UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

ANÁLISIS PARA LA SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001 EN EL ÁREA DE CÓMPUTO DE LA DIRECCIÓN REGIONAL DE EDUCACIÓN – TUMBES; 2020.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL

DE INGENIERO DE SISTEMAS

AUTOR

SANCHEZ PALACIOS, EDINSON SAMIR

ORCID: 0000-0002-5137-7321

ASESOR

MGTR. ING. NEYRA ALEMAN, KARKA JUVICZA

ORCID: 0000-0002-2482-8692

TUMBES – PERÚ

2020

EQUIPO DE TRABAJO

AUTOR

SÁNCHEZ PALACIOS, EDINSON SAMIR

ORCID: 0000-0002-5137-7321

Universidad Católica Los Ángeles de Chimbote, Estudiante de Pregrado, Tumbes, Perú

ASESOR

Neyra Alemán, Karla Juvicza

ORCID: 0000-0002-2482-8692

Universidad Católica Los Ángeles de Chimbote, Facultad de Ingeniería, Escuela Profesional de Ingeniería de Sistemas, Tumbes, Perú

JURADO

Castillo Boggio, Luis Vicente

ORCID: 0000-0002-7011-9192

Céspedes Cornejo, César Augusto

ORCID: 0000-0002-8823-1895

Yovera Morales, Rosita Elizabeth

ORCID: 0000-0002-2482-8692

JURADO EVALUADOR DE TESIS Y ASESOR

MGTR. ING. CIP. LUIS VICENTE CASTILLO BOGGIO

PRESIDENTE

YOVERA MORALES ROSITA ELIZABETH

MIEMBRO

ING. CIP. CÉSAR AUGUSTO CÉSPEDES CORNEJO

MIEMBRO

MGTR. ING. CIP. KARLA JUVICZA NEYRA ALEMÁN

ASESORA

DEDICATORIA

A mis abuelos y madre, quienes con sus consejos y su apoyo incondicional me dan impulso para salir adelante. Por ser una parte importante de mi vida y a quienes les debo muchas cosas, porque han estado ahí a lo largo de mi vida; tanto en momentos felices y tristes, brindándome su apoyo emocional.

Edinson Samir Sánchez Palacios

AGRADECIMIENTO

A Dios, por darme la oportunidad de vivir; y que con su fuerza divina siempre me guía por el buen camino, y por ayudarme a superar obstáculos y dificultades a lo largo de mi vida.

A mi asesora, Ing. Karla Neyra Alemán, a quien aprecio mucho, por quien he recibido buenos consejos y quien me brindo todo su apoyo, y sobre todo paciencia para llegar a desarrollar esta investigación.

Edinson Samir Sánchez Palacios

RESUMEN

La presente investigación desarrollada bajo la línea de investigación en evaluación y propuestas de implementación de normas o estándares, tuvo como objetivo realizar el análisis para la seguridad informática basado en la norma ISO 27001 que permita mejorar la gestión en los activos de información en la DRET. La investigación es no experimental, descriptiva porque tiene como finalidad examinar, desarrollando un análisis de la seguridad informática, de nivel aplicativo; pues se dirige a la aplicación inmediata. Se trabajó con una población de 52 trabajadores, con una muestra de 46 trabajadores. Utilizando el instrumento cuestionario y la técnica encuesta obtuvimos los siguientes resultados: En lo que concierne a la primera dimensión, en la Tabla Nro. 4: sobre políticas y procedimientos de seguridad, se determina que el 100 % de los trabajadores, manifiestan que No saben de la existencia de políticas y/o procesos de seguridad de la información, en la segunda dimensión de seguridad de la información, en la Tabla Nro. 22: sobre análisis de seguridad informática, los trabajadores manifestaron que el 100% de los trabajadores encuestados manifiestan que SI consideran que se debe realizar un análisis de la seguridad informática para conocer cómo se lleva a cabo este proceso para mantener a salvo los activos de la institución. Lo que nos lleva a analizar que la seguridad informática es aprobada por parte de los trabajadores quienes creen que si se debería realizar un análisis de las amenazas hacia los activos de la información de la DRET.

Palabras clave: Información, ISO2700, Seguridad informática

ABSTRAC

The present investigation developed under the line of investigation in evaluation and proposals for the implementation of norms or protocols, had the objective of carrying out the analysis for computer security based on the ISO 27001 standard that allows improving the management of information assets in the DRET. The research is non-experimental, descriptive because its purpose is to examine, carry out an analysis of computer security, at the application level; it is directed to immediate application. With a sample of 46 workers, with a sample of 46 workers. Using the questionnaire instrument and the survey technique, we obtained the following results: Regarding the first dimension, in Table Nro. 4: on security policies and procedures, it is determined that 100% of the workers declare that they do not know of the existence of information security policies and / or processes, in the second dimension of information security, in Table Nro. 22: on analysis of computer security, the workers stated that 100% of the surveyed workers stated They DO consider that they should carry out an analysis of computer security in order to know how this process is carried out to keep the institution's assets safe. Which leads us to analyze that computer security is approved by the workers who believe that an analysis of the threats to the information assets of the DRET should be carried out.

Keywords: Computer security, information, ISO27001

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRAFICOS

I. INTRODUCCIÓN

Como sabemos la informática y el uso de las tecnologías de la información ha cambiado la forma en que las organizaciones desempeñan, llegando a tener un papel primordial en el desarrollo de estas. Las redes de comunicación y sistemas de información vienen desempeñando un papel esencial para el desarrollo económico y social de las naciones. A medida que han venido apareciendo nuevas plataformas de tecnologías y la incorporación de las empresas, también ha traído consigo grandes beneficios pero también nuevos retos, cómo el saber manejar la seguridad de la información, siendo uno de los más relevantes. Los sistemas informáticos están propensos a diferentes amenazas, trayendo consigo grandes pérdidas económicas. Los perjuicios pueden ser desde simples errores en la gestión comprometiendo la integridad de la información, hasta catástrofes que dañen la totalidad de los sistemas. Por lo antes mencionado, las aplicaciones de estas medidas a tomar en cuenta para la seguridad de la información se deben realizar de manera racional y planificada, para no realizar esfuerzos e invertir en recursos en áreas que no lo requieran.

Actualmente la DRET no cuenta con un área o departamento dedicado a la gestión de la Seguridad de la información, por tanto cada área (computación, administración, remuneración, tesorería, etc.) tiene sus propias metodologías y procedimientos para velar por la seguridad de la información. Tampoco cuentan con un SGSI documentado, ni políticas de seguridad definidas ni divulgadas. Por estos motivos es muy importante que con este análisis se motive a que la DRET implemente el SGSI planteado para fortalecer los controles que aseguren la disponibilidad, confidencialidad e integridad de la información de la DRET. Y para administrar los riesgos de seguridad de la información

para mantenerlos en niveles aceptables teniendo en cuenta la clasificación de los riesgos e incrementar la capacidad, el desarrollo y buen uso de las tecnologías de información y comunicación en la DRET (1).

En primera instancia se realizó la visita a la Dirección Regional de Educación, y se pudo observar el modo en que se desarrolla el desempeño de sus labores en las diferentes áreas que tienen al cuidado la información y el área de computo que es de donde se controla toda la red de computadoras que están conectadas en red y comparten información a través de este, así mismo; se hizo efectiva una entrevista con el encargado del área de computo. Posteriormente se hizo uso de una encuesta para medir los conocimientos de los trabajadores en cuanto a la seguridad informática. La investigación es no experimental, descriptiva porque tiene como finalidad examinar y revisar sus variables, desarrollando un análisis de la seguridad informática, de nivel aplicativo; pues se dirige a la aplicación inmediata. Se trabajó con una población constituida por 52 trabajadores de las distintas áreas de la Dirección Regional de Educación, que están comprometidas entre sí, junto al área de cómputo, siendo esta el área principal. Con una muestra de 46 trabajadores.

Debido a la problemática se planteó la siguiente interrogante, ¿El análisis para la seguridad informática basada en la norma ISO/IEC 27001 permitirá una adecuada gestión en la seguridad de los activos de información en la Dirección Regional de Educación – TUMBES, 2020?, formulando el siguiente objetivo general: Realizar el análisis para la seguridad informática basado en la norma ISO/IEC 27001 que permita mejorar la gestión en los activos de información en la Dirección Regional de Educación – TUMBES, 2020. Por otro lado, los objetivos específicos del presente trabajo de investigación son los siguientes:

1. Identificar los riesgos existentes teniendo en cuenta la seguridad informática de la dirección regional de educación – Tumbes, 2020.
2. Evaluar los procedimientos de seguridad, después de identificar los riegos en los activos de información que presenta la dirección regional de educación.
3. Analizar la norma ISO/IEC 27001 basada en la seguridad informática para la dirección regional de educación – Tumbes, 2020.

La presente investigación se justifica en que la seguridad de la información es de gran importancia en cualquier tipo de organización al punto de que no es necesario hacer inversiones de gran nivel en sistemas o dispositivos de seguridad, para mantener la confidencialidad, integridad y la disponibilidad, sino se debe llevar a cabo la implementación y poner en funcionamiento sistemas de gestión de seguridad de la información, por lo que para llevar a cabo esto se debe desarrollar un análisis respectivo en la Dirección Regional de Educación, basándose en los estándares de seguridad de la información a través de la metodología MAGERIT, la cual se basa estrechamente en los requerimientos de la ISO 27001, de tal manera que se permita minimizar y salvaguardar la seguridad de la información, así como detectar amenazas o eventos adversos al buen funcionamiento de la institución.

Como justificación académica porque permite manifestar en la práctica los conocimientos adquiridos durante años de estudio en La Universidad Católica Los Ángeles De Chimbote Tumbes, lo cual nos sirvió para poder desarrollar un análisis determinado para conocer cuál es estado actual en que se da la seguridad informática, permitiéndonos proponer mejoras, de tal manera de minimizar el riesgo de pérdida de información.

En cuanto a justificación operativa nos vamos a basar estrechamente en la metodología MAGERIT que también se encuentra basada en los requerimientos brindados por la norma ISO27001, que ofrecen la identificación de debilidades en la seguridad tanto física como lógica, contando con procedimientos que permitirán afrontar alguna eventualidad, brindando a la organización integridad, privacidad, disponibilidad de la información gestionada por la empresa.

Como justificación económica, el análisis de la seguridad informática reduce gastos y perdidas, ya que minimiza el impacto de las amenazas en la información, equipos o ya sea a través de la infraestructura o desastres naturales. Debido a que con el análisis basado en estándares y requerimientos de la ISO27001 se logrará tener conocimientos en prevención y como mantener seguridad tanto de la información como de la infraestructura.

Asimismo como justificación tecnológica, tenemos el análisis de la seguridad informática de la Dirección Regional de Educación Tumbes, lo que va a proveer a la institución una herramienta de soporte de información apropiado para el manejo de los procesos que ayudaran a la entidad con los objetivos a cumplir sobre la seguridad de la información, efectuando principios de seguridad de la información e innovación tecnológica, asegurando el cumplimiento de la confidencialidad, disponibilidad, integridad, y confiabilidad de la información.

Como justificación institucional, debido a que la Dirección Regional de Educación Tumbes, requiere aumentar en soporte de seguridad para poder poner a buen recaudo los activos de la institución, desde el punto de vista físico como lógico, para poder lograr una mejora continua de la organización. (2) Además que, mediante Resolución Ministerial N°

004-2016-PCM, se aprobó de manera obligatoria el uso de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la información, sistema de gestión de seguridad de la información, con requisitos de 2ª. Edición, en todas las entidades integrantes del Sistema Nacional de Informática.

EL presente estudio se llevó a cabo en la Dirección Regional de Educación Tumbes, específicamente en el área de cómputo, y con estudios en las distintas áreas, realizando un análisis de la situación actual de la institución, con el objetivo de conocer y determinar las sus deficiencias, teniendo en cuenta los estándares de seguridad de información, según los requerimientos de MAGERIT basados en la Norma Técnica Peruana y en la norma ISO27001.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a nivel internacional

Esta investigación respalda su temática en las siguientes investigaciones internacionales:

En el año 2018, Amoguimba, D. (3), en su tesis "Propuesta de políticas de seguridad de la información aplicado al entorno empresarial de Soft Warehouse S.A." tiene como objetivo "Proporcionar una directriz que permita solventar los problemas de seguridad de la información en Soft Warehouse S.A. de acuerdo con las leyes y regulaciones vigentes que dispone el estado" que se desarrolló en la "Pontificia Universidad Católica Del Ecuador". Del trabajo de investigación realizado se concluye que: en las diferentes organizaciones se recopilan, almacenan, procesan y transmiten diariamente información, no solo como un escrito, nombres cuentas, direcciones, sino como un valioso activo que requiere protección para con cualquier incidente que atente contra la continuidad e integridad de la misma. Por lo que, considerando las amenazas que atentan contra la organización se procedió a elaborar un manual de políticas de seguridad de la información, lo que permitirá mitigar las amenazas, vulnerabilidades y amenorar el riesgo para con los activos.

Otro aporte se realizó en el año 2017, Changoluisa, W. (4), en su tesis "Optimización del proceso de alta y baja de usuarios a través de la implementación de gestión de

seguridad de la información, basado en la norma ISO 27001:2013 en una empresa de consultoría para la industria petrolera" desarrollado en la línea de investigación: sistemas de gestión de producción y operaciones, tiene como objetivo "Optimizar la Gestión de Seguridad de la Información para el Proceso de "Alta y Baja de Usuarios" en una empresa de Consultoría para la Industria Petrolera basado en la Norma ISO 27001, para reducir el porcentaje de re procesos que actualmente se presentan." que se desarrolló en la "Pontificia Universidad Católica Del Ecuador". Del trabajo de investigación realizado se concluye que: El diagnóstico de la situación actual del proceso de "Alta y Baja de Usuarios", basado en la Norma ISO 27001:2013 permitió identificar cuarenta y cuatro (44) objetivos de control y controles aplicables de los cuales: se cumplía con quince (15) controles, no se cumplía con nueve (9) controles y se cumplía parcialmente con veinte y uno (21) controles, sobre los cuales se aplicaron las acciones de mejora para cubrir estos requisitos aplicables a una empresa de consultoría para la Industria Petrolera. Optimizar el desempeño del proceso de "Alta y Baja de Usuarios" mediante el desarrollo e implementación de requisitos aplicables de la norma ISO 27001:2013, además de reducir el porcentaje de re procesos en un 76,84%, permitió realizar reducción de tiempos promedio para el subproceso de "Alta de Usuarios" en un 71% y para el subproceso de "Baja de Usuarios" en un 37,04%, mediante el Estudio del Tiempo aplicado a una empresa de consultoría para la Industria Petrolera

Asimismo en el año 2015, Nicasio, O. (5), en su tesis "Diseño e implementación de un sistema de gestión de calidad en seguridad de la información SGSI" tiene como objetivo "definir los procesos que en materia de TIC regirán hacia el interior de la Unidad de Tecnologías de la información y Comunicaciones (UTIC), con el propósito de lograr la

cobertura total de la gestión, de manera que, independientemente de la estructura organizacional con que cuenten o que llegarán a adoptar; los roles definidos puedan acoplarse a los procesos establecidos para lograr la cohesión total para una mejor gestión", que se desarrolló en la "Universidad Nacional Autónoma de México". La normatividad que utilizó es MAAGTIC, para la eficiencia de las operaciones del área de tecnología de la información. Del trabajo de investigación se concluye que: todos y cada uno de los entornos en TI tienen problemas en su estructura, servicios, aplicaciones, configuración, red, etc. Y esto conlleva a innumerables vulnerabilidades que pueden ser explotadas y llegar a afectar los planes estratégicos de la organización. En el principal efecto perjudicial para una organización que no implante y mantenga correctamente su SGSI en el aumento importante de riesgo, los cuales se convierten en problemas, no solo aquellos referidos a la seguridad de la información, sino que también afecta a la consecución de objetivos establecidos, a la toma de decisiones y a la posición competitiva en el mercado.

2.1.2. Antecedentes a nivel nacional

Asimismo se fundamenta en las siguientes investigaciones nacionales: En el año 2017, Olaza, H. (6), en su tesis titulada "Implementación de NTP ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin", en la línea de investigación auditoria de sistemas y seguridad de la información, tiene como objetivo "Determinar el efecto de la implementación de la NTP ISO/IEC 27001 para la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación – Sede Centromin", que se desarrolló en la "Universidad César Vallejo". La metodología que se uso es la norma

ISO 27001. Se usó diseño experimental del tipo pre-experimental, se realizó una medición post-test, para comparar resultados. Con una población constituida por 4783 registros y una muestra de 136 registros. Del trabajo de investigación se concluye que: Se ha determinado que la implementación de la NTP ISO/IEC 27001, mejoró la seguridad de información en el área de Configuración y Activos del Ministerio de Educación - Sede Centromin, logrando demostrar las hipótesis planteadas con una confidencialidad del 95%, y esto se vio reflejado al incrementar el nivel de seguridad en la misma. También se ha determinado que el número de información confidencial divulgada implementando la NTP ISO/IEC 27001 en la seguridad de información en el área de Configuración y Activos del Ministerio de Educación - Sede Centromin, sin la NTP fue un promedio de 6.07 de información confidencial y con la implementación de la NTP fue de 1.67 información confidencial, logrando una reducción 4.4 información confidencial, que representa el 72.5% en el número de información confidencial divulgada.

También en el año 2017, Agurto, M. (7), en su tesis titulada "Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001" en la línea de investigación auditoria de sistemas y seguridad de la información, tiene como objetivo "Elaborar un Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001.", que se desarrolló en la "Universidad César Vallejo". La metodología que se uso es la norma ISO 27001. El diseño de la investigación es no experimental, de tipo descriptivo. Del trabajo de investigación realizado se concluye que: Con la culminación

de la presente investigación se elaboró el diagnóstico de los activos de información de los procesos implementados, revelando que existe la percepción de un alto número de incidentes de fuga y acceso indebido a la información, y también existe una cantidad relativamente alta de equipos portátiles usándose en el área QHSE sin ningún control alguno por parte del personal autorizado. Mediante la investigación se pudo determinar los indicadores de seguridad que presentan inconvenientes en el área QHSE, enlazados con la indisponibilidad de servidores y sistemas de información, por lo que es necesario mejorar los mecanismos preventivos y correctivos de soporte, así como los mecanismos de contingencia de seguridad de la información.

Por otro lado en el año 2016, Castillo, R. (8), en su tesis titulada "Sistema de gestión de seguridad de la información en la Municipalidad distrital de Pira aplicando la norma ISO/IEC 27001:2013", tiene como objetivo "Evaluar el sistema de gestión de seguridad de la información en la Municipalidad Distrital de Pira basado en la norma ISO/IEC 27001:2013; la cual permitirá una mejor administración en los activos de información", que se desarrolló en la "Universidad Católica los Ángeles de Chimbote". Diseño de investigación, cuantitativo de estudio descriptivo, no experimental y de acuerdo a orientación es aplicada. Con una población de 16 trabajadores y dado el número de elementos se trabajó con una población muestral. Del trabajo de investigación realizado se concluye que: ciertos procesos no cuentan con una buena administración para su operación tales como: manuales, planes y más recursos necesarios. Al efectuar la evaluación se pudo determinar el alto nivel de riesgos que existe en el manejo de los activos de información dentro de la municipalidad, ello debido al poco control. Esta evaluación permite a la empresa tomar medidas preventivas y correctivas en los

procesos que necesitan ser atendidos con mayor brevedad a nivel de seguridad para el mejor funcionamiento de los mismos.

2.1.3 Antecedentes a nivel regional

También se fundamenta en las siguientes investigaciones regionales: En el año 2018, Lara, K. (9), en sus tesis titulada "Propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la clínica SIMEDIC diagnóstica S.A.C – Piura; 2018", tiene como objetivo "Realizar la propuesta para la seguridad informática basada en la norma ISO/IEC 27001 en la clínica Simedic Diagnóstica S.A.C – Piura; 2018, que permitirá mejorar la gestión en los activos de información.", que se desarrolló en la "Universidad Católica los Ángeles de Chimbote". Diseño de investigación de tipo cuantitativo con nivel descriptivo, y diseño de investigación no experimental. Se trabajó con una población de 30 trabajadores y con una muestra de 28 trabajadores. Del trabajo de investigación realizado se concluye que: De acuerdo con los resultados obtenidos en la investigación titulada el análisis y diseño del sistema de gestión basado en la norma ISO/IEC 27001 para la seguridad de información, en la clínica Simedic Diagnóstica S.A.C – Piura; queda demostrada que para se necesita mejorar la atención al cliente y la seguridad de información en la clínica Simedic Diagnóstica; este resultado es semejante al indicado en la hipótesis general por lo que se concluye que queda aceptada. Los trabajadores encuestados opinaron que, SI están de acuerdo con la que se debería realizar la propuesta para la seguridad informática para la clínica Simedic Diagnóstica S.A.C, por lo tanto, se requiere la implementación de la norma ISO 27001, este resultado es similar al indicado en la hipótesis específica por lo que se concluye que queda aceptada.

Por otro lado en el año 2017, Pangalima, R. (10), en su tesis titulada "Auditoría en seguridad de tecnologías de información y comunicación en la Municipalidad Provincial de Paita; 2015", tiene como objetivo "Realizar la propuesta de una Auditoría en Seguridad de Tecnologías de Información y comunicación, para minimizar los riesgos que atentan contra el normal funcionamiento de los servicios en la Municipalidad Provincial de Paita", que se desarrolló en la "Universidad Católica los Ángeles de Chimbote". Tipo de investigación es cuantitativo, con nivel de investigación descriptiva y con diseño de investigación no experimental. Se trabajó con una población de 130 trabajadores y con una muestra de 50 trabajadores. Del trabajo de investigación realizado se concluye que: para Realizar la propuesta de una Auditoría en seguridad de TIC en la Municipalidad Provincial de Paita, queda demostrada la necesidad de minimizar los riesgos que atentan contra el normal funcionamiento de los servicios en la Municipalidad; este resultado es similar al indicado en la hipótesis general, lo que concluye que la hipótesis general queda aceptada, ya que los trabajadores encuestados asumen que es de suma importancia aplicar la Auditoría para elevar el nivel de seguridad de la organización en el área de las TIC.

Asimismo en el año 2016, De La Cruz, R. (11), en su tesis titulada "propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016", tiene como objetivo "Realizar la propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; en el año 2016, de tal forma que se minimice el riesgo de pérdida de información.", que se desarrolló en la "Universidad Católica los Ángeles de Chimbote". El tipo y diseño de la investigación es no experimental,

descriptivo de corte transversal y por características de la variable es cuantitativa. Se trabajó con una población de 152 trabajadores y con una muestra dividida en 3 secciones de 152 trabajadores, 08 trabajadores y 02 trabajadores según las dimensiones. Del trabajo de investigación realizado se concluye que: la Municipalidad Provincial de Paita carece de políticas y controles eficientes en cuanto a la protección de los activos de la información (los servidores públicos y/o contratistas, la creación de información, los procesos, las tecnologías de información incluido el hardware y el software y las instalaciones), por esta razón si resulta beneficioso el diseño e implementación de la propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016, el mismo que permitirá minimizar la pérdida de información, con lo que queda demostrado que la hipótesis general es aceptada.

2.2. Bases teóricas

2.2.1 Empresa investigada

Grafico N° 1: Ubicación Geográfica

Av. Tumbes N 350 - Centro de Tumbes

Fuente: Google Maps

Base Legal

La Constitución Política del Perú establece los derechos fundamentales de todos los peruanos, que en su artículo 13 destaca: "La educación tiene como finalidad el desarrollo integral de la persona humana. El Estado reconoce y garantiza la libertad de enseñanza.

Los padres de familia tienen el deber de educar a sus hijos y el derecho de escoger los centros de educación y de participar en el proceso educativo".

De esta forma, la Dirección Regional de Educación Tumbes asume el encargo de fomentar y fortalecer la gestión educativa en las UGELES de Tumbes, Zarumilla y Contralmirante Villar, y basa sus acciones en los siguientes documentos normativos:

Ley General de Educación (Ley n.° 28044)

Ley del Código de Ética de la Función Pública (Ley n.° 27815)

Reglamento de la Ley del Código de Ética de la Función Pública (Ley n.° 27815)

Ley del Procedimiento Administrativo General (Ley n.° 27444)

Áreas de la Empresa

- Dirección
- Órgano de control
- Dirección de Gestión Pedagógica DGP
- Órganos de asesoramiento
- Tesorería
- Psicología
- Remuneraciones
- Mesa de partes
- Administración

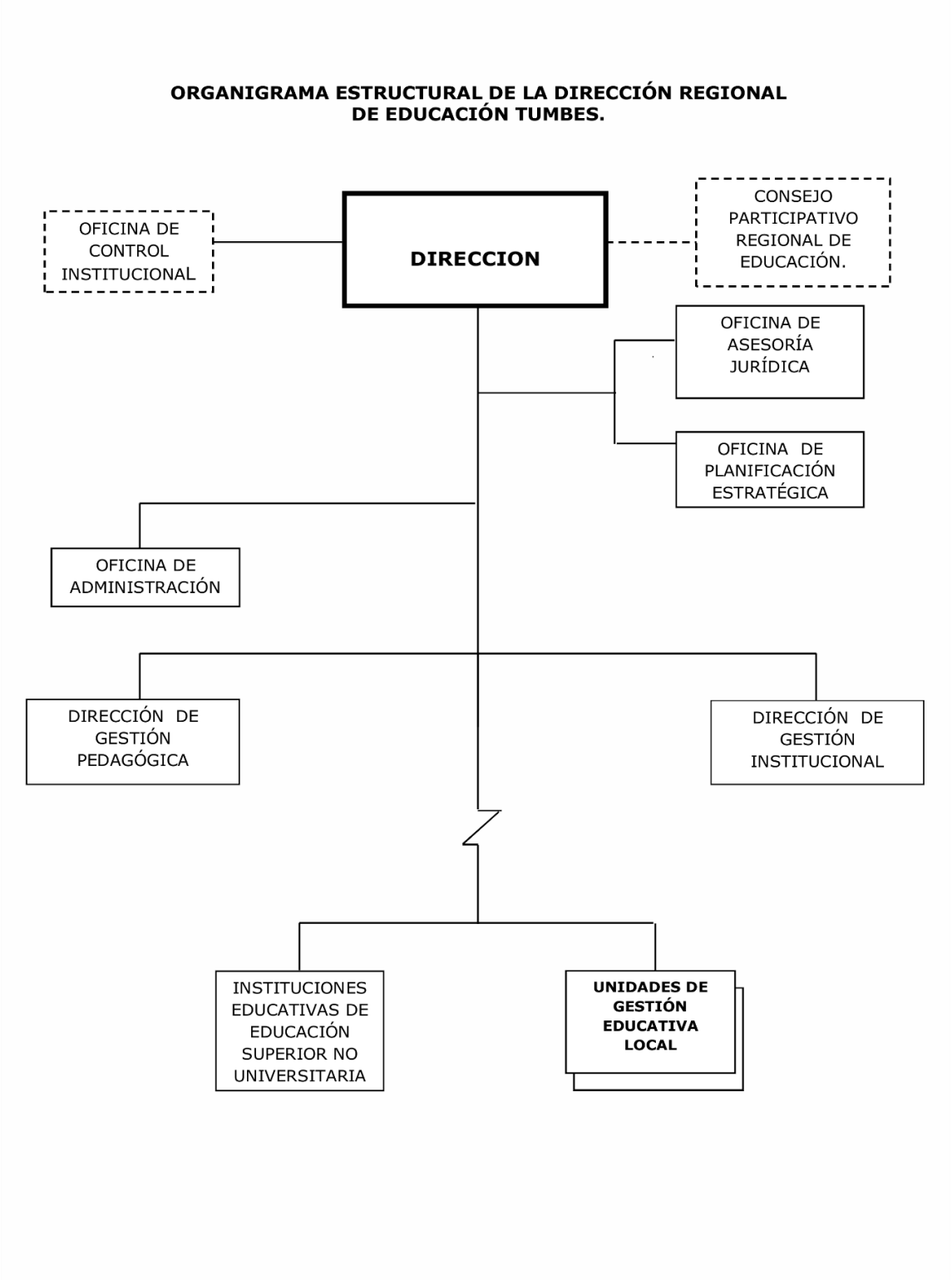
Visión

La Dirección Regional de Educación promueve en las Unidades de Gestión Educativas Locales servicios de calidad y equidad para que a su vez las instituciones educativas brinden de manera articulada educación básica y superior; logrando el desarrollo integral de los niños y jóvenes. En toda la instancia se practica una educación en democracia, en valores y respeto a la naturaleza, articulada al proceso de desarrollo y al mejoramiento de la calidad de vida del poblador de Tumbes. Las instituciones, autoridades y sociedad civil organizada participan activamente del proceso educativo; los sistemas administrativos brindan servicios de calidad; los maestros se encuentran adecuadamente capacitados en pedagogía, ciencia y tecnología demuestran sus competencias en el logro de aprendizajes de sus alumnos e intercambian permanentemente experiencias educativas.

Misión

Somos un órgano especializado del Gobierno Regional de Tumbes que promueve la educación, la cultura, el deporte, la ciencia y la tecnología; aseguramos que los servicios educativos, se brinden con equidad y calidad en los diferentes niveles y modalidades acorde con los avances científicos y tecnológicos y al desarrollo demandado por la Región.

Grafico N° 2: Organigrama



Fuente: Dirección Regional de Educación Tumbes

2.2.2 Seguridad

La seguridad no se basa únicamente a garantizar la existencia física, sino que se extiende y va mucho más allá, a la estabilidad social que llega a permitir la esencia de la vida libre de riegos y amenazas. Se describe la seguridad como uno de los motivos del establecimiento de la modernidad, llegando a buscar la protección del individuo en sí, logrando satisfacer el bien general como alegato de supervivencia (12). Beekman define la seguridad como algo muy relevante para cualquier organización, pueda o no estar conectada a una red, manifiesta que no solo es importante sino que también es compleja debido a que los niveles de seguridad a implementar pueden ser varios y queda en manos del usuario hasta que nivel de seguridad quiere alcanzar para proteger su información (13).

2.2.3 Seguridad física

Es un conjunto de acciones preventivas y de detección dirigidas a evadir los daños físicos en los sistemas informáticos y proteger los datos recopilados en ella. Se puede pensar que la pérdida de este patrimonio tangible de la empresa (mobiliario, ordenadores, etc.) puede ser relevante, pero aún más importante son los bienes intangibles (los datos). Ciertamente, la pérdida de un equipo físico eventualmente será reemplazada fácilmente; en cambio, es muy probable que los datos perdidos por la empresa sean irremplazables. Además, los datos que la empresa pueda llegar a perder pueden ser utilizados por personas inescrupulosas para fines ilícitos, ya sea chantajear a la empresa, para averiguar sus secretos. Por estas razones la seguridad física toma una

importancia relevante a la hora de salvaguardar ya sea los datos que poseen las empresas, o equipos y dispositivos encargados del almacenamiento de estos.

2.2.4 Seguridad lógica

Antiguamente cuando las empresas tenían sus datos en grandes servidores de proceso por fracciones de trabajo, para poder avalar la seguridad lógica suponía que solo tenían que asegurar el acceso físico al sistema con las personas autorizadas (esto es, garantizar la seguridad física) y cuidar una política sólida de copias de seguridad de los datos para que puedan ser recuperados en caso de ser necesario (haya pasado un incidente grave).

Sin embargo en la actualidad, con la gran interconexión que existe entre los sistemas con el establecimiento masivo de Internet y de datos, la seguridad lógica se ha venido convirtiendo en el centro de atención de todos los departamentos de tecnologías de las empresas. Esto ha resultado así porque todos los sistemas pueden llegar a ser intervenidos de manera remota por atacantes por medio de una red mal protegida o llegándose a aprovechar de los sistemas sin los adecuados sistemas de seguridad. Por otro lados, cada vez más grande el acceso a diversos dispositivos móviles y se puede manipular desde allí actividades como la adquisición de bienes o servicios, viajes, restaurantes, etc. Y estamos ya acostumbrados a varios tipos de protección en nuestra vida cotidiana, como por ejemplo con el PIN del celular, la clave de acceso a cajeros automáticos o a través de usuarios y contraseñas para compras/pedidos online, etc. Están vienen siendo medidas de protección lógica. Por lo que se define como un conjunto de acciones orientadas a la protección de los datos y aplicativos informáticos, así como a avalar la información únicamente a personas autorizadas (14). Por lo que los riesgos informáticos o lógicos derivan de internet u otro tipo de red, ya sea pública o privada,

radican en alteraciones en el ejercicio de cualquier tipo de software que contenga al menos una pc en esa red, desde la que se puede difundir en las diferentes redes. La mayor parte de los riesgos que provienen de internet son originados por personas con malas intenciones, teniendo en cuenta que una mala programación o un mal diseño puede causar un mal funcionamiento (15).

2.2.5 Informática

La informática palabra originaria del francés, se define como las técnicas y conocimientos científicos que llevan al tratamiento o manejo de la información a través de los ordenadores. La informática avanza debido a las metodologías de desarrollo, así como también el diseño de sistemas, por lo que se le considera tanto ciencia como ingeniería. Esta disciplina de informática desarrolla el conocimiento del diseño, análisis, implementación, aplicación y eficiencia de procesos que convierten la información (16). Es el conjunto de conocimientos que tenemos como referencia a lo que en la actualidad se llama ordenador. A lo largo de la historia e inventos de la humanidad se podría decir que el ordenador es un invento relativamente reciente. Hablando de algo que se inventó a mediados del siglo xx, es decir, hace poco más de unos 60 años. Y a pesar del tiempo de su creación los conocimientos acerca de este artilugio son grandes. Se podría decir que alrededor del ordenador hay grandes conocimientos, constituyendo lo llamado sistema técnico. La informática abarca a todo aquel conocimiento que nos ermita diseñar y construir sistemas informáticos. Estos constan de una parte física: máquinas de los distintos ordenadores y una parte que no es, esto son el conjunto de programas o también llamado “software” y lo primero “hardware”. Así pues, la tecnología se asocia a es tos componentes (17).

2.2.6 Seguridad informática

La seguridad informática trata de resguardar el almacenamiento, procesamiento y transmisión de información digital. Se considera que a pesar de todas las medidas que tomemos, la seguridad completa es imposible. Y que debido al presupuesto es poco probable aplicar medidas de seguridad a todos los equipos de la organización. Por lo que se debe identificar los activos a proteger: los equipos que tienen mayor importancia y que medidas aplicar a cada una. Por mencionar un ejemplo, todos los equipos deben contar con antivirus y firewall. Aunque, el activo más importante es la información que está almacenada en los equipos, debido a que un equipo en mal estado o descompuesto se puede reemplazar. Sin embargo, los datos de la organización nadie los puede restaurar si se pierden. En esta instancia la única opción son las copias de seguridad y el almacenamiento redundante. Los quipos de las organizaciones deben llevar las aplicaciones estrictamente necesarias, ni más ni menos. Siendo evidente que menos aplicaciones impedirían cumplir las tareas, pero tener en cuenta no instalar software de más, ya que pueden conllevar a una serie de vulnerabilidades que puede dañar el sistema completo (18).

La seguridad informática, por lo general, está logrando una importancia cada vez más grande. Los usuarios, trabajadores y particulares de las organizaciones, tienen que ser conscientes de que para que su sistema funcione de manera correcta deben de protegerlo como su más grande tesoro. La seguridad informática consiste en resguardar los recursos del sistema de información (programas o material informático) de una empresa sean manejados de una manera estricta y que el acceso a esta información sea manipulada, modificada, sólo por personas debidamente acreditadas y dentro de los límites de

autorización (19). Los sistemas informáticos están expuestos a diferentes tipos de amenazas. El primer paso es saber identificar, para luego evaluarlas y tomar las medidas de seguridad para mitigar el riesgo que sospechan. Intentar eliminar el riesgo en su totalidad es imposible. Lo que se debe hacer es aprender a reducirlo hasta niveles aceptables, que permitirán convivir con él. Debido que, aunque muchas cosas fallen, sí sé es capaz de controlar el riesgo que este evidencia, podrá sentirse cómodo, confiable ante la informática, y obtener el máximo provecho. El error más desdichado que puede realizar una empresa o un articular es esperar que un desastre ocurra para recién optar por una postura segura.

2.2.7 Activos de información

Son recursos útiles para que las empresas lleguen a sus objetivos y funcionen según lo propuesto. Estos se encuentran coligados, directa o indirectamente. Por la cantidad de activos que pueden haber, podría volverse algo abrumador, pero hay que comenzar a clasificarlos de alguna forma. Los activos de información son cambiantes, la situación puede ser distinta en semanas, meses e incluso años. Por lo que se recomienda mantener un inventario de los activos, como parte de la mejora continua (20).

2.2.8 Seguridad de información

La seguridad de la información es una disciplina que está encargada de gestionar el riesgo en los sistemas informáticos. Entendiéndose de otra manera, las medidas de seguridad encargadas de contrarrestar amenazas se implantaran en los sistemas informáticos, donde están expuestas los activos de la empresa: información, hardware y software que la mantienen. Todo se basa en evaluar los riesgos reales a la que los activos de la empresa están expuestos y mitigarlos a través de necesarias medidas y en el grado

adecuado, con el propósito de satisfacer las expectativas de seguridad a adoptar. Una de las dificultades prácticas consiste en identificar el valor de los activos, y el coste que conlleva a los riesgos. Se suele identificar los riesgos según su coste económico para la empresa, y ordenar las amenazas según su nivel de riesgo y en función al espacio de ataque (21). A pesar que la tecnología trae consigo enormes ventajas, también es de gran fragilidad. Malware es uno de los principales enemigos de la seguridad de la información, es aquellos programas que afectan el comportamiento del sistema de cómputo, estos tienen efectos destructivos, al igual que los virus, o molestos como el spam. Los virus en su mayoría son creados por expertos programadores que buscan robar información, estropear sistemas de cómputo, o incluso solo por diversión. Estimando que hasta el 2012 había más de 90 millones de programas maliciosos (22).

2.2.9 Estándar de gestión de la seguridad de la información

Normativa ISO /IEC

ISO es una organización mundial de normalización. En el mundo de la normalización se hace referencia a nivel internacional en la Internatinal Organization for Estándar, viene funcionando de manera independiente en su sede de Ginebra, cuyos orígenes se remontan a 1906. Habiéndose creado también en ese año en reino unido la (CEI/IEC), entidad de normalización sólida que se transforma en (ISA) en 1926, extendiéndose hasta la ingeniería mecánica, pero llegando a su fin en 1942ª consecuencia de la segunda guerra mundial. En 1946 después de una reunión organizada por el ingeniero británico Charles Maestre, quien fue un apasionado de la normalización, delegados de 25 países en Londres llevan en marcha la creación de la Organización internacional de normalización optando por las siglas ISO debido a que en griego clásico este significa

“igual o equivalente” con misión de facilitar la unificación y organización de normas industriales, desde ese momento de su creación se decide que su sede sea en Ginebra (Suiza). Su actividad se basa en: la normalización de prácticas en la gestión de documentos asegurando la existencia de información confiable, y que sirva de convicción de las actividades que desempeña cualquier empresa. Establecer la infraestructura de gestión para asegurar el control eficiente y sistemático de la creación, registro, clasificación, acceso, conservación y disponibilidad de los archivos n cualquier formato. Estableciendo los requerimientos para dar soluciones técnicas que puedan existir en la gestión de documentos digitales, incluyendo la recuperación, distribución y comunicación, intercambio, migración, presentación, conservación y eliminación. Excluyendo de su trabajo las publicaciones digitales e información de los sistemas de procesos industriales (23).

Aplicación de las normas ISO a documentos y archivos

Desde hace mucho que las normas ISO se manifiestan en los distintos archivos de los equipamientos y materiales que se manejan. Por mencionar, mobiliario de archivos, y otros materiales semejantes. Asimismo se presenta en el soporte de documentos, ya sea en papel industrial o microfilm, o soportes de informática. Sin embargo, introducir las normas de este tipo en los archivos de un país no se realiza de forma simultánea, mientras que en archivos un poco más tradicionales su aparición fue tardía, y en diferentes tipos de archivos, como las que conllevan imagen y sonido, su introducción fue más rápida como resultado fue el uso de soporte altamente normalizado y tecnificado (24).

Normativa ISO /IEC 27001

ISO / IEC 27001 es universalmente conocido, debido a que proporciona una serie de requisitos para un sistema de gestión de seguridad de la información (SGSI), no obstante podemos encontrar más de una docena de estándares de la familia ISO / IEC 27000. El uso de este les proporciona a las organizaciones de cualquier índole poder gestionar la seguridad de sus activos, ya sea la información financiera, detalles de sus empleados, propiedad intelectual, o la información de terceros. De la misma manera que todas las normas de sistema de gestión ISO, esta certificación ISO / IEC 27001 es posible de adecuar pero no es de carácter obligatorio. Ciertas empresas optan por su implementación del estándar para lograr beneficiarse de las mejores prácticas que contiene, a diferencia de otras que optan por la certificación para asegurar a los clientes que siguen sus recomendaciones. ISO no realiza certificación (25).

Objeto y campo de aplicación de la norma

La norma ISO/IEC 27001, como todas las normas que se aplican a los sistemas de gestión, se reguló para emplearla en cualquier tipo de organización (tanto empresas privadas como públicas, entidades sin ánimo de lucro, etc.), sin diferenciar el tamaño o la actividad. La norma en mención específica los requerimientos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento, y la mejora de un SGSI documentado, considerando los riesgos empresariales de la organización. Es decir, nos explica a como tener que diseñar un SGSI y aplicar los controles de seguridad, teniendo en cuenta las necesidades de una empresa o en partes de la misma, sin embargo no nos aclara mediante qué proceso se pone en práctica. Por ejemplo, uno de los

requisitos principales es la elaboración de un análisis de los riegos teniendo en cuenta ciertas características de objetividad y precisión, sin embargo tampoco nos menciona indicaciones de la mejor manera de llevar el análisis. La realización se puede realizar con una herramienta comercial, con una aplicación elaborada expresamente para la organización, a través de entrevistas, reuniones, o cualquier otro método que se considere el adecuad. Los recursos en su totalidad servirán para aplicar la norma, siempre y cuando el método tenga los requisitos de objetividad, donde los resultados sean repetibles y sea documentada la metodología (26).

2.2.10 Metodologías de gestión de riesgo

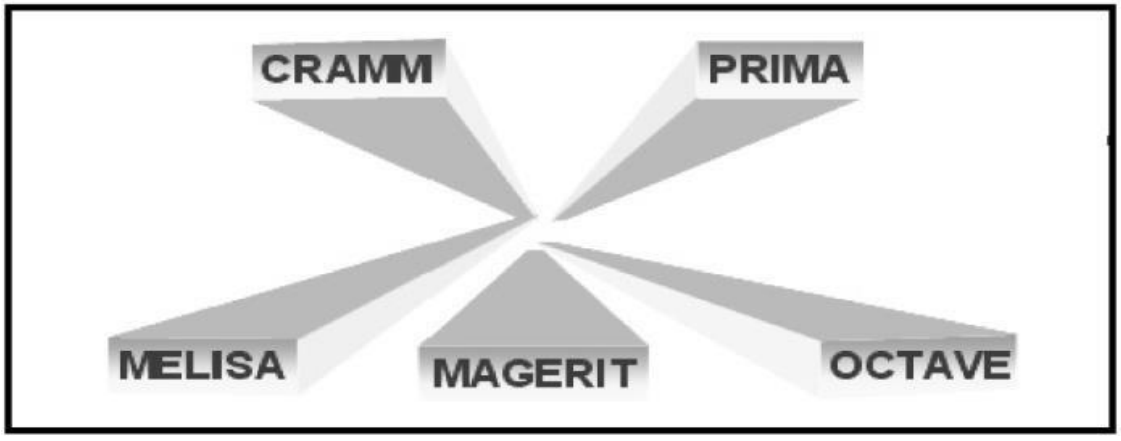
Las metodologías de gestión de riesgo son desarrolladas con la finalidad de identificar la falta de control y la elaboración de planes de contramedidas. Se conocen dos tipos: las cuantitativas y las cualitativas. El hecho de tener un conocimiento relativamente alto acerca de los marcos de referencia en el análisis de los riesgos no nos asevera que el procedimiento se lleve de forma exitosa. Es por ello que se requiere una metodología que, de manera eficaz y eficiente, desarrolle los marcos de referencias de manera exitosa en la labor de análisis de riesgos de TI. Lo ya mencionado anteriormente nos lleva a que sean identificados y priorizados exhaustivamente los distintos riesgos para lograr definir planes de acción y protección, conforme a cada uno. En general esta labor no es una tarea fácil, debido a que involucra el estudio conciso de todas las áreas de las empresas y un detallado análisis crítico que nos avale una adecuada identificación y priorización de las vulnerabilidades y riegos. Es necesario, entonces, optar por estas metodologías que facilitan lograr los objetivos en los altos volúmenes de información (27).

Figura 3: Tipo de metodologías para el análisis de riesgo.

	CUANTITATIVA	CUALITATIVA
PROS	Enfoca pensamientos mediante el uso de números. Facilita la comparación de vulnerabilidades muy distintas. Proporciona una cifra justificante para cada contramedida.	Enfoque lo amplio que se desee. Plan de trabajo flexible y reactivo. Se concentra en la identificación de eventos. Incluye factores intangibles.
CONTRAS	Estimación de probabilidad de estadísticas fiables inexistentes. Estimación de las pérdidas potenciales sólo si son valores cuantificables. Metodología estándares. Difíciles de mantener o modificar. Dependencia de un profesional.	Depende fuertemente de la habilidad y calidad del personal involucrado. Pueden excluir riesgos significantes desconocidos (depende de la capacidad del profesional para usar el check-list/guía). Identificación de eventos reales más claros al no tener que aplicarles probabilidades complejas de calcular. Dependencia de un profesional.

Fuente: Metodologías de gestión de riesgo.

Figura 4: Principales métodos de análisis y gestión de riesgos.



Fuente: Metodologías de gestión de riesgo.

PRIMA

PRIMA por sus siglas (Prevención de riesgos informáticos con metodología abierta) Es un conjunto de metodologías de origen español que se desarrollaron entre los 90´s y la actualidad de enfoque subjetivo. Sus características son: resguardar las necesidades de los encargados de desarrollar los proyectos requeridos en un plan de seguridad. Se puede adaptar a cualquier tipo de herramienta. Consta de un cuestionario de interrogantes para poder identificar las debilidades o faltas de control. Tiene integrado una lista de ayuda para los usuarios que no tienen mucha experiencia en debilidades, riesgos y contramedidas. Facilita la generación de informes finales. En la "lista de ayuda" es posible introducir información nueva o cambiar la información ya existente, debido a que los cuestionarios son abiertos. De ahí la expresión de su nombre "metodología abierta". Tiene capacidad de aprendizaje debido al conocimiento de su base o registro de incidentes por lo que va basándose al entorno de trabajo (28).

MAGERIT

De origen español se destaca la metodología MAGERIT, metodología de que se encarga del análisis y gestión de riesgos de los sistemas de información de administración pública, se publicó en 1997 por el ministerio de administración pública, con posterior revisión en el año 2005. Los objetivos de MAGERIT son 4: La concienciación a los encargados de los sistemas de información de la existencia de los riegos, para poder adoptar medidas y eliminar su impacto. Brindar un método sistemático para lograr analizar determinados riesgos. Organizar las medidas oportunas para conservar los

riegos identificados bajo control. Facilitar los procesos a evaluar, auditar, certificar o acreditar (29).

CRAMM

Es una metodología de análisis y control de riesgos de la central de cómputo y agencia de telecomunicaciones (CCTA) del gobierno británico, nos da la posibilidad de identificar, medir y reducir los ataques al mínimo, alas que están expuestas las empresas día a día y es conocida como una metodología de aplicación de conceptos de manera formal, disciplinada y estructurada dando protección a los principios de la seguridad de la información y de los activos. SE destaca que, CRAMM maneja un análisis de riesgos cualitativos y cuantitativos por lo que se da a conocer como una metodología mixta, apoyando las herramientas de gestión, permitiendo a las empresas llevar una visión clara y priorizando las amenazas a las que se expone y que puedan afectar recursos y la continuidad del negocio, considerándose en una matriz donde se representan los activos en filas y en las columnas se manejan los riegos que llegaría a afectar la integridad, confidencialidad y disponibilidad de los mismos. Por otro lado, CRAMM nos ofrece información sobre las características del funcionamiento del sistema, e identificación clara y profunda de los activos que están más expuestos. Para tener un adecuado análisis de riesgos se debe tener en cuenta con la metodología CRAMM son: activos, vulnerabilidades, riesgos, amenazas, implementación, contramedidas y auditoria, para obtener un mejor resultado y asegurar la continuación del negocio (30).

OCTAVE

Es una metodología de evaluación de riesgos que se desarrolló en el Centro de Coordinación CERT. OCTAVE trae consigo un conjunto de herramientas, técnicas y métodos para poder realizar la evaluación de riesgo. En su definición de activos incluye: personas, software, hardware, sistemas e información. En sus orígenes, definida para grandes empresas, describe criterios conjuntos como (principios, atributos y resultados). Octave ofrece una línea base utilizando un enfoque de mitigación y mejorar actividades; también, iguala los riesgos operativos de las prácticas de tecnología y seguridad, permitiendo tomar decisiones para proteger la información en base a riesgos de confidencialidad, disponibilidad e integridad de los bienes de información crítica (31).

III. HIPÓTESIS

3.1. Hipótesis General

El análisis para la seguridad informática basada en la norma ISO/IEC27001 permite una adecuada gestión en la seguridad de los activos de información en la Dirección Regional de Educación – Tumbes, 2020.

3.2 Hipótesis Específicas

1. La evaluación de riesgos existentes teniendo en cuenta la seguridad informática de la Dirección Regional de Educación, permite identificar falencias en la seguridad de la información.
2. La evaluación de procedimientos de seguridad en la Dirección Regional de Educación; después de identificar los riesgos en los activos, permite una adecuada gestión en la seguridad de la información.
3. Conocer la norma ISO/IEC 27001 basada en la seguridad informática, permite conocer los estándares y requerimientos para lograr un adecuado análisis de la seguridad de la información.

IV. METODOLOGÍA

4.1. Diseño de la investigación

La investigación presenta un diseño no experimental, debido a que no se manipulan las variables del estudio, esta se utiliza debido a que se dispone de poca información para dar solución al problema planteado, se observa el fenómeno de forma natural; para después analizarlo. Descriptiva porque tiene como finalidad examinar y revisar sus variables recolectando una serie de información, para así lograr describir lo que se investiga, desarrollando un análisis de la seguridad informática en la institución. De nivel aplicativo; pues se dirige a la aplicación inmediata.

Se utilizó el diseño de la investigación descriptivo de una sola casilla, el cual se grafica de la siguiente manera:

M => O

Dónde:

M = Muestra

O = Observación

4.2. Población

Luego de precisar el problema que requiere análisis, se debe decidir si conviene estudiar toda la población o sólo una muestra extraída de ella. (32)

Se trabajó con una población constituida por 52 trabajadores de las distintas áreas de la Dirección Regional de Educación, que están comprometidas entre sí, junto al área de cómputo, siendo esta el área principal.

4.3 Muestra

Se aplicó el método de muestreo probabilístico, obteniendo como tamaño de muestra a 46 trabajadores de las distintas áreas.

La fórmula para calcular el tamaño de muestra cuando se conoce el tamaño de la población es la siguiente:

$$n = \frac{N \times Z_a^{\,2} \times p \times q}{d^2 \times (N-1) + Z_a^{\,2} \times p \times q}$$

En donde:

N = tamaño de la población

Z = nivel de confianza

P = probabilidad de éxito, o proporción esperada

Q = probabilidad de fracaso

D = precisión (Error máximo admisible en términos de proporción).

4.4 Definición operacional de las variables en estudio

Tabla Nro. 1: Matriz de operacionalización.

Variable	Definición conceptual	Dimensiones	Indicadores	Escala de medición	Definición operacional
Análisis para la seguridad informática basado en la norma ISO/IEC 27001	Se define como una disciplina que está encargada de gestionar el riesgo en los sistemas informáticos. Entendiéndose de otra manera, las medidas de seguridad encargadas de contrarrestar amenazas se implantaran en los sistemas informáticos, donde están expuestas los activos de la empresa: información, hardware y software que la mantienen (18).	Situación actual	- Organización de la información. - Gestión de activos - Control de accesos - Transferencia de información. - Adquisición de sistemas, desarrollo y mantenimiento	Ordinal	La Dirección Regional de Educación, brinda servicios a los diferentes docentes de la región de Tumbes, por lo que guarda información privada. El análisis de la seguridad informática basado en la ISO 27001, lo que permitirá una mayor confidencialidad y seguridad en dicha información.
		Seguridad de información	- Políticas de seguridad. - Seguridad en recursos humanos. - Cumplimiento con requerimientos legales y contractuales. - Gestión de los incidentes de seguridad.		

Fuente: Elaboración propia

4.5. Técnicas e instrumentos de recolección de datos.

4.5.1. Técnica

La técnica de recolección de información, se considera la manera de obtener datos de los sujetos que conforman la población, es utilizada cuando lo investigado forma parte de la experiencia. Se trata de estrategias que utiliza el investigador para recolectar información sobre un hecho o fenómeno, que está siendo objeto de estudio. Toda investigación tiene como punto de inicio la búsqueda de datos con fundamento, por lo que se debe seleccionar técnicas e instrumentos adecuados, para conseguir datos relevantes que servirán de base para su investigación. (33)

Observación directa y entrevista: Se realizó la visita a la Dirección Regional de Educación Tumbes y se hizo efectiva una entrevista a encargado del área de cómputo, para conocer el trabajo que se realiza y si se tienen ciertos criterios, estándares con respecto a salvaguardarla información, y también si se tienen identificados las posibles amenazas en la información.

4.5.2. Instrumentos

Son aquellos que proporcionaron ayuda para la recolección de la información se tomó en cuenta el instrumento del cuestionario estructurado que contiene una serie de preguntas cerradas para obtener información específica sobre el tema de investigación (34)
Posteriormente se realizó un cuestionario a los trabajadores de la institución, para saber el nivel de conocimiento que tienen sobre la seguridad de la información, y los procedimientos que realizan al cumplir sus funciones laborales en la institución y los cuidados que mantienen al momento de manipular la información.

4.6. Plan de análisis

Corresponde a la evaluación de la información recopilada considerando cada ítem del esquema propuesto en el planeamiento y otros que sirvan para mejorar la interpretación de los hechos. (32) Los datos obtenidos fueron ingresados en una hoja de cálculo usando el programa MS Excel 2013. También se analizaron los datos presentando los resultados a través de tablas y gráficos facilitando su comprensión e interpretación.

4.7. Matriz de consistencia

Titulo: Análisis para la seguridad informática basado en la norma ISO/IEC 27001 en el área de cómputo de la Dirección Regional de Educación – Tumbes; 2020.

Autor: Sánchez Palacios, Edinson Samir

Problema	Objetivos	Hipótesis	Tipo y Diseño de Investigación	Población y Muestra
¿El análisis para la seguridad informática basada en la norma ISO/IEC 27001 permitirá una adecuada gestión en la seguridad de los activos de información en la Dirección Regional de Educación – TUMBES, 2020?	**Objetivo general** Realizar el análisis para la seguridad informática basado en la norma ISO/IEC 27001 que permita mejorar la gestión en los activos de información en la Dirección Regional de Educación – TUMBES, 2020. **Objetivos específicos** 1. Identificar los riesgos existentes teniendo en cuenta la seguridad informática de la dirección regional de educación – Tumbes, 2020. 2. Evaluar los procedimientos de seguridad, después de identificar los riegos en los activos de información que	El análisis para la seguridad informática basada en la norma ISO/IEC 27001 permite una adecuada gestión en la seguridad de los activos de información en la Dirección Regional de Educación – Tumbes, 2020.	La investigación es no experimental, descriptiva porque tiene como finalidad examinar y revisar sus variables, desarrollando un análisis de la seguridad informática en la institución.	Se trabajó con una población constituida por 52 trabajadores de las distintas áreas de la Dirección Regional de Educación, que están comprometidas entre sí, junto al área de cómputo, siendo esta el área principal. **Muestra** Se aplicó el método de muestreo probabilístico, obteniendo como tamaño de muestra a 46 trabajadores de las distintas áreas.

	presenta la dirección regional de educación. 3. Analizar la norma ISO/IEC 27001 basada en la seguridad informática para la dirección regional de educación – Tumbes, 2020.			

4.8. Principios éticos

Durante el desarrollo de la presente investigación se ha considerado en forma estricta el cumplimiento de los principios éticos que permitan asegurar la originalidad de la Investigación. Asimismo, se han respetado los derechos de propiedad intelectual de los libros de texto y de las fuentes electrónicas consultadas, necesarias para estructurar el marco teórico.

En esta investigación se ha tomado en cuenta los siguientes principios éticos:

- Transparencia en la recolección de datos de la población en estudio
- Énfasis en la autenticidad de los resultados obtenidos
- Confidencialidad en las respuestas a las encuestas aplicadas
- Honestidad al momento de realizar el análisis
- Veracidad de los resultados

V. RESULTADOS

5.1 Resultados

Situación actual

Tabla Nro. 2: Distribución de frecuencias sobre las actividades y funciones de los trabajadores.

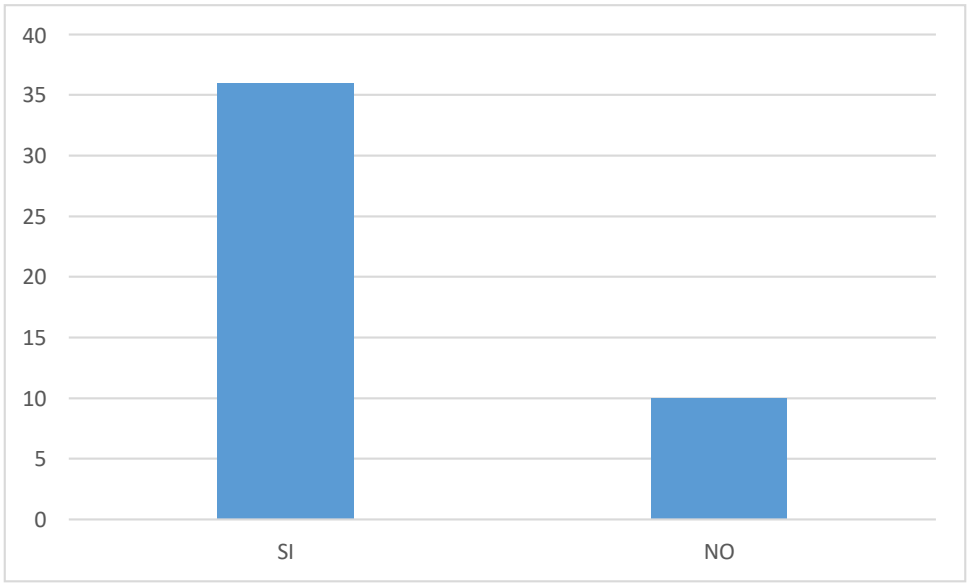
		n	%
	SI	36	78 %
	NO	10	22 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Tiene usted claras sus actividades y funciones a realizar en su área de trabajo?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 78% de los trabajadores encuestados indicaron que, SI tienen claras sus actividades y funciones en su área de trabajo, mientras que el 22% de los trabajadores indican NO conocerlas.

Gráfico Nro. 1: Distribución de frecuencias porcentual sobre las actividades y funciones de los trabajadores.



Fuente: Tabla Nro. 2

Tabla Nro. 3: Distribución de frecuencias sobre la seguridad de los datos registrados de forma manual.

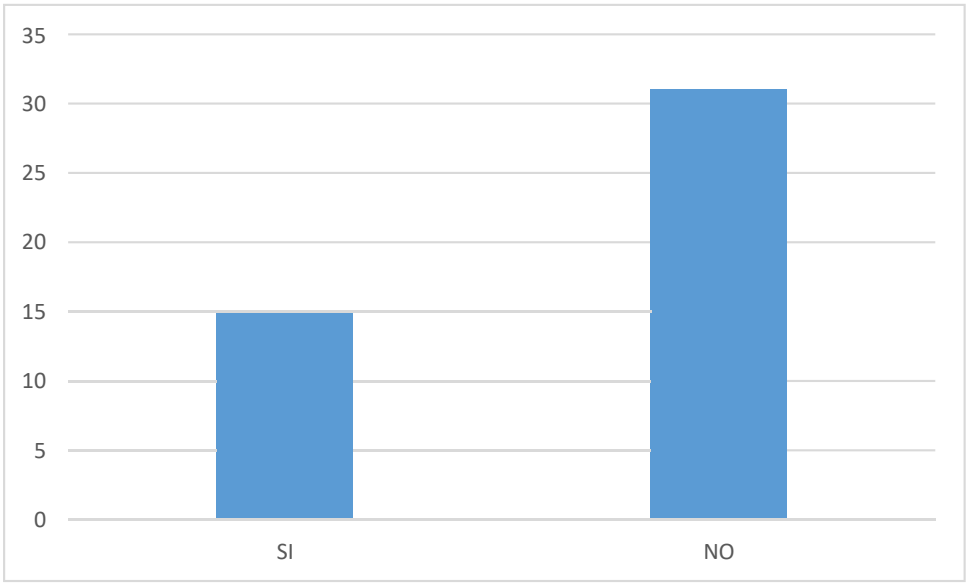
		n	%
	SI	15	33 %
	NO	31	67 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Cree que en el sistema manual los datos registrados son seguros?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que, el 33% de los encuestados indican que SI creen que los datos registrados de forma manual estén seguros, mientras que el 67% de los trabajadores encuestados manifiestan que No están seguros.

Gráfico Nro. 2: Distribución de frecuencias porcentual sobre la seguridad de los datos registrados de forma manual.



Fuente: Tabla Nro. 3

Tabla Nro. 4: Distribución de frecuencias sobre políticas y procedimientos de seguridad.

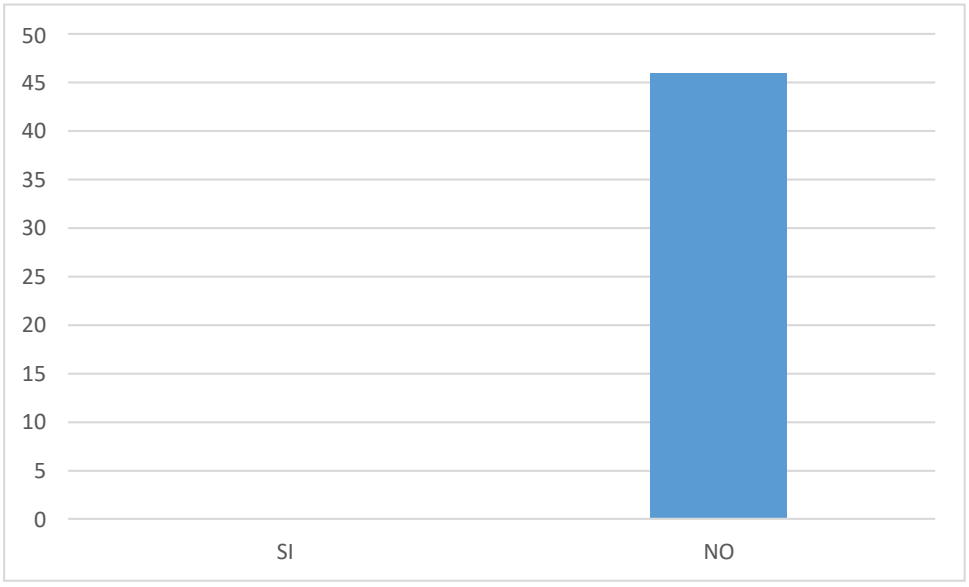
		n	%
	SI	0	0 %
	NO	46	100 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Sabe de la existencia de políticas y/o procesos para asegurar que se proporciona seguridad en la información de sus usuarios?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 100% de los trabajadores manifiestan que No saben de la existencia de políticas y/o procesos de seguridad de la información.

Gráfico Nro. 3: Distribución de frecuencias porcentual sobre políticas y procedimientos de seguridad.



Fuente: Tabla Nro. 4

Tabla Nro. 5: Distribución de frecuencias sobre información que ya no es utilizada.

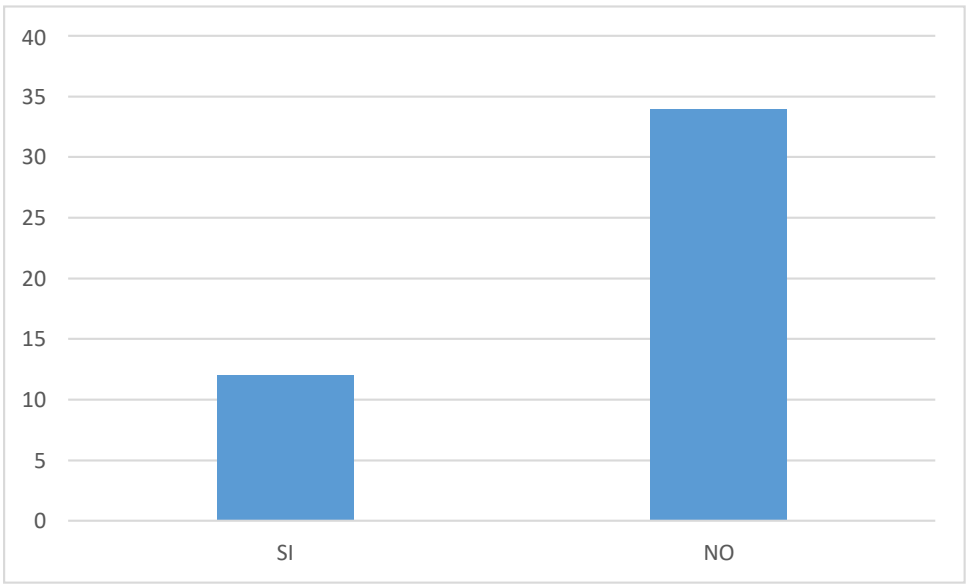
		n	%
	SI	12	26 %
	NO	34	74 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Usted desecha la información que ya no necesita?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 26% de los trabajadores encuestados manifiestan que SI desechan información que no necesitan, mientras que el 74% de los trabajadores manifiesta que NO se deshace de esta información.

Gráfico Nro. 4: Distribución de frecuencias porcentual sobre información que ya no es utilizada.



Fuente: Tabla Nro. 5

Tabla Nro. 6: Distribución de frecuencias sobre los documentos clasificados como confidencial.

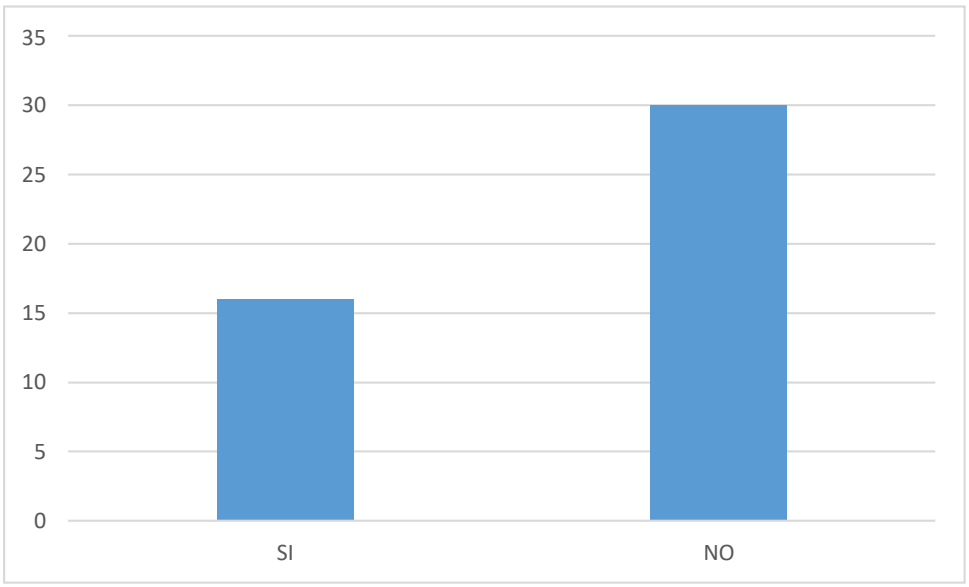
		n	%
	SI	16	35 %
	NO	30	65 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Cree usted que los documentos que manipula son clasificados como confidencial o acceso restringido?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 35% de los trabajadores manifiesta que SI creen que la información que manipula es de acceso restringido, mientras que el 65% de los trabajadores manifiesta que NO se clasifica como acceso restringido.

Gráfico Nro. 5: Distribución de frecuencias porcentual sobre los documentos clasificados como confidencial.



Fuente: Tabla Nro. 6

Tabla Nro. 7: Distribución de frecuencias sobre las copias de seguridad que se deben realizar.

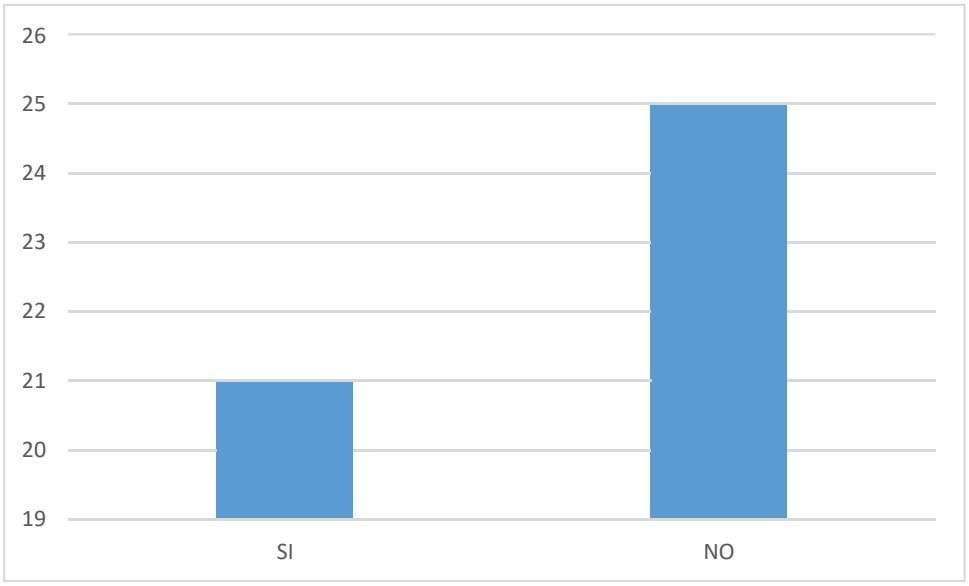
		n	%
	SI	21	46 %
	NO	25	54 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Tiene conocimiento si se realizan copias de seguridad?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 46% de los trabajadores manifiesta que SI tienen que conocimiento que se realicen copias de seguridad, mientras que el 54% de los trabajadores manifiesta que NO tienen conocimiento.

Gráfico Nro. 6: Distribución de frecuencias porcentual sobre las copias de seguridad que se deben realizar.



Fuente: Tabla Nro. 7

Tabla Nro. 8: Distribución de frecuencias sobre responsabilidad de los equipos informáticos.

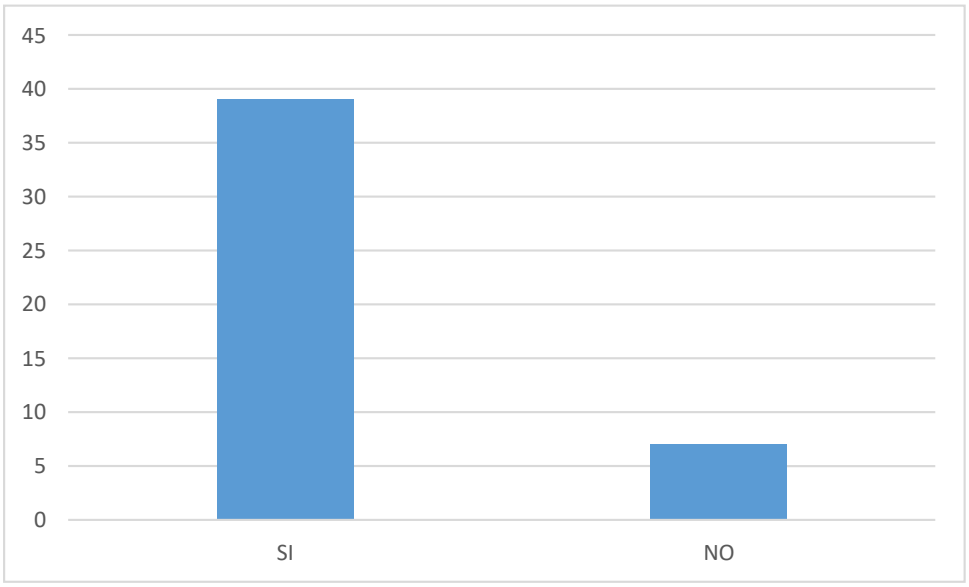
		n	%
	SI	39	85 %
	NO	07	15 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Cree usted que es responsable del equipo informático que utiliza para realizar sus funciones en la institución?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 85% de los trabajadores manifiestan que SI ser responsable de los quipos que usa para realizar sus funciones, mientras que el 15% de los trabajadores afirma que NO es responsable.

Gráfico Nro. 7: Distribución de frecuencias porcentual sobre responsabilidad de los equipos informáticos.



Fuente: Tabla Nro. 8

Tabla Nro. 9: Distribución de frecuencias sobre exposición de información.

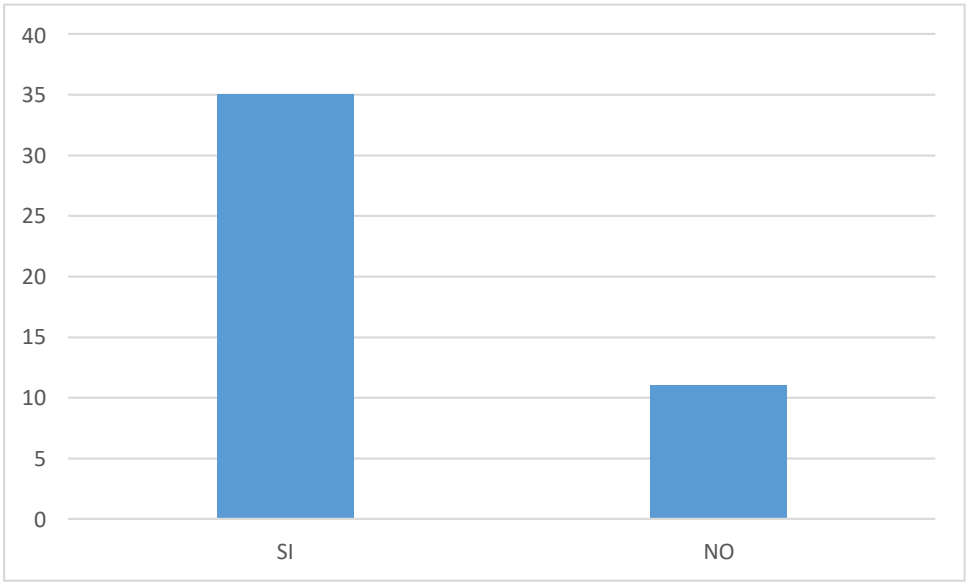
		n	%
	SI	35	76 %
	NO	11	24 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Cuándo no se encuentra en su área de trabajo, deja documentación visible en su escritorio?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 76% de los trabajadores afirma que SI deja información visible en su escritorio cuando se ausenta de sus labores, mientras que el 24% de los trabajadores manifiesta que NO deja información visible.

Gráfico Nro. 8: Distribución de frecuencias porcentual sobre exposición de información.



Fuente: Tabla Nro. 9

Tabla Nro. 10: Distribución de frecuencias sobre acceso a equipos de cómputo.

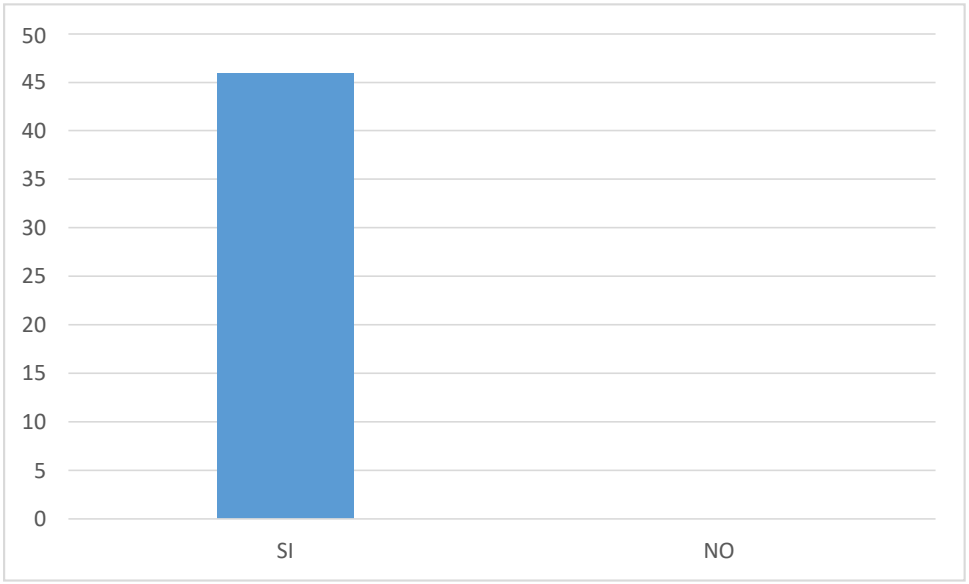
		n	%
	SI	46	100 %
	NO	0	0 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿La clave de acceso es la misma para ingresar a todos los equipos de cómputo?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 100% de los trabajadores manifiestan que SI, la clave de acceso en los equipos de cómputo es la misma.

Gráfico Nro. 9: Distribución de frecuencias porcentual sobre acceso a equipos de cómputo.



Fuente: Tabla Nro. 10

Tabla Nro. 11: Distribución de frecuencias sobre ingerir bebidas y/o alimentos cerca de equipos de cómputo.

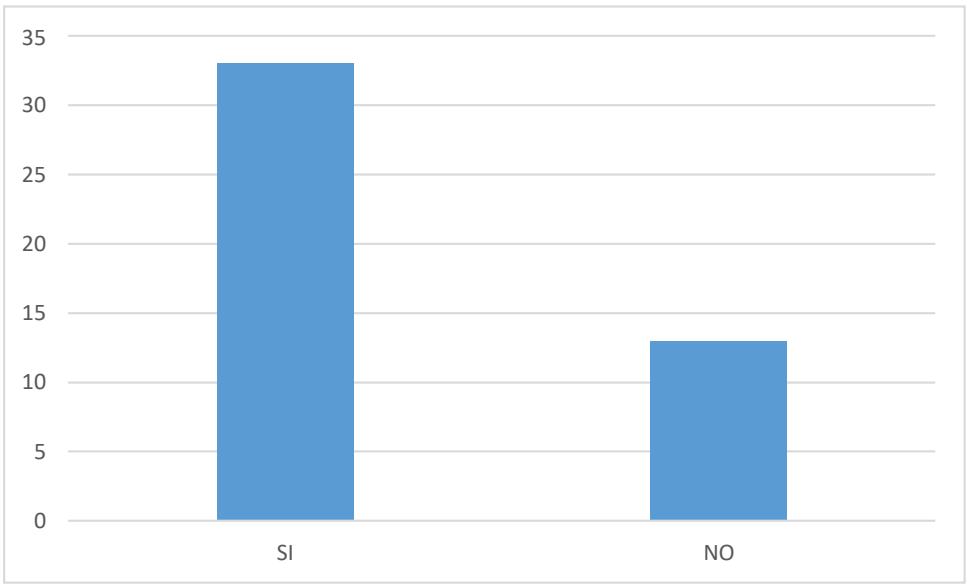
		n	%
	SI	33	72 %
	NO	13	28 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Conoce de casos en el que alguno de sus compañeros ha ingerido alguna bebida y/o alimentos cuando están en su área de trabajo cerca de equipos de cómputo?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 72% de los trabajadores manifiestan que SI conoce de casos en los que sus compañeros han ingerido alimentos cerca de equipos de cómputo, mientras que el 28% de los trabajadores manifiesta NO conocer de dicha situación.

Gráfico Nro. 10: Distribución de frecuencias porcentual sobre ingerir bebidas y/o alimentos cerca de equipos de cómputo.



Fuente: Tabla Nro. 11

Tabla Nro. 12: Distribución de frecuencias sobre el antivirus, funcionamiento y actualización.

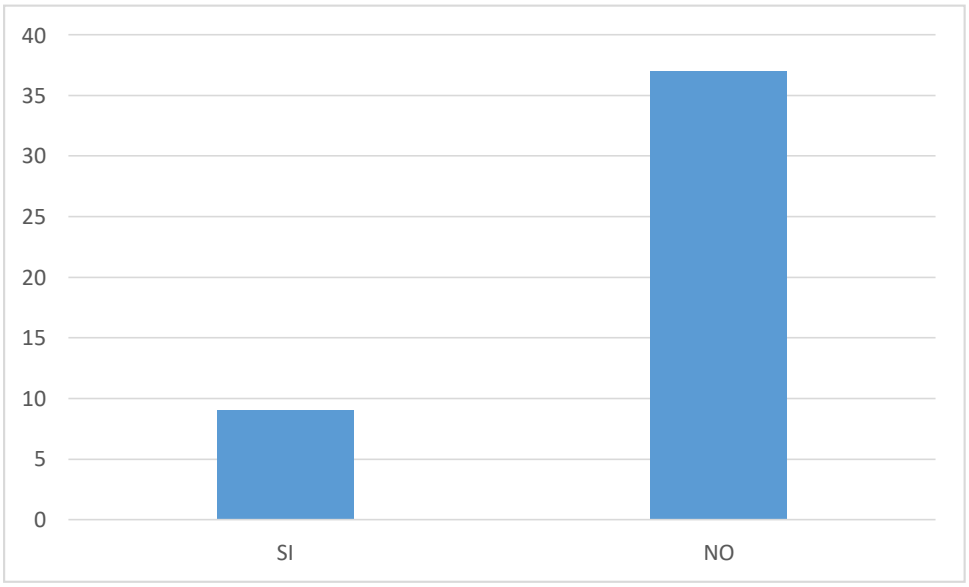
		n	%
	SI	09	20 %
	NO	37	80 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Tiene conocimiento si el antivirus de la institución funciona y se encuentra actualizado?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 20% de los trabajadores afirman que, SI tienen conocimiento sobre el buen funcionamiento y actualización del antivirus, mientras que el 80% de los trabajadores afirman NO tener conocimiento sobre antivirus actualizados y en buen funcionamiento.

Gráfico Nro. 11: Distribución de frecuencias porcentual sobre el antivirus, funcionamiento y actualización.



Fuente: Tabla Nro. 12

Tabla Nro. 13: Distribución de frecuencias sobre existencia de alarma de emergencia.

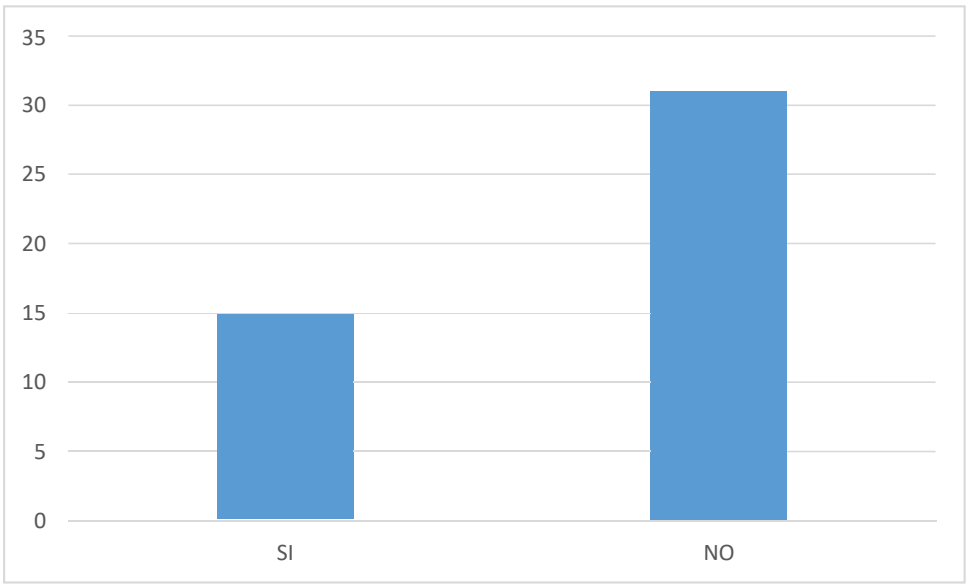
		n	%
	SI	15	33 %
	NO	31	67 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Tiene conocimiento de la existencia de alguna alarma contra incendios, robos u otros?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 33% de los trabajadores manifiestan que SI tienen conocimiento de la existencia de alguna alarma de emergencia, mientras que el 67% de los trabajadores afirma NO tener conocimiento de la existencia de alarma de emergencia.

Gráfico Nro. 12: Distribución de frecuencias porcentual sobre existencia de alarma de emergencia.



Fuente: Tabla Nro. 13

Tabla Nro. 14: Distribución de frecuencias sobre existencia de plan de contingencia.

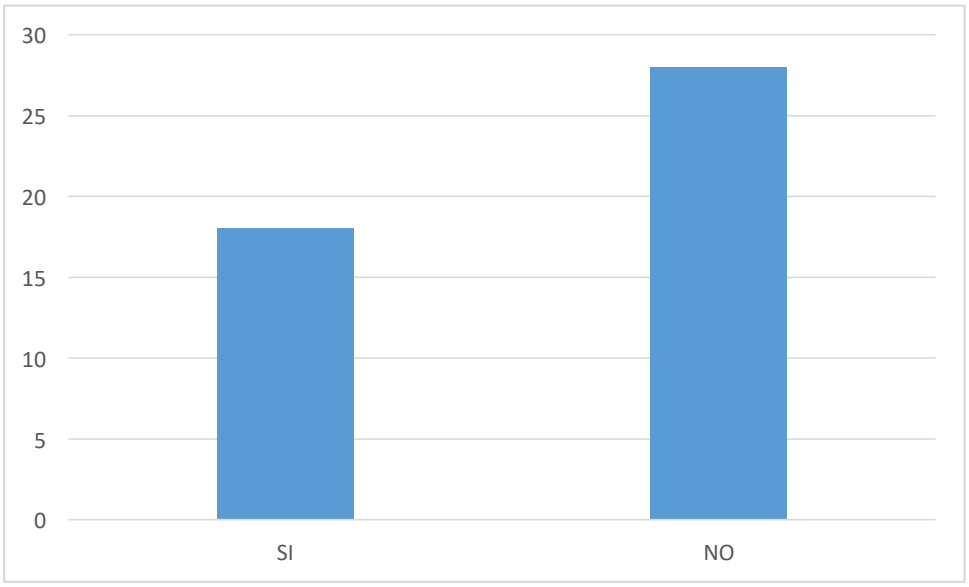
		n	%
	SI	18	39 %
	NO	28	61 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Sabe usted de la existencia de un plan de contingencia para algún incidente en la DRET?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 39% de los trabajadores manifiestan que SI saben de la existencia de un plan de contingencia, mientras que el 61% de los trabajadores afirman no saber de la existencia de este.

Gráfico Nro. 13: Distribución de frecuencias porcentual sobre existencia de plan de contingencia.



Fuente: Tabla Nro. 14

Seguridad de la información

Tabla Nro. 15: Distribución de frecuencias sobre conocimiento de seguridad informática.

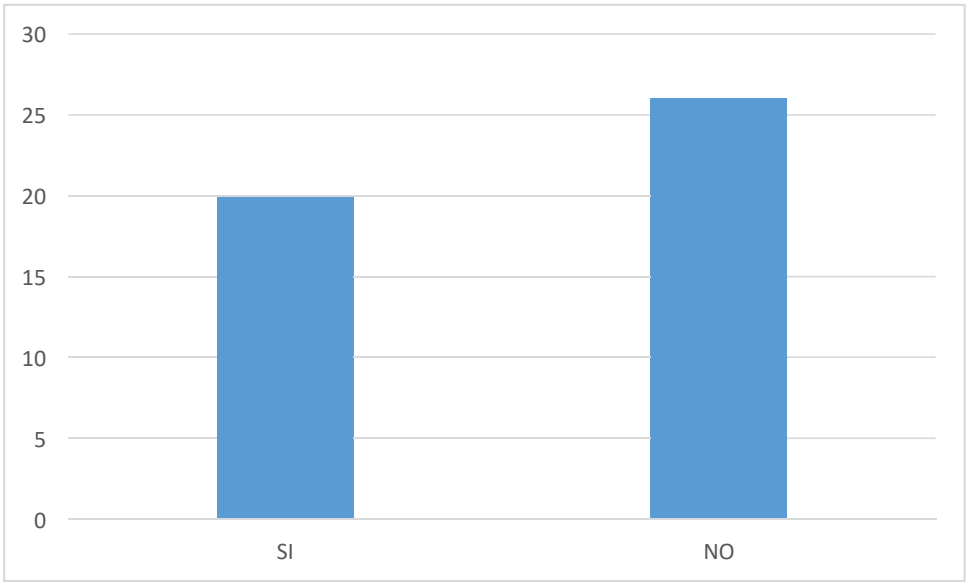
		n	%
	SI	20	43 %
	NO	26	57 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Sabe usted de qué trata el tema de seguridad informática?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 43% de los trabajadores afirman que SI conocen acerca de la seguridad informática, mientras que el 57% de los trabajadores afirma No conocer sobre el tema.

Gráfico Nro. 14: Distribución de frecuencias porcentual sobre conocimiento de seguridad informática.



Fuente: Tabla Nro. 15

Tabla Nro. 16: Distribución de frecuencias sobre control de seguridad.

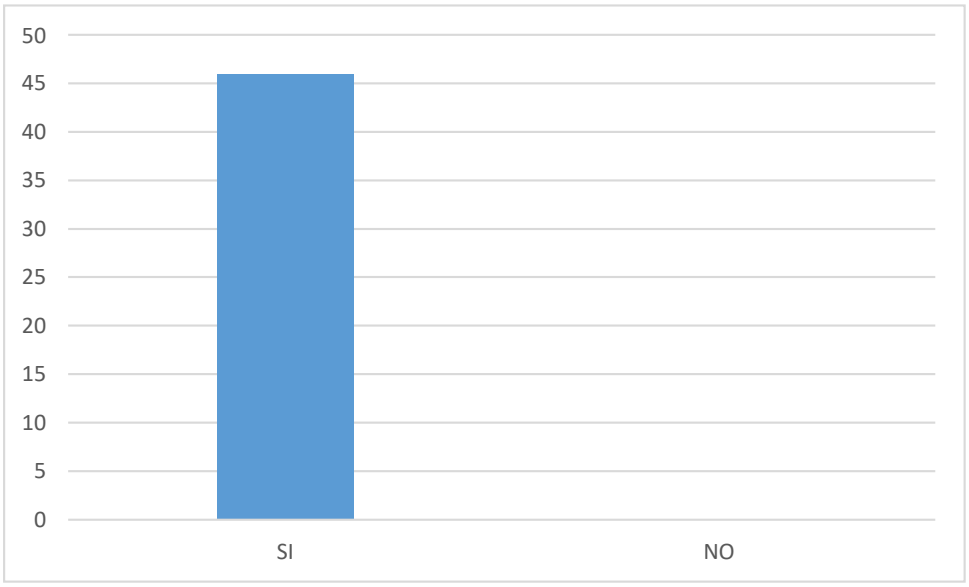
		n	%
	SI	46	100 %
	NO	0	0 %
TOTAL		46	100

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Considera que es necesario aplicar controles de seguridad para evitar robo o daño de información importante en la DRET?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 100% de los trabajadores encuestados afirma que SI es necesario aplicar controles de seguridad para evitar perdida de información.

Gráfico Nro. 15: Distribución de frecuencias porcentual sobre control de seguridad.



Fuente: Tabla Nro. 16

Tabla Nro. 17: Distribución de frecuencias sobre responsable de seguridad informática.

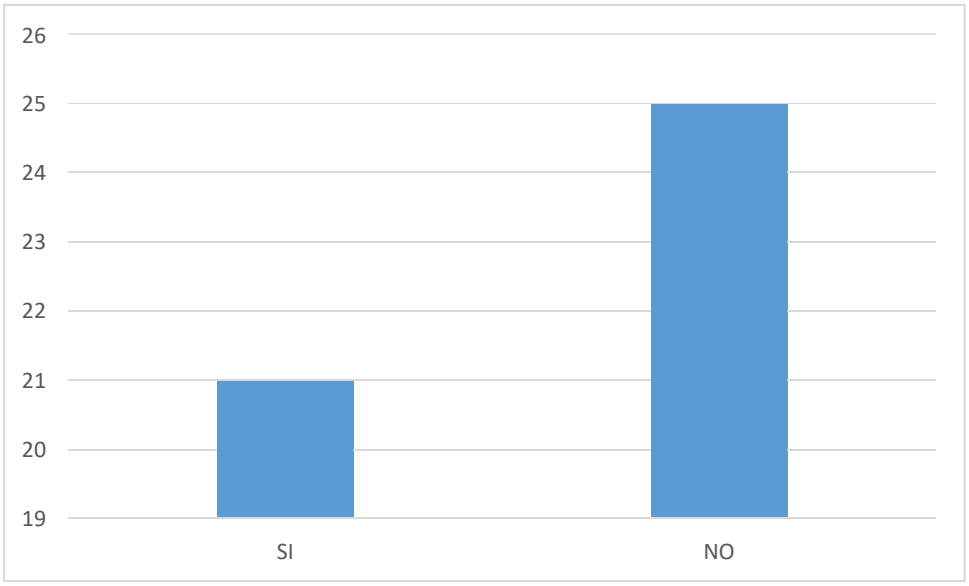
		n	%
	SI	21	46 %
	NO	25	54 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Tiene conocimiento de la existencia de un responsable de la seguridad informática?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que 46% de los trabajadores encuestados manifiestan que SI tienen conocimiento de la existencia de un encargado de la seguridad informática, mientras que el 54% de los trabajadores manifiesta NO tener conocimiento de ello.

Gráfico Nro. 16: Distribución de frecuencias porcentual sobre responsable de seguridad informática.



Fuente: Tabla Nro. 17

Tabla Nro. 18: Distribución de frecuencias sobre incidente de seguridad.

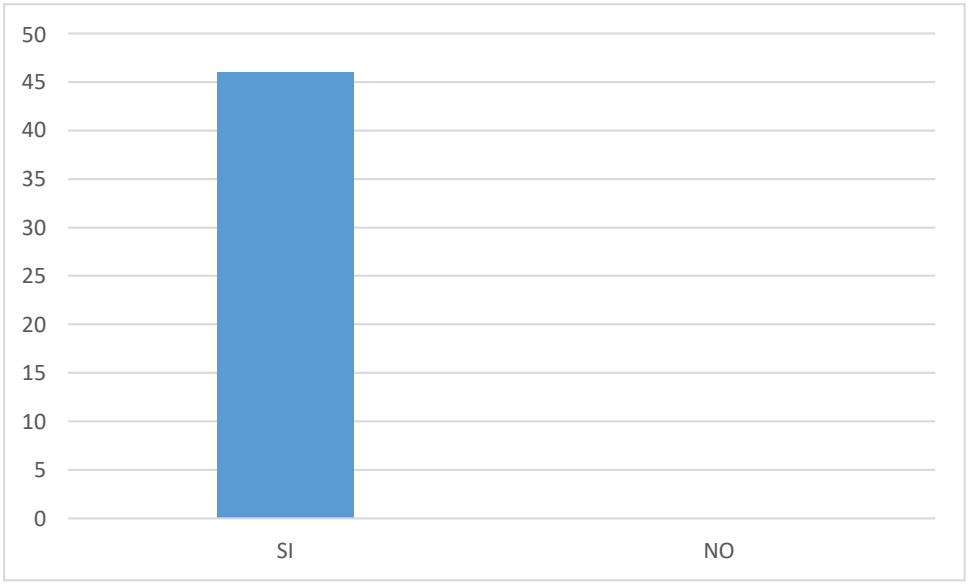
		n	%
	SI	46	100 %
	NO	0	0 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Sabe de algún incidente de seguridad en su área de trabajo en el último año?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 100% de los trabajadores encuestados manifiestan que SI conocen de algún incidente de seguridad de información ocurrido en su área de trabajo.

Gráfico Nro. 17: Distribución de frecuencias porcentual sobre incidente de seguridad.



Fuente: Tabla Nro. 18

Tabla Nro. 19: Distribución de frecuencias sobre importancia que se le otorga a la seguridad.

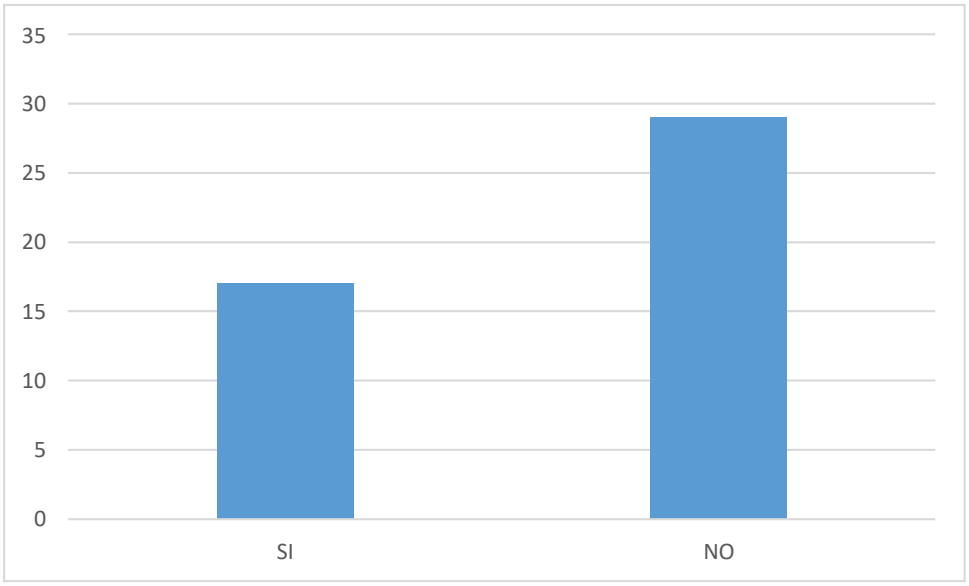
		n	%
	SI	17	37 %
	NO	29	63 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Considera que la DRET le da importancia suficiente a la seguridad?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 37% de los trabajadores encuestados afirman que SI considera que la institución le da importancia a la seguridad de información, mientras que el 63% considera que NO se le brinda la importancia suficiente.

Gráfico Nro. 18: Distribución de frecuencias porcentual sobre importancia que se le otorga a la seguridad.



Fuente: Tabla Nro. 19

Tabla Nro. 20: Distribución de frecuencias sobre seguridad de la información.

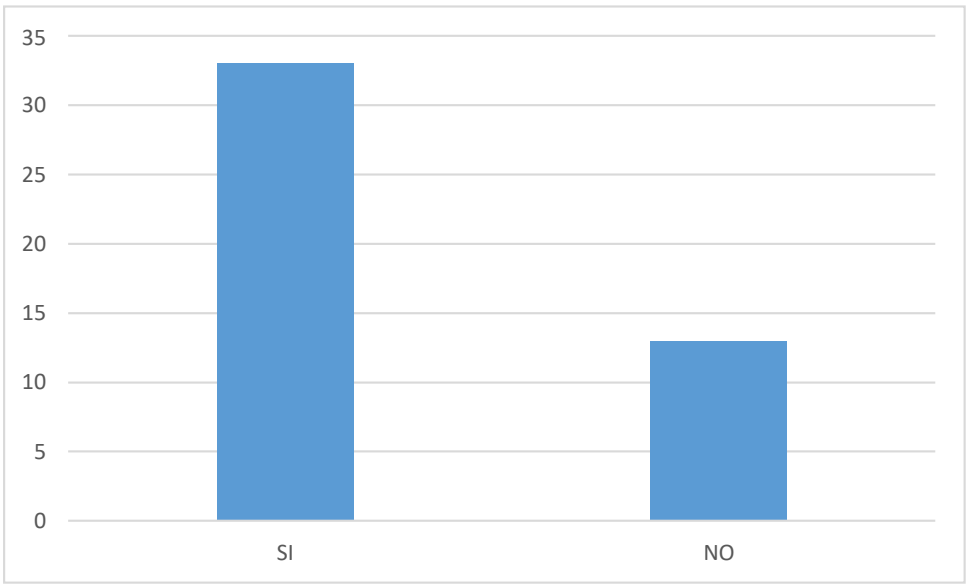
		n	%
	SI	33	72 %
	NO	13	28 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Considera que la seguridad de información debe ser vital en la institución?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 72% de los trabajadores encuestados manifiestan que SI debe ser vital la seguridad de la información en la institución, mientras que el 28% de los trabajadores manifiesta que NO la considera vital.

Gráfico Nro. 19: Distribución de frecuencias porcentual sobre seguridad de la información



Fuente: Tabla Nro. 20

Tabla Nro. 21: Distribución de frecuencias sobre protocolos de seguridad informática.

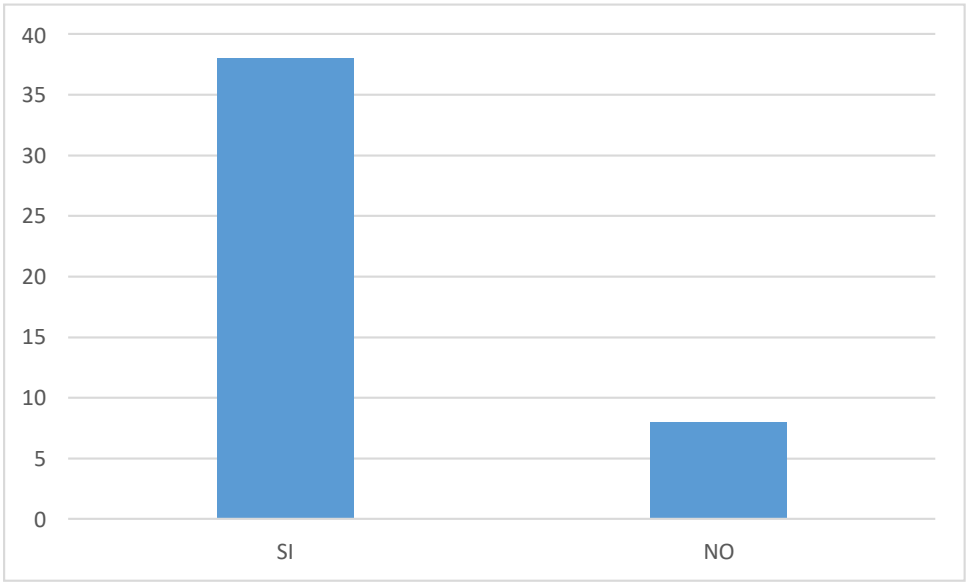
		n	%
	SI	38	83 %
	NO	8	17 %
TOTAL		46	100 %

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Usted como trabajador tiene la cultura de seguir con protocolos de seguridad?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 83% de los trabajadores manifiestan que como trabajador SI tiene la cultura de seguir protocolos de seguridad, mientras que un 17% de los trabajadores manifiesta que NO sigue protocolos de seguridad.

Gráfico Nro. 20: Distribución de frecuencias porcentual sobre protocolos de seguridad informática.



Fuente: Tabla Nro. 21

Tabla Nro. 22: Distribución de frecuencias sobre análisis de seguridad informática.

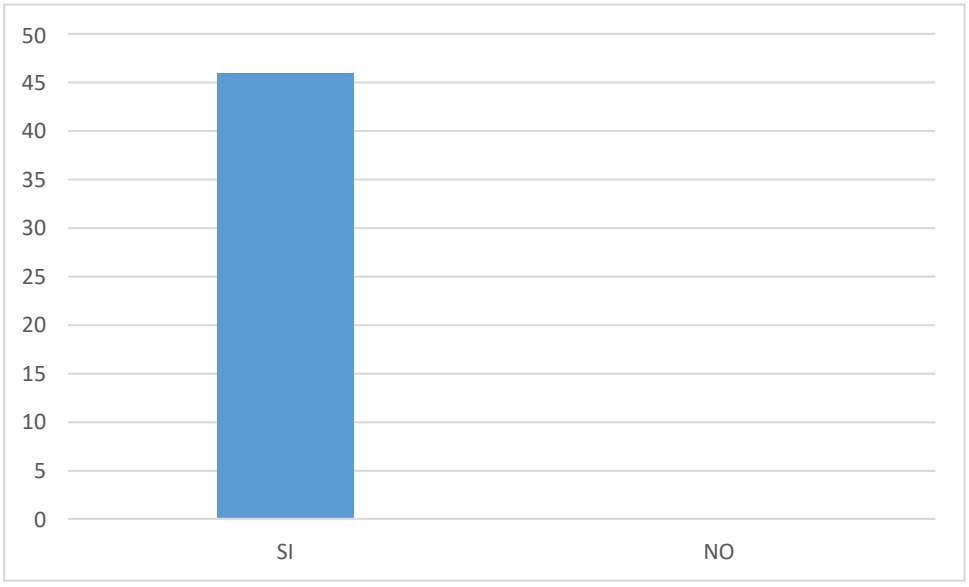
		n	%
	SI	46	100 %
	NO	0	0 %
TOTAL		46	100

Fuente: Encuesta realizada a 46 trabajadores entre hombres y mujeres de la Dirección Regional de Educación Tumbes, para responder la interrogante: ¿Considera usted que se debe realizar un análisis de la seguridad informática para conocer cómo se está llevando a cabo este proceso tan importante?

Aplicado por: Sánchez, E; 2020

Interpretación: Según los datos resultantes se puede observar que el 100% de los trabajadores encuestados manifiestan que SI consideran que se debe realizar un análisis de la seguridad informática para conocer cómo se lleva a cabo este proceso.

Gráfico Nro. 21: Distribución de frecuencias porcentual sobre análisis de seguridad informática.



Fuente: Tabla Nro. 22

5.2 Análisis de resultados

Esta investigación se centró en la elaboración de un análisis para la seguridad informática basándose en la norma ISO 27001 en la Dirección Regional de Educación Tumbes, se tomaron en cuenta 02 dimensiones, como son: la realidad actual y la seguridad de la información. En las cuales tienen sus respectivas preguntas.

En lo que concierne a la primera dimensión, en la Tabla Nro. 4: Distribución de frecuencias sobre políticas y procedimientos de seguridad, se determina que el 100 % de los trabajadores encuestados en la Dirección Regional de Educación Tumbes, manifiestan que No saben de la existencia de políticas y/o procesos de seguridad de la información. Este resultado tiene similitud con el de Lara, K. (9) quien en su investigación para una dimensión similar, en la Tabla Nro. 8 manifiesta que el 100% de los trabajadores encuestados expresaron que NO existen políticas y procedimientos para asegurar que se proporciona seguridad en la información de sus usuarios. También tiene similitud con los resultados de Pangalima, R. (10) quien en su investigación para una dimensión similar, en la Tabla Nro. 17 en el nivel de procesos de seguridad el 98% de los trabajadores manifiestan desconocer que existan políticas de seguridad de la información.

En lo que concierne a la segunda dimensión de seguridad de la información. En la Tabla Nro. 22: Distribución de frecuencias sobre análisis de seguridad informática, con la interrogante ¿Considera usted que se debe realizar un análisis de la seguridad informática para conocer cómo se está llevando a cabo este proceso tan importante?, los trabajadores manifestaron que el 100% de los trabajadores encuestados manifiestan que SI consideran que se debe realizar un análisis de la seguridad informática para conocer cómo se lleva a cabo este proceso para mantener a salvo los activos de la institución.

Este resultado tiene similitud con el de De La Cruz, R. (11) en la Tabla Nro. 15: Aceptación de la aplicación del plan de seguridad de la información, donde el 86.84% de los trabajadores municipales encuestados expresaron que SI creen que la aplicación de un plan de seguridad de la información en la plataforma tecnológica lograra cambios positivos a nivel tecnológico, mientras que el 13.16% NO cree que se logrará un cambio positivo con la aplicación del plan de seguridad de la información. Lo que nos lleva a analizar que la seguridad informática es aprobada por parte de los trabajadores quienes creen que si se debería realizar un análisis de las amenazas hacia los activos de la información de la Dirección Regional de Educación Tumbes.

5.3 Propuesta de mejora

5.3.1 Análisis del estado actual

La elección por la norma ISO 27001 es porque esta norma se basa en la mejora continua y con un monitoreo periódico de la seguridad de la información, y para poder tomar medidas necesarias para abordar nuevos riesgos. Proporciona una manera de asegurar la información por medio de políticas, procedimientos y controles establecidos para administrar riesgos de la seguridad de la información. El uso de esta norma permite a las instituciones de cualquier índole, gestionar la seguridad de sus activos.

Basándonos en la norma ISO 27001, la presenta investigación está orientada a analizar todos los controles y requerimientos de seguridad que se detallan en el Anexo A: ISO/IEC 27001 con los procesos de la Dirección Regional de Educación, para lo que se tendrá que considerar dentro de sus capítulos el numeral 5- políticas de seguridad de la información y concluyendo con el 18- Cumplimiento. En cada capítulo hay controles que se deben implementar. Los siguientes hallazgos son resultado del análisis de las medidas de la seguridad y los reglamentos que consideran dentro de la institución en relación con la seguridad de la información. El mencionado análisis nos permitirá acercarnos de manera global a la realidad de la Dirección Regional de Educación Tumbes, en relación con la seguridad de la información.

Se agregará un determinado valor a cada control en base a la realidad en la que se encuentra. Siendo:

0. No está implementado.
1. Está parcialmente implementado.
2. Completamente implementado.

Tabla Nro. 23: Análisis del estado actual Norma ISO 27001 Anexo A						
Norma	**Sección**	**N°**	**Descripción**	**Hallazgos positivos**	**Hallazgos negativos**	**Valor**
27001 - A.5	5. Políticas de la Seguridad de la Información.	5.1	Orientación de la dirección para la gestión de la seguridad de la información.			
		5.1.1	Documentación de las políticas de seguridad de la información.	Existe un documento de políticas	Se debe publicar y comunicar a todos los trabajadores y entidades externas relevantes, y enfatizar en el correcto seguimiento de los procesos de seguridad.	1
		5.1.2	Revisión de las políticas de seguridad de la información.		No hay un claro proceso a seguir en seguimiento y aseguramiento de la información vital.	0
A.6	6. Organización de la seguridad de la información.	6.1	Organización Interna			

		6.1.1	Compromiso con la seguridad de la información.	Se tiene documentado los roles de la compañía y de los trabajadores.	No hay un rol específico para el encargado del área en cuanto a la seguridad de la información y el trato con los servidores.	1
		6.1.2	Coordinación de la seguridad de la información en funciones.	Existen cargos y funciones.		2
		6.1.3	Asignación de responsabilidades de la seguridad de la información.	El personal trabajador está orientado a no compartir información con personas no autorizadas.	No hay documentación específica que índice el proceso de seguridad de la información con funciones y responsabilidades definidas.	1
		6.1.4	Asignación de nuevos grupos de activos de información.		No hay documentación de nuevos grupos de activos de información.	0
	Organización de la seguridad de la información.	6.2	Dispositivos móviles y teletrabajo			

		6.2.1	Políticas de dispositivo móvil		No hay políticas sobre el uso de dispositivos móviles en el área de trabajo y no se han analizado riesgos de cómo esta puede afectar en la filtración de información de la institución.	0
		6.2.2	Teletrabajo	Existe ya una iniciativa piloto de trabajo de manera remota en el área de administración.	Se deben implementar políticas, procedimientos y planes operativos en cuanto a las actividades de manera remota.	1
A.7	7. Seguridad de los recursos humanos.	7.1	Antes del empleo			
		7.1.1	Documentación de responsabilidades del personal.	Existe documentación en cuanto a cargo y funciones, responsabilidades del trabajador.		2
		7.1.2	Selección de candidato ha empleado.	Se lleva a cabo la verificación de antecedentes		1

				de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones requeridas.		
		7.1.3	Términos y condiciones de empleo.	Existencia de contratos donde incluye confidencialidad de la información.	No se especifica el tiempo por el cual esta información debe permanecer confidencial.	1
	Seguridad de los recursos humanos.	7.2	Durante el empleo.			
		7.2.1	Responsabilidad de la gestión.	Existencia de contratos donde incluye confidencialidad de la información.	No se realizan recomendaciones de seguridad y cómo proceder con la información según su trabajo.	1
		7.2.2	Educación y capacitación sobre la seguridad de la información.		Los trabajadores no reciben el apropiado conocimiento, capacitación sobre procedimientos de seguridad	0

					de la información según su función laboral.	
		7.2.3	Proceso disciplinario	Se abre procesos disciplinarios, o por medio de seguimiento judicial.	Pero las personas con procesos aún pueden ir a su área de labor, esto se debería restringir.	1
		7.3	Al terminar, cambiar de empleo o contrato.			
		7.3.1	Responsabilidades de culminación del empleo.		Se lleva un proceso de retiro de personal, pero no con los debidos requerimientos de seguridad de la información. No se solicita la entra de activos correspondientemente.	0
A.8	8. Gestión de activos	8.1	Responsabilidad para con los activos.			
		8.1.1	Inventario de activos	El área de cómputo maneja varios inventarios de activos de información en bloc de notas, y Excel.	No se tiene un proceso documentado para el inventario de todos los activos importantes.	1

		8.1.2	Propiedad de los activos	Todo activo de la información tiene que tener un responsable asignado, en el caso es que esta información está distribuida en las diferentes áreas.	No se tiene un seguimiento documentado sobre la seguridad de dichos activos.	1
		8.1.3	Uso aceptable de los activos	Existen ciertas reglas asignadas para las áreas de la institución, como por ejemplo no comer dentro de estas o ingerir bebidas, las que podrían afectar los equipos, identificándose como falta al cuidado de los activos de computo.	No existe un documento donde se les facilite la responsabilidad de cada empleado frente a los recursos que se les entregan.	1
		8.2	Clasificación de la información.			
		8.2.1	Lineamientos de clasificación.	Existen directorios compartidos de manera local.	No existe una clasificación formal de la información, debido a que mucha de ella se	1

					encuentra en los equipos de los usuarios administrativos.	
		8.2.2	Manejo de activos.	Existe un inventario con el registro de las maquinas, modelos, área y su responsable, así mismo como impresoras, Acces Point.	Pero el registro de estas máquinas no está organizadas por nivel de importancia, según la información que almacene.	1
		8.3	Manipulación de medios.			
		8.3.1	Gestión de medios extraíbles.	Existe un estrategia de extracción de estos medios, que solo involucra al área encargada (computo)	No se tiene un control me medios extraíbles para personal administrativo no autorizado. No hay un monitoreo de manera periódica establecido.	1
		8.3.2	Eliminación de los medios.	Se pone a disposición del área encargada con documento de por medio, dando de baja al equipo.	No hay un procedimiento de pasos a seguir para tener la certeza de que la eliminación de la información se llevó de manera segura.	1

A.9	9. Control de accesos	9.1	Requerimientos del negocio para el control de acceso.			
		9.1.1	Política de control de acceso.	Se tiene una política sobre el acceso a la información, debiendo seguir un proceso de solicitud.	x	1
		9.1.2	Acceso en red	Todas las áreas previa aceptación, tienen acceso en red, donde se les asigna el acceso a la información.	Se debe realizar revisiones en la otorgación de información y ser documentada, para no tener la información dispersa.	1
		9.2	Gestión de acceso a usuarios.			
		9.2.1	Registro de usuarios	Se registra a usuarios con autorización para el uso de sus sistemas de gestión.	No se lleva un control para que los usuarios no compartan sus claves.	1
		9.2.2	Acceso al usuario.	Existe el proceso de ingreso, actualización y retiro de usuarios de los servicios de gestión informáticos de los trabajadores.	No se tiene un debido control de acceso de información para los espacios físicos.	1

		9.3	Responsabilidad de los usuarios.			
		9.3.1	Uso de contraseñas	Los usuarios tienen contraseñas establecidas para ingresar a los diferentes sistemas de gestión.	Se debe exigir que los usuarios cumplan las buenas prácticas de seguridad y no compartir sus contraseñas con compañeros.	1
		9.3.2	Gestión de contraseñas	LA política de seguridad en creación de contraseñas seguras, determina en cuanto a seguridad un mínimo de 8 caracteres y bloqueo de acceso al hacer 3 intentos fallidos,		2
		9.3.3	Equipos desatendidos	Los usuarios tienen criterio de responsabilidad para con el cuidado de los equipos.	No todos cumples con las reglas de no llevar bebidas o alimentos a sus áreas.	1
A.10	10. Criptografía	10.1	Controles criptográficos.			
		10.1.1	Política de controles criptográficos.		No se tiene política de uso de controles criptográficos, que	0

					son necesarios para discos externos que tienen información sensible de la institución.	
A.11	11.Seguridad física y ambiental	11.1	Áreas seguras.			
		11.1.1	Perímetro de seguridad física	Se tiene registro de controles del hardware, y control de puertas de ingreso para proteger las áreas que almacenan esta información.		2
		11.1.2	Controles de entrada física	Hay control en el ingreso de personas a información y documentos.	No existe registro de las personas que han tenido acceso a la información, ni solicitan identificación.	1
		11.1.3	Protección contra amenazas externas y ambientales		No hay procesos a seguir para la seguridad contra las amenazas externas y ambientales (fuego,	0

					inundación, terremoto, explosión, disturbios civiles).	
		11.2	Equipos			
		11.2.1	Protección de equipos		No existen procesos documentados, alineados a riegos ambientales.	0
		11.2.2	Seguridad del cableado		Se identificó falta de canaletas y cableado eléctrico cruzado en el suelo del área de cómputo.	0
		11.2.3	El mantenimiento del equipo	Se realizan mantenimientos de los quipos, tanto preventivo como correctivo, tanto lógico como físico.	Sin embargo no existe un cronograma para llevar a cabo este mantenimiento preventivo.	1
		11.2.3	Seguridad de los equipos y activos fuera de la institución.	Existe personal que controla en la salida de la institución.	No se tiene claro cuáles son los equipos de la institución y cuáles de los trabajadores, por otra parte en momentos el vigilante suele ausentarse de la puerta.	1

A.12	12.Seguridad operacional	12.1	Operacionales y responsabilidades			
		12.1.1	Gestión de capacidad	En lo que refiere a desarrollo de software hay procesos que rigen para manejar indicadores de calidad y reporte de defectos.	Se debe hacer seguimiento del uso de recursos, así como tener requerimientos de capacidad futura.	1
		12.1.2	Separación de desarrollo, prueba y entornos operativos.		No se evidencian prácticas de desarrollo, ni hay un seguimiento en cuanto a control de calidad.	0
		12.2	Protección contra código malicioso.			
		12.2.1	Controles contra códigos malicioso.		Se debe mejorar sus antivirus, realizando la implementación de controles de detección, prevención y recuperación	0
		12.3	Copias de respaldo			
		12.3.1	Copias de seguridad.	Se realizan copias de seguridad todos los días.	Los procesos de copias de seguridad no están unificados.	1

		12.4	Registro y seguimiento			
		12.4.1	Registros de administrador	Se lleva un proceso diario de monitoreo, por parte de la administración.		2
		12.4.2	Sincronización de reloj	Se lleva un proceso para la sincronización de hora de todos los equipos de cómputo.		2
		12.5	Control de software			
		12.5.1	Instalación de software en sistemas operativos.		No hay controles de instalación de aplicaciones en los equipos. Por lo que se pueden instalar software ajeno a los requeridos por la institución.	0
		12.6	Gestión de vulnerabilidades técnicas			
		12.6.1	Control de vulnerabilidades	Se realiza mantenimiento al servidor, checando vulnerabilidades, evaluando de la exposición de la		2

				organización a estas vulnerabilidades.		
A.13	Gestión de la seguridad de redes	13.1	Seguridad de las redes.			
		13.1.1	Control de la red.	Se tiene un proceso incorporado y se tenía previsto un cambio la estructura de redes,		2
		13.1.2	Seguridad de los servicios de red	Se tiene configurado el acceso a los dispositivos conectados en red a través de grupos.	No se incluyen la identificación y características de seguridad.	1
		13.2	Transferencia de información			
		13.2.1	Políticas y procedimientos de transferencia de información.	En capacitaciones se explica la importancia de correo electrónico, y transferencia de archivos en red.	Se debe manejar una política para la transferencia segura de información con clientes, y trabajadores.	1

		13.2.2	Acuerdos de transferencia de información	En el contrato se incluye cláusulas de confidencialidad.		1
A.14	14.Seguridad de los SI	14.1	Requerimientos de seguridad de los SI			
		14.1.1	Análisis de los requerimientos de seguridad de la información		No se mantiene documentación sobre los requerimientos de seguridad y estrategias de tratamiento de riesgos.	0
		14.1.2	Restricciones en los cambios en paquetes del software		Se debe restringir la realización de modificaciones de paquetes de software, limitándolo a cambios necesarios, que deben ser controlados estrictamente.	0
		14.1.3	Pruebas de funcionalidad de los sistemas	Siguiendo la metodología de desarrollo de software se realizan pruebas funcionales.	Se deben incorporar y poner énfasis en pruebas de seguridad.	1

A.15	15.Relación con los proveedores	15.1	Seguridad de la información en relación con los proveedores			
		15.1.1	Políticas de seguridad de la información en consideración a los proveedores.	En el contrato se menciona las condiciones para confidencialidad y política de información.	Se debe acordar con los proveedores estipular con los proveedores el tratamiento y transmisión de información.	1
		15.2	Gestión de servicios de proveedor			
		15.2.1	Revisión y seguimiento de proveedores	Se lleva a cabo un proceso de selección, haciendo un análisis y estudio de cotizaciones, y evaluaciones de servicio a los proveedores.		2
	16.Gestión de incidentes de la seguridad de la información	16.1	Gestión de incidentes y mejoras en la SI			
		16.1.1	Responsabilidades y procedimientos	Se tiene un informe donde se encuentran registrados los		2

				incidentes que afectan a la integridad y confidencialidad, se especifica quienes clasifican los incidentes de seguridad.		
		16.1.2	Eventos que afectan la seguridad de la información	Los trabajadores están orientados a informar sobre algún incidente y los procedimientos a seguir para reportar el mismo.		2
		16.1.3	Reporte de informes sobre debilidades de seguridad.	Existe un procedimiento por parte de los trabajadores para reportar incidentes		2
		16.1.4	Valoración de eventos de seguridad de la información		No se tiene un análisis mensual de los resultados de los reportes atendidos y el proceso que se llevó acabo.	0
		16.1.5	Respuesta a incidentes de seguridad de la información	Hay informes de incidentes reportados por los trabajadores,	No se lleva a cabo la documentación del proceso que se siguió.	1

		16.1.7	Acopio de pruebas		No se tiene un proceso establecido en la recolección de evidencia formal.	0
A.17	17. Seguridad de la información de la gestión de la continuidad	17.1	Continuidad de seguridad de la información.			
		17.1.1	Implantación de continuidad de la SI		No hay un procedimiento en cuanto a la seguridad de la información, no hay un comité de seguridad para velar por las revisiones.	0
		17.1.2	Verificar, revisar y evaluar información de continuidad.		No hay un plan documentado de simulacros para verificar los procesos de seguridad de la información.	0
A.18	18.Cumplimiento de los requisitos legales	18.1	Cumplimiento de los requisitos legales.			

		18.1.1	Derechos de propiedad intelectual	Existen políticas sobre instalación de software.	Se deben incluir procedimientos para el cumplimiento de requisitos legales sobre el uso de software patentados y derechos de propiedad intelectual.	1
		18.1.2	Protección de registros de la institución.	Hay control en el acceso a la información de la organización, garantizando confidencialidad, integridad y disponibilidad.	No se tiene documentación del proceso a llevar ara este control, en concordancia con los requisitos reglamentarios.	1
		18.1.3	Privacidad y protección de datos personales	Hay control en el acceso a la información de la organización, garantizando confidencialidad, integridad y disponibilidad.	No se tiene clasificado los procesos y cuidados para con la información personal.	1
		18.1.4	Cumplimiento de políticas y normas de seguridad de información.		Se debe implementar una política en definición del trato a la información segura, estableciendo controles para	0

					monitorear y reportar el uso ilícito de los sistemas de información.	
		18.1.5	Verificación del cumplimiento técnico.		La verificación de los sistemas de información se debe realizar de manera periódica, para monitorear el cumplimiento de la seguridad de la información.	0

Fuente: Elaboración propia

Luego del análisis de los diferentes controles del anexo A de la norma ISO 27001, se encontró que, de todos los ítem procesados, 19 no se cumplen, 35 se cumplen de manera parcial y 12 se cumplen de manera satisfactoria.

En consideración a las políticas de seguridad, hay una documentación con los procedimientos y controles necesarios para garantizar la seguridad de la información. Se conoce que la institución cuenta con acuerdos de confidencialidad, aunque, no hay documentación que establezca roles claros y adecuados en cuanto a la seguridad de la información. También, se observó que la seguridad de los recursos humanos no hay un control apropiado, como por ejemplo, aunque hay un inventario de los activos, no se encuentra actualizado, por otro lado, no hay instrucciones en cuanto a la forma en clasificar la información. Con respecto al control de accesos, se conoce el uso de contraseñas, sin embargo, hay conocimiento de que algunos de los trabajadores comparten su contraseña de los sistemas de gestión, lo que conllevaría a ciertos riegos con la seguridad de la información. Siguiendo con la seguridad ambiental y física, no hay una buena protección en cuanto a la electricidad, puesto que hay cables cruzados en las diferentes áreas, como se observó en el área de cómputo. También se logró evidenciar la precaria infraestructura en la que se encuentra el área de cómputo, puesto que en la parte superior, para ser específicos en el techo del mismo, se evidencio que existen "calaminas" en mal estado, lo que significaría alto riesgo en cuanto a los equipos informáticos e información física que se encuentra en esa área. El análisis realizado, nos revela en términos generales, que se requiere realizar mejoras en cuanto a las políticas documentadas y bien establecidas en seguridad informática., control de accesos, seguridad de infraestructura, donde se tiene índice de incumplimiento o parcialmente adecuado.

Gestión de riesgos

El análisis de los riegos tiene como objetivo identificar los riegos de manera clara, a lo que se enfrenta la institución, y según lo identificado se deberá determinar las medidas de seguridad a tomar en cuenta para los diferentes activos de información, también nos permite establecer medidas de contingencia La metodología a utilizar para la gestión de riesgos es MAGERIT, nos permitirá tener en cuenta los procesos de gestión de riesgos según sus estándares, teniendo en cuenta riesgos derivados del uso de tecnologías. Este análisis servirá para que los trabajadores responsables de las diferentes áreas de la institución concienticen, de acuerdo a la existencia de riesgos que se manifiestan en el uso de las tecnologías de la información, por otro lado podrán tener conocimiento del tratamiento oportuno a estos riesgos.

Inventario de los activos.

Este es generado en relación al análisis de los riesgos, los activos serán etiquetados según su nivel de confidencialidad.

Tabla Nro. 24: Inventario de los activos.

Ámbito	Activo
Instalaciones	El lugar donde se encuentra ubicado la institución. Instalaciones eléctricas, telecomunicaciones.
Hardware	Servidores. Equipos de cómputo (escritorio, portátil) Routers, switchs. Telefonía.
	Sistema operativo.

Software	Paquete de office Sistema de backups. Antivirus.
Datos	Información contable, administrativa Formatos documentales.
Red	Red de telefonía Red de internet Red de caramas de vigilancia
Equipos adicionales	Aire acondicionado.
Personal	Director. Personal administrativo. Personal de salud. Encargado del área de cómputo.
Soporte de información.	Discos duros de los servidores. Almacenamiento de backups. Memorias USB, CD, DVD.

Fuente: elaboración propia.

Valoración de los activos.

En concordancia con la metodología, existe una tabla de valoración de los activos. Las escalas de valoración son las siguientes: muy bajo, bajo, medio, alto y muy alto.

Tabla Nro. 25: Valoración de los activos.

MA	Muy alto
A	Alto
M	Medio
B	Bajo
MB	Muy bajo

Fuente: MAGERIT.

En el cuadro se pueden observar las abreviaturas que serán usadas en la valoración de los activos de la información. Esto servirá para que desde el punto de la valoración se indique el aspecto más crítico en la seguridad. Usando la valoración ACIDT se medirá la criticidad en las cinco dimensiones.

- **[A]**utenticidad: nos permite saber quién ha hecho o hace cada cosa.
- **[C]**onfidencialidad: garantiza que la información solo se revela a personal autorizado.
- **[I]**ntegridad de datos: garantiza que los activos no han sido alterados u modificados por personal no autorizado.
- **[D]**isponibilidad: dimensión que refiere a los usuarios del activo a tener acceso cuando lo requieran.
- **[T]**razabilidad: permite saber quién presta/accede a tal servicio.

Para ver el coste que supondría para la organización, se usara la tabla de criterios de valoración, se muestra a continuación:

Tabla Nro. 26: Escala de valoración

Valor	Criterio
10	Daño muy grave
De 7 a 9	Daño grave
De 4 a 6	Daño importante
De 1 a 3	Daño menor
0	Irrelevante

Fuente: Magerit.

Seguidamente se muestra la valoración de las dimensiones, siguiendo la valoración de ACIDT:

Tabla Nro. 27: Valoración de seguridad de los activos

Valoración de las dimensiones de seguridad de los activos							
Ámbito	Activo	Valor	Dimensiones				
			A	C	I	D	T
Instalaciones	El lugar donde se encuentra ubicado la institución.	MA				9	
	Instalaciones eléctricas, telecomunicaciones.	A				7	
Hardware	Servidores.	MA	10	10	10	10	10
	Equipos de cómputo (escritorio, portátil)	A	8	6	7	7	7
	Routers, switchs.	A	9	9	9	8	9
Software	Sistema operativo.	MA	10	9	8	10	10
	Paquete de office	M	5	6	6	7	7

			A	C	I	D	T
	Sistema de backups.	MA	9	10	9	9	8
	Antivirus.	A	7	8	8	6	8
Datos	Información contable, administrativa	MA	10	10	10	10	10
	Formatos documentales (manuales, y accesos).	MA	9	9	9	10	9
Red	Red de telefonía	M				7	
	Red de internet	A				9	
	Red de caramas de vigilancia	MA			10	10	10
Equipos adicionales	Aire acondicionado.	M					6
Personal	Director.	MA		10		10	
	Personal administrativo.	MA		10		10	
	Encargado del área de cómputo.	MA		10		10	
Soporte de información	Discos duros de los servidores.	MA	10	10	10	10	10
	Almacenamiento de backups.	MA	9	7	10	9	10
	Memorias USB, CD, DVD.	A		6	8	7	

Fuente: Elaboración propia.

Análisis de Amenazas

A continuación se realizó un análisis para evidenciar los activos que se encuentran más expuestos a amenazas y que eventualmente afectarían a los distintos puntos de seguridad, estimando el nivel de vulnerabilidad de la amenaza. Se utilizó la guía del libro de Magerit para agrupar las amenazas en 4 grupos: Desastres naturales, errores y fallas no intencionadas, industriales, y amenazas intencionales.

Tabla Nro.28: Análisis de amenazas.

	Amenazas	Dimensión afectada					Activos afectados							
		A	C	I	D	T	Hardware	Red	Instalaciones	Software	Información	Datos	Adicionales	Personal
Desastres naturales	Fuego				x		x	x	x		x		x	
	Daños por agua				x		x	x	x		x		x	
	Inundación				x		x	x			x		x	
	Siniestro mayor				x		x	x	x		x		x	
	Fenómeno sísmico				x		x	x	x		x		x	
	Fenómeno meteorológico				x		x	x	x		x		x	
	Fuego				x		x	x	x		x		x	
	Daños por agua				x		x	x	x		x		x	

De origen industrial	Sobrecarga eléctrica			x	x		x	x	x		x		x	
	Corte de suministro eléctrico				x		x	x	x				x	
	Condiciones inadecuadas de temperatura o humedad				x		x		x		x		x	
	Fallos de servicios de comunicación				x			x						
Errores y fallas no intenciona das	Errores de los trabajadores		x	x	x					x	x	x	x	
	Errores del administrador		x	x	x		x	x		x	x	x	x	
	Errores de monitorización			x		x					x			
	Errores de configuración			x							x			
	Difusión de software dañino		x	x	x					x	x			
	Escapes de información		x								x			
	Destrucción de información			x	x			x	x	x	x	x	x	
	Mantenimiento / actualización de software			x	x						x			

	Mantenimiento preventivo y correctivo de hardware				x		x	x						
	Perdida de equipos		x		x		x				x			
	Indisponibilidad del personal				x									x
Amenazas intencionales	Manipulación de los registros			x		x					x			
	Suplantación de identidad		x	x							x	x		
	Abusos de privilegios de acceso		x	x	x					x	x	x		
	Intercepción de información		x							x	x	x		
	Modificación deliberada de la información			x							x	x		
	Destrucción de información				x						x	x		
	Divulgación de información			x						x	x	x		

	Manipulación del software		x	x	x					x	x	x	x	
	Manipulación de equipos		x		x		x	x			x	x		
	Robo		x		x		x	x			x	x		
	Indisponibilidad del personal				x									x
	Extorsión		x	x	x									x
	Ingeniería social		x	x	x									x

Fuente: Elaboración propia.

Después de realizado el análisis de los activos, se identifica que los que más resaltan son: la información y la infraestructura, así como también, los datos, recursos humanos, y copias de seguridad. En las posibles amenazas se identificaron las siguientes: las que se relacionan a desastres naturales, que puedan afectar a las distintas áreas de la institución dejando en alto riesgo la información. Tras la observación del área de cómputo, donde se encuentran los servidores, conexión a internet, equipos de cómputo, existe peligro latente en infraestructura, puesto que hay calaminas en mal estado, lo que se vería afectado si hubiera fuertes lluvias. La difusión de software dañino es una amenaza de gran relevancia, puesto que podría comprometer la seguridad de la información, donde se conoce que algunos trabajadores instalan software en los equipos de cómputo sin la autorización pertinente, pudiendo llegar a comprometer la información.

VI. CONCLUSIONES

Según los resultados obtenidos en esta investigación se concluye que: la Dirección Regional de Educación Tumbes no cuenta con políticas y controles establecidos y eficientes en cuanto a la seguridad de los activos de la información (las tecnologías de la información incluida el hardware y software, la infraestructura), los trabajadores. Por lo que un análisis de la seguridad de la información para identificar los activos de la información de la institución y las posibles amenazas que puedan existir, sería beneficioso, para la mejora en la gestión de la seguridad de la información, lo que permitirá disminuir la perdida de información, con lo que queda demostrado que la hipótesis general queda aceptada.

También se concluyó que:

1. En la tabla Nro. 4: sobre políticas y procedimientos de seguridad. Se identificó que el 100% de los trabajadores manifestaron que NO saben de la existencia de políticas y procesos para asegurar que se proporciona seguridad. Por lo tanto los trabajadores no tienen un proceso a seguir o desconocen de este, poniendo los activos de la Dirección Regional de Educación bajo peligro de diferentes amenazas.
2. En la tabla Nro. 16: sobre control de seguridad. Se observó que el 100 % de los trabajadores manifestaron que SI es necesario aplicar controles de seguridad para evitar la pérdida de la información. Por lo tanto se requiere que se apliquen controles según los estándares de la seguridad informática basándose en la norma ISO 27001, en la cual se presentan una serie de requerimientos.

3. En la tabla Nro. 22 sobre seguridad informática. Se observó que el 100% de los trabajadores manifiestan que SI consideran que se debe realizar un análisis de la seguridad informática para conocer cómo se está llevando a cabo este proceso tan importante, puesto que para mantener la seguridad de la información se deben llevar a cabo procesos que tienen que estar guiados por los requerimientos y estándares que proporciona la Norma ISO 27001.

VII. RECOMENDACIONES

Se darán a conocer algunas recomendaciones para el buen desarrollo de los procesos a seguir en la seguridad informática.

1. Se recomienda que la Dirección Regional de Educación Tumbes implemente los estándares de seguridad de la norma ISO 27001 que le brindará un mejor proceso de seguridad en los activos de información, protegiéndolos de las posibles amenazas.
2. Se recomienda que los trabajadores tengan capacitaciones sobre la seguridad informática, y puedan estar preparados para seguir los procesos y protocolos de seguridad según recomienda la Norma ISO27001.
3. Se recomienda que se nombre un equipo que este encargado de la seguridad de la información en específico, que vea la aprobación, implementación, de divulgar, controlar las políticas basadas en buenas prácticas para la buena gestión de la seguridad de información.

REFERENCIAS BIBLIOGRÁFICAS

1. Gil Vera VD, Gil Vera JC. Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia Et Technica. 2017 Junio; 22(2).

2. PCM. Resolución Ministerial Nº 004-2016-PCM. 2016 Enero 08..

3. Amoguimba Silva DL. Propuesta de políticas de seguridad de la información aplicado al entorno empresarial de Soft Warehouse S.A. Tesis de Postgrado. Quito: Pontificia Universidad Católica del Ecuador, Sistemas y Computación ; 2018.

4. Changoluisa Criollo WF. optimización del proceso de alta y baja de usuarios a través de la implementación de gestión de seguridad de la información, basado en la norma ISO 27001:2013 en una empresa de consultoría para la industria petrolera. Quito: Pontificia Universidad Católica del Ecuador-Matriz", Ciencias administrativas contables; 2017.

5. Nicasio Chavez O. Diseño e implementación de un sistema de gestión de calidad en seguridad de información SGSI. Tesis de postgrado. Ciudad de México: Universidad nacional autónoma de México, Departamento de computación; 2015.

6. Olaza Aliano HD. Implementación de NTP ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin. Tesis de postgrado. Lima: Universidad César Vallejo, Ingeniería de Sistemas; 2017.

7. Agurto CAstillo MA. Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER

S.A.C Talara, basado en la norma ISO 27001. Tesis de postgrado. Piura: Universidad César Vallejo, Ingeniería de Sistemas; 2017.

8. Castillo Collazos RE. Sistema de gestión de seguridad de la información en la Municipalidad distrital de Pira aplicando la norma ISO/IEC 27001:2013. Tesis de postgrado. Huaráz: Universidad Católica los Ángeles de Chimbote, Ingenieía de Sistemas; 2016.

9. Lara Morales KS. Propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la clínica SIMEDIC diagnóstica S.A.C – Piura; 2018. TEsis de postgrado. Piura: Universidad Católica los Ángeles de Chimbote, Ingeniería de Sistemas; 2018.

10. Pangalima Albán A. Auditoría en seguridad de tecnologías de información y comunicación en la Municipalidad Provincial de Paita; 2015. Tesis de postgrado. Piura: Universidad Católica Los Ángeles de Chimbote, Ingeniería de Sistemas; 2017.

11. DeLaCruz Vargas RE. Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016. Tesis de postgrado. Piura: Universidad Católica los Ángeles de Chimbote, Ingeniería de Sistemas; 2016.

12. Orozco G. El concepto de la seguridad en la Teoría de las Relaciones Internacionales: CIDOB d'Afers Internacionals.

13. Beekman. Introducción a la informática. sexta edición ed.

14. Escrivá Gascó. Seguridad informática. Primera ed. Madrid: Macmillan Iberia, S.A.; 2013.

15. Baca Urbina G. Introducción a la seguridad informática: Grupo Editorial Patria; 2016.

16. Prieto Espinosa A. Conceptos de informática Madrid: McGraw-Hill España; 2005.

17. Marco Galindo J. Escaneando la informática: Editorial UOC; 2012.

18. Roa Buendía J. Seguridad informática Madrid: McGraw-Hill España; 2013.

19. Costas Santos. Seguridad informática: RA-MA Editorial; 2015.

20. Eíto-Brun. Gestión de contenidos: procesos y tecnologías para gestionar activos de información: Editorial UOC; 2014.

21. Álvarez Marañón G. Seguridad informática para empresas y particulares Madrid: McGraw-Hill España; 2014.

22. Vasconcelos Santillán J. Informática 1: Grupo Editorial Patria; 2015.

23. Núñez Fernández E. Archivos y normas ISO: Ediciones Trea; 2007.

24. Normalización) I(Id. ISO 14001:2015 para la pequeña empresa: AENOR - Asociación Española de Normalización y Certificación; 2017.

25. ISO. ISO. [Online]. [cited 2020 Abril 15. Available from: https://www.iso.org/isoiec-27001-information-security.html.

26. Gómez Fernández L. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes: AENOR - Asociación Española de Normalización y Certificación; 2012.

27. Gómez R, Perez DH, Donoso Y, Herrera A. Metodología y gobierno de la gestión de riesgos de tecnologías de la información. Revista de Ingeniería. 2010 Enero - Junio;(31).

28. Piattini Velthuis M. Auditoría de tecnologías y sistemas de información: RA-MA Editorial; 2015.

29. Gómez Vieites Á. Seguridad en equipos informáticos: RA-MA Editorial; 2015.

30. Abril A, Pulido J, Bohada JA. Análisis de riesgos enseguridad de la información. Revista Ciencia, Innovación y Tecnología (RCIYT). 2013 Enero - Diciembre; I.

31. Vanegas Devia GA, Pardo CJ. Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT. Red de Revistas Científicas de América Latina, el Caribe, España y Portugal. 2014; 12(30).

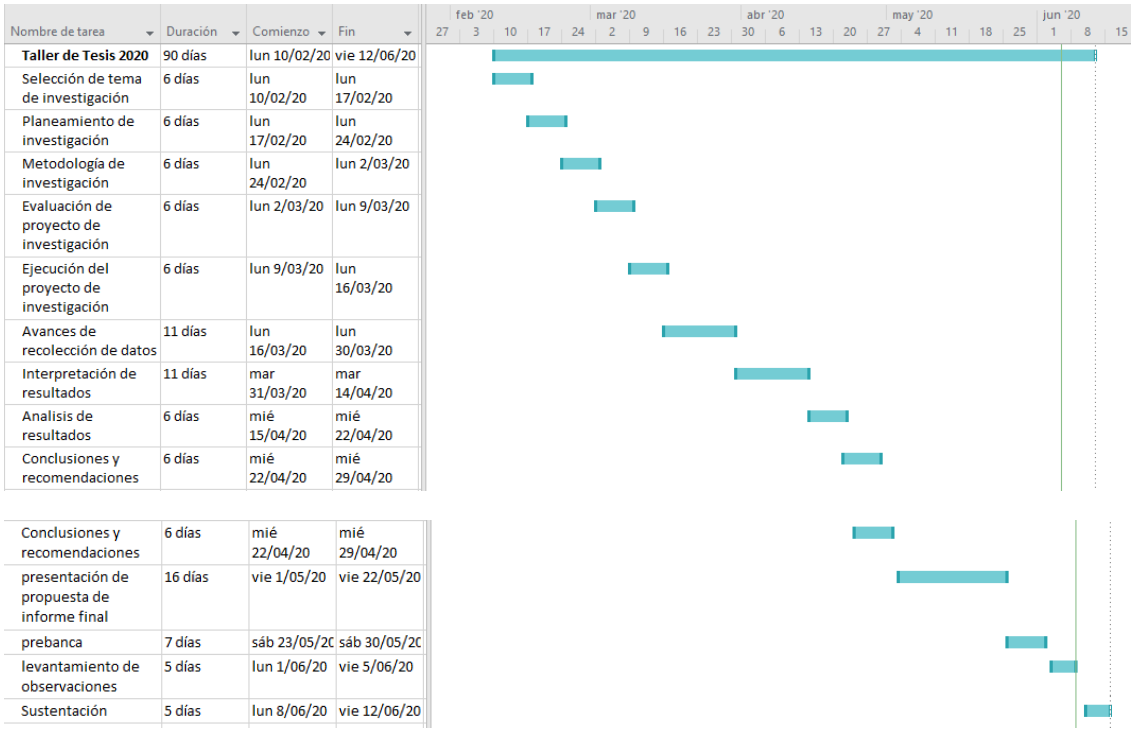
32. Domínguez Granda J. Dinámica de Tesis. Tercera ed. Chimbote: Ediciones de la; 2007.

33. Torres. Técnicas e instrumentos de recolección de datos en investigación cuantitativa. Universidad Yacambú. 2017 Abril; 16.

34. Hernández Sampieri R FCCBLM. Metodología de la investigación. Quinta ed. ed. Ciudad de México: McGRAW-HILL / INTERAMERICANA EDITORES; 2010.

ANEXOS

ANEXO NRO. 1: CRONOGRAMA DE ACTIVIDADES



Nombre de tarea	Duración	Comienzo	Fin
Taller de Tesis 2020	90 días	lun 10/02/20	vie 12/06/20
Selección de tema de investigación	6 días	lun 10/02/20	lun 17/02/20
Planeamiento de investigación	6 días	lun 17/02/20	lun 24/02/20
Metodología de investigación	6 días	lun 24/02/20	lun 2/03/20
Evaluación de proyecto de investigación	6 días	lun 2/03/20	lun 9/03/20
Ejecución del proyecto de investigación	6 días	lun 9/03/20	lun 16/03/20
Avances de recolección de datos	11 días	lun 16/03/20	lun 30/03/20
Interpretación de resultados	11 días	mar 31/03/20	mar 14/04/20
Analisis de resultados	6 días	mié 15/04/20	mié 22/04/20
Conclusiones y recomendaciones	6 días	mié 22/04/20	mié 29/04/20
Conclusiones y recomendaciones	6 días	mié 22/04/20	mié 29/04/20
presentación de propuesta de informe final	16 días	vie 1/05/20	vie 22/05/20
prebanca	7 días	sáb 23/05/20	sáb 30/05/20
levantamiento de observaciones	5 días	lun 1/06/20	vie 5/06/20
Sustentación	5 días	lun 8/06/20	vie 12/06/20

Imagen Elaborada con Software licenciado “Microsoft Project”

ANEXO NRO. 2: PRESUPUESTO

DESCRIPCIÓN	CANTIDAD	COSTO	TOTAL
Equipos y materiales			
Laptop	01	1500.00	1500.00
impresora	01	200.00	200.00
Papel bond A-4 80	300u	45.00	45.00
Tóner para impresora	01	1.00	1.00
Lapiceros	02	1.00	1.00
Lápices	01	5.00	5.00
		1751.00	1751.00
Servicios			
Servicios de Internet	4 meses	410.00	410.00
Pasajes locales		85.00	85.00
		495.00	495.00
Recurso humano			
Consultor en el tema	01	200.00	200.00
Total			**2446.00**

Fuente: Elaboración Propia

ANEXO NRO. 3: CUESTIONARIOS

Encuesta de opinión

Instrucciones: Se solicita su colaboración, respondiendo el presente cuestionario. El objetivo del presente es conocer su opinión sobre la seguridad de información en esta institución. Este instrumento presentará 21 preguntas, que debe desarrollar marcando con una ("X") en el cuadro correspondiente ("Sí" o "No") según su conocimiento. El presente cuestionario es anónimo.

	Preguntas	**Si**	**No**
A. Situación actual			
1	¿Tiene usted claras sus actividades y funciones a realizar en su área de trabajo?		
2	¿Cree que en el sistema manual los datos registrados son seguros?		
3	¿Sabe de la existencia de políticas y/o procesos para asegurar que se proporciona seguridad en la información de sus usuarios?		
4	¿Usted desecha la información que ya no necesita?		
5	¿Cree usted que los documentos que manipula son clasificados como confidencial o acceso restringido?		
6	¿Tiene conocimiento si se realizan copias de seguridad?		
7	¿Cree usted que es responsable del equipo informático que utiliza para realizar sus funciones en la institución?		
8	¿Cuándo no se encuentra en su área de trabajo, deja documentación visible en su escritorio?		
9	¿La clave de acceso es la misma para ingresar a todos los equipos de cómputo?		
10	¿Conoce de casos en el que alguno de sus compañeros ha ingerido alguna bebida y/o alimentos cuando están en su área de trabajo cerca de equipos de cómputo?		

11	¿Tiene conocimiento si el antivirus de la institución funciona y se encuentra actualizado?		
12	¿Tiene conocimiento de la existencia de alguna alarma contra incendios, robos u otros?		
13	¿Sabe usted de la existencia de un plan de contingencia para algún incidente en la DRET?		
B. Seguridad de la información			
14	¿Sabe usted de qué trata el tema de seguridad informática?		
15	¿Considera que es necesario aplicar controles de seguridad para evitar robo o daño de información importante en la DRET?		
16	¿Tiene conocimiento de la existencia de un responsable de la seguridad informática?		
17	¿Sabe de algún incidente de seguridad en su área de trabajo en el último año?		
18	¿Considera que la DRET le da importancia suficiente a la seguridad?		
19	¿Considera que la seguridad de información debe ser vital en la institución?		
20	¿Usted como trabajador tiene la cultura de seguir con protocolos de seguridad?		
21	¿Considera usted que se debe realizar un análisis de la seguridad informática para conocer cómo se está llevando a cabo este proceso tan importante?		