	4	5	5	4	4	5	5	5	4	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5	5	4
Los equipos de computo tienen licenciamiento vigente.	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Como define el password para el ingreso al sistema .	4	4	4	4	4	4	4	4	4	3	4	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4	3	4	4	4	4	3	4	4	3	4	4	4	3	4	3	4	4	3	4	4	3	4	4	4	3	3	4	4
El nivel de seguridad cumple con los parametros establecidos para el ingreso al sistema.	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Anexos 03: FICHA TÉCNICA DE PROCEDIMIENTO DE CAPACITACIÓN.

POLICÍA NACIONAL DEL PERÚ | PERÚ Ministerio del Interior

FICHA TÉCNICA DE PROCEDIMIENTO

Nombre:	Selección de Personal	**Tipo:**	Apoyo
Código:	DIVATJ-PRO-001	**Versión:**	1.0
Dueño del procedimiento:	Responsable de Apoyo Técnico Judicial		

Objetivo del procedimiento:

Establecer el Protocolo para la selección del personal de la División de Apoyo Técnico Judicial (DIVATJ) – DIRANDRO PNP, con la finalidad de establecer los controles y responsabilidades en este proceso de capacitación de Seguridad de la información.

Alcance del procedimiento:

Este procedimiento es aplicable a todos los procesos involucrados en el Sistema de Gestión de la seguridad de la Información.

Base normativa

1. Norma ISO 27001

Siglas y definiciones

1. DIVATJ: División Apoyo Técnico Judicial de la Dirección Antidrogas

Requisitos para iniciar el procedimiento:

Descripción del requisito (entradas)	Fuente (proveedor)
- Perfil de Puesto - Relación de Personal postulante (Escuela de Formación Policial)	Personal del Área Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones

Descripción de actividades

Nº	Descripción de la actividad	Unidad de organización	Responsable
1.	Elaborar el Informe y Plan de Trabajo, sobre la necesidad de personal para los puestos que se requieren cubrir y enviar al Director Antidrogas para su aprobación y la del Comandante General de la PNP.	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Responsable de Administración
2.	Realizar la convocatoria considerando los siguientes criterios: • El grado, mínimo S3 y máxima ST2 • Años de servicio: mínimo 01 y máximo 25 • Deseable haber participado en cursos de capacitación o especialización en TID, Crimen Organizado, terrorismo, Lavado de Activos, inteligencia. • Deseable tener experiencia laboral en el campo de investigación e inteligencia.	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Equipo Responsable Autorizado
3.	Solicitar información personal del candidato (a el mismo y/o a las entidades a cargo de brindar información referencial), • Hoja de vida • Hoja de Información Básica PNP registrados en el Sistema Integrado de Gestión de la Carrera de la PNP.	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Equipo Responsable Autorizado

	• Referencias otorgadas por los organismos de inteligencia de la PNP y MININTER.		
4.	Evaluar al personal candidato en los siguientes aspectos: • Evaluación de competencias • Entrevistas personales • Pruebas psicométricas • Referencias de Contrainteligencia	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Equipo Responsable Autorizado
5.	Evaluar al personal candidato en los siguientes aspectos: • Confiabilidad, • Entorno social • Situación patrimonial, • Evaluación psicométrica, • Uso de polígrafo u otros medios tecnológicos.	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Equipo Responsable Autorizado
6.	Una vez contratado el personal, proceder con la inducción en el aspecto técnico el Sistema de Intervención de las Comunicaciones, el aspecto legal / procedimental y en las medidas de seguridad personal, restricciones y prohibiciones.	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Equipo Responsable Autorizado
Fin del procedimiento			

Documentos que se generan:	
Productos o servicios	**Destinatario**
Evaluaciones de selección Declaración jurada	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)

Registros
1. Lista Maestra de Documentos Internos 2. Lista Maestra de Documentos Externos.

Proceso relacionado	**Formatos utilizados en el procedimiento**
	-

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Anexos 04: PROGRAMA DE CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

PROGRAMA DE CAPACITACIONES	Versión	1
	Fecha	
	Página	1 de 1

N°	SEMANAS / NOMBRE DE LA CAPACITACIÓN	TIPO	HRS	PROCESOS INVOLUCRADOS	RESPONSABLE	ACCION	Jul-23				Ago-23				Set-23				Oct-23				Nov-23				Dic-23					%	OBSERVACIONES
							1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4			
1	Sistema Básico de Intervencion de Comunicaciones.	Entrenamiento	32	asistentes obligatorios (08) Analistas Tácticos	JSI Telecom	Programado		P	P																					2	100.0%	
						Ejecutado		E	E																					2		
2	Taller de Crimen Organizado	Seminario	30	* asistentes obligatorio (115) Analistas Tácticos * asistentes libres (35)	Pesquisas de Unid. Policiales	Programado		P	P																					2	100.0%	
						Ejecutado		E	E																					2		
3	Recolección Control y Análisis de las Comunicaciones en el Proceso de Intervención Legal	Diplomado	108	* asistentes obligatorios(42) Analistas Tácticos * asistentes libres (12)	Universidad ESAN	Programado	P	P	P	P	P	P																		6	100.0%	
						Ejecutado	E	E	E	E	E	E																			6		
4	Sistema Avanzado de Intervencion de Comunicaciones.	Entrenamiento	40	asistentes obligatorios (32) efectivos Analistas Tácticos y Adm. de Sistemas	JSI Telecom	Programado							P	P	P	P														4	100.0%	
						Ejecutado							E	E	E	E														4		
5	Introducción en la Norma ISO 27001 y Segurida de la Información	Taller	4	203 efectivos Todo el Personal	DIVATJ	Programado									P	P	P	P												4	100.0%	
						Ejecutado									E	E	E	E												4		
6	Gestión de Indicadores de calidad	Taller	4	16 efectivos Jefes	DIVATJ	Programado												P	P	P										3	100.0%	
						Ejecutado												E	E	E										3		
7	Formación de Auditores Internos	Curso	9	5 efectivos Jefes y Analistas	DIVATJ	Programado													P	P	P									3	100.0%	
						Ejecutado													E	E	E									3		
8	Sistema de Soporte de Inteligencia para Vigilancia Electrónica	Entrenamiento	24	4 efectivos Jefes	ISS World (Panama)	Programado															P	P	P	E						4	100.0%	
						Ejecutado															E	E	P	E						4		
9	Intervención y Análisis de Comunicaciones	Capacitación	240	23 Efectivos Analistas Tácticos	ESANDRO	Programado																		P	P	P	P	P		5	100.0%	
						Ejecutado																		E	E	E	E	E		5		
						Programado	3				4				2				3				1				1						
						Ejecutado	3				4				2				1				2				0					**100.0%**	
						Cumplimiento	100%				100%				100%				100%				100%				100%						

% DE CUMPLIMIENTO DEL PROGRAMA DE CAPACITACIONES	**100.0%**

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Anexos 05: PROGRAMA DE MANTENIMIENTO PARA EL SISTEMA DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

	PROGRAMA DE MANTENIMIENTO PARA EL SISTEMA DE LA GESTIÓN DE LA SEGURIDAD.	Versión	*1*
		Fecha	
		Página	*1 de 1*

N°	CÓDIGO	ENCARGADO	ACCION	Ene-23				Feb-23				Mar-23				Abr-23				May-23				Jun-23				Jul-23				Ago-23				Set-23				Oct-23				Nov-23				Dic-23					%	OBSERVACIONES
				1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4			
1	L1	DIVATJ	Programado			P	P																																											2	0.0%	
			Ejecutado																																																0		
2	L2	DIVATJ	Programado							P	P																																							2	0.0%	
			Ejecutado																																															0		
3	L3	DIVATJ	Programado											P	P																																		2	0.0%	
			Ejecutado																																															0		
4	L4	DIVATJ	Programado															P	P																														2	0.0%	
			Ejecutado																																															0		
5	S1	DIVATJ	Programado	P	P	P	P																																										4	0.0%	
			Ejecutado																																															0		
6	S2	DIVATJ	Programado					P	P	P	P																																						4	0.0%	
			Ejecutado																																															0		
7	S3	DIVATJ	Programado									P	P	P	P																																		4	0.0%	
			Ejecutado																																															0		
8	H1	DIVATJ	Programado																					P	P	P	P																						4	0.0%	
			Ejecutado																																															0		
9	H2	DIVATJ	Programado																									P	P	P	P																		4	0.0%	
			Ejecutado																																															0		
10	H3	DIVATJ	Programado																													P	P	P	P														4	0.0%	
			Ejecutado																																															0		
11	H4	DIVATJ	Programado																																	P	P	P	P										4	0.0%	
			Ejecutado																																															0		
12	H5	DIVATJ	Programado																																										P	P	P	P					4	0.0%	
			Ejecutado																																															0		
13	T1	DIVATJ	Programado	P	P																																										P	P	4	0.0%	
			Ejecutado																																															0		
14	T2	DIVATJ	Programado												P												P																						4	0.0%	
			Ejecutado																																															0		
15	T3	DIVATJ	Programado																																													P	P	P	P	4	0.0%	
			Ejecutado																																															0		
52			Programado	8				6				7				2				0				5				4				4				5				0				4				7					**0.0%**	
0			Ejecutado	0				0				0				0				0				0				0				0				0				0				0				0						

% DE CUMPLIMIENTO DEL PROGRAMA DE MANTENIMIENTO PREVENTIVO	**0.0%**

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Anexos 06: FICHA DE PROCEDIMIENTO PARA LA APLICACIÓN DE LA GESTION DE SEGURIDAD DE LA INFORMACIÓN.

POLICÍA NACIONAL DEL PERÚ		PERÚ Ministerio del Interior	
FICHA TÉCNICA DE PROCEDIMIENTO			
Nombre:	Intervención y Control de las Comunicaciones como Instrumento Procesal Penal. – Procedimientos para la aplicación de la gestión de la seguridad de la información.	**Tipo:**	Misional
Código:		**Versión:**	1.0
Dueño del procedimiento:	Responsable de la División de Apoyo Técnico Judicial		
Objetivo del procedimiento:			
Asegurar que los mandatos judiciales de levantamiento del secreto de las comunicaciones como instrumento procesal penal, se realicen mediante una intervención y control de las comunicaciones, bajo los principios de legalidad y confiabilidad, mediante un proceso que garantice la seguridad de la Información.			
Alcance del procedimiento:			
Dirección Antidrogas y demás unidades de organización encargadas de Investigación. El procedimiento se inicia con la recepción de la solicitud de intervención de las comunicaciones y finaliza con la remisión del Informe Final del caso a la Fiscalía solicitante de la medida y el archivamiento de los documentos, así como la emisión de disco con grabación de audios, en la carpeta correspondiente.			
Base normativa			
1. Constitución Política del Perú, Artículo 2, Inciso 10. 2. Ley Nº 27697, Ley que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en Caso Excepcional. 3. Ley Nº 30077, Ley Contra el Crimen Organizado. 4. Ley N° 29733 Ley de Protección de Datos Personales. 5. Decreto Legislativo N° 957, Código Procesal Penal, Artículos 230 y 231. 6. Resolución Ministerial Nº 1217-2014-IN, que aprueba los Protocolos de Actuación Conjunta.			
Siglas y definiciones			
1. DIRANT: Dirección Antidrogas 2. DIVINANT: División de Inteligencia Antidrogas 3. 4SIGHT-UCM: Sistema Unificado de Monitoreo de Llamadas 4. IMEI: *International Mobile Equipment Identity* - Identidad Internacional de Equipo Móvil 5. LIID: Código del Número IMEI (código de identificación celular) 6. SLI: Sistema de Interceptación de Líneas.			

Requisitos para iniciar el procedimiento:	
Descripción del requisito (entradas)	**Fuente (proveedor)**
Solicitud de intervención de las comunicaciones que adjunta: - Resolución Judicial que autoriza la medida limitativa - Reporte del Módulo de Gestión de Números del Sistema de Intervención de las Comunicaciones.	Ministerio Publico - Fiscal Administrador del componente de gestión de interceptación en el Sistema de Intervención de las Comunicaciones

Descripción de actividades

Nº	Descripción de la actividad	Unidad de organización	Responsable
1.	Recibir la solicitud de intervención de las comunicaciones y verificar: - Que en la base de datos de números intervenidos (excel), el número solicitado no se encuentre activo en los sistemas 4SIGHT-UCM, RELIANT, SLI. - Que los datos de la solicitud coincidan con los datos de la Resolución Judicial y el Reporte del Módulo de Gestión de Números (número telefónico, plazos y forma en tiempo real) Si hay observaciones continuar con la actividad 2, caso contrario continuar con la actividad 3. **Nota:** Para el caso de las solicitudes con más de un número a intervenir, es suficiente que uno de ellos se encuentre activo para continuar con la actividad 2.	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Operador de Sistemas
2.	Comunicar la observación al solicitante y devolver la solicitud. Fin del Procedimiento; verificación si en el procedimiento es seguro la identificación de la información no es cumplida se retorna a la autoridad.	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Operador de Sistemas
3.	Dar conformidad a la recepción de la solicitud, sellando y firmando el cargo.	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Operador de Sistemas
4.	Asignar código al caso, designarlo a la sala-grupo correspondiente (por delegación del responsable del procedimiento), y configurar en el sistema respectivo (SLI), la cuenta de los analistas con el caso, previa coordinación con el responsable de grupo. La responsabilidad de obtener la información respecto al IMEI intervenido es de carácter RESERVADO. Entregar copia de la solicitud y el Parte Resolutiva del mandato judicial al Analista Táctico.	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Operador de Sistemas
5.	Recibir y firmar el cargo. Verificar que los datos del expediente coincidan con los datos registrados en el sistema que corresponda (SLI). Si hay observaciones continuar con la actividad 6, caso contrario continuar en paralelo con las actividades 7 y 14.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Analista Táctico
6.	Subsanar las observaciones indicadas en el sistema que corresponda (SLI), ir a la actividad 5.	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Operador de Sistemas
7.	Formular el Parte correspondiente en 3 ejemplares dando cuenta al responsable de Apoyo Técnico Judicial, de las acciones efectuadas, derivar los partes y el expediente (solicitud, resolución y reporte) para su distribución.	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Operador de Sistemas
8.	Recibir los documentos (partes, solicitud, resolución y reporte), elaborar el Oficio a la Fiscalía solicitante de la medida, para la remisión del Parte.	DIVATJ (Apoyo Técnico Judicial - Unidad de Recepción Documental)	Secretaria

9.	Firmar el Oficio.	DIVATJ (Apoyo Técnico Judicial)	Responsable de Apoyo Técnico Judicial
10.	Remitir el Oficio a la Fiscalía solicitante de la medida, adjuntando un Parte.	DIVATJ (Apoyo Técnico Judicial - Unidad de Recepción Documental)	Secretaria
11.	Distribuir los documentos de la siguiente manera: - Un Parte y el expediente ingresado (solicitud, resolución y reporte) al responsable de Gabinete de Gestión de Casos, continuar con la actividad 12. - Un Parte al responsable del grupo asignado, continuar con la actividad 13.	DIVATJ (Apoyo Técnico Judicial - Unidad de Recepción Documental)	Secretaria
12.	Generar una carpeta para el caso y archivar los documentos (parte, solicitud, resolución y reporte).	DIVATJ (Apoyo Técnico Judicial)	Responsable de Gabinete de Gestión de Casos
13.	Recibir, firmar cargo y derivar documentos al analista asignado.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Responsable de Grupo
14.	Verificar si el caso es nuevo. Si el caso es nuevo, continuar con la actividad 15, caso contrario, continuar con la actividad 16.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Analista Táctico
15.	Contactar vía telefónica al Fiscal para intercambiar contactos, designar Pesquisa del caso (de corresponder), solicitar la reunión inicial, establecer el periodo de control y otros. Durante el periodo de intervención indicado en la Solicitud se realizan las actividades del 16 al 20. **Nota:** Las comunicaciones telefónicas se realizan al número autorizado por la Fiscalía.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Analista Táctico
16.	Recolectar comunicaciones, escuchar, analizar y difundir vía telefónica la información, de acuerdo con su competencia, al Fiscal y Pesquisa del caso. Continuar en paralelo con las actividades 17 (bajo requerimiento del Fiscal) y 18.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Analista Táctico
17.	Grabar los audios y datos en soporte magnético. Llenar y firmar (Fiscal y Operador de Sistemas) el Registro de Cadena de Custodia, adherirlo al sobre plastificado y entregarlo al Fiscal. **Nota:** La entrega de audios y datos en cadena de custodio se realiza en las instalaciones del Apoyo Técnico Judicial.	DIVATJ (Apoyo Técnico Judicial -Tecnología de la Información y Comunicaciones)	Operador de Sistemas
18.	Realizar reuniones de coordinación con los fiscales y el grupo operativo cuando corresponde o sea requerida. Formular y firmar (Analista Táctico, responsable del grupo y Fiscal a cargo del caso) el Acta de Reunión de Coordinación, exclusivo con las autoridades que se encuentran en resolución y disposición fiscales.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Analista Táctico

19.	Atender al Pesquisa a cargo de la investigación y/o traductor y brindar acceso a la sala de uso externo cuando requiera la escucha de comunicaciones puntuales, previa autorización escrita del Fiscal del caso.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Analista Táctico
20.	Apoyar al Fiscal, brindando acceso a la sala de uso externo para el control de las comunicaciones, cuando lo requiera. Elaborar y firmar (Fiscal, responsable del grupo y analista táctico), el Acta de Recolección y Control, en coordinación con el Fiscal del caso. **Nota:** Para los casos de provincia, el Fiscal adscrito al Apoyo Técnico Judicial firma el Acta de Recolección y Control.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Analista Táctico
21.	Entregar al responsable del grupo, las Actas de Recolección y Control, el parte, la solicitud de intervención de comunicaciones, la Resolución Judicial, guías de destino y demás documentos generados durante el proceso de intervención de la comunicación.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Analista Táctico
22.	Formular en duplicado el Informe Final del caso y el Parte de Culminación. Remitir documentos a la Unidad de Recepción Documental del Apoyo Técnico Judicial.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Responsable de Grupo
23.	Recibir y revisar documentos (Informe Final del caso y el Parte de Culminación). Si existen observaciones, ir a la actividad 22, caso contrario continuar con la actividad 24.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Responsable de Gabinete de Gestión de Casos
24.	Elaborar el Oficio a la Fiscalía solicitante de la medida, para la remisión del Informe Final del caso. En paralelo se realizan las actividades 25 y 27.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Responsable de Gabinete de Gestión de Casos
25.	Firmar el Oficio.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Responsable de Apoyo Técnico Judicial
26.	Remitir el Oficio a la Fiscalía solicitante de la medida, adjuntando el Informe Final del caso.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Secretaria
27.	Archivar el Informe Final del caso y el Parte de Culminación en la carpeta correspondiente.	DIVATJ (Apoyo Técnico Judicial – Intervención en Tiempo Real)	Responsable de Gabinete de Gestión de Casos
Fin del procedimiento			

Documentos que se generan:	
Productos o servicios	**Destinatario**
Informe de Culminación del Caso Grabación de audios y datos en soporte magnético, en cadena de custodia. Actas de Recolección y Control	Ministerio Publico – Fiscalía a cargo de la investigación
Registros	
1. Solicitud de intervención de las comunicaciones	

2. Resolución Judicial que autoriza la medida limitativa 3. Reporte del Módulo de Gestión de Números del Sistema de Intervención de las Comunicaciones. 4. Base de datos de números intervenidos (excel) 5. Oficios de remisión 6. Actas de Recolección y Control 7. Actas de Reunión de Coordinación 8. Registro de Cadena de Custodia 9. Actas de reuniones 10. Guías de destino 11. Partes 12. Audios y datos en cadena de custodia 13. Informe Final del caso 14. Parte de Culminación del Caso	
Proceso relacionado	**Formatos utilizados en el procedimiento**
- Investigación Criminal contra la delincuencia y/o crimen organizado, que tienen alcance de la Gestión de la Seguridad de la Información.	- Protocolo de intervención o grabación de registro de comunicaciones telefónicas o de otras formas de comunicación. - Registro de Cadena de Custodia - Oficios de remisión - Actas de Recolección y Control - Actas de Reunión de Coordinación - Informe Final del caso - Parte de culminación del caso

Diseño de Gestión de Seguridad de la información bajo la norma ISO 27001.

Anexo 7 RESULTADOS DE LA ENCUESTA QUE DETERMINAR EL NIVEL DE SEGURIDAD DE LA INFORMACIÓN EN LA OFICINA DE SALA DE INTERVENCIÓN Y OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN BASADA EN LA NORMA ISO 27001 EN LA DIVISIÓN DE APOYO TÉCNICO JUDICIAL DE LA DIRECCIÓN ANTIDROGAS, MEDIANTE PORCENTAJES POR PREGUNTA.

1. Conocimiento en la seguridad de la Información.						
Item	**1.1**	**1.2**	**1.3**	**1.4**	**1.5**	**1.6**
Nivel de sadisfacción	27%	50%	67%	60%	91%	100%
Nivel de insadisfaccion	73%	50%	33%	40%	9%	0%
Promedio de sadisfacción	66%					

2. Tecnicas para la protecion de Datos y Seguridad de la Información.								
Item	**2.1**	**2.2**	**2.3**	**2.4**	**2.5**	**2.6**	**2.7**	**2.8**
Nivel de sadisfacción	**62%**	**49%**	**72%**	**67%**	**71%**	**77%**	**80%**	80%
Nivel de insadisfaccion	38%	51%	28%	33%	29%	23%	20%	20%
Promedio de sadisfacción	**70%**							

3. Aplicación de Herramientas para la protección de datos y la seguridad de la información.						
Item	**3.1**	**3.2**	**3.3**	**3.4**	**3.5**	**3.6**
Nivel de sadisfacción	63%	56%	96%	60%	75%	80%
Nivel de insadisfaccion	37%	44%	4%	40%	25%	20%
Promedio de sadisfacción	71%					