UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

FACULTAD DE CIENCIAS ADMINISTRATIVAS CONTABLES Y COMERCIO

INFORME DE TRABAJO DE INTEGRACIÓN CURRICULAR

PARA OTORGAR EL TITULO DE:

Licenciatura en Gestión de Información Gerencial

AUTOR:

Cárdenas Alava Aldo Xavier

TEMA:

Normas de estandarización para la implementación de políticas de seguridad de la información en la Empresa Pública ULEAM, Manta 2023 (Estudio de caso).

TUTOR/A:

Lcda. Mercy Celinda Rojas Once

Manta, 2024

	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-04-F-004
Uleam	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1
		Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor(a) de la Carrera de Gestión de la Información Gerencial de la Facultad de Ciencias Administrativas Contables y Comercio de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular – Estudio de Caso bajo la autoría del/de la estudiante **CARDENAS ALAVA ALDO XAVIER**, legalmente matriculado/a en la Carrera de Gestión de la Información Gerencial, período académico 2024-1, cumpliendo el total de 240 horas (96 horas Fase de Diseño y 144 horas Fase de Resultados), cuyo tema del trabajo es **"Normas de Estandarización para la Implementación de Políticas de Seguridad de la Información en la Empresa Pública ULEAM, Manta 2023 (Estudio de Caso).**

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad del mismo, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Manta, 29 de julio de 2024

Lo certifico,

Lic. Mercy Celinda Rojas Once, Mgt.D.U.
Docente Tutor(a)

Nota 1: Este documento debe ser realizado únicamente por el/la docente tutor/a y será receptado sin enmendaduras y con firma física original.

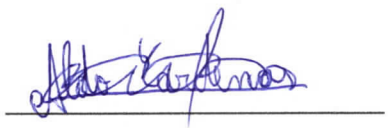
Nota 2: Este es un formato que se llenará por cada estudiante (de forma individual) y será otorgado cuando el informe de similitud sea favorable y además las fases de la Unidad de Integración Curricular estén aprobadas.

AUTORIA

Yo, Cardenas Alava Aldo Xavier, autor del proyecto de investigación "Normas de estandarización para la implementación de políticas de seguridad de la información en la Empresa Pública ULEAM"; declaro que; las ideas, opiniones y contenido del estudio de caso en cuestión son absolutamente originales y propios de mi patrimonio intelectual.

Además, expreso que los textos que provienen de otras fuentes están debidamente citados y referenciados. Como autor, asumo la responsabilidad del contenido de este proyecto de estudio de caso.

Manta, 16 de agosto de 2024



Aldo Xavier Cardenas Alava

CC. 131777915-3

DEDICATORIA

Dedico este proyecto en primer lugar a mis padres Angela Alava y Luis Cardenas, a mis hermanos Andy, Kevin y Deivis quienes han sido el soporte necesario para seguir a delante en mi vida no solo académica sino también de manera general y a mis primeras compañeras, Crisbel Pilligua y Madeleine Cantos. Además, hago dos menciones especiales hacia mis compañeras Lady Posligua y Alisson Villafuerte, las cuales conocí casi a mediados de todo este proceso, fueron mis amigas, compañeras, guía, motor, etc. A lo largo del tiempo se ganaron mi amistad, cariño y respeto. Pues son las personas que se encargaron de que el camino sea ameno y llevadero. Y a todas aquellas personas que indirectamente aportaron un granito de arena para construir mi cimiento que aspiré desde el primer momento que comenzó mi vida universitaria.

Cardenas Alava Aldo Xavier

RECONOCIMIENTO

En primer lugar, a mis padres por su cariño, apoyo, comprensión, consejos y paciencia. A mis hermanos, amigos y a cada una de las personas que me dieron el soporte necesario para culminar mi licenciatura.

Agradezco a cada uno de los docentes que hicieron parte de mi formación académica universitaria, con cada una de sus enseñanzas forjaron mi experiencia pre-profesional. Además, estoy totalmente agradecido con la Universidad Laica Eloy Alfaro como institución educativa que cada año se encomienda a formar profesionales de calidad a beneficio del país.

También, agradezco la Empresa Pública ULEAM, pues fue la institución que me abrió las puertas para realizar mi estudio de caso dentro de las instalaciones de esta, especialmente al Ing. Cristhian Flores, debido a que fue la persona que me facilitó la realización de mis actividades en el espacio de estudio, guiándome y explicándome el contexto de la organización.

Cardenas Alava Aldo Xavier

TEMA: Normas de estandarización para la implementación de políticas de seguridad de la información en la Empresa Pública ULEAM, Manta 2023 (Estudio de caso).

TABLA DE CONTENIDO

Índice de Ilustraciones

Índice de Tablas

INTRODUCCIÓN

En la actual era digital, donde la información se ha convertido en uno de los activos más valiosos para las organizaciones, la protección de los datos es crucial para garantizar la integridad, confidencialidad y disponibilidad de la información. En este contexto, las empresas enfrentan el desafío de implementar políticas de seguridad de la información efectivas, por ello, las normas de estandarización ofrecen un marco esencial para la creación y gestión de estas políticas, asegurando que los procesos internos no solo cumplan con las regulaciones vigentes, sino que también protejan la confianza de los clientes externos y la reputación institucional en un entorno cada vez más amenazado por ciberataques o brechas de seguridad de la información.

La presente investigación es un estudio de caso sobre las normas de estandarización para la implementación de políticas de seguridad de la información en la Empresa Pública ULEAM, el interés para realizar el estudio surge a través de una previa observación participante, esto aprobó la ausencia de políticas estandarizadas de seguridad de la información. Dicha observación permitió identificar la necesidad de contribuir positivamente en la seguridad de la información de la empresa como espacio de estudio.

La finalidad del estudio fue la revisión de las principales normalizaciones de políticas de seguridad existentes. Entonces, el objetivo fue identificar normas de estandarización aplicables para la implementación de políticas de seguridad de la información en la Empresa Pública ULEAM de la ciudad de Manta.

Las metodologías utilizadas para el desarrollo del proyecto fueron, el método de investigación inductivo, analítico, de campo y bibliográfico. Se usó como herramientas y técnicas, guía de observación, encuestas y entrevista para realizar el análisis de información, las

mismas que permitió demostrar resultados que fue útil para la toma de decisiones en la distribución de actividades durante la investigación.

La estructura de este proyecto comenzó con el estudio teórico de los antecedentes del problema, en la cual se comprendió que las variables normas de estandarización y políticas de seguridad de la información son temas que ha captado la atención de muchos investigadores a nivel internacional, nacional y local. Evidenciando que la información es uno de los insumos más importantes en las organizaciones.

La definición del caso del estudio fue de carácter participativo, la misma que fue realizada a través de una guía de observación. Esta sirvió como insumo relevante para comprender el estado actual de la organización respecto a las normas de estandarización y las políticas de seguridad de información. Además, se definió el suceso, fenómeno, problema y se planteó las preguntas de investigación.

El resultado obtenido con más relevancia fue mediante el estudio del nivel de madurez de los principios de seguridad de información, la confidencialidad mostró un nivel excelente de 4.73 sobre 5, además los principios de integridad y disponibilidad tuvieron una madurez aceptable. Lo mencionado también fue evidenciado cualitativamente a través de la entrevista, los datos de esta fueron analizado mediante una matriz de triangulación de información. Donde quedó demostrado mediante las respuestas de los entrevistados que la organización cuenta con una base sólida de prácticas de seguridad de la información basado en sus principios. Además, la encuesta realizada demostró a criterio de los encuestados que las normas ISO 27002 y los códigos de las mejores prácticas de seguridad de la información es la mejor opción para implementar políticas estandarizadas.

Antecedentes del Problema

Todas las empresas, sin importar el tamaño o sector, deben consolidarse con una ética corporativa que las dirija hacia el éxito. Cada actuar de una entidad refleja valores ante la sociedad en general, especialmente a sus clientes, debido a que estos forman parte de la responsabilidad social de cada organización. Es decir, las empresas están envueltas en un contexto social. El cumplimiento legal, la transparencia y la responsabilidad son fundamentales para mantener la confianza y la fidelidad del público. Dicho esto, las políticas de seguridad de la información como problema de estudio surgen a partir de un entorno socio-empresarial en el que están involucrados individuos que interactúan de forma constante dentro de cada área funcional de la Empresa Pública ULEAM.

Este tema por su relevancia ha sido tratado desde los siguientes estudios:

Internacional

En Perú se realizó una investigación por parte de Bustamante, Valles, Cuellar y Lévano (2021) con el tema políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. El propósito de este estudio era mejorar la administración de la seguridad de la información en una municipalidad peruana específica. El enfoque metodológico utilizado consistió en la implementación de un conjunto de políticas fundamentadas en la ISO 27001:2013.

Además, los investigadores realizaron un estudio preexperimental con una muestra de 30 empleados a quienes se les aplicó un cuestionario para evaluar su nivel de satisfacción con el modelo implementado. En términos generales, más del 90% de los encuestados informaron mejoras en la municipalidad, representando un notable cambio entre las mediciones antes y después, pasando del 49% al 96%. Este estudio culminó con la implementación de un conjunto

de políticas de seguridad basadas en tres pilares esenciales: confidencialidad, integridad y disponibilidad. Esto resultó en una mejora significativa en la gestión de la seguridad de la información, asegurando una protección adecuada de los datos.

Nacional

En Sangolquí, Ecuador, Baldeón Gutiérrez & Guanopatín Safla (2015) llevaron a cabo un estudio centrado en el desarrollo de políticas de seguridad de la información para la Dirección de Tecnologías de la Información de la Universidad Central del Ecuador, siguiendo los estándares ISO/IEC 27000 y COBIT 5. El propósito de esta investigación era establecer políticas específicas de seguridad de la información para dicha dirección. La metodología empleada se basó en la implementación de políticas de seguridad de la información alineadas con los estándares ISO/IEC 27000 y COBIT 5.

Como resultado, lograron crear un mapeo que facilitó al personal de la Dirección de Tecnologías de la Información la comprensión de la relación entre estos estándares. Esto permitió que ambos estándares fueran utilizados de manera conjunta, complementándose mutuamente en el tratamiento de la seguridad de la información dentro de dicha organización.

Regional

En Guayaquil, Mahecha Guzmán & Coello Falcones (2017) llevaron a cabo un proyecto de investigación que se enfocó en el desarrollo de un sistema de información para facilitar la implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información, basado en la norma ISO 27001:2013 en la empresa Astilleros Navales Ecuatorianos. El objetivo principal era diseñar un sistema de información que gestionara las fases del sistema de gestión de seguridad de la información.

La metodología de la investigación se basó en las buenas prácticas estipuladas en el estándar ISO 27001:2013, el cual proporciona pautas para la implementación adecuada de un sistema de gestión de seguridad de la información. Asimismo, los autores seleccionaron la norma ISO 27005 para la gestión de riesgos y utilizaron este estándar para programar todas las reglas de negocio relacionadas con la gestión de la seguridad de la información.

Como resultado, lograron desarrollar un software, un sistema de información que facilitó y agilizó la gestión y aplicación del sistema de gestión de seguridad de la información. Este software permitió mantener una trazabilidad completa para cada activo de información. Además, los autores confirmaron que la solución propuesta proporciona un seguimiento de los riesgos asociados con cada activo de información, lo que les permitió verificar los planes de acción respecto al tratamiento de los riesgos y las acciones llevadas a cabo por el personal para cumplir con las políticas establecidas.

Una vez realizado el estudio a nivel maso, meso y micro se analiza lo siguiente:

Los estudios previos realizados por los autores mencionados se basaron en investigaciones bibliográficas y de campo sobre las normas de estandarización para implementar políticas de seguridad de la información.

A partir de la revisión literaria del objeto y campo de estudio, se evidencia que las normas de estandarización para implementar políticas de seguridad de la información han despertado la curiosidad de los investigadores, estos han dado a conocer lo fundamental de establecer normas estandarizadas que aporte de forma positiva a la seguridad de la información en las organizaciones.

Definición del Estudio de Caso

La Empresa Pública ULEAM, con sede en el cantón Manta, una organización creada en sesión celebrada, en segunda instancia, el 26 de junio de 2013, mediante resolución expedida por honorable Consejo Universitario de la Universidad Laica “Eloy Alfaro” de Manabí.

La empresa se compromete a llevar a cabo diversas acciones relacionadas con la ejecución, supervisión y seguimiento de varios planes, programas y proyectos. Esto se logra mediante acuerdos y colaboraciones con individuos, entidades legales, así como organismos tanto locales como internacionales. Su enfoque se centra en ofrecer servicios sobresalientes en consultorías, asesorías y gestión de proyectos vinculados a la producción, capacitación, investigación e inversión, con el objetivo de contribuir al desarrollo integral del país. Además, busca fomentar el crecimiento económico sostenible, impulsando la creación de empleos significativos y productivos a nivel local.

La misión de la Empresa Pública ULEAM, es brindar servicios de excelencia en el ámbito de consultorías, asesorías, ejecución y/o administración de proyectos de producción, capacitación, investigación, inversión y demás afines a la ULEAM, con la participación de personal altamente capacitado para impulsar el desarrollo multidisciplinario del país; todo en línea con la Ley Orgánica de Empresas Públicas (LOEP).

Por otro lado, la visión de la empresa apunta a ser reconocida como la principal empresa pública universitaria en Ecuador, destacándose por ofrecer servicios de investigación, capacitación, consultoría y producción de alta calidad. Esto se logra gracias a una gestión eficaz, eficiente y proactiva.

El suceso principal para efectuar la presente investigación empieza a través de un diagnóstico de carácter observacional en el espacio de estudio. Esta metodología de diagnóstico

permitió de forma objetiva observar e identificar el estado actual de la implementación de políticas de seguridad de la información en la Empresa Pública ULEAM.

En base a la observación realizada, se dio por hecho que la empresa tiene carencias en competencias relacionadas a la implementación de políticas de seguridad de la información a partir de normas estandarizadas, las mismas que ayudan a salvaguardar el activo de la información, otorgan confidencialidad, disponibilidad e integridad.

La guía de observación aplicada dio como resultado la no implementación de ningún tipo de políticas de seguridad de información, no se realizan evaluaciones de riesgos de manera periódica, no se lleva a cabo la formación y concientización sobre el tema, no se realizan auditorías internas para verificar el cumplimiento de la seguridad de la información, sin embargo, la empresa si cuenta con un sistema informático con medidas de autenticación (contraseña) para acceder a la información dependiendo el rol del usuario.

Por ello, se desarrollaron las siguientes preguntas de investigación que sirvieron como guía del presente estudio, delimitando los aspectos claves a explorar:

- ¿Cuáles son los fundamentos teóricos de las normas de estandarización e implementación de políticas de seguridad de la información?
- ¿Cuál es el estado actual del uso de normas de seguridad la información en la Empresa Pública ULEAM?
- ¿Cuáles son las principales características de las normas estandarizada de seguridad de la información?
- ¿Cuál es el nivel de madurez en los principios de seguridad de la información en la Empresa Pública ULEAM?

- ¿Cuál es la norma estándar recomendada para establecer las mejores prácticas de seguridad de la información en la Empresa Pública ULEAM?

Justificación

En la actualidad, las amenazas cibernéticas están en constante evolución, es crucial comprender cómo la información se convierte en un insumo fundamental para la implementación de políticas de seguridad enfocadas en la confidencialidad, integridad y disponibilidad de la información. Esto es esencial para prevenir posibles vulnerabilidades informacionales que podrían afectar de forma negativa a la reputación de las empresas.

El presente estudio de caso destaca la importancia de las normas estandarizadas para implementar políticas de seguridad de la información en las organizaciones, dado que estas constituyen un pilar fundamental para salvaguardar uno de los activos más vitales: la información.

En el actual contexto empresarial, la gestión de la seguridad de la información ha adquirido una relevancia considerable en organizaciones de distintos tamaños y sectores. El continuo avance tecnológico a nivel global ha convertido a la gestión de la seguridad de la información en un componente esencial para todas las organizaciones que se ven inmersas en un flujo de información abundante.

Esta investigación ha despertado un notable interés en la Empresa Pública ULEAM por mejorar sus prácticas de seguridad de la información. También, el actual estado de la empresa en lo que respecta a políticas de seguridad de la información confirma la alta importancia de implementar normas estandarizadas. En otras palabras, la disponibilidad de la organización, el

estado actual de la misma, la relevancia del tema, el potencial de impacto positivo, la observación previa realizada y analizada, confluyen para certificar la factibilidad de este proyecto.

La presente investigación tiene una importancia crítica en un contexto donde la protección de la información y la ciberseguridad deben ser imperativos debido a la gran importancia de estos, especialmente para instituciones como la Empresa Pública ULEAM. Este proyecto no solo estudia las normas estandarizadas para implementar políticas de seguridad de la información, sino que también describe las ventajas obtenibles a través del cumplimiento de estas.

El impacto social de este proyecto consiste en que el presente estudio de caso no solo tiene impacto en la empresa estudiada en particular, sino que también puede contribuir a elevar los estándares de seguridad de la información en organizaciones similares, con el fin de llevar a cabo una mayor confiabilidad en el manejo de datos. Proteger la información confidencial; aporta transparencia y reputación en las organizaciones. Además, la presente investigación tiene un impacto más allá de la empresa específica de estudio, beneficia a la sociedad empresarial en general y fortalece la necesidad de implementar políticas de seguridad de la información en las empresas.

Objetivo General

Identificar normas de estandarización aplicables para la implementación de políticas de seguridad de la información en la Empresa Pública ULEAM de la ciudad de Manta.

Objetivos Específicos

- Caracterizar desde la teoría las categorías de las normas de estandarización e implementación de políticas de seguridad de la información.
- Determinar el estado actual del uso de normas de seguridad la información en la Empresa Pública ULEAM.
- Realizar una revisión de las principales normas estandarizada de seguridad de la información.
- Identificar el nivel de madurez en los principios de seguridad de la información en la Empresa Pública ULEAM.
- Recomendar una norma estandarizada basada en las mejores prácticas de seguridad de la información a la Empresa Pública ULEAM.

MARCO TEÓRICO

Normas

El autor Kelsen expresa su concepto sobre las “normas”, en base a su pensamiento, afirma lo siguiente:

> “Las normas representan un precepto o mandato que indica que algo debe suceder u ocurrir. Su expresión lingüística suele ser un imperativo o una oración deóntica. Se trata de una acción que indica un mandato o prescripción”.
>
> En su esencia, la norma implica una voluntad, un acto de deseo. Es un precepto o mandato que se dirige hacia la conducta de otros, una acción que establece que otro individuo debe comportarse de una manera específica. (Kelsen, 1994, pág. 27)

Entonces, el autor distingue las normas como el sentido de querer o un acto de voluntad, se refiere a las normas como la conducta de los individuos, establecen cómo las personas deben comportarse. La naturaleza de las normas y mandatos son fundamentales en el ámbito legal, social, ético y empresarial.

En las organizaciones, tales como la Empresa Pública ULEAM, la implementación de normas basadas en la seguridad de la información supone una actividad esencial. Debido que, llevar a cabo buenas prácticas en términos de integridad, disponibilidad y confidencialidad de la información concierne a una identidad organizacional positiva en términos de reputación empresarial. Así mismo, la implementación no solo establece normas, también es imperativo una excelente comunicación, capacitación del personal y establecer monitoreo del cumplimiento de las normas.

Estandarización

Según la Guía de los Fundamentos para la Dirección de Proyectos de PMBOK la estandarización "es un documento que provee, para uso común y repetitivo, las reglas, pautas o características que deberían cumplir las actividades (o sus resultados), a fin de obtener un óptimo grado de orden en un contexto dado" (PMBOK, 2013, pág. 478).

El autor Borbón Sanabria afirmó lo siguiente:

> La estandarización se refiere a un modelo o norma que proporciona pautas para llevar a cabo una actividad o procedimiento específico.
>
> Su uso se ha vuelto común en la actualidad, debido que busca garantizar que los procesos y actividades realizados por organizaciones y sus colaboradores sean consistentes, organizados y estructurados. (Borbón Sanabria, 2011, pág. 14)

Sin embargo, según Peña y Angulo consiste en desarrollar soluciones para situaciones reales, comunes y repetidas, buscando alcanzar una estructura óptima en un entorno específico, ya sea tecnológico, político o económico, que sea compartida y utilizada de manera regular". (Solís Peña & Angulo Arriaza, 2012, pág. 2)

Es decir, la estandarización se refiere a la creación y utilización de documentos que contienen reglas a seguir, de forma repetitiva en un contexto en cuestión, es decir, los estándares tienen como objetivo proporcionar un marco de referencia para llevar a cabo diligencias de manera ordenada y efectiva.

Normas de Estandarización

Una vez sintetizado ambos términos; las normas de estandarización son políticas que brinda reglas a cumplir en las actividades repetitivas o procesos empresariales, con el objetivo de aplicar una optimización u orden de una cuestión en particular. Se refiere a herramientas importantes en diferentes ámbitos, ya sea tecnológico, político, económico, establecen formatos que dirigen la ejecución de actividades, asimismo, fomenta que los procesos operativos de las empresas sean organizados y estructurados, facilitando la consistencia, eficiencia y calidad en la ejecución de tareas.

Por ejemplo, la aplicabilidad de estándares según a PMBOK corresponde a que las actividades se efectúen de forma eficaz, conlleva a mayor control sobre los resultados y reduce la incertidumbre, por supuesto, en referencia a la gestión de proyectos. En el contexto de la seguridad de la información, la familia ISO 27000, suponen la mejor referencia para la gestión de la seguridad de la información en una organización, debido que las mismas proporcionan una conceptualización de la seguridad de la información, directrices y requisitos específicos para implementarla, además la guía de certificación en dichas normas.

En resumen, las normas estandarizadas son reglas, especificaciones o pautas, con el propósito de establecer un orden o lineamiento en actividades repetitivas dentro de un contexto específico. Se trata de un formato diseñado, actualizable e implementable creado por organizaciones internacionales de normalizaciones.

Importancia

Mahecha Guzmán & Coello Falcones (2017) destacan la importancia de las normas de estandarización debido al "auge entre las organizaciones con el fin de destacar de la competencia, para ello las normas ISO son unas de las alternativas más aceptadas a la hora de estandarizar procesos" (pág. 29).

Entonces, la importancia recae en que la implementación de estándares ofrecen un marco de referencia o un formato establecido de normas, el mismo que tiene como objetivo que las organizaciones cuenten con procesos operativos automatizados y se lleve a cabo una cuestión en particular con eficacia. A la par, puedan diferenciarse de las demas empresas (certificación que otorga las organizaciones de normalización) y ganar la confianza de los clientes externos con la significante ventaja competitiva que conlleva la implementación de estándares.

Beneficios

Las normas de estandarización desempeñan un papel fundamental en muchos entornos, brindando directrices claras y una serie de beneficios significativos que impactan positivamente en las organizaciones. Respecto a lo mencionado, Añez considera lo siguiente:

> Al definir las tareas a realizar, se logra estabilizar el rendimiento, ofreciendo así una plataforma sólida desde la cual se puede trabajar hacia la mejora. De esta manera, se establece el primer paso en el proceso de mejora.
>
> La estandarización del trabajo facilita la visualización de las actividades en un proceso y proporciona una línea de base para su comparación. Esto, a su vez, permite identificar problemas y brechas que pueden abordarse posteriormente (Añez, 2014).

Es decir, el autor orienta las normas de estándarización a los procesos operativos que se llevan a cabo en las empresas, indicando que las beneficia en:

Rendimiento estable y mejora continua: La estandarización de tareas, son cimientos para un cumplimiento eficaz de los procesos, establecer formatos estandarizados crea una "plataforma sólida" en pro de la mejora continua.

Visualización y detección de problemas: La estandarización basada en tareas, permite una visualización de las actividades y procedimientos que se llevan a cabo en los procesos, facilitando la identificación de posibles procesos o irregularidades entre lo realizado y lo planificado en el formato establecido.

En resumen, los estándares prometen una estructura sólida, ofrece a las organizaciones; estabilizar el rendimiento operativo, identificar problemas, una guía hacia la mejora continua, conduce a una mayor eficiencia, calidad y consistencia en las actividades y diligencias diarias.

Proceso de Implementar normas estandarizadas

La implementación de normas estandarizadas corresponde un elemento fundamental en la eficiencia operativa en diversos contextos organizacionales. El proceso de implementar normas estandarizadas es el siguiente.

Comprensión de las normas. Es fundamental para las empresas adquirir una comprensión absoluta de las normas en cuestión. Esto requiere una familiarización detallada con los requisitos y directrices que estas normativas requieren. Esta comprensión proporciona el fundamento esencial para llevar a cabo una implementación eficaz.

Identificación de la aplicabilidad. Significa realizar un análisis de la norma de estandarización a implementar, previamente se determina la aplicabilidad de esta y en qué área

en específico se va a efectuar. Es necesario identificar las áreas de la empresa que se va a implementar las normas, con el fin de dirigir los recursos y esfuerzos para la implementación de manera efectiva.

Formación y capacitación. La capacitación y formación del personal juegan un papel central en este proceso. El talento humano debe recibir la educación adecuada sobre los requisitos y procedimientos asociados con las normas. Esto no solo incluye la comprensión de las directrices, sino también la utilización de estas en las actividades cotidianas.

Designación de responsabilidades. Asignar roles y responsabilidades específicas es importante para garantizar que las normas se cumplan a cabalidad. Al mismo tiempo, se puede incluir la elección de un personal o equipo responsable en la gestión de la norma implementada.

Implementación piloto. Realizar pruebas de diagnóstico de la norma de estandarización es fructuoso, una implementación piloto en un área limitada de la empresa para probar los procedimientos. Esta fase de prueba permite identificar posibles desafíos y clarificar los procedimientos antes de la implementación definitiva.

Auditorías y revisiones internas. Establecer un programa de auditorías internas para evaluar el cumplimiento de las normas. Esto permite identificar áreas de mejora y asegurar que se mantenga la conformidad.

Política

Etimológicamente la palabra política proviene del latín politicus adjetivo de político; del griego polítikos, de los ciudadanos; de polites ciudadano; y de pòlis ciudad. Sin embargo, la Real Academia Española (2014) expresa que la política significa “cortesía y buen modo de portarse,

conjunto de directrices que determina el comportamiento de los individuos o entidad en un asunto o campo determinado".

Entonces, el establecimiento de políticas es un documento que indica el seguimiento ético y/o moralmente correcto de acciones, actividades, procedimientos o tareas. Las políticas corresponden a un conjunto de criterios basado en reglamentos, directrices, estándares, normativas. Las políticas, representan un conjunto de principios que delinean el comportamiento esperado de individuos u organizaciones dentro de un contexto especifico. Dichas directrices definen un enfoque ético o correcto de acciones. Se sustentan con una base legal, el mismo que tiene como objetivo garantizar el cumplimiento de las políticas. Esta estructura normativa es fundamental para mantener la integridad, eficiencia y responsabilidad en el funcionamiento de un contexto en particular.

Políticas de Seguridad

La ISO (2013) afirma lo siguiente:

> Una declaración de política de seguridad de la información debe expresar el compromiso formal de la administración para la implementación y mejora de su sistema de gestión de la seguridad de la información y debe incluir objetivos de seguridad de la información o facilitar su desarrollo.
>
> Según la definición del ISO-27000, el propósito de la seguridad de la información es proteger y preservar la confidencialidad, integridad y disponibilidad de la información. También puede implicar proteger y preservar la autenticidad y fiabilidad de la información y garantizar que las entidades puedan ser consideradas responsables.

La información

(Lapiedra Alcami y otros, 2016) definen la información como:

> "Un conjunto de datos que ha sido procesado de manera que ayuda a disminuir la incertidumbre". Básicamente los datos son elementos con una potencial importancia mientras este sea convertido en información con el tratamiento de este a través de los sistemas informáticos.
>
> Así mismo. Lapiedra, Devece y Guiral señalan que "la información es la representación significativa de datos transformados, que otorgan un valor real y que influye en las decisiones y acciones de las personas y organizaciones". (pág. 18).

La información es un componente esencial en el ciclo de transformación de datos en conocimiento. En el contexto matemático básico, un número (2) se considera un dato, sin embargo, la adición de otros datos numéricos y simbólicos (2 + 2 =) concierne a una información significativa y de valor. Por último, en una operación matemática el conocimiento se manifiesta cuando existe la toma de decisiones a partir de una información, en este caso, descifrar el resultado de la operación (4). El conocimiento implica comprender objetivamente las acciones que conlleva realizar acciones con información. Un ejemplo exacto y cotidiano, sucede al sumar dinero disponible (datos) en un momento en cuestión y verificar si corresponde al precio de un producto (información), luego realizar la compra de este (conocimiento).

Lapiedra, Devece y Guiral sostienen que la información se constituye por datos que han sido descifrados y percibidos por quien recibe el mensaje. Los datos y la información se asemejan a la relación entre la materia prima y el producto final. La información adquiere relevancia al ser útil como materia prima para una decisión específica.

Activos de Información

En la actualidad, la información representa como uno de los insumos más importante con respecto a la era de las Tecnologías de Información y Comunicación, por ende, las organizaciones deben aplicar competencias relacionadas a las buenas prácticas con el objetivo de llevar a cabo una gestión de la información eficiente.

Respecto a los activos de información, autores como Guzman y Falcones afirman que:

> Corresponde a toda aquella información que es procesada por sistemas tecnológicos, almacenada en medios portátiles o granjas de servidores y que circula por redes de telecomunicaciones puede estar en constante riesgo de ser violentadas con las posibles consecuencias mencionadas en la sección anterior. Cada uno de estos componentes; información, sistemas, medios, equipos, archivos físicos y digitales se catalogan como activos de información.
>
> En algunos casos, incluso el potencial humano (las personas) también se lo puede considerar como activo de información, en especial quienes producen y manejan estratégicamente la información. En una compañia con un sistema de gestión de la información implantado en la seguridad de la información son identificados y codificados para evaluar y tratar los posibles riesgos con el objetivo de "hacerlos más seguros". (Mahecha Guzmán & Coello Falcones, 2017, pág. 12)

Seguridad de la Información

Mahecha Guzmán & Coello Falcones (2017) manifiestan que la seguridad de la información "comprende todo lo relacionado con la protección de la información perteneciente a las organizaciones y las personas. El autor enfatiza la necesidad de salvaguardar la información frente a riesgos potenciales, abarcando tecnología, personas y procesos.

Por otra parte, Moreno Zamudio (2020) indica que la seguridad de la información implica proteger la información de riesgos que puedan afectarla diferentes formas y estados. También, indica que los principios de la seguridad de la información, corresponde a aplicar un manual de normas a seguir, con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de la información.

Importancia en la seguridad de la información

Se toma en cuenta el siguiente criterio relacionado con la importancia de la seguridad de la información a partir de Berciano (2010):

> Este enfoque en Seguridad de la Información resalta la necesidad de no depender únicamente de herramientas o tecnologías para resolver los desafíos planteados. Se hace hincapié en la implementación de políticas, procedimientos y buenas prácticas respaldadas por diversas tecnologías, lo que permite mejorar la protección de la información sensible. Además, se reconoce que, en este proceso, el factor humano juega un papel crucial. Se concluye que la Seguridad de la Información es un proceso holístico que requiere la combinación efectiva de diversas medidas de seguridad para lograr sus objetivos.” (Berciano, 2010).

Es decir, en el ámbito de la seguridad de la información, la resolución de problemas no se centra únicamente en la elección de herramientas o tecnologías específicas, se basa en la implementación de políticas, procedimientos y prácticas efectivas respaldadas por diversas tecnologías. Además, es crucial reconocer que esta gestión de seguridad se fundamenta también en la participación del factor humano. Esta reflexión reitera la idea de que la seguridad de la información requiere la combinación de diferentes componentes.

Principios de la seguridad de la información

A continuación, se presentan los tres principios de la seguridad la seguridad de la información:

Confidencialidad. Significa que la información solo está disponible para el personal autorizado, siguiendo el principio del "necesidad de saber" ("need-to-know"). Este término implica que la información solo se comparte con personas, entidades o sistemas que están autorizados y tienen la necesidad de acceder a ella para realizar sus funciones o tareas específicas (Moreno Zamudio, 2020, pág. 52).

Entonces, la confidencialidad se refiere a que la información esté disponible para aquellas personas o entidades autorizadas. El concepto de “need-to-know”, establece que la divulgación de información debe estar limitada solo para fuentes confiables.

Integridad: Se hace referencia a preservar la información sin modificaciones, manteniendo su valor original en todos los aspectos. Esto implica que cualquier persona que acceda a esta información debe tener la confianza de que, al consultarla, conservará sus valores originales y no habrá sido alterada de una manera que pueda comprometer la funcionalidad institucional. (Moreno Zamudio, 2020)

Según lo mencionado por Moreno, la integridad en la información consiste en que la presentación de información no tenga ningún cambio en el contenido de este, debe ser un reflejo exacto de la realidad.

Disponibilidad. Según el Instituto Nacional de Ciberseguridad, se centra en asegurar que la información esté accesible en el momento requerido. Esto implica el acceso y uso de la

información, así como de los sistemas que la manejan, por parte de individuos, entidades o procesos autorizados cuando sea necesario.

Objetivo de la seguridad de la información

Las entidades, ya sean públicas o privadas, establecen políticas de seguridad informática para resguardar su información. Los autores presentan de manera efectiva procesos asociados con la seguridad de la información, partiendo de la premisa fundamental de que la protección de esta, mediante sus políticas, no depende exclusivamente de la tecnología. (Altamirano Yupanqui, 2017)

Sin embargo, la Segunda Cohorte del Doctorado en Seguridad Estratégica (2014) ha afirmado lo siguiente:

> El objetivo fundamental de la seguridad de la información es salvaguardar los sistemas de procesamiento de datos y garantizar la transferencia segura de información entre distintas organizaciones. Los servicios de seguridad son concebidos para contrarrestar posibles ataques y emplean una variedad de mecanismos con el fin de asegurar la prestación exitosa de este servicio.

En resumen, se considera que proteger la información bajo una perspectiva netamente tecnológica, tendría un enfoque incompleto, pues otros estudios que se han realizado a la fecha demuestran que, para conseguir objetivos más eficaces relacionados con la seguridad de la información, es necesario tener una visión amplia a través de un enfoque interdisciplinario, donde el principal factor, el humano, juega un papel fundamental. Por ejemplo, Gutiérrez y Safla en la implementación de normas estándares ISO/IEC 27000 y COBIT 5 en la Dirección de TICs de la Universidad Central del Ecuador, crearon un mapeo que ayudó al a entender la relación

entre ambas normas; pudiendo asi utilizarlos de forma conjunta y sean un complemento para el tratamiento de la seguridad de la información dentro de dicha Institución.

Necesidad de la seguridad de la información

Una vez reconocido la importancia y objetivo sobre la seguridad de la información, es deducible la necesidad de esta, existen muchas razones que obliga a que sea necesario la implementación de prácticas relacionadas a la seguridad de la información en la Empresa Pública ULEAM.

Según Gutiérrez, J & Tena, J (2003), la prioridad de la seguridad de la información radica en proteger la información manejada. Debido que una deficiente gestión en la seguridad de esta provocaría una divulgación de datos sensibles en las organizaciones. Además, se destaca la relevancia de capacitar al personal encargado de desarrollar, implementar, utilizar y administrar los sistemas.

Entonces, se afirma la necesidad de la implementación de seguridad de la información. Además, Ledezma Espin (2015) manifiesta que “luego de reconocer la conceptualización de la seguridad de información, sus objetivos, importancia y la necesidad, es preciso encontrar formatos para lograr la seguridad informática deseada, la misma que puede ser lograda a través de la implementación de políticas”.

Políticas de Seguridad de la Información

Los autores Barbosa y Saibel (2005, citados en Arévalo, 2017) sostienen que:

> Son documentos que contienen recomendaciones, reglas, responsabilidades y prácticas de seguridad. Sin embargo, no existe una "política de seguridad modelo" que sea aplicable universalmente en todas las organizaciones.

> Cada política debe adaptarse a las particularidades de cada caso, lo que convierte la elaboración de una política de seguridad en una labor compleja que requiere monitoreo constante, revisiones y actualizaciones periódicas. (Barbosa Martins, A & Saibel, C., 2005, pág. 7)

Por otra parte, Trujillo comparte con los autores mencionados anteriormente, pues expresa que "las políticas de seguridad informática generalmente son un documento de alto nivel que detalla el principal objetivo del sistema de gestión de seguridad de la información. No tiene que ver con sanciones, es una descripción de aquello valioso que se desea proteger en la organización". (Hurtado Trujillo, 2021, pág. 26)

En resumen, Barbosa y Saibel enfatizan la complejidad de implementar políticas de seguridad en la información, debido que no solo se aplican en una organización en cuestión, también existe actividades posteriores, tales como el monitoreo, revisión y actualización de las normas. Sin embargo, Trujillo enfoca las políticas de seguridad de información como un documento que no imponer sanciones, sino comunicar a los usuarios sobre la importancia de proteger el insumo de la información, el mismo que es uno de los recursos más importantes de las organizaciones.

Sistemas de Gestión de Seguridad de la Información

Según ISO ISO27001, citado en Zamudio 2020, representa una estrategia que colabora en el establecimiento de políticas y procedimientos que se alinean con los objetivos comerciales de la organización. Su propósito es mantener un nivel de exposición siempre por debajo del nivel de riesgo que la propia organización ha determinado asumir. A través de un SGSI, la organización logra una comprensión de los riesgos a los que se enfrenta su información, y los maneja al

asumirlos, reducirlos, transferirlos o controlarlos mediante un proceso sistemático que está definido, documentado y conocido por todos los involucrados.

Según la ISO 27001, citado en Arévalo, 2017, un sistema de gestión de seguridad de la información está basado en cuatro niveles:

Nivel 1 de un SGSI (Manual de seguridad). Este documento se convierte en el fundamento esencial que dirige todo el sistema. En él se presentan y describen las intenciones, el alcance, los objetivos, las responsabilidades, las políticas y las principales directrices vinculadas específicamente al Sistema de Seguridad de la Información que se pretende instaurar en una empresa o institución. Funciona como el documento principal que establece la visión y la estructura completa del sistema de seguridad de la información.

Nivel 2 de un SGSI (Procedimientos). Documentación a nivel operativo que garantiza la correcta ejecución de la planificación, operatividad y supervisión de los procesos relativos a la seguridad de la información

Nivel 3 de un SGSI (Instrucciones, checklists y formularios). comprende las instrucciones, checklists y formularios. Estos documentos detallan el procedimiento para llevar a cabo tareas y actividades específicas relacionadas con la seguridad de la información. Son guías operativas que describen paso a paso cómo ejecutar acciones y actividades en este ámbito.

Nivel 4 de un SGSI Alcances. Engloba la porción específica de la organización sujeta al sistema, lo que incluye identificar con precisión las conexiones, relaciones y límites entre el ámbito definido y las áreas no incluidas. En situaciones donde el alcance del SGSI cubra una parte particular de la organización, como delegaciones, divisiones, áreas, procesos, sistemas o tareas específicas, es crucial delimitar claramente estos límites y conexiones.

A continuación, se presentan los alcances de un sistema de gestión de seguridad de la información:

Política y objetivos de seguridad: se trata de un documento de carácter general que establece el compromiso de la dirección y la orientación de la organización en la gestión de la seguridad de la información.

Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.

Enfoque de evaluación de riesgos: consiste en la descripción detallada de la metodología que se utilizará. Esto incluye cómo se llevará a cabo la evaluación de amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos relacionados con los activos de información dentro del alcance definido. Además, implica la creación de criterios para aceptar riesgos y establecer niveles de riesgo que sean considerados aceptables.

Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

Plan de tratamiento de riesgos: El análisis obtenido tras emplear la metodología de evaluación previamente referida a los activos de información de la entidad.

Procedimientos documentados: son aquellos necesarios para garantizar la planificación, ejecución y supervisión de los procesos de seguridad de la información, así como para evaluar la eficacia de los controles implementados.

Registros: documentos que ofrecen pruebas de cumplimiento con los requisitos y demuestran el funcionamiento efectivo del SGSI.

Declaración de aplicabilidad: es un documento que alberga los objetivos de control y los controles incorporados por el SGSI. Estos se fundamentan en los resultados obtenidos de la evaluación y gestión de riesgos, explicando las razones detrás de las inclusiones y exclusiones. Como se mencionó previamente, esta declaración es una parte esencial dentro de un SGSI, las cuales son:

- Llevar a cabo un análisis detallado de los riesgos asociados a los activos de información presentes en una organización o empresa.
- Establecer políticas orientadas a fomentar prácticas efectivas, basadas en el análisis de riesgos previamente realizado.

La familia ISO 27000

En un contexto general, existen diferentes formatos, técnicas y normas para estandarizar una cuestión en específico. Sin embargo, es la ISO quien consta con mayor autoria en esta actividad. Siendo una de las organizaciones más reconocidas por el significante aporte que brindan a las empresas que se hacen partícipe en la implementación de normas estandarizadas para un objetivo en particular. Entonces la familia ISO 27000 se trata de un conjunto de normas creadas por los organismos de estandarización ISO (Organización Internacional de Normalización) y IEC (Comisión Electrotécnica Internacional).

ISO 27000 (2016, como se citó en Arévalo, 2017) afirma que:

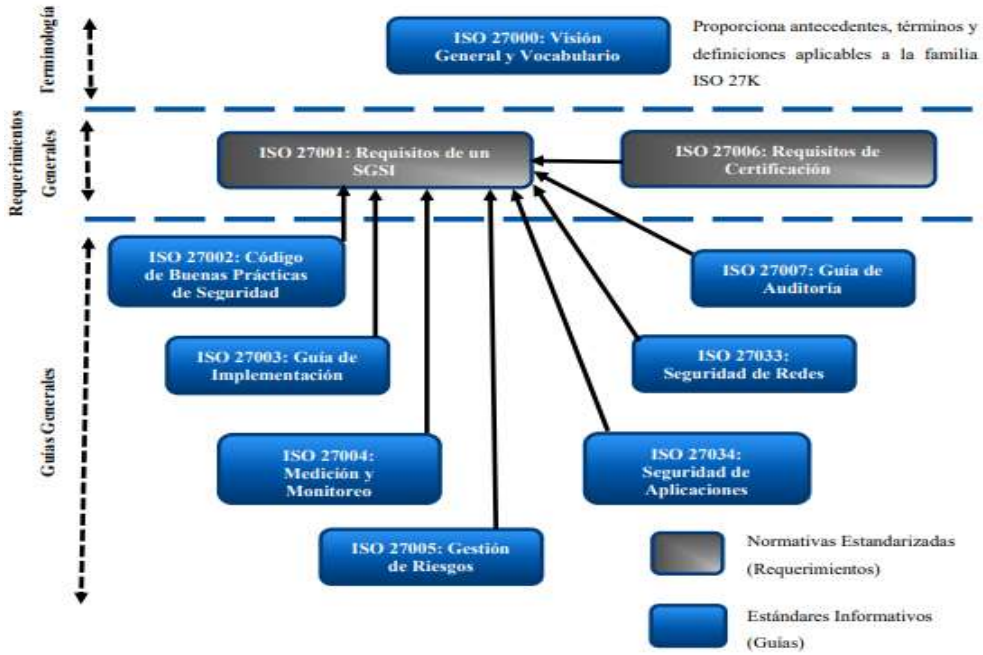
> La norma fue inicialmente lanzada en 2009 para ofrecer una perspectiva general sobre la familia de normas ISO 27K y establecer una base conceptual común. La versión más reciente, emitida en 2016.

Esta brinda un marco de gestión para la seguridad de la información adaptable a organizaciones de cualquier índole, ya sean públicas o privadas, así como de diferentes escalas, desde pequeñas hasta grandes. (Arévalo Moscoso, 2017, págs. 46-47)

En el siguiente gráfico se presenta un análisis comparativo de toda la familia ISO 27000 de Disterer (2013), enfocándose en el desarrollo y su clasificación:

Ilustración 1

Relaciones entre la familia de estándares ISO 27K



Nota. Arévalo Moscoso, expresa que la imagen corresponde a las relaciones que existen en la familia de estándares ISO 27000. Detalla cada una de las características de la familia ISO 27K.

Norma ISO 27000. La ISO indica que el documento proporciona un marco de los sistemas de gestión de seguridad de la información (SGSI). Esta provee términos y definiciones comúnmente utilizados en la familia de estándares. Es adaptable a cualquier tipo de

organizaciones, tales como empresas públicas y privadas, agencias gubernamentales, entidades sin fines de lucro. (ISO, 2018)

Entonces, la norma ISO 27000 corresponde a una visión general de los términos relacionados a la seguridad de la información. Es un documento que tiene el objetivo de brindar información a través de su vocabulario.

Norma ISO 27001. Esta norma detalla los criterios para establecer, implementar, mantener y mejorar de manera continua un SGSI en el contexto de la organización. Asimismo, abarcan requisitos para evaluar y manejar los riesgos de seguridad de la información según las necesidades específicas de cada organización. Los requisitos establecidos en ISO / IEC 27001:2013 son universales y están diseñados para ser utilizados por organizaciones de cualquier tipo, tamaño o índole. (Arévalo Moscoso, 2017, pág. 75)

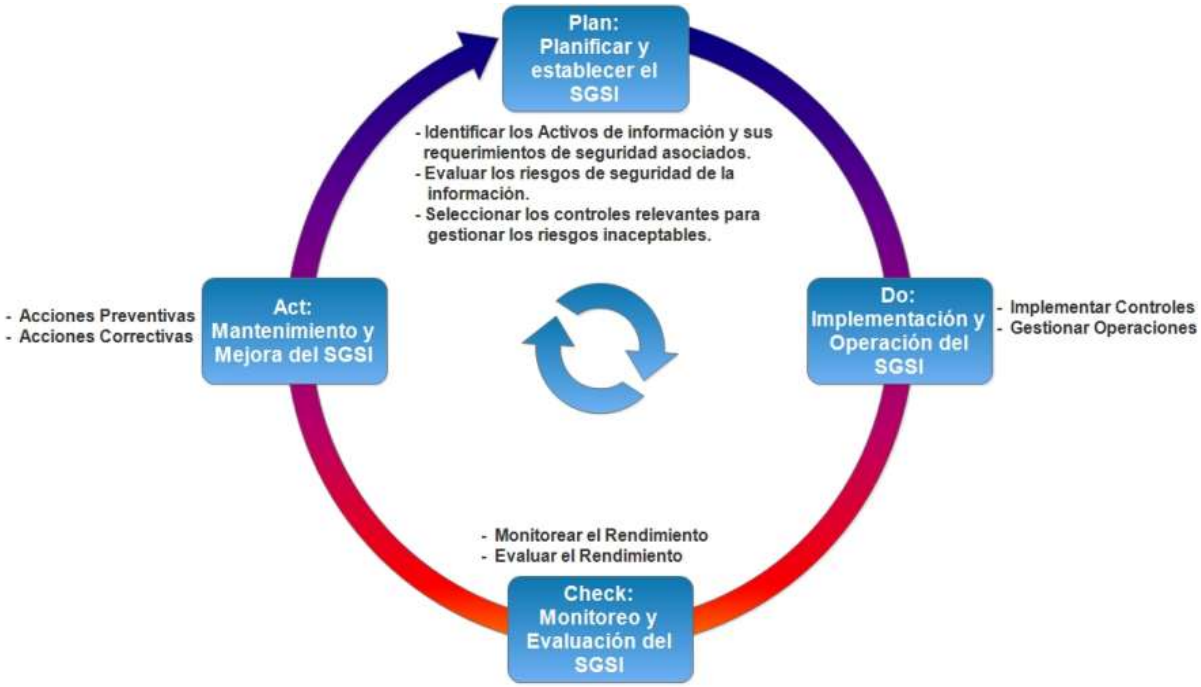
El mismo autor señala que “la norma ISO/IEC 27001 se centra en establecer los requisitos para planificar, implementar, operar, monitorear y mejorar continuamente un SGSI. También, en la versión ISO/IEC 27001:2005, el enfoque está alineado con el ciclo PDCA”.

Dicha norma es comúnmente empleada en proyectos de análisis y diseño de un SGSI debido a su detallada descripción de los pasos implicados en este procedimiento. (Arévalo Moscoso, 2017, pág. 48).

En resumen, la norma ISO 27001 se trata de un documento que ofrece una guía para la implementación de un sistema de seguridad de la información. Está dirigida a las organizaciones la cuales buscan alinear la seguridad de los datos sensibles a través de una estandarización.

Ilustración 2

Etapas del ciclo PDCA según ISO 27000 (2005)



Nota: El autor (Disterer, 2013) coincide en que, la implementación de las normas ISO 27001 en 2005 requería seguir un ciclo que se conoce como PDCA, por sus siglas en inglés.

Norma ISO 27002. En septiembre del 2013, la ISO publicó un conjunto de recomendaciones y mejores prácticas de seguridad de la información. Esta publicación está disposición para todas las organizaciones, independientemente del sector, puesto que no tiene ningún tipo restricción o excepcione.

En concordancia, la ISO (2013, como se citó en Jara Arenas 2019) indica que “las normas ISO 27002 son códigos de prácticos relacionadas que establece los objetivos de control y controles frente a los entornos de riesgo que está expuesta la seguridad de la información en una organización”. Las cláusulas de control de seguridad de la información en la norma ISO 27002 son 14 son la siguientes (ISO, 2013):

- Administración de activos.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Aspectos de SI en la gestión de continuidad del negocio.
- Cifrado 7. Seguridad física y ambiental.
- Control de accesos.
- Cumplimiento.
- Gestión de incidentes de seguridad de la información.
- Organización de la seguridad de la información.
- Políticas de seguridad de la información
- Relación con proveedores.
- Seguridad de los recursos humanos.
- Seguridad de operaciones.
- Seguridad de telecomunicaciones.

En resumen, las norma ISO 27002 es una guía de buenas prácticas, detalla los objetivos de control en los aspectos de seguridad de la información

MARCO METODOLÓGICO

La presente investigación se trata de un estudio de caso que se enfoca en identificar y recomendar normas de estandarización para mejorar la seguridad de la información en la Empresa Pública ULEAM. La investigación se lleva a cabo durante el año 2023, concentrándose en el estudio de las normas de estandarización como fuente para implementar políticas de seguridad de la información en la Empresa Pública ULEAM. Las metodologías utilizadas para el desarrollo del proyecto son:

Tipo de Investigación

El desarrollo del estudio se sustentó a partir de los siguientes tipos de investigación:

De campo

La investigación de campo implica la recopilación, procesamiento y análisis metódico de datos. Es decir, se utilizó encuestas y entrevistas en la Empresa Pública ULEAM a los informantes claves dentro de los procesos operativos, producto que servirá como presentación de información en los resultados del proyecto.

Bibliográfica

Las fuentes bibliográficas, ensayos, revistas, conferencias, documentos de investigación publicados en la web. La revisión exhaustiva desde la literatura ayudó a comprender las normas de estandarización, específicamente la familia ISO 27000, y su relación con las políticas de seguridad de la información. Entonces, la investigación bibliográfica proporcionó el respaldo teórico necesario para el desarrollo del tema.

Métodos de Investigación

Los métodos que se aplicó en la presente investigación de estudio de caso fueron los siguientes:

Método inductivo

Se basa en la observación de la realidad empírica, identificar tendencias o patrones y aplicación de conceptos en situaciones específicas. El método inductivo permitió identificar las características recurrentes del fenómeno.

Método analítico

Es un proceso que descompone un todo en partes, es decir, de lo general a lo específico. En el estudio de caso de esta investigación, el método analítico fue fundamental, puesto que se usó el análisis de información a través de los datos recolectados a partir de la encuesta y entrevista.

Herramientas y Técnicas

Para desarrollar la investigación de estudio de caso se utilizó las siguiente herramientas y técnicas:

Guía de observación

Sirvió como fuente de información fundamental para el desarrollo de la definición del estudio de la investigación, pues este producto se utilizó mediante la observación participante con el objetivo de estudiar el suceso, hecho y fenómeno del caso investigado.

Encuesta

Se utilizó para desarrollar el proceso de transformación de datos a información, es decir se diseñó y aplicó a los informantes claves una herramienta de medición (encuesta), la misma que sirvió para la recolección y análisis de datos para obtener una información condensada para la toma de decisiones en el proyecto

Entrevista

Sirvió para recolectar datos cualitativos, se aplicó a tres informantes claves dentro de la organización, estos proporcionaron datos importantes para realizar la triangulación de información. La entrevista es una de las mejores herramientas para la recolección de datos, pues al ser de carácter cualitativo permite extraer información más precisa basado en el análisis de las narrativas detalladas de los entrevistados, ayuda a entender percepciones, actitudes, lenguaje corporal, expresiones faciales y otras señales no verbales del entrevistado.

Lógica de Análisis

Los tipos de métodos, herramientas y técnicas mencionadas sirvieron como fuente esencial para recolectar e interpretar datos mediante el uso de tabla de frecuencia e interpretación de datos cualitativos. El análisis lógico sirvió como producto fundamental para desarrollar los resultados, conclusiones y recomendaciones del proyecto.

RESULTADOS OBTENIDOS

Resultados de Encuesta

A continuación, se evidencian los resultados obtenidos a través de la encuesta realizada, la cual se aplicó a una población de 8 trabajadores de diferentes áreas funcionales alrededor de la Empresa Pública ULEAM. El propósito de esta encuesta fue determinar el estado actual de las normas de estandarización y políticas de seguridad de la información. Así mismo identificar cuál de la norma ISO dentro del marco 27k es la mejor propuesta para la organización.

Tabla 1

Prácticas de seguridad de información

Alternativas	Frecuencia	Porcentaje
Si	7	88
No	1	12
Total	**8**	**100%**

Nota. La tabla muestra el conocimiento del personal encuestado sobre las prácticas de seguridad de la información.

Gráfico 1

Nota. Gráfico del ítem 1 (Fuente: elaborado por el autor a partir de los datos recolectados).

Interpretación

La mayoría de los encuestados (87%) están familiarizados con dichas prácticas, mientras que un 13% no lo están. Este alto porcentaje de respuestas positivas indica que la empresa ha logrado una buena difusión y comprensión de sus prácticas de seguridad entre la mayoría de los empleados.

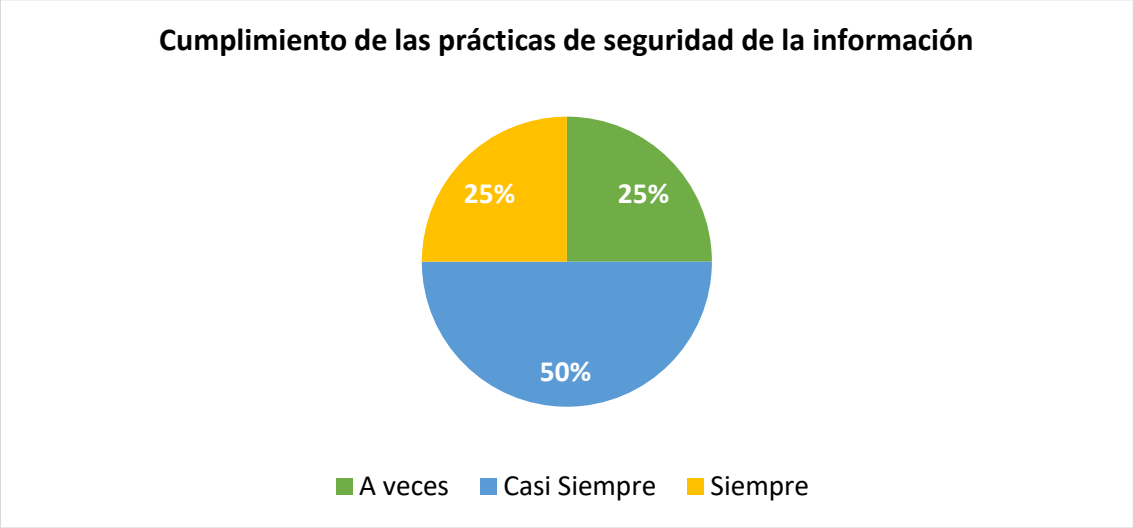
Tabla 2

Cumplimiento de las prácticas de seguridad de la información

Alternativas	Frecuencia	Porcentaje
Siempre	2	25
Casi siempre	4	50
A veces	2	25
Casi nunca	0	0
Nunca	0	0
Total	**8**	**100%**

Nota. La muestra expresa cuan pendiente del cumplimiento de las prácticas de seguridad de la información por parte de los encuestados.

Gráfico 2



Nota. Gráfico del ítem 2 (Fuente: elaborado por el autor a partir de los datos recolectados).

Interpretación

La mitad de los encuestados (50%) indican que casi siempre están pendiente de las prácticas de seguridad de información en la Empresa Pública ULEAM. Un cuarto de los encuestados (25%) reporta estar siempre pendiente de estas prácticas, mientras que el otro cuarto (25%) indica estar pendiente “a veces”. Esto sugiere que, aunque la mayoría de los empleados están pendiente del cumplimiento de las prácticas de seguridad de información, hay variabilidad en la frecuencia de los encuestados que casi siempre están pendiente o a veces.

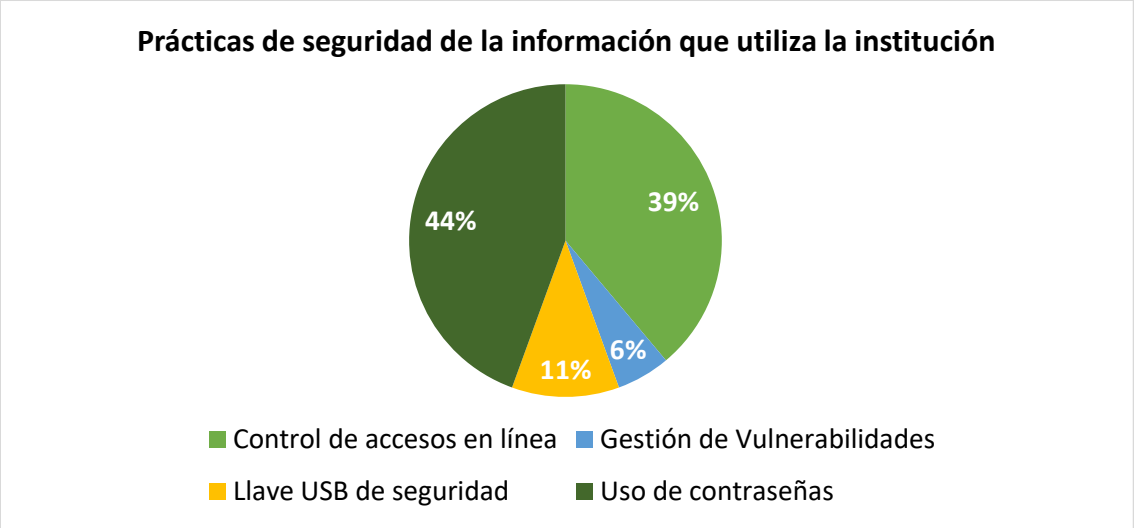
Tabla 3

Prácticas de seguridad de la información que utiliza la institución

Alternativas	Frecuencia	Porcentaje
Control de accesos en línea	7	39
Gestión de Vulnerabilidades	1	6
Uso de contraseñas	8	44
Cifrado de datos	0	0
Llave USB de seguridad	2	11
Ninguno	0	0
Total	**18**	**100%**

Nota. La tabla muesta las prácticas de seguridad de información en los sistemas informáticos de la organización.

Gráfico 3



Nota. Gráfico del ítem 3 (Fuente: elaborado por el autor a partir de los datos recolectados).

Interpretación

La práctica de seguridad de información más utilizada entre los encuestados es el uso de contraseñas, con un 44% de respuestas. Le sigue el control de accesos en línea con un 39%. Las prácticas menos comunes incluyen el uso de llaves USB de seguridad (11%) y la gestión de vulnerabilidades (6%). Esto sugiere que, hay una adopción significativa de ciertas medidas de seguridad básicas, como el uso de contraseñas y el control de accesos.

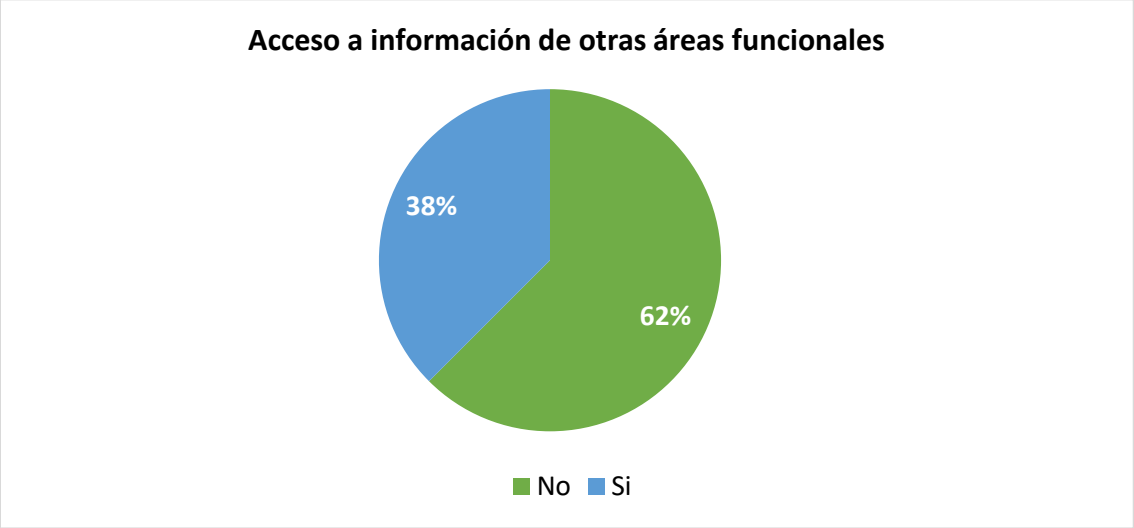
Tabla 4

Acceso a información de otras áreas funcionales

Alternativas	Frecuencia	Porcentaje
Si	3	38
No	5	62
Total	**8**	**100%**

Nota. La tabla muestra el poder de acceso a información de otras áreas funcionales a partir de un rol asignado.

Gráfico 4



Nota. Gráfico del ítem 4 (Fuente: elaborado por el autor a partir de los datos recolectados).

Interpretación

La mayoría de los encuestados (62%) no tienen acceso a información de otras áreas funcionales de la institución a partir de su rol asignado en el sistema informático, mientras que el 38% sí tiene dicho acceso. Este resultado sugiere que el acceso a la información de otras áreas está relativamente restringido para la mayoría de los empleados, lo cual puede ser una medida de seguridad adecuada para proteger la información sensible y mantener la confidencialidad. Sin embargo, el hecho de que el 38% de los encuestados tenga acceso a otras áreas debido a roles con responsabilidades interdepartamentales para realizar sus tareas.

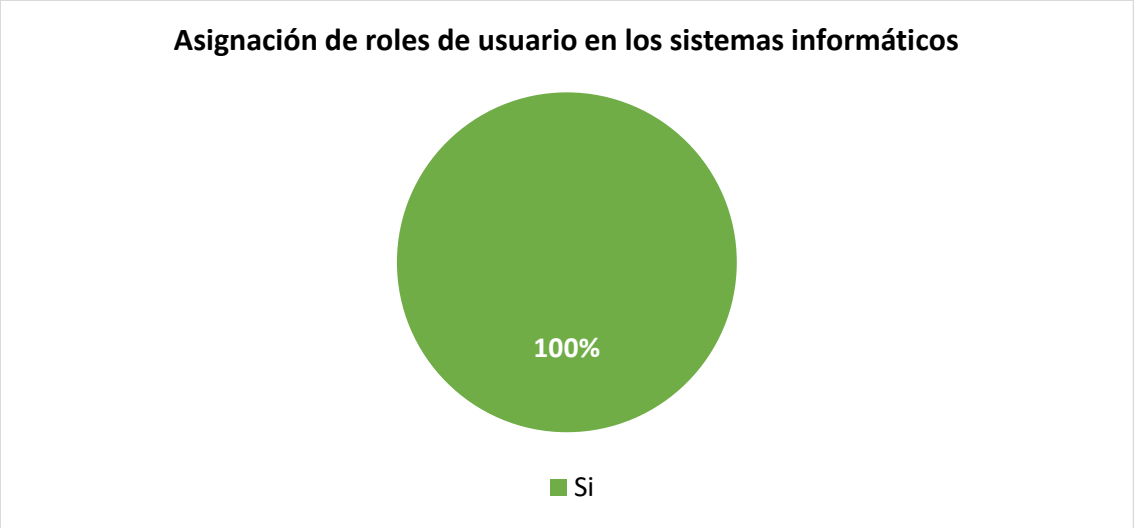
Tabla 5

Asignación de roles de usuario en los sistemas informáticos

Alternativas	Frecuencia	Porcentaje
Si	8	100
No	0	0
Total	**8**	**100%**

Nota. La siguiente tabla evidencia la asignación de roles en los sistemas informáticos. Siendo la respuesta positiva totalmente dominante con un 100%.

Gráfico 5



Nota. Gráfico del ítem 5 (Fuente: elaborado por el autor a partir de los datos recolectados).

Interpretación

Todos los encuestados (100%) afirman que se asignan roles de usuario en los sistemas informáticos con el objetivo de limitar el acceso a la información según el rol. Este resultado indica que la política de asignación de roles para limitar el acceso a la información está completamente implementada y es reconocida por todos los empleados encuestados. Las respuestas sugieren que la institución tiene un enfoque claro en el control de acceso, asegurando que los usuarios solo tengan acceso a la información necesaria para sus funciones.

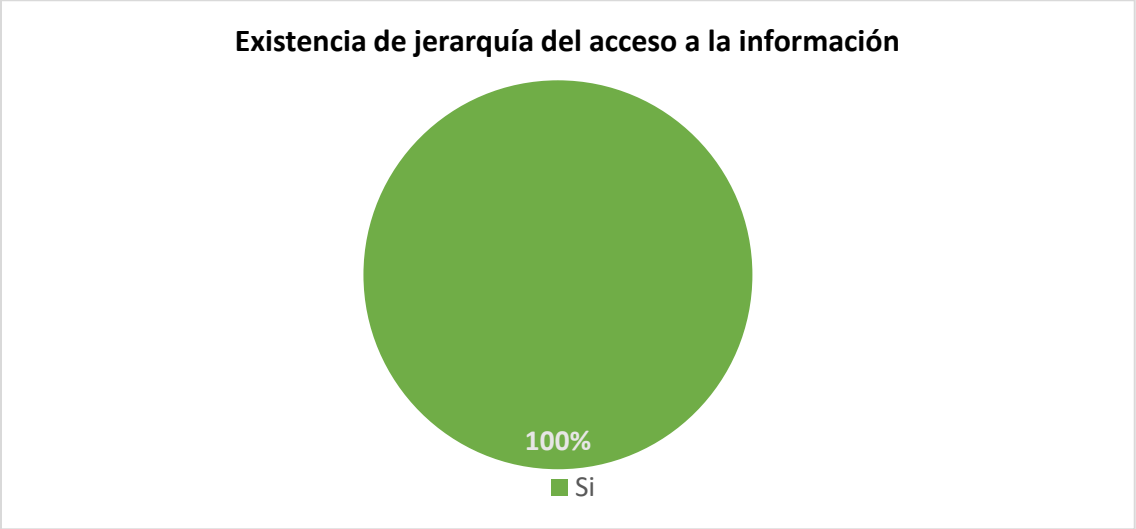
Tabla 6

Existencia de jerarquía del acceso a la información

Alternativas	Frecuencia	Porcentaje
Si	8	100
No	0	0
Total	**8**	**100**

Nota. La presente tabla demuestra la existencia de una jerarquía con relación al acceso a la información que está al alcanze de los usuarios internos de la organización.

Gráfico 6



Nota. Gráfico del ítem 6 (Fuente: elaborado por el autor a partir de los datos recolectados).

Interpretación

La encuesta revela que todos los encuestados (100%) confirman la existencia de una jerarquía o mapeo de acceso a la información en la empresa, dependiendo del rol de los usuarios. Este resultado sugiere que la política de asignación de acceso basada en roles está ampliamente implementada y reconocida por todos los empleados encuestados.

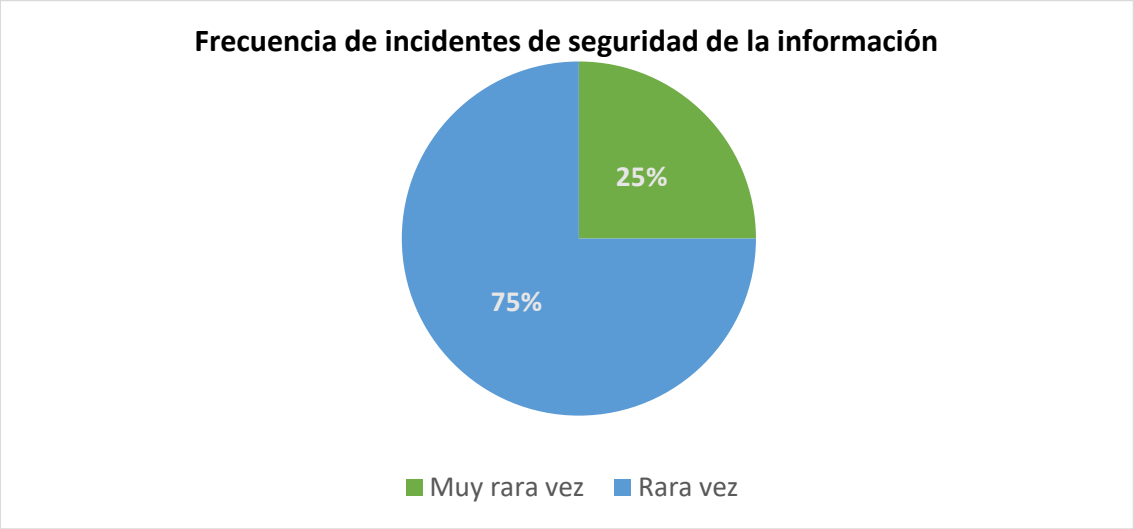
Tabla 7

Frecuencia de incidentes de seguridad de la información

Alternativas	Frecuencia	Porcentaje
Muy rara vez	2	25
Rara vez	6	75
A veces	0	0
Frecuentemente	0	0
Muy frecuentemente	0	0
Total	**8**	**100**

Nota. La tabla demuestra la frecuencia de la existencia de incidentes relacionado a la seguridad de la información en la organización.

Gráfico 7



Nota. Gráfico del ítem 7 (Fuente: elaborado por el autor a partir de los datos recolectados).

Interpretación

La mayoría de los encuestados (75%) indicaron que los incidentes de seguridad de información son poco frecuentes en la institución, debido que 6 de ellos respondieron "rara vez" y los dos restantes (25) indicaron que estos incidentes son "muy rara vez". Esto sugiere que, en general, la institución experimenta una baja incidencia de problemas de seguridad de la información.

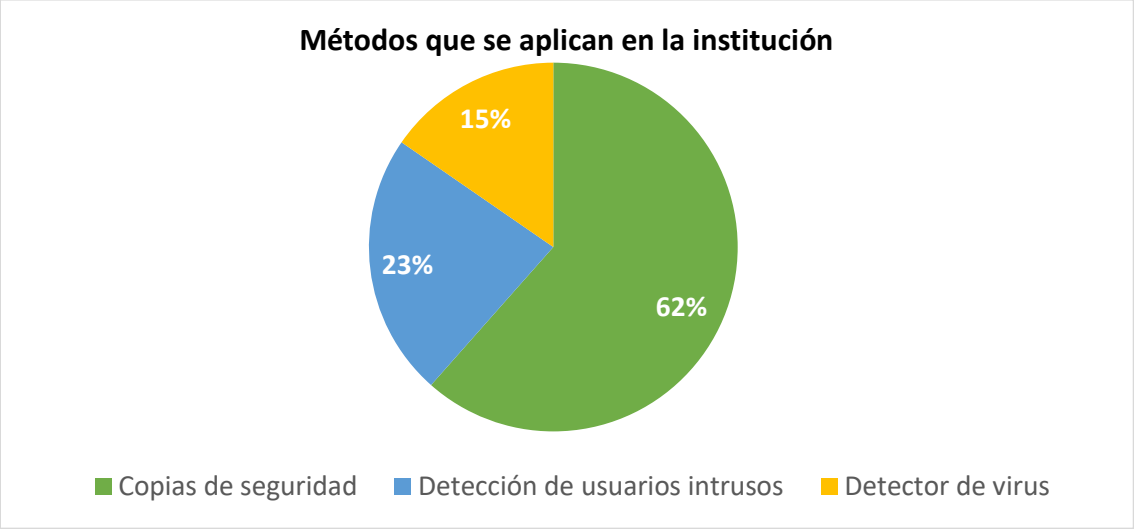
Tabla 8

Métodos que se aplican en la institución

Alternativas	Frecuencia	Porcentaje
Detección de usuarios intrusos	3	23
Detector de virus	2	15
Copias de seguridad	8	62
Papelera de archivos	0	0
Total	**13**	**100**

Nota. La tabla demuestra los métodos que utiliza la empresa para salvaguardar la información ante incidentes.

Gráfico 8



Nota. Gráfico del ítem 8 (Fuente: elaborado por el autor a partir de los datos recolectados).

Interpretación

La gran mayoría de los encuestados (62%) confía en las copias de seguridad como método principal para salvaguardar la información en caso de un incidente, seguido por un 23% que mencionó la detección de usuarios intrusos y un 15% que señaló el uso de detectores de virus, ninguno de los encuestados mencionó el uso de la papelera de archivos para este propósito. Estos resultados sugieren una preocupación generalizada por la protección de datos basada mayormente en las copias de seguridad.

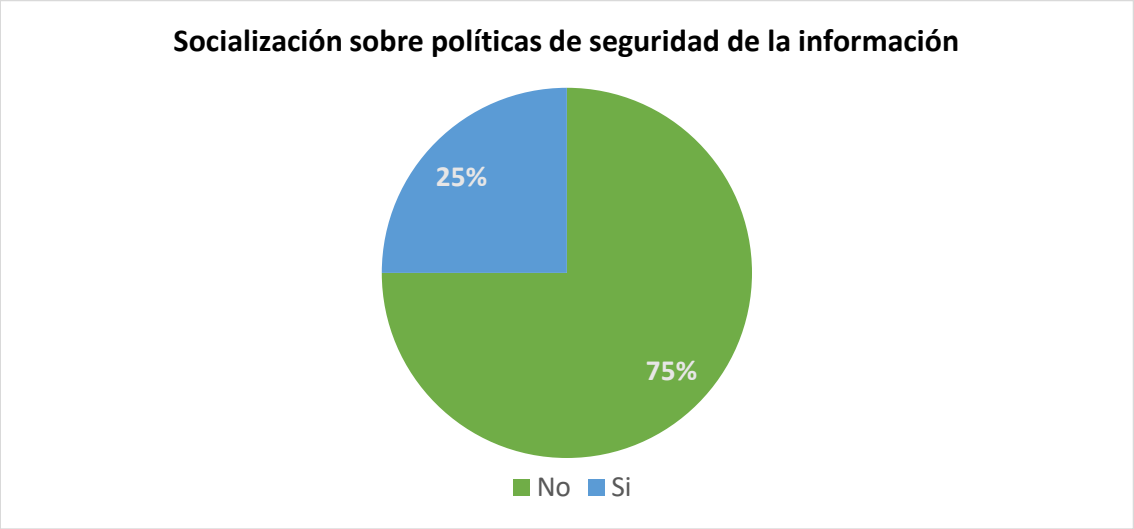
Tabla 9

Socialización sobre políticas de seguridad de la información

Alternativas	Frecuencia	Porcentaje
Si	2	25
No	6	75
Total	**8**	**100**

Nota. La tabla demuestra la aceptación y negación de el recibimiento de algún tipo de socialización, taller sobre las políticas de seguridad de la información.

Gráfico 9



Nota. Gráfico del ítem 9 (Fuente: elaborado por el autor a partir de los datos recolectados).

Interpretación

El 25% de los encuestados indicaron haber recibido talleres o socializaciones sobre políticas de seguridad de la información, mientras que el 75% restante afirmó no haber recibido tal capacitación. Este resultado sugiere que, aunque una minoría ha sido expuesta a estas sesiones, la mayoría de los empleados carecen de esta preparación. Esto podría implicar un riesgo potencial para la seguridad de la información, debido que los empleados podrían no estar plenamente conscientes de la importancia de las políticas de seguridad de la información.

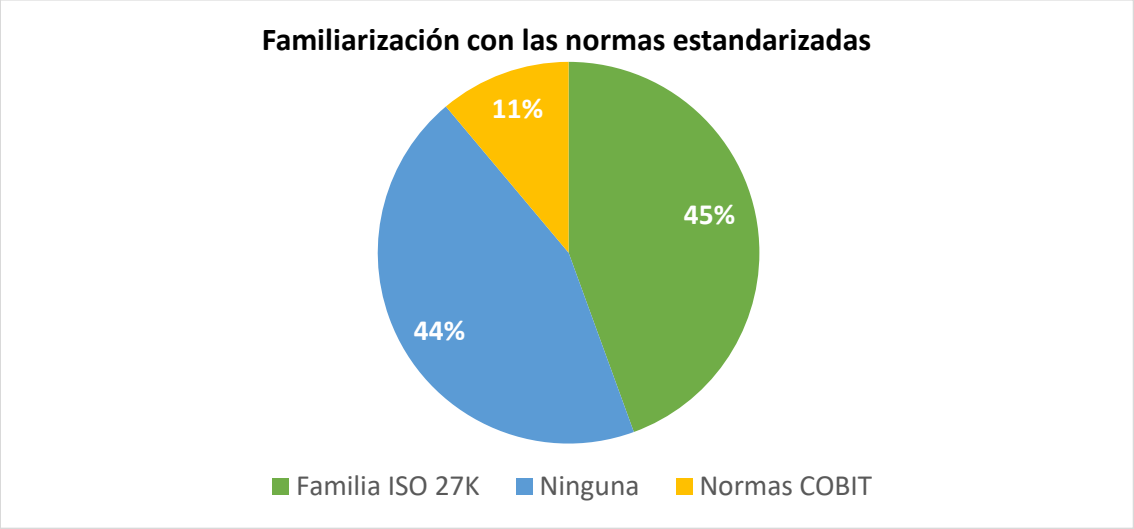
Tabla 10

Familiarización con las normas estandarizadas

Alternativas	Frecuencia	Porcentaje
Familia ISO 27K	4	44
Normas COBIT	1	11
Normas NIST	0	0
Ninguna	4	45
Total	**9**	**100**

Nota. La tabla evidencia la familiarización del personal encuestado con relación a las normas estandarizadas más populares.

Gráfico 10



Nota. Gráfico del ítem 10 (Fuente: elaborado por el autor a partir de los datos recolectados).

Interpretación

Almenos el 55% de los encuestados indicó estar familiarizado con alguna norma estandarizada sobre seguridad de la información, principalmente la familia ISO 27K (44%), seguida por un 11% que mencionó conocer las normas COBIT, mientras que ninguno estaba familiarizado con las normas NIST. Sin embargo, el 45% restante afirmó no estar familiarizado con ninguna norma estandarizada. Este resultado abre la oportunidad para mejorar la educación y conciencia sobre las políticas de seguridad de la información dentro de la organización.

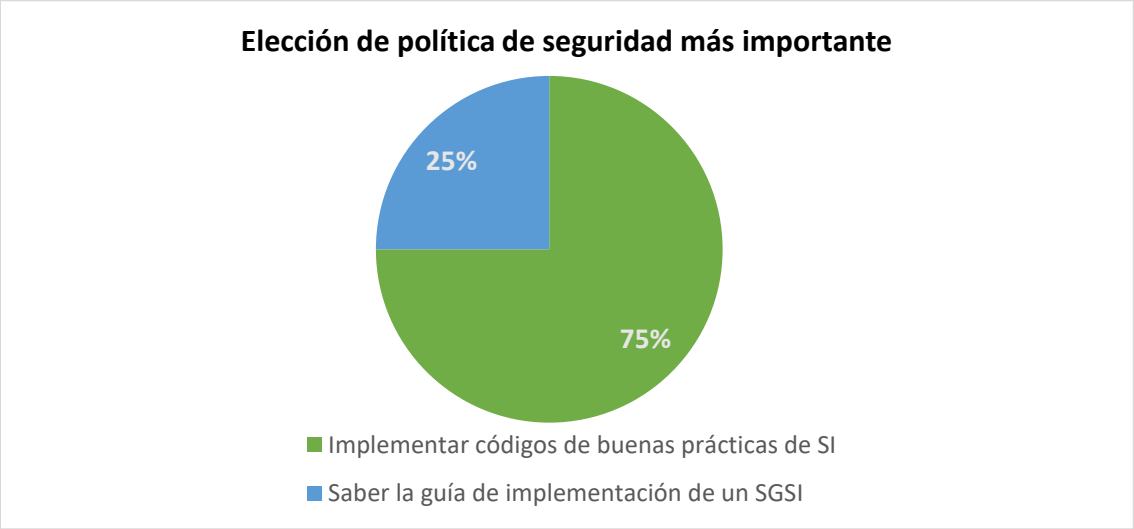
Tabla 11

Elección de política de seguridad más importante

Alternativas	Frecuencia	Porcentaje
Revisar un vocabulario de SGSI	0	0
Reconocer requisitos de un SGSI	0	0
Implementar códigos de buenas prácticas de SI	6	75
Saber la guía de implementación de un SGSI	2	25
Reconocer requisitos certificación en SI	0	0
Total	**8**	100

Nota. La presente tabla demuestra cuales aplicaciones de políticas de seguridad de la información consideran más importante para mejorar dichas competencias.

Gráfico 11



Nota. Gráfico del ítem 11 (Fuente: elaborado por el autor a partir de los datos recolectados).

Interpretación

El 75% de los encuestados considera que la implementación de códigos de buenas prácticas de seguridad de la información es la aplicación más importante para mejorar competencias en Sistemas de Gestión de la Seguridad de la Información (SGSI). Por otro lado, un 25% de los encuestados indican la guía de implementación de un SGSI como una contribución significativa para mejorar estas competencias. Este resultado resalta la valoración de la implementación efectiva de medidas de seguridad como una herramienta clave para fortalecer la postura de seguridad de la organización y mejorar la comprensión y aplicación de los principios fundamentales de la seguridad de la información.

Análisis general de encuesta

En general, las prácticas más comunes en la organización son el uso de contraseñas (44%) y el control de accesos en línea (39%). Menos comunes son el uso de llaves USB de seguridad (11%) y la gestión de vulnerabilidades (6%). Un 62.5% de los encuestados no tienen acceso a información de otras áreas funcionales, lo que sugiere una política restrictiva adecuada para proteger la información sensible. Sin embargo, un 37.5% sí tiene dicho acceso, debido a roles con responsabilidades interdepartamentales.

Por otra parte, la mayoría de los encuestados (87.5%) están familiarizados con las prácticas de seguridad de la información, lo que indica una buena difusión y comprensión de estas prácticas entre los empleados. El 50% de los encuestados están casi siempre pendientes del cumplimiento de estas prácticas, mientras que el 25% lo está siempre y el 25% solo a veces. Esto muestra una variabilidad en el grado de atención al cumplimiento de las políticas de seguridad.

Así mismo, todos los encuestados (100%) confirmaron que se asignaron roles de usuario para limitar el acceso a la información, lo que demuestra que esta política se está aplicando de manera efectiva y reconocida. Además, se descubrió que existe una jerarquía de acceso o un mapeo de acceso basado en roles, lo que fortalece la política de control de acceso de la empresa. La mayoría (75%) afirmó que los problemas de seguridad no ocurrían en la institución.

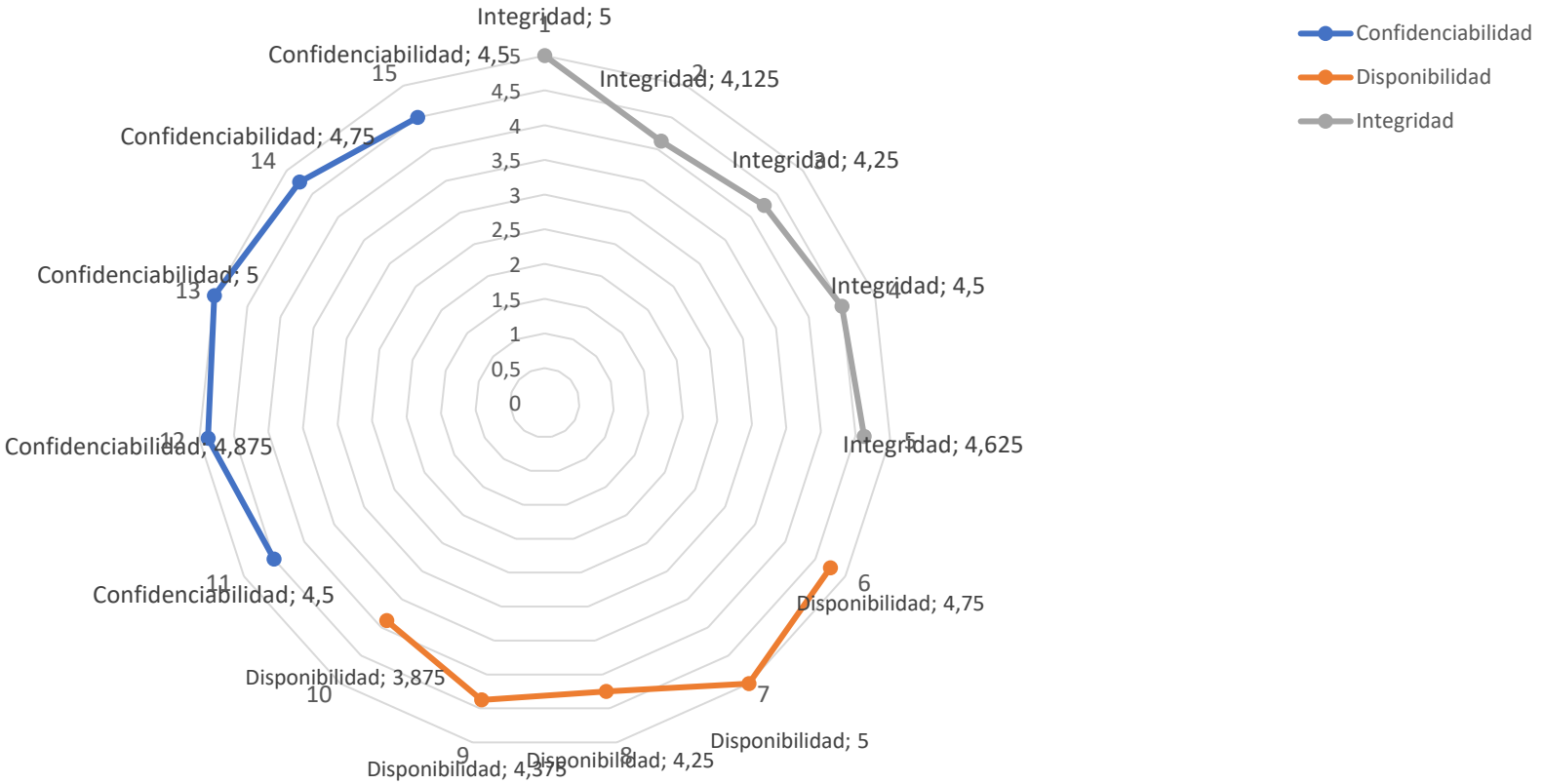
Además, el 62% de las personas indican que las copias de seguridad son el método más utilizado; los detectores de virus y la detección de usuarios intrusos, respectivamente. La papelera de archivos no se usa para este propósito. Y solo el 25% de los encuestados ha participado en talleres sobre políticas de seguridad, esto demuestra la gran necesidad de capacitación para reducir los riesgos potenciales.

Finalmente, un 55% de los encuestados están familiarizados con alguna norma estandarizada, principalmente la familia ISO 27K. Sin embargo, un 44% no conoce ninguna norma, lo que indica la oportunidad de mejorar la educación en este aspecto. La implementación de códigos de buenas prácticas de seguridad de la información es considerada la más importante (75%), seguida por la guía de implementación de un SGSI (25%). Esto destaca la importancia de la implementación efectiva de medidas de seguridad.

Nivel de Madurez: Principios de Seguridad de la Información

Gráfico 12

Gráfico Radial del nivel de madurez



Nota: Gráfica que proviene de la recolección de datos del presente estudio. Indica los promedios en los principios de seguridad de la información.

Siendo la confidencialidad (4.73) el promedio más alto y 4.56 el promedio general.

Análisis del nivel de madurez

El análisis de los principios de seguridad de la información (integridad, disponibilidad y confidencialidad) a través de los ítems y sus puntuaciones promedio proporciona una evaluación del nivel de madurez en cada uno de estos principios. A continuación, se presenta un análisis detallado basado en los porcentajes obtenidos.

Integridad

La integridad de la información, evaluada a través de cinco ítems, obtuvo una puntuación promedio de 4.50/5. Este alto puntaje indica que la mayoría de los encuestados considera que la información de la empresa se difunde sin alteraciones y se mantienen sistemas adecuados de respaldo, recuperación y validación de datos. Los resultados muestran una variación mínima en las respuestas, reflejando una práctica consistente y robusta en el manejo de la integridad de la información.

Disponibilidad

La disponibilidad, evaluada a través de cinco ítems, obtuvo una puntuación promedio de 4.45/5. Los encuestados generalmente consideran que la información está disponible y accesible cuando se necesita, con algunos casos puntuales que podrían beneficiarse de mejoras. La puntuación más baja, 3.88, sugiere que hay ciertas áreas en las que la accesibilidad rápida y eficiente a la información podría optimizarse. A pesar de esto, la mayoría de las respuestas indican una alta disponibilidad, reflejando un entorno donde la información está mayormente disponible y accesible para cumplir con las tareas.

Confidencialidad

La confidencialidad, evaluada a través de cinco ítems, obtuvo la puntuación promedio más alta de 4.73/5. Esto indica un alto nivel de madurez en la protección y control de acceso a la información. Los ítems relacionados con la verificación de usuarios, el uso de claves de seguridad, y la gestión de cuentas de usuarios obtenían puntuaciones consistentemente altas,

con un ítem alcanzando la puntuación perfecta de 5.0. Esta uniformidad sugiere que la organización tiene controles sólidos y efectivos para garantizar que solo los usuarios autorizados tengan acceso a la información, manteniendo así su confidencialidad.

Nivel General de Madurez

El promedio general de 4.56/5 refleja un alto nivel de madurez en los principios de seguridad de la información en la organización. Este puntaje sugiere que la organización tiene prácticas bien establecidas y efectivas en cuanto a integridad, disponibilidad y confidencialidad. Sin embargo, hay margen para mejoras específicas, particularmente en la disponibilidad de la información, donde ciertas áreas podrían beneficiarse de procesos más eficientes.

En resumen, el análisis basado en los porcentajes muestra que la organización mantiene altos estándares de seguridad de la información. La confidencialidad es el área más fuerte, seguida de la integridad y la disponibilidad. Mejoras en la accesibilidad rápida y eficiente de la información podrían elevar aún más el nivel general de madurez en la gestión de la seguridad de la información.

Análisis de la matriz de triangulación de datos basado en la entrevista

A continuación, se presenta el análisis de las respuestas de los informante claves, el mismo que proporciona una visión integral sobre la gestión en seguridad de la información en la organización, abarcando tres principios: integridad, disponibilidad y confidencialidad.

Integridad: Todos los participantes coinciden en que la información de la empresa se difunde sin alteraciones, manteniendo su valor original intacto. Las respuestas también indica que la empresa sigue rigurosamente técnicas relacionadas a seguridad de la información en este principio, especialmente en un contexto de empresas públicas donde la integridad es fundamental. Las respuestas reflejan una cultura organizacional comprometida con la

transparencia de la información, lo cual es esencial para mantener la confianza tanto interna como externa.

Disponibilidad: La disponibilidad de la información muestra ser eficaz, con la mayoría de los participantes indicando que pueden acceder a la información necesaria para sus tareas. Sin embargo, un participante mencionó la necesidad de hacer requerimientos formales, lo que podría señalar áreas de mejora en términos de eficiencia. Este punto sugiere que, aunque la información está accesible, el proceso para obtenerla podría ser más directo y menos burocrático. Mejorar este aspecto podría aumentar la productividad y reducir el tiempo de espera para los usuarios, asegurando que la información esté disponible de manera más inmediata y sin obstáculos.

Confidencialidad: En términos de confidencialidad, las respuestas indican que existen controles robustos para verificar y gestionar el acceso de los usuarios a los sistemas. Se menciona el uso de contraseñas personales y la revisión regular de los registros de uso, lo que asegura que solo los usuarios autorizados tengan acceso a la información sensible. Este enfoque garantiza que la confidencialidad se mantenga y que los riesgos de acceso no autorizado se minimicen. La consistencia en las respuestas sugiere que los procedimientos de seguridad están bien implementados y son efectivos, lo cual es crucial para proteger la información de la organización.

En resumen, el análisis revela que la organización tiene prácticas sólidas en la gestión de la información, alineadas con los principios teóricos de integridad, disponibilidad y confidencialidad. No obstante, hay margen para mejorar, particularmente en la eficiencia del acceso a la información. Abordar estos pequeños obstáculos podría fortalecer aún más la infraestructura de la gestión de la información en la organización, asegurando la protección y exactitud de esta. Es decir, la empresa demuestra un compromiso fuerte con la gestión adecuada de la información complicaciones.

CONCLUSIONES Y RECOMENDACIONES

Una vez finalizado el análisis de los resultados obtenidos a través de las encuestas y entrevista, se revelan las conclusiones y recomendaciones:

Conclusiones

- La revisión teórica a partir de la descomposición de las variables permitió identificar y describir las principales categorías y normas de estandarización para la implementación de políticas de seguridad de la información. Entre las más destacadas se encuentran las normas de la familia ISO 27K, que facilitan la gestión de la seguridad de la información. Estas normas destacan la importancia de establecer un Sistema de Gestión de Seguridad de la Información (SGSI), que incluye políticas, procedimientos y controles diseñados para proteger la confidencialidad, integridad y disponibilidad de la información. La caracterización teórica de las categorías de normas de estandarización e implementación de políticas de seguridad de la información proporciona una base sólida para la Empresa Pública ULEAM en fortalecer su postura de seguridad en la información. Esta revisión teórica no solo cumple con el objetivo específico planteado, sino que también sienta las bases para los siguientes pasos en la implementación práctica de las políticas de seguridad de la información en la organización.
- La Empresa Pública ULEAM no cuenta con políticas de seguridad de la información basadas en normas estandarizadas. A través del diagnóstico observacional, se identificó que la empresa no ha implementado políticas específicas de seguridad de la información, no realiza evaluaciones periódicas de riesgos, ni lleva a cabo formación y concientización sobre el tema. Sin embargo, la empresa posee un sistema informático que utiliza medidas de autenticación, como contraseñas, para acceder a la información según el rol del usuario. Es decir, la empresa utiliza meramente técnicas

de seguridad de información más comunes, es decir, no han adoptado una norma estandarizada de seguridad de información. Esta situación evidencia la necesidad de adoptar y aplicar normas para garantizar la confidencialidad, disponibilidad e integridad de los datos en la organización.

- La familia de normas ISO 27000 corresponde a un grupo de normas basada en la seguridad de información, cada uno de ellos con un objetivo como proporcionar términos y definiciones aplicadas a la ISO 27K, el reconocimiento de los requisitos de un sistema de seguridad de información, aplicar códigos de buenas prácticas de seguridad, reconocer la guía de implementar un sistema de seguridad de información y los requisitos para que una organización esté certificada por la ISO. Es importante realizar una revisión de esta familia de normas, debido que aportan a las empresas que quieran fortalecer competencias basada en la seguridad de datos.
- El estudio de los principios de la seguridad de la información evidenció a la confidencialidad como el principio con mayor nivel de madurez (4.73) con poca diferencia a los demás. Cabe mencionar que los principios de disponibilidad e integridad mostraron un promedio mayor de 4. Esta situación indica que la Empresa Pública ULEAM muestra un nivel de madurez excelente en lo que respecta a prácticas de seguridad de la información, sin embargo, la organización no ha aplicado normas estandarizadas para una mejora continua.
- La encuesta aplicada en la organización evidenció cuál norma de la familia ISO 27K consta con la mejor característica a partir de la opinión de los encuestados, debido que el 75% de los encuestados consideró que la implementación de códigos de buenas prácticas de seguridad de la información es la mejor opción, dichos códigos tienen relación con la norma ISO 27002, la misma que es un conjunto de recomendaciones y mejores prácticas para establecer y mantener la seguridad de la información, esta

publicación está a disposición y aplicable en toda organización, puesto que no tiene restricción alguna.

Recomendaciones

La familia ISO 27k cuenta con una página web oficial donde se obtiene información para todo público en cuanto a cada una de las normas que contiene. Por ello, se sugiere a la Empresa Pública ULEAM la obtención del recurso relacionado a el glosario basado en seguridad de información, la difusión en la organización de este insumo correspondería a la norma ISO 27000, la misma que está enfocada a la comprensión de cada uno de los términos que conciernen a seguridad de información.

En consecuencia, una vez aplicado la norma ISO 27000 se recomienda la implementación de la guía de buenas prácticas (ISO 27002) que describe los objetivos de control recomendables en cuanto a seguridad de la información. Dicha norma, tuvo mayor interés por parte de los trabajadores encuestados, a comparación de las demás aplicaciones relacionadas a los estándares ISO 27k.

Además, se recomienda capacitar al personal mediante programas de formación continua, asegurando que comprendan y sigan las políticas de seguridad de la información y los procedimientos establecidos. Asimismo, es esencial realizar auditorías periódicas para identificar y corregir debilidades, con el objetivo de asegurar el cumplimiento de las normas. Esto también mejorará la gestión de incidentes mediante el desarrollo de planes de respuesta que permitan a la organización reaccionar de manera rápida y efectiva ante cualquier suceso no deseado relacionado con la información interna de la empresa.

Cada una de las recomendaciones promueve una cultura organizacional que valora y prioriza la seguridad de la información, asegurando que todos los miembros de la

organización comprendan la importancia de seguir las mejores prácticas seguridad enfocada a la familia de normalización ISO 27K.

BIBLIOGRAFÍA

Altamirano Yupanqui, J. R. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su cumplimiento. *Revista lbérica de Sistemas y Tecnologías de Información*, 1-23. https://doi.org/https://doi.org/10.17013/risti

Añez, J. (25 de Marzo de 2014). *Estandarizacion del trabajo: Web y Empresas*. Web y Empresas: https://www.webyempresas.com/estandarizacion-del-trabajo/

Arévalo Moscoso, F. M. (2017). *Elaboración y plan de implementación de políticas de seguridad de la información aplicadas a una empresa industrial de alimentos.* Universidad de Cuenca. http://dspace.ucuenca.edu.ec/handle/123456789/28655

Asociación Internacional de Archivos. (2017). *Professional Standards for Archivists and Records Managers.*

Avenía Delgado, C. A. (2017). *Fundamentos de seguridad informática.* Fundación Universitaria del Área Andina. Bogotá: Areandino. Retrieved 26 de Junio de 2024, from https://digitk.areandina.edu.co/handle/areandina/1367

Baca Urbina, G. (2016). *Proyectos de sistemas de información.* Grupo Editorial Patria. https://elibro.net/es/ereader/uleam/40423?page=184

Baldeón Gutiérrez, M., & Guanopatín Safla, J. (2015). *Políticas de seguridad de la información para la Universidad Central del Ecuador bajo los estándares ISO/TEC*

27000 y Cobit 5. Universidad de las Fuerzas Armadas ESPE. Matriz Sangolquí. Maestría en Evaluación y Auditoría de Sistemas Tecnológicos.

Barbosa Martins, A, & Saibel, C. (2005). A Methodology to Implement an Information Security Management System. *Information Systems and Technology Management, II*(2), 121-136. https://doi.org/1807-1775

Berciano, J. (2010). *La importancia y la necesidad de proteger la información sensible: Redseguridad*. Redseguridad: https://www.redseguridad.com/especialidades-tic/proteccion-de-datos/la-importancia-y-la-necesidad-de-proteger-la-informacion-sensible_20120229.html

Borbón Sanabria, J. S. (2011). *Revista seguridad: Buenas prácticas estándares y normas*. Revista seguridad: https://revista.seguridad.unam.mx/numero-11/buenas-prácticas-estándares-y-normas

Briceño, E. (2021). *Seguridad de la información* (Primera ed.). https://doi.org/10.17993

Bustamante García , S., Valles Coral, M., Cuellar Rodríguez, I., & Lévano Rodríguez, D. (2021). *Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú* (Duodécima ed.). Perú: Enfoque UTE. https://doi.org/https://doi.org/10.29019/enfoqueute.743

Cardenas, A., Rojas Mercy, & Briones Rivas. (2024). *Gestion de la información.* obeja negra.

Disterer, G. (4 de Abril de 2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security,*, 92–100 . https://doi.org/10.4236/jis.2013.42011

Fernández Guzmán, R. (2012). *Gestión documental: teoría y práctica. Editorial UOC.*

García, J. A. (2016). *Gestión de trámites y servicios en línea: una revisión de la literatura.*

Goldes, S. S. (2017). Building a viable information security management system. *3rd IEEE International Conference on Cybernetics.* https://doi.org/10.1109/CYBConf.2017.7985763

Gómez-Mejía, L. R. (2008). *Gestión de Recursos Humanos.*

Gutiérrez, J, & Tena, J. (2003). *Protocolos criptográficos y seguridad en redes. Ed Servicio de.* Servicio de Publicaciones de la Universidad de Cantabria, 2003. Santander, España.

Hurtado Trujillo, D. R. (2021). *Políticas de seguridad de la información en salas de internet de la comuna 2 de la ciudad de Neiva.* Universidad Cooperativa de Colombia. https://repository.ucc.edu.co/items/d82ca35f-94a9-4c1c-8345-89d05b9a49ec

Instituto Nacional de Ciberseguridad. (2016). *PROTECCIÓN DE LA INFORMACIÓN.* Recuperado de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-dela-informacion.pdf#page=32&zoom=100,0,0

ISO 15489-1:2016. (2016). *ISO 15489-1:2016 Information and documentation.* https://www.iso.org/obp/ui/en/#iso:std:iso:15118:-5:ed-1:v2:en

ISO. (2013). *ISO/IEC 27002:2013 Information Technology - Security techniques – Code of practice for information security controls.*

ISO. (2016). *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Visión general y vocabulario.*

ISO. (2018). *Sistemas de gestión de seguridad de la información, descripción general y vocabulario.* Organización Internacional de Normalización. Retrieved 10 de Octubre de 2023, from https://www.iso27000.es/iso27000

Jara Arenas, J. A. (2019). *Framework de seguridad de la información basado en los controles de la ISO 27002 para el proceso académico de la UNT.*

Kelsen, H. R. (1994). *Teoría general de las normas.* Trillas. https://etica.uazuay.edu.ec/sites/etica.uazuay.edu.ec/files/public/9788491235125.pdf

Lapiedra Alcami, R. D. (2005). *La gestión documental en la empresa: conceptos y aplicaciones.* Pearson Educación.

Lapiedra Alcami, R., Devece Carañana, C., & Guiral Herrando, J. (2016). *Introducción a la gestión de sistemas de información en la empresa.* Universitat Jaume I. Castelló de la Plana: Comunicació i Publicacions. https://elibro.net/es/ereader/uleam/51689?page=18

Ledezma Espin, D. N. (2015). *Desarrollo de políticas de seguridad de la información basadas en las normas ISO 27002 para una coordinación zonal del INEC.* Pontificia Universidad Católica del Ecuado, Departamento de Investigación y Postgrados, Ambato.

Mahecha Guzmán, M. L., & Coello Falcones, G. R. (2017). *Desarrollo de un sistema de información para gestionar la implantación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013.* Tesis de maestría, Escuela Superior Politécnica del Litoral, Guayaquil. https://www.dspace.espol.edu.ec/xmlui/handle/123456789/38691

Martínez, G. y. (2015). *Gestión de archivos pasivos en la empresa. Revista de Administración de Empresas.*

Moreno Zamudio, T. (2020). *Creación de Políticas de Seguridad de la Información a partir de un Análisis de Riesgos de los Activos de la Información dentro de la Unidad*

Académica de Psicología de la Universidad Autónoma de Zacatecas. Tesis de grado, Universidad Autónoma de Zacatecas, Zacatecas. http://ricaxcan.uaz.edu.mx/jspui/handle/20.500.11845/2091

Pérez, J. (. (2018). *Las diligencias empresariales y su importancia en la gestión de empresas. Revista de Administración Empresarial.*

PMBOK. (2013). *Guía de los Fundamentos para la Dirección de proyectos* (Quinta ed.).

Real Academia Española. (2014). *Diccionario de la lengua española «política»* (23.ª edición ed.). Retrieved 18 de Noviembre de 2023, from <https://dle.rae.es>

Sánchez, J. A. (2015). *Gestión documental: una necesidad empresarial.*

Segunda Cohorte del Doctorado en Seguridad Estratégica. (2014). *Seguridad de la Información.* Universidad de San Carlos. Guatemala, Guatemala: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica.

Solís Peña, S. H., & Angulo Arriaza, R. A. (2012). *Desarrollo de una norma técnica para la estandarización de contenidos de asignaturas en línea.* Editorial Universidad Don Bosco.

ANEXOS

Propuesta de Solución

Tema: Normas de estandarización para la implementación de políticas de seguridad de la información en la Empresa Pública ULEAM, Manta 2024.

Datos informativos

Institución: Empresa Pública ULEAM

Ciudad: Manta

Dirección: Avenida Universidad 5

Investigador: Cardenas Alava Aldo Xavier

Tutor/a: Lcda. Mercy Celinda Rojas Once

Antecedente

Toda organización tiene en común el insumo de la información, la misma que es procesada mediante los sistemas informáticos con el objetivo de llevar a cabo la toma de decisiones informadas. Dicho eso, es importante una eficiente gestión de la información en las empresas desde el procesamiento de datos hasta la distribución de información, pues es en esta fase donde los subordinados portan este recurso valioso y debe ser la misma empresa la que tiene la obligación de garantizar los principios de integridad, disponibilidad y confidencialidad informacional.

Por otro lado, la misión de la Empresa Pública ULEAM, es brindar servicios de excelencia en el ámbito de consultorías, asesorías, ejecución y/o administración de proyectos de producción, capacitación, investigación, inversión y demás afines a la ULEAM, con la participación de personal altamente capacitado para impulsar el desarrollo multidisciplinario del país; todo en línea con la Ley Orgánica de Empresas Públicas (LOEP).

La encuesta realizada al personal de diferentes áreas de la organización evidenció el reconocimiento de la implementación de mejores prácticas de seguridad de la información como como la mejor opción para mejorar la eficacia en dicha competencia. Es decir, la norma ISO 27002 indica ser la propuesta de solución más acertada para que la Empresa Pública ULEAM implemente políticas de seguridad de información

Justificación

El insumo de la información en toda organización independientemente del sector debe ser gestionada con eficiencia, debido que puede estar expuesta a una divulgación malintencionada. Dicho esto, cada empresa tiene la oportunidad de contar con un sistema de gestión de información en términos de seguridad con el objetivo de proteger los datos importantes de cada compañía.

En la organización no se encuentra implementados estándares de seguridad de la información. Por ello, se ha considerado la Norma ISO 27002 que engloba los códigos de mejores prácticas de seguridad informática.

La presente propuesta se puede realizar porque la empresa cuenta con una base excelente en los principios de seguridad de información. Además, el personal del Departamento de Sistema cuenta con un talento humano capacitado y recurso tecnológico excelente para la normalización de la ISO 27002 como política de seguridad de información.

Objetivos

A continuación, se presentan los objetivos de la propuesta de solución, cada uno de los objetivos específicos significa un hito alcanzar lo propuesto.

Objetivo General

Implementar las normas estandarizadas ISO 27000 y 27002 en la Empresa Pública ULEAM, para garantizar la mejora continua a los niveles de madurez en los principios de seguridad de información.

Objetivos Específicos

- Obtener y trasmitir dentro de la organización el vocabulario de términos generales de seguridad de información como introducción a la familia ISO 27K.
- Adquirir la versión más actualizada del documento ISO 27002 basado en los códigos de mejores prácticas de seguridad de la información.

Análisis de Factibilidad

Factibilidad operativa

Para alcanzar el objetivo, se implementará la norma ISO 27002 de seguridad informática con la colaboración de todo el personal del departamento de sistemas y con la aprobación del Gerente de la organización.

Factibilidad económica

La implementación de la norma ISO 27002 es factible de realizarse debido que existen plataformas como AENOR. Es una organización que se dedica a la normalización y certificación en todos los sectores industriales y de servicios. La AENOR Tienda es la plataforma en línea de esta organización donde se pueden adquirir normas, publicaciones, libros y otros documentos relacionados con la normalización y la certificación. La implementación de la norma es factible porque adquirir el documento económicamente asequible.

Factibilidad técnica

Para la implantación de las políticas de seguridad de información en la Empresa Pública ULEAM se cuenta con la siguiente documentación:

- Vocabulario de términos (ISO 27000).
- Documento de los códigos de buenas prácticas (ISO 27002)

Beneficios

Imagen corporativa: Mejora la credibilidad y confianza de la empresa ante socios, clientes y el mercado en general, demostrando compromiso con la integridad de la información. Ayuda a minimizar los riesgos de seguridad, lo que puede evitar daños reputacionales asociados a brechas de seguridad.

Usuarios internos: La implementación de normas de seguridad fomenta una cultura de conciencia y responsabilidad en la protección de la información. Un entono seguro reduce los incidentes, a su vez disminuye la carga de trabajo relacionado a la intervención de inconvenientes informacional.

Conclusión

La implementación de las normas ISO 27002 en la Empresa Pública ULEAM no solo incrementa la seguridad de la información. Además, trae consigo numerosos beneficios en la organización. Respecto a la imagen corporativa, esta mejora la credibilidad y la confianza de la organización ante los clientes, demostrando un fuerte compromiso con la protección de la información.

Para los usuarios internos, adoptar estas normas fomenta una cultura organizacional más consciente y responsable en términos de seguridad de la información, lo que disminuye la frecuencia de incidentes de seguridad y, como resultado, reduce la carga de trabajo relacionada

con la gestión de crisis. Para los usuarios externos, esta certificación aumenta la confianza y satisfacción al garantizar la protección de sus datos y la transparencia en las operaciones.

En resumen, la implementación de la ISO 27002 mejoraría la gestión de la información dentro de la organización y también mejora la reputación de la empresa con relación a las partes interesadas, contribuyendo de manera integral al desarrollo y éxito sostenido de la Empresa Pública ULEAM.

Guía de Observación

GUIA DE OBSERVACIÓN: Implementación de Políticas de Seguridad de la Información	
Fecha:	22/09/2023
Empresa:	Empresa Pública ULEAM
Sector:	Público
Observador:	Aldo Cardenas
Objetivo:	Observar la implementación de políticas de seguridad de información basado en ISO 27000, COBIT u otro modelo en la Empresa Pública ULEAM.

PREGUNTAS	**Respuesta**
1. ¿La empresa tiene documentadas políticas de seguridad de la información?	No
2. ¿Están claramente definidos los roles y responsabilidades con relación a la seguridad de la información?	No
3. ¿Se realizan evaluaciones de riesgos de seguridad de la información de manera periódica?	No
4. ¿La empresa tiene procedimientos para el manejo de incidentes de seguridad de la información?	No
5. ¿Se lleva a cabo la formación y concienciación sobre seguridad de la información para el personal?	No
6. ¿Se realizan auditorías internas para verificar el cumplimiento técnicas de seguridad de la información?	No
7. ¿La empresa tiene un proceso de mejora continua en lo que respecta a la seguridad de la información?	No
8. ¿Los empleados utilizan medidas de autenticación (por ejemplo, contraseñas, tarjetas de acceso) para acceder a sistemas y datos críticos?	Si

Encuestas

Encuestador:

Ciudad:

Fecha:

Nº de cuestionario:

Objetivo de encuesta

Conocer que norma es recomendable en la seguridad de la información para la Empresa Pública ULEAM. La información se utilizará para fines netamente académicos. La encuesta es anónima, invito a contestar con sinceridad.

Datos iniciales

Edad: Género: Estado Civil:

Área de trabajo en la institución: Cargo:

1. **¿Conoce usted las prácticas de seguridad de información en la Empresa Pública ULEAM?**

   Si O No O

2. **¿Está pendiente del cumplimiento de las prácticas de seguridad de la información establecidas en la Empresa Pública ULEAM?**

O Siempre	O Casi siempre	O A veces	O Casi nunca	O Nunca

3. **¿Qué prácticas de seguridad de información utiliza la institución en los sistemas informáticos?**

   Control de accesos en línea

   Gestión de vulnerabilidades

   Uso de contraseñas

   Cifrado de datos

   Llave USB de seguridad

   Ninguna

4. **¿Tiene acceso a información de otras áreas funcionales de la institución a partir de su rol asignado en el sistema informático?**

   Si O No O

5. **¿Se asignan roles de usuario en los sistemas informáticos con el objetivo de limitar el acceso a la información, dependiendo del rol?**

   Si O No O

6. **¿En la empresa existe una jerarquía o mapeo de acceso a la información dependiendo el rol de los usuarios?**

   Si O No O

7. **¿Qué tan frecuente son incidentes de seguridad de información en la institución?**

O Muy rara vez	O Rara vez	O A veces	O Frecuentemente	O Muy Frecuentemente

8. **Ante un incidente, cuál de los siguientes métodos para salvaguardar la información se aplica en la institución**

   Detección de usuarios intrusos

   Detector de virus

   Copias de seguridad

   Papelera de archivos

9. **¿Ha recibido algún taller o socialización sobre políticas de seguridad de la información?**

   Si O No O

10. **¿Se familiariza con alguna de las siguientes normas estandarizada sobre la seguridad de la información?**

    Família ISO 27K

    Normas COBIT

    Normas NIST

    Ninguna

11. **¿Cuál de las siguientes aplicaciones considera la más importante con relación a mejorar competencias de Sistemas de Gestión de la Seguridad de la Información (SGSI)?**

    Revisar un vocabulario de SGSI

    Reconocer requisitos de un SGSI

    Implementar códigos de buenas prácticas de SI

    Saber la guía de implementación de un SGSI

    Reconocer requisitos de certificación en SI

Instrumento para el estudio del nivel de madurez en los principios de seguridad de la información

Nº	PRINCIPIO	ÍTEMS	Siempre	Casi siempre	A veces	Casi nunca	Nunca
1	Integridad	¿La información de la empresa se difunde sin alteraciones, manteniendo integro el valor original del mismo?					
2		¿La empresa cuenta con sistemas de respaldo de la información en caso de fallos o incidentes?					
3		¿La empresa cuenta con sistemas de recuperación de la información en caso de fallos o incidentes?					
4		¿Existe validación en la entrada de archivos al sistema informático?					
5		¿Se realizan controles de acceso para proteger la información de la empresa?					
6	Disponibilidad	¿La información siempre está disponible para los involucrados que la necesiten para cumplir con sus tareas?					
7		¿Se puede acceder a la información de manera confiable y en el momento adecuado?					
8		¿La información que recibe es oportuna?					
9		¿El personal tiene acceso rápido y eficiente a la información que necesita para realizar sus funciones?					
10		¿La información que recibe para realizar sus tareas es puntual?					
11	Confidencialidad	¿Las capacidades de acceso de usuarios a los sistemas son revisadas para la verificación de usuarios confiables?					
12		¿Los sistemas informáticos, disponen de claves de seguridad para el ingreso de datos?					
13		¿Las cuentas de los usuarios que cambian de funciones o son retirados de la organización, son removidas inmediatamente?					
14		¿Los sistemas validan que las contraseñas de ingreso al sistema no sean inferiores a seis caracteres?					
15		¿Los sistemas validan que las contraseñas de ingreso no hayan sido utilizadas antes?					

Nota La presente tabla corresponde al instrumento para realizar el nivel de madurez que tiene la Empresa Pública con relación a los principios de seguridad de la información (integridad, disponibilidad y confidencialidad). Siempre equivale a 5, casi siempre a 4, A veces 3, Casi nunca 2 y Nunca 1.

Resultados del instrumento de recolección de datos

Nº Ítem	Principio	Encuestado 1	Encuestado 2	Encuestado 3	Encuestado 4	Encuestado 5	Encuestado 6	Encuestado 7	Encuestado 8	Promedio
1	Integridad	5	5	5	5	5	5	5	5	5
2	Integridad	4	3	4	4	3	5	5	5	4,13
3	Integridad	4	3	5	4	3	5	5	5	4,25
4	Integridad	4	4	4	5	4	5	5	5	4,5
5	Integridad	5	5	5	3	5	5	5	4	4,63
6	Disponibilidad	5	5	5	4	5	5	4	5	4,75
7	Disponibilidad	5	5	5	5	5	5	5	5	5
8	Disponibilidad	4	3	4	5	5	4	5	4	4,25
9	Disponibilidad	4	3	5	4	5	5	5	4	4,38
10	Disponibilidad	4	2	5	4	4	4	4	4	3,88
11	Confidencialidad	4	5	4	4	4	5	5	5	4,5
12	Confidencialidad	5	5	5	5	4	5	5	5	4,88
13	Confidencialidad	5	5	5	5	5	5	5	5	5
14	Confidencialidad	5	4	5	4	5	5	5	5	4,75
15	Confidencialidad	4	4	4	4	5	5	5	5	4,5

Nivel de madurez en los principios de seguridad de la información

Etiquetas de fila	Promedio
Confidencialidad	4,73 / 5
Disponibilidad	4,45 / 5
Integridad	4,50 / 5
Total general	**4,56** / 5

Triangulación

Tabla 12

Matriz de triangulación de datos

Nº	PREGUNTA	ENTREVISTADO 1	ENTREVISTADO 2	ENTREVISTADO 3	ENTREVISTADO 4	TEORÍA	ANÁLISIS
1	¿La información de la empresa se difunde sin alteraciones, manteniendo integro el valor original del mismo? **Indicador:** Integridad	Dentro de nuestra institución, nuestra información que se maneja normalmente debe ser íntegra, ya que nosotros somos empresas públicas y nos debemos a ciertas normas y procedimientos que se dan en a mí. Por ende, no puede haber ninguna alteración a la información de esta empresa pública.	Si, tal cual indica la pregunta, la información cuando se difunde mantiene su valor e integridad cuando es receptado.	La información se difunde sin alteraciones, todo funciona de forma correcta.	Hoy se difunden de manera íntegra. Ya que son unidades de negocio.	Avenía delgado indica que la integridad de información "Garantiza la autenticidad y exactitud de la información en cualquier momento que se solicitó o se envía de un entorno tecnológico en que los datos no han sido alterados o destruidos de forma no autorizada. El objetivo de la integridad, entonces, evitar la modificación no autorizada de la información". (Avenía Delgado, 2017)	Los entrevistados coinciden en que la información se maneja de manera íntegra. La consistencia en las respuestas coincide a excelentes técnicas orientada a la integridad de los datos. Según Avenía Delgado (2017), la integridad de la información implica garantizar la autenticidad y exactitud de esta, asegurando que no haya alteraciones no autorizadas. Las respuestas de los entrevistados confirman que la EP ULEAM está envuelta positivamente con este principio.
2	¿La información siempre está disponible para los involucrados	La información debe estar disponible, ya	Cuando necesito una información para cumplir mis	Claro, la información está disponible,	El área de informática y financiera	La Organización ISO manifiesta que la disponibilidad	Los entrevistados indican que la información en la

	que la necesiten para cumplir con sus tareas? **Indicador:** Disponibilidad	que es el medio de que nos va a permitir tomar las decisiones respectivas dependiendo la necesidad que se nos presente.	tareas hago un requerimiento. Yo lo solicito al departamento Financiero, porque es la última área donde llega la información que se maneja con integridad.	conforme a las tareas asignadas. esta la tenemos de forma inmediata.	Siempre están Predispuesta a colaborar cuando se necesita una información fundamental para el cumplimiento de las actividades.	"Permite que la información pueda estar disponible cuando sea necesaria. Hace alusión al acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran". (ISO, 2016)	empresa está generalmente disponible para aquellos que la necesitan. La disponibilidad se asegura a través de procedimientos de solicitud y colaboración entre departamentos, especialmente los de informática y finanzas. De acuerdo con la ISO (2016), la disponibilidad implica que la información esté accesible cuando sea necesaria para los procesos. Es decir, la disponibilidad de la información en la empresa es eficaz.
3	¿Las capacidades de acceso de usuarios a los sistemas son revisadas para la verificación de usuarios confiables? **Indicador:** Confidencialidad	Hoy en día, el acceso de un usuario normalmente se maneja de manera personal. Por ende, muchas veces se está revisando la verificación, nuestra empresa es pequeña. Normalmente siempre hay un	Si, existe un control de acceso en las capacidades de conexiones en línea de usuarios, se revisan mediante el registro de uso de los sistemas.	Son pocas las veces que el sistema se colapsa, quiere decir que las capacidades de acceso están óptimas con la cantidad de usuarios que acceden al sistema.	Siempre ingresan usuarios confiables, debido que las claves son personales para cada uno de los trabajadores que utilizan el sistema. Entonces.	Briceño señala que "la confidencialidad es un componente necesario de la privacidad y se refiere a nuestra capacidad de proteger nuestros datos de aquellos que no están autorizados para verlos". (Briceño, 2021)	Los entrevistados señalan que en la organización aplican controles de acceso para verificar la confiabilidad de los usuarios. Estos controles incluyen la revisión periódica de las capacidades de acceso, lo que contribuye a garantizar que solo usuarios autorizados pueden acceder a la información. Briceño

		registro del uso de las aplicaciones o sistemas contables. Para su verificación de acceso correcto.					(2021) menciona que la confidencialidad es esencial para proteger los datos de accesos no autorizados. Las respuestas de los entrevistados muestran que la EP ULEAM está alineada con este principio, debido que aplican medidas de control de acceso asegurando que solo las personas autorizadas puedan acceder a los sistemas y la información crítica.

Fotografías

Aplicación de encuesta y entrevista al personal de diferentes áreas de la Empresa Pública ULEAM.