UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL GAD INTERCULTURAL DE EL TAMBO.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

AUTOR: CARLOS FRANCISCO CHIMBORAZO QUIZHPI

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS, MSC.

CAÑAR - ECUADOR

2021

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CARRERA DE INGENIERIA DE SISTEMAS

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL GAD INTERCULTURAL DE EL TAMBO.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

AUTOR: CARLOS FRANCISCO CHIMBORAZO QUIZHPI

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILES, MGS.

CAÑAR - ECUADOR

2021

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARACIÓN

Yo, Carlos Francisco Chimborazo Quizhpi, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Católica de Cuenca extensión Cañar puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y la Normativa actual de la institución.

Carlos Francisco Chimborazo Quizhpi
C.I: **0302362645**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el Est. Carlos Francisco Chimborazo Quizhpi, bajo mi supervisión.

Ing. Cristhian Flores Urgilés, Mgs

DIRECTOR DELTRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA

DEDICATORIA

A mis padres y hermano por confiar en mis capacidades a pesar mis limitaciones visuales e inculcar la importancia de estudiar, a mi abuelita Salomé Quizhpi por brindarme su gran amor incondicional en afán de ver y formarme como una persona de bien.

A mi hija, por ser una parte muy importante en mi vida y la inspiración para culminar este proyecto académico.

Carlos Francisco Chimborazo Quizhpi.

AGRADECIMIENTO

Expreso mi agradecimiento en primera instancia a Dios por ser mi fortaleza en los momentos más críticos de mis estudios, por colmarme de su bendición y sabiduría que se han presentado durante el trayecto educativo y cotidiano;

A mis familiares por brindarme el aliento de positivismo de manera especial a mis padres por su apoyo económico, moral y ético. A mis abuelitas María Datan y Salomé Quizhpi quienes me han inculcado valores de esfuerzo, perseverancia y honestidad para alcanzar los sueños que me proponga.

A la UNIVERSIDAD CATÓLICA DE CUENCA, EXTENSIÓN CAÑAR que, por medio de sus recursos, programas de apoyo y catedráticos de la carrera de Ingeniería de Sistemas ha permitido formarme profesionalmente, de manera especial, a mi tutor de tesis Ing. Cristhian Humberto Flores Urgilés, Mgs., quien, con su paciencia, conocimientos, profesionalismo, experiencia ha aportado activamente para culminar el presente trabajo y posteriormente obtener el título profesional.

A los directivos y personal del Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo (GADMIET) quienes estuvieron prestos y dispuestos en permitirme desarrollar el trabajo de titulación en su prestigiosa institución sin prejuicios ni reservas en el acceso a la información.

Carlos Chimborazo Q.

Tabla de contenido

INDISE DE ILUSTRACIONES

RESUMEN

El Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo (GADMIET) viene desarrollando diferentes gestiones en todo su territorio, brindado a la ciudadanía servicios que mejoren la calidad de vida. La falta de normas de seguridad de la información en el GADMIET provoca que la información manejada dentro de la organización sea vulnerable a manipulaciones. La presente investigación consiste en el diseño de un "MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL GAD INTERCULTURAL DE EL TAMBO.", para el desarrollo eficiente del trabajo de tesis, se toma como base la norma ISO 27001:2013 y la guía de buenas prácticas ISO 27002, para determinar los controles que permitan el aseguramiento de la información, para ello se realizó una encuesta al encargado de TI, para determinar la situación actual de la organización, el levantamiento de activos del departamento de Tecnologías de Información y Comunicación (TIC) y la calificación respectiva, se determinó el nivel de riesgo en base a las amenazas de dichos activos y se establecieron los controles pertinentes, obteniendo como resultado el manual de políticas para el Gad Intercultural El Tambo.

Palabras Claves: norma iso 27001, controles, gestión de riesgos, tic, gadmiet.

ABSTRACT

The Intercultural Decentralized Autonomous Municipal Government from El Tambo (GADMIET by its acronym in Spanish) has been developing different procedures throughout its territory to provide its citizens with services that improve their quality of life. The lack of information about security standards in the GADMIET makes the information handled within the organization vulnerable to manipulation. Therefore, this research aims at designing a manual of information security policies based on the ISO 27001 standard in the GADMIET from El Tambo. Thus, to efficiently develop this thesis work, the ISO standard is taken as a basis for the 27001: 2013 and the ISO 27002 good practice guide, to determine the controls that allow the assurance of the information. Accordingly, a survey was applied to the IT manager to determine the current situation of the organization. Additionally, the survey of assets of the department of Information and Communication Technologies (ICT) and the respective qualification. The level of risk was determined based on the threats of the aforementioned assets and the pertinent controls were established, obtaining, as a result, the policy manual for the intercultural GAD from El Tambo.

Keywords: ISO 27001 standard, controls, risk management, ICT, GADMIET

INTRODUCCIÓN

El Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo (GADMIET) establece la información como el activo más importante para el manejo de la entidad el cual permite el desarrollo continuo de la misión y el cumplimiento de los objetivos estratégicos. Razón por la cual, surge la necesidad de determinar políticas que ayuden a proteger la confidencialidad, integridad y la disponibilidad de la información.

Con la evolución de nuevas tecnologías de la información los GAD optan por servicios tecnológicos para optimizar sus procesos, el uso y el manejo inadecuado de estas tecnologías han ocasionado problema a las organizaciones ya que son vulnerables a las amenazas que se presentan en el medio, las mismas que pueden convertirse en riesgo y afectar enormemente la integridad de la información.

Por ende, la presente investigación se enfocará en determinar políticas de seguridad de la información para el GAD intercultural El Tambo tomando como referencia el estándar ISO/IEC 27000, la misma que comprende todo un conjunto de normas relacionadas con la seguridad de la información, siendo la ISO/IEC 27001 seleccionada para el desarrollo del proyecto, ya que al ser un Sistema de Gestión de la Seguridad de la Información permite a las organizaciones realizar la evaluación de riesgos y de la misma manera la implementación de controles necesario para minimizar o eliminarlos.

CAPITULO I

MARCO REFERENCIAL

1.1. Planteamiento del Problema

Hoy en día el tema de la seguridad informática ha despertado un gran interés en las organizaciones ya que la información o datos viene siendo el activo más importante de aseguramiento. Las entidades u organizaciones han sufrido constantes ataques informáticos estos pueden ser usuarios internos o externos a las entidades.

Con el uso y el manejo inadecuado de las tecnologías han ocasionado problema a las organizaciones ya que son vulnerables a las amenazas que se presentan en el medio, las mismas que pueden convertirse en riesgo y afectar enormemente la integridad de la información.

La implementación de un manual de políticas de información en las municipalidades permite optimizar la seguridad de la información en la entidad.

Es por esto que se pretende diseñar un manual de políticas de seguridad de la información para el Gad intercultural de El Tambo la que permita proteger y conservar la información de la entidad. El manual de políticas será debidamente documentado, puesto en conocimiento de los empleados de la entidad será de uso obligatorio.

1.1.1. Formulación del Problema

- ¿Qué procesos o activos son los que necesitan mayor nivel de prioridad en atención a la seguridad dentro de la municipalidad?
- ¿En qué medida mejoraría la seguridad de los sistemas de información del Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo, con el planteamiento de la propuesta?

1.2. Antecedentes de la investigación

Existen varios autores que han desarrollado diversos estudios de investigación sobre el tema, cuyos resultados han generado una guía a tomarse en consideración. A continuación, se mencionan algunos de ellos:

Un estudio similar realizado en la Universidad Internacional SEK de la facultad de Arquitectura e Ingenierías, proyecto de investigación, presentado por el estudiante Henry Percy Cabrera Cubas que lleva el título "DISEÑO DE UNA POLÍTICAS EN LA NORMA ISO 27001, PARA MEJORAR LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE FLORIDA -BOGARA - AMAZONA", donde recomienda realizar talleres, programas de capacitación de seguridad de la información más seguido, y especialmente al personal nuevo que ingresa; pero primero debemos implementar el programa de seguridad para los administrativos, jefes de cada área administrativa, liego trabajadores, y a todo el personal eterno que brinda servicios. (Cabrera Cubas, 2018)

Esta investigación será de ayuda para profundizar las bases teóricas y tener en cuenta los controles y dominios que presenta la norma ISO 27001, las mismas que serán utilizadas en el desarrollo de esta investigación.

Otro estudio similar realizado en la Universidad de las Américas, de la facultad de Ingeniería y Ciencias Agropecuarias por el estudiante Gustavo Xavier Lema Pazmiño con título "DISEÑO DE LAS BUENAS PRÁCTICAS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN NORMAS ISO 27001 PARA LA DIRECCIÓN GENERAL DE AVIACIÓN CIVIL", la presente tesis describe una investigación referente a un mejoramiento de los procesos de seguridad, políticas y mejoras

del área técnica de la Dirección Aviación Civil del Ecuador (DGAC), por ello se ha generado una evaluación y análisis de la información obtenida para verificar la vulnerabilidad existente en la red de datos, así como también evidencia la falla en los procesos que se generan en dicha institución. (Lema Pazmiño, 2017)

En base a este proyecto se podrá determinar las vulnerabilidades, los riesgos que pueden afectar a los sistemas, determinar los procesos críticos las cuales necesiten de la implementación de controles para que la información se encuentre protegida.

1.3. Justificación de la investigación

La seguridad de la información es un proceso en el que se da cabida a un creciente número de elementos: aspectos tecnológicos, de gestión-organizacionales, de recursos humanos, de índole económica, de negocio, de tipo legal, de cumplimiento, etc., abarcando no solo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medioambientales, humanos, etc., (AREITIO BERTOLIN, 2008).

Un nivel de protección total de la información es prácticamente imposible, por lo que un sistema de gestión de la seguridad de la información debe garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización (Galisteo Pradillo, 2014).

Es por esto que se propone realizar un manual de políticas de información para el Gad intercultural El Tambo con la finalidad de especificar el manejo y uso adecuado de las tecnologías para obtener un mayor grado de ventajas que brindan estas herramientas y sobre todo, la integridad de la información.

1.4. Objetivos

1.4.1. Objetivo General

Diseñar un Manual de Políticas de Seguridad de la Información para el Gad Intercultural del Tambo basado en la norma ISO/IEC 27001:2013 con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información existente en el departamento de TI.

1.4.2. Objetivos Específicos

- Realizar un estudio teórico con los temas relacionados a la investigación.
- Realizar el levantamiento y análisis de información para determinar el diagnóstico de la situación actual de la seguridad de información y de amenazas, vulnerabilidades y riesgos relacionados a la información del área de TI en el Gad Intercultural de El Tambo en base a la norma ISO/IEC27001:2013.
- Elaborar un manual de políticas de seguridad de la información en base a la norma ISO/IEC 27001:2013 para el Gad Intercultural de El Tambo.

1.5. Limitaciones

Las limitaciones mencionadas a continuación restringirán la investigación.

- Falta de colaboración por parte de los funcionarios de la institución.
- El tiempo prolongado para llevar acabo el desarrollo de la presente investigación sea corto y resulte inalcanzable cumplir con los objetivos propuestos.

1.6. Delimitaciones

- El estudio solo propondrá un modelo del manual de políticas, por lo que dependerá de la municipalidad la implementación de la misma.

CAPITULO II

MARCO TEÓRICO

2.1. Seguridad de la Información

La seguridad de la información es la protección de la integridad, disponibilidad y confidencialidad de la información, según el nivel requerido para los objetivos de negocio de la empresa (Miguel Pérez, 2015).

2.2. Seguridad Informática

No existe una definición estricta de lo que se entiende por Seguridad Informática, puesto que esta abarca múltiples y muy diversas áreas relacionadas con los SI. Tampoco es único el objetivo de la seguridad informática: la confidencialidad, la integridad y la disponibilidad (Sánchez Garreta, 2003).

2.3. Familia de Norma ISO/IEC 27000

2.3.1. Norma ISO/IEC 27001:

La norma establece los requisitos que debe cumplir un SGSI (sistema de Gestión de la Seguridad de la Información) para su certificación en términos de procesos de seguridad a nivel organizativo (CASTRO GIL , DÍAZ ORUETA, ALZÓRRIZ ARMENDÁRIZ, & SANCRISTÓBAL RUIZ, 2014).

2.3.1.1. Beneficios de la Norma ISO/IEC 27001

"La norma ISO 27001 permite identificar riesgos asociados a la información importante y pone en su lugar los controles apropiados para ayudar a reducir el riesgo.

Esta norma ofrece garantía independiente de los controles internos, para el cumplimiento de los requisitos de la organización" (Francisco, 2019, pág. 14).

2.3.1.2. Dominios de seguridad de la norma ISO/IEC 27001

- Políticas de seguridad
- Organización de la seguridad
- Gestión de activos
- Seguridad física y del entorno
- Gestión de comunicación y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas
- Gestión de incidentes de seguridad de la información
- Gestión de la continuidad de los negocios
- Cumplimiento

2.3.1.3. Estándar ISO 27001:2013

Permite a las organizaciones sean grandes o pequeñas a evaluar los riesgos y la aplicación de controles necesarios que permitan mitigar, eliminar, asumir o transferir.

La última versión 2013, se refuerza la mejora continua, basándose en un ciclo de planificación, ejecución, monitorización y mejora donde se adapta referentemente al modelo PDCA más conocido como ciclo de Deming, como se visualiza en la ilustración Nº 1 (Francisco, 2019).

2.3.2. Norma ISO/IEC 27002:

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, esta norma no es certificable.

Contiene 35 objetivos de control y 114 controles agrupados en 14 dominios (ISO 27000, 2005).

2.4. Sistema de Gestión de la seguridad de la información (SGSI)

Frente a la dependencia de los sistemas de información y al crecimiento de las amenazas existentes, se hace necesario para las organizaciones establecer un Sistema de 1gestion de Seguridad de la Información. Hay que tener en cuenta una premisa fundamental: la seguridad no es un producto, es un proceso; por tanto, la seguridad no puede comprarse, pero puede gestionarse (Miguel Pérez, 2015).

2.4.1. Beneficios del SGSI

- Reducción de riesgos debido al establecimiento y seguimiento de controles.
- Reducción de las amenazas hasta alcanzar el nivel de asumible por las organizaciones.
- Reducción de daños ante incidentes presentados, asegurando la continuidad de negocio.
- Ahorro de costes de una racionalización de los recursos.
- La seguridad deja de ser un conjunto de actividades organizadas y pasa a formarse un ciclo de vida metódico y controlado, en donde toda la organización será participe.
- La organización se asegura del cumplimiento de la legislación vigente y se evita riesgos y costes innecesarios.
- La certificación del SGSI contribuye a mejorar la operatividad en el mercado.

2.4.2. Pilares de la seguridad de la información:

- **Confidencialidad:**

La confidencialidad es un atributo de la seguridad de la información en cual se encarga a que la información no se divulgue a personas o sistemas que no tengan la autorización correspondiente, es decir que el acceso a la información lo puede realizar la persona que esté debidamente autorizada (Aguilera Lopez, 2010).

- **Integridad:**

La integridad es otro de los atributos de la seguridad de la información, su objetivo es mantener la información de manera exacta es decir tal cual fue creada al principio, sin modificación o alteración por otras personas que no están autorizadas (Aguilera Lopez, 2010).

- **Disponibilidad:**

Es la garantía de que los usuarios autorizados tiene acceso a la información y a los activos asociados cuando lo requieran. (INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR, 2014)

2.4.3. Riesgos en la seguridad de la información

- **Activos de información:**

Los activos de información son cualquier componente sean esta (humanos, tecnológicos, software, documental o de infraestructura) que soportan uno o más procesos de negocios de cualquier organización que ameritan ser protegidos para el funcionamiento del mismo. (Escuela Tecnologica Instituto Tecnico Cnetral, 2021)

- **Amenazas:**

Una amenaza representa la acción que tiende a causar un daño a los dispositivos o sistemas en donde se encuentra almacenada la información, atentando contra su confidencialidad, integridad y disponibilidad. (Veiga, 2020)

- **Vulnerabilidades:**

Es la debilidad de cualquier tipo que compromete la seguridad del sistema Informático. (Lorena)

- **Control:**

Es toda actividad o proceso encaminado a mitigar o evitar un riesgo, en donde incluye políticas, procedimientos, guías, estructuras organizacionales y venas prácticas, que pueden ser de carácter administrativos, tecnológico, físico o legal. (Escuela Tecnologica Instituto Tecnico Cnetral, 2021)

2.5. Análisis y Gestión de riesgos

"La gestión de riesgo es considerada como un conjunto de decisiones administrativas, de organización y conocimiento operacionales desarrollados por sociedades y comunidades para implementar políticas, estrategias y fortalecer sus capacidades a fin de reducir el impacto de las amenazas ambientales y tecnológicos". (Orellana, 2017)

2.5.1. Metodologías para gestión de riesgos informáticos

"Las metodologías de análisis de riesgos, son utilizadas para identificar de una forma general y cualitativa tanto amenazas como las vulnerabilidades de personas o recursos, con el fin de determinar el nivel de riesgo". (Orellana, 2017, pág. 88)

Hoy en día, existe un gran número de metodologías para el análisis y gestión del riesgo, las cuales deben ser elegidas de acuerdo a las necesidades de la seguridad de la información que solicite la Organización.

A continuación, se menciona alguna de ellas:

- Metodología Magerit
- Metodología Cramn
- Metodología Octave
- Metodología Mehari
- Metodología ISO 27005

2.6. Políticas de Seguridad:

El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de una organización, y en particular al involucrado directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados. (Aguilera López)

CAPITULO III

MARCO METODOLOGICO

3.1. Enfoque de la investigación

Por los objetivos planteados para llevar a cabo la investigación, el enfoque de investigación que se utilizo fue cualitativo. Con el fin de comprobar la problemática del objeto de estudio se desarrolló técnicas de investigación, que permita determinar las políticas de seguridad de la información para el GADMIET.

Adicional a lo mencionado, se empleó en enfoque cuantitativo primaria que busca medir los datos y aplicar un análisis estadístico.

Para la recolección de información se empleó la técnica de:

- Encuesta al personal encargado del departamento de TIC del GADMIET
- Observación directa a las instalaciones del GADMIET, la infraestructura tecnológica y el personal del área de Tic de la institución.

3.2. Nivel de investigación

El diseño de la investigación fue de tipo descriptivo, debido a que el presente estudio tiene como fin describir las políticas de seguridad que permita la salvaguarda de información del Gobierno Autónomo Descentralizado Municipal intercultural El Tambo.

3.3. Población y muestra

La investigación se llevó a cabo en el Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo. La muestra se plasmó estrictamente en el departamento de TIC de la municipalidad.

3.4. Técnicas e instrumentos de recolección

Para la recolección de la información se aplicó una encuesta al personal encargado del departamento de TIC, con el fin de determinar el estado actual de la organización referente a la seguridad de la información, por otra parte, se realizaron investigaciones en bases científicas como: Artículos, Revistas, libros digitales, etc.

3.5. Interpretación de resultados

El análisis del nivel de madures, se realizó en base a la encuesta realizada al personal de TI, siendo el 100% de la población, las cuales se encuentran clasificadas por dominios de la norma ISO 27001, tomando como referencia los controles de la norma ISO 27002 para el planteamiento de cada pregunta.

3.5.1. Diagnóstico de la situación actual

En esta etapa se llevará a cabo el desarrollo de diversas actividades tales como: Conclusiones & gráficos de la investigación, levantamiento de los activos, análisis de los riesgos, etc.

- **Conclusiones y gráficos de la investigación**

Pregunta Nº 1: Las peguntas establecidas corresponden al primero dominio de la norma ISO 27001 **"Políticas de Seguridad".** Preguntas en el anexo 2.

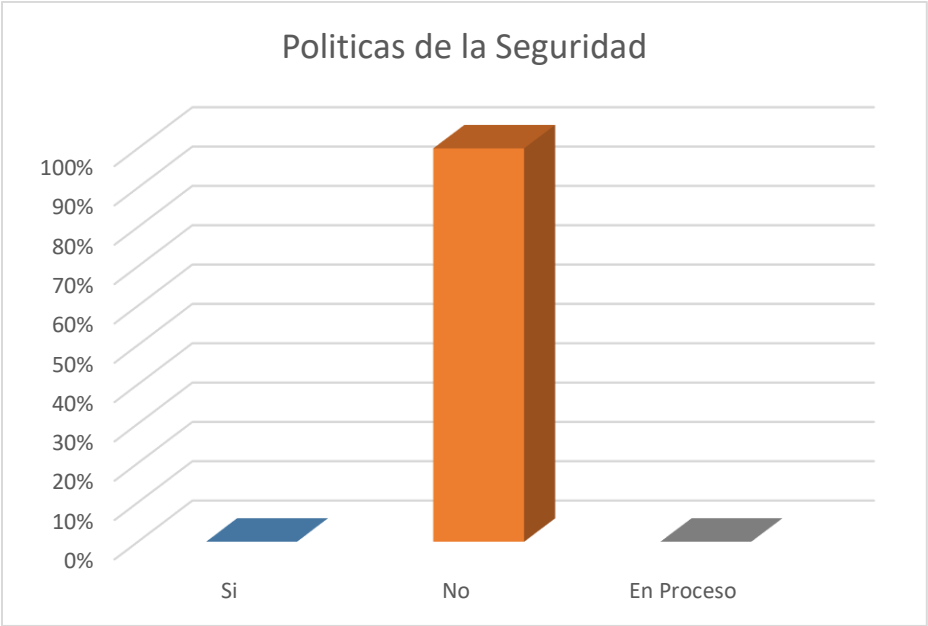


Ilustración 1: Opciones sobre el dominio Políticas de seguridad; Autor: Propio

Resultado:

Para determinar el cumplimiento del dominio se planteó 4 preguntas, 1. ¿Existe en su organización un documento que contenga las políticas de seguridad de la información? Obteniendo como respuesta NO, se pudo determinar que la municipalidad no cuenta con un manual de políticas, la encuesta completa se encuentra en el (Anexo 2). El porcentaje (100%) de la gráfica demuestra la falta de documentación por parte del GADMIET el cual genera un problema para la organización ya que quedaría expuesto a riesgos debido a la falta de conocimiento por parte del personal en cuanto al funcionamiento y manejo de activos de información al interior de la entidad.

Pregunta Nº 2: Las preguntas establecidas corresponden al segundo dominio de la norma ISO 27001 **"Aspectos organizativos de la Seguridad de la Información."** Preguntas en el anexo 2.

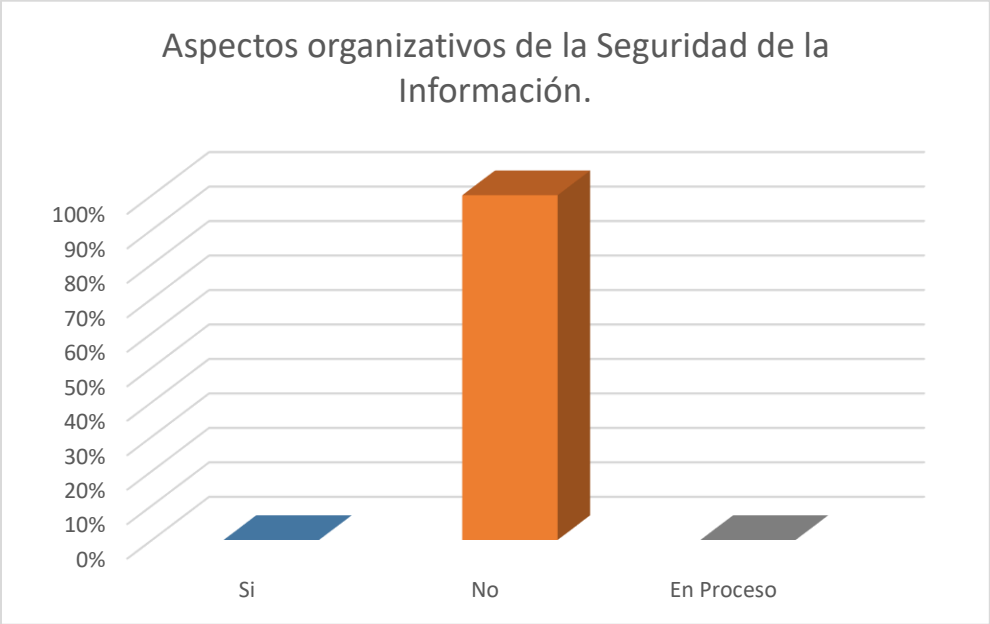


Ilustración 2: Aspecto organizativo de la seguridad de la información; Autor: Propio.

Resultado:

El presente dominio consta de 7 preguntas para determinar su cumplimento, en el cual sus respuestas lanzan que existe un (100%) de incumplimiento, debido a que, el GAMIET cuenta con un solo personal para el área de TI, el cual lleva toda la responsabilidad en cuanto a la seguridad, siendo un riesgo para la municipalidad ya que al no contar con más personal capacitado, se acumula el trabajo para uno solo y al exceso del mismos no le permitirá ejercer el control adecuado sobre los activos y sistemas de información.

Pregunta Nº 3: Las preguntas establecidas corresponden al tercer dominio de la norma ISO 27001 **“Seguridad Ligada a los Recursos Humanos.”**

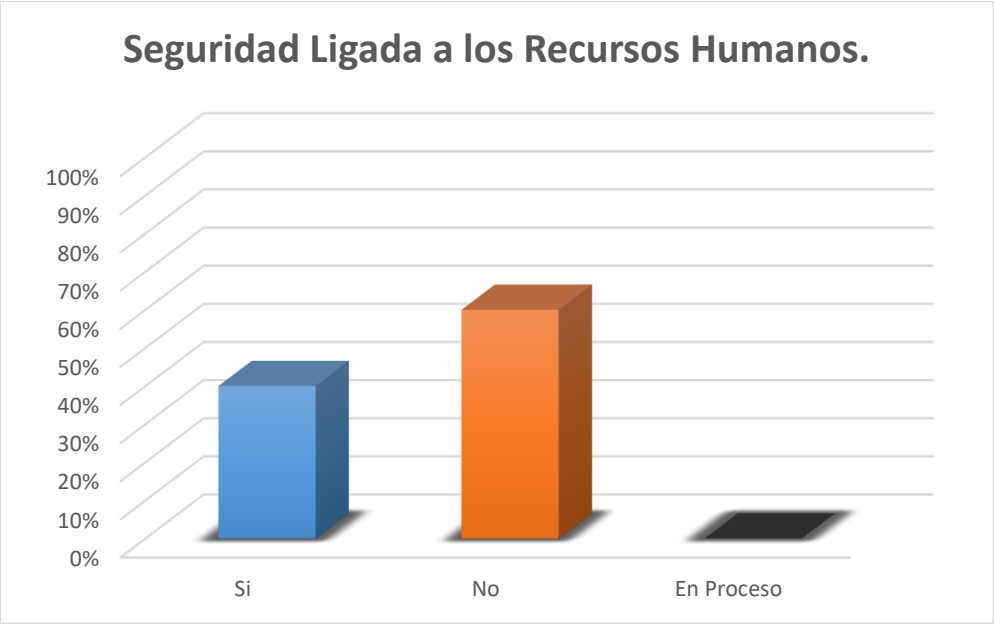


Ilustración 3: Seguridad ligada a los recursos humanos; Autor: Propio

Resultado:

De acuerdo al análisis de la encuesta aplicada, constada de 5 preguntas (Anexo 2), se pudo constatar que el (40%) se está dando cumplimiento, es decir que el GADMIET junto con el departamento de TI, siguen un proceso claro con lo que respecta a la contratación de un nuevo personal, es decir que cuentan con políticas de contratación, y se firman acuerdos de confidencialidad al ingresar a ocupar un cargo en la institución, se obtiene un (60%) de incumplimiento, debido a que no tiene definido los procesos disciplinarios para sancionar a aquellos que incumplan las políticas, no conocen los procedimientos para reporte de amenazas o cualquier otro incidente de seguridad y no se capacita al nuevo personal en lo referente a la seguridad de la información, lo que provocaría un mal manejo de los sistemas, siendo un riesgo para la institución.

Pregunta Nº 4: Las preguntas establecidas corresponden al cuarto dominio de la norma ISO 27001 **“Gestión de Activos.”**

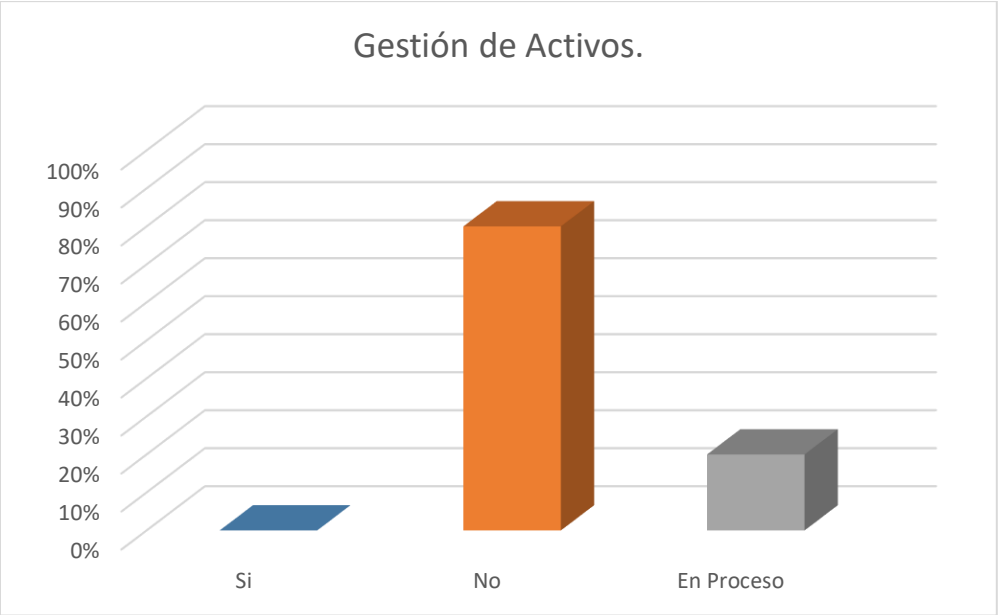


Ilustración 4: Gestión de Activos; Autor: Propio.

Resultado:

Con respecto al dominio de gestión de activos, se obtuvieron los siguientes resultados en cuanto a las 5 preguntas planteadas, el (20%) de los controles que pertenecen al presente domino se encuentran en proceso para ser ejecutadas, es decir que en cuanto a los inventarios de activos asociados a los recursos de tratamiento de información está en procesos de elaboración, el (80%) es el porcentaje de incumplimientos, no cuenta con un esquema de calificación de la información dependiendo de su grado de importancia, no se encuentran definidos con controles, procedimiento para el etiquetado y manejo de activos de información, etc., que son prioridad para una buenas administración de la entidad.

Pregunta Nº 5: Las preguntas establecidas corresponden al quinto dominio de la norma ISO 27001 **“Control de Accesos.”**

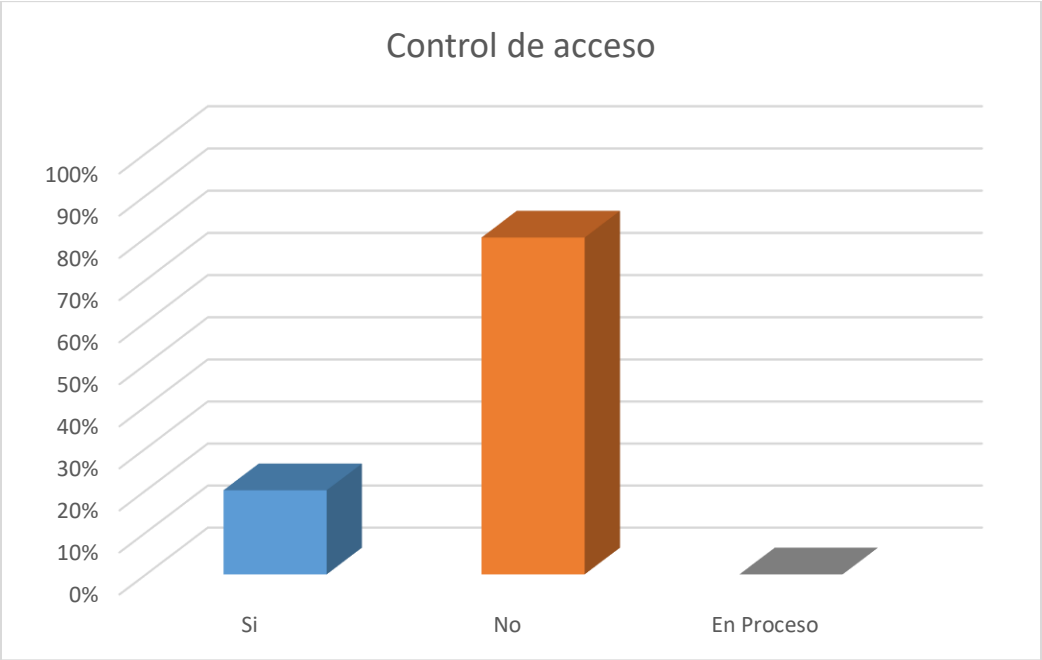


Ilustración 5: Control de Acceso; Autor: Propio

Resultado:

De acuerdo a la encuesta en base al presente dominio, se determinó que el GADMIET cumple con un 20% de los controles establecidos por este dominio, el 60% son controles que no se está aplicando en la institución, es decir que no cuentan con políticas de servicio de red, no cuentan con mecanismos y herramienta de monitoreo para detectar irregularidades en red.

Pregunta Nº 6: Las preguntas establecidas corresponden al sexto dominio de la norma ISO 27001 **“Seguridad física y ambiental.”**

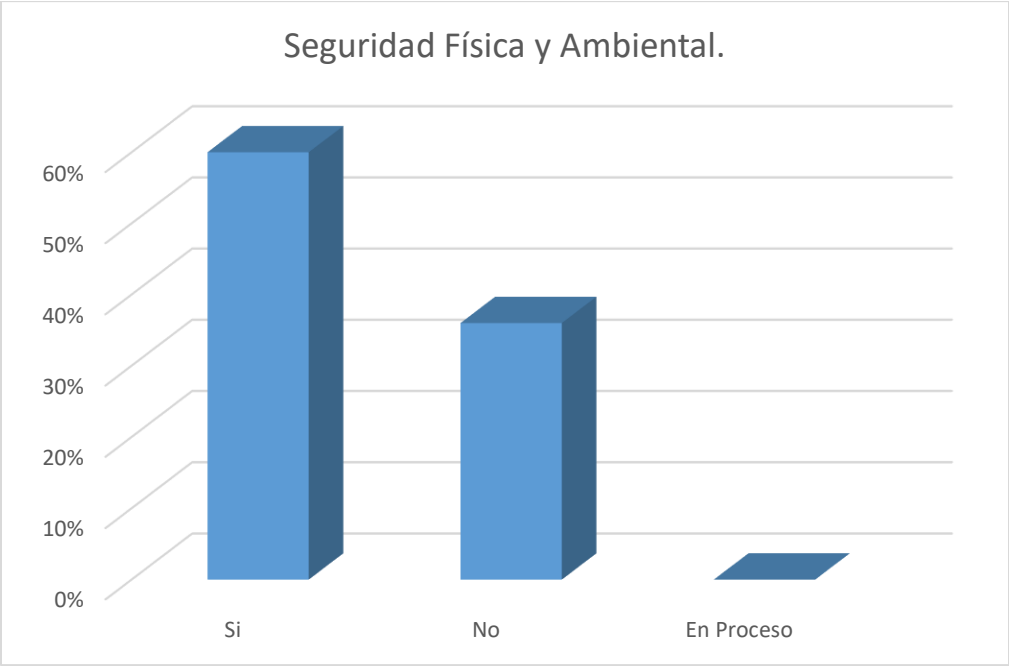


Ilustración 6: Seguridad física y ambiental; Autor: Propio.

Resultado:

Según la encuesta realizada, con lo que respecta al dominio Seguridad física y ambiental se determina que el departamento de TI cuenta con una infraestructura tecnología estable, en el cual desarrolla cada una de sus actividades como el control de los equipos y la información almacenada en ella en caso de que el equipo este previo a su desincorporación o reúso.

También se pudo constatar que, en caso de existir fallos en el cableado de datos, el equipo técnico está listo para dar solución a la misma. Por otra parte, también existe control de puntos de acceso a la organización como las áreas de entrada y salida, parqueaderos demostrando un (60%) de cumplimiento de los controles correspondiente al presente domino.

Pregunta Nº 7: Las preguntas establecidas corresponden al séptimo dominio de la norma ISO 27001 **“Seguridad en la Operativa.”**

Ilustración 7: Seguridad en la Operativa; Autor: Propio

Resultado:

De acuerdo a la encuesta en base al presente dominio, se determinó que el GADMIET cumple con un 20% de los controles establecidos por este dominio, el 60% son controles que no se está aplicando en la institución, es decir que no se tiene establecido los procedimientos y roles para el manejo de incidentes, no cuentan con controles que les ayude a prevenir o recuperar información afectadas por malware.

Pregunta Nº 8: Las preguntas establecidas corresponden al octavo dominio de la norma ISO 27001 **“Seguridad en las telecomunicaciones.”**

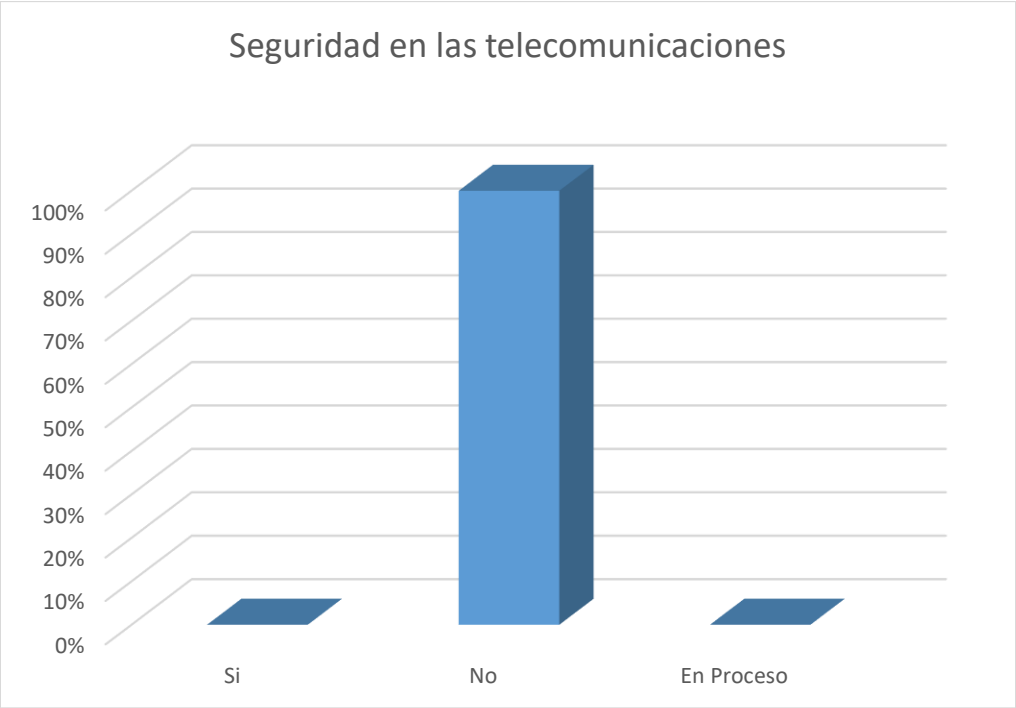


Ilustración 8: Seguridad en las telecomunicaciones; Autor: Propio.

Con lo que respecta al dominio de Seguridad en las telecomunicaciones, el GADMIET no cuenta con mecanismos, que les permita proteger la información del sistema, aplicaciones y servicios, no cuentan con un canal seguro para los vínculos de los usuarios externos, no dispone de procedimientos seguros para proteger la información que viaja a través del canal de comunicaciones instaurados con el servidor.

Pregunta Nº 8: Las preguntas establecidas corresponden al noveno dominio de la norma ISO 27001 **“Gestión de incidentes en la Seguridad de la información.”**

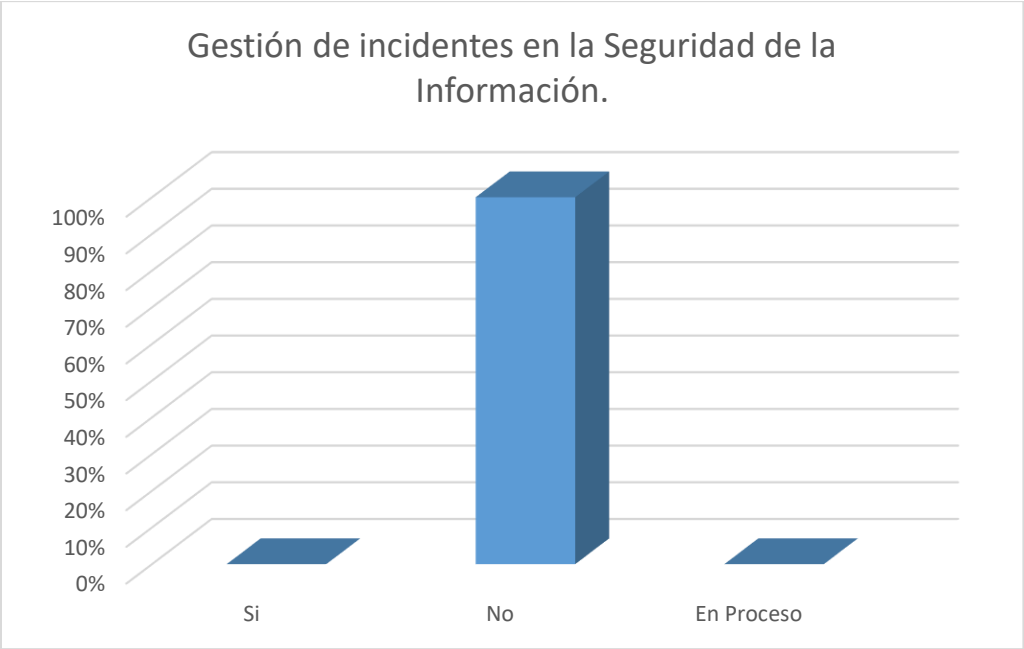


Ilustración 9: Gestión de incidentes en la seguridad de la información; Autor: Propio.

Resultado:

De acuerdo al análisis, el GADMIET no cuenta con procedimientos documentados, que le permitan comunicar, gestionar, y evaluar los incidentes de seguridad de forma inmediata. Se debería implementar mecanismos de reporte de incidentes en donde todos los funcionarios del GADMIET se comprometan a notificar los puntos débiles de la seguridad con el fin de prevenir futuros incidentes.

Pregunta Nº 8: Las preguntas establecidas corresponden al décimo dominio de la norma ISO 27001 **"Cumplimiento."**

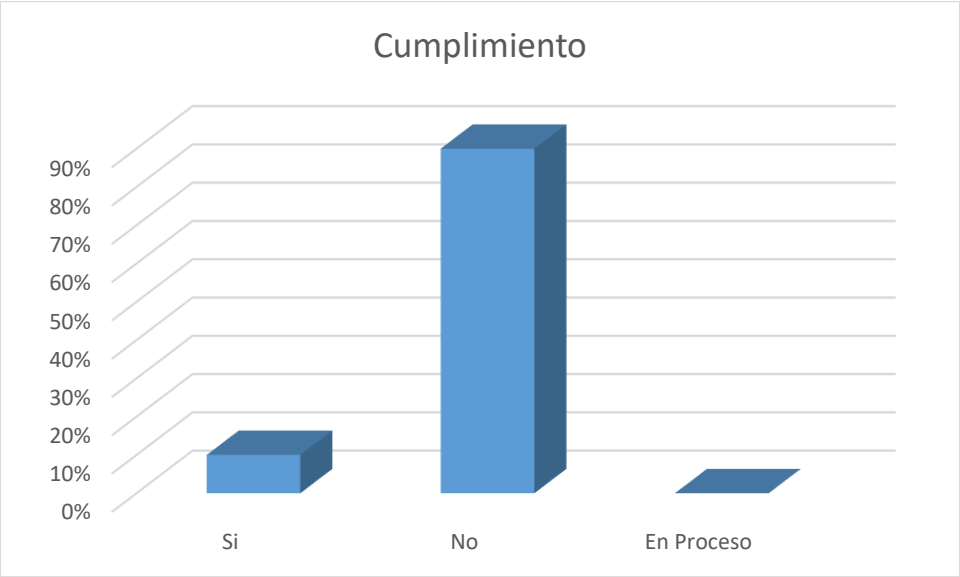


Ilustración 10: Cumplimiento; Autor: Propio

Resultado:

El GADMIET no cuenta con políticas de protección de datos, mediante el análisis a la encuesta aplicada en base al dominio de Cumplimiento, se determinó que la información manejada en la entidad es publica, cabe recalcar que el presente dominio busca comprobar el cumplimiento de las políticas y normas mencionadas anteriormente, en base al análisis realizados del 100% existe un 20% de cumplimiento de los controles respectivos por parte del Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo.

3.5.1.1. Levantamiento de activos

El departamento de TI del GADMIET cuenta con diferentes activos que son de gran importancia para el desarrollo del proyecto. Se tomará en cuenta los activos más relevantes para el tratamiento de la información.

Codigo	Descripcion	Ubicación
A	CPU, NEGRO, serie MXL1411J6Z	Alcaldia
A1	Alimentador de corriente estuche negro marca TARGUS	Alcaldia
A2	UPS-APC-4B1035P18177	Contabilidad
A3	Servidor doble nucleo core 2 DUO 2,93 GHZ	Contabilidad
A4	Licencia windows 7 Pro, 32 bit	Desarrollo Social
A5	Regulador CDP serial N0 100123-0570171	
A6	Lecttro biometrico motorola	Bodega
A7	Scanner Epson Worforce DS-560-26PPM	jefe de contratacion publica
A8	Regulador de voltaje THOR	Transporte terrestre y seguridad vial
A9	Servidor HP con dos tragetas de red SERVER HP, proliant DL360E-Gen 8 - 7-2 k -Sata 1TB 657739	Tecnico Informatico
A10	Lincencia de Checkpoit	
A11	Servidor, intel XEON E5-2609, 1.9 MHZ 32MB memoria, disco de 300, GB, 4T, DVD ROOM - POWEREDGE R430	Avaluo y catastros
A12	Disco Duro externo Toshiba	Informatica
A13	SINAT - Sistema Nacional de Administracion	Planificacion
A14	Equipo de Computo CPU INTEL CELERON-4 GB- 1TB-2.0 GHZ, QC PASS	
A15	Impresora Multifuncion wifi Epson L395	Planificacion
A16	"Monitor SONY BRAVIA de 32", Modelo KDL-32R429B/SERIAL	
A17	Computador XTRATECH CORE I3 memoria de 4GB, disc de 1 TERA, LECTOR DVD + lector de memoria	

Ilustración 11: Lista de activos del departamento de TIC (GADMIET); Autor; Propio.

3.5.1.2. Análisis de riesgo

El riesgo para la seguridad de la información es la capacidad de que una amenaza explote, de manera que pueda causar daño a un activo o varios activos, es decir que mide la probabilidad de daño de la amenaza sobre el activo.

Para el cálculo de riesgo, se debe establecer escala de valoración tanto para los activos como para el riesgo.

- *Valoración de activos*

VALOR	NIVEL	Confidencialidad	Integridad	Disponibilidad
		Acceso no autorizado al Activo de información.	Perdida de la exactitud de los Activos de Inf.	La Ausencia del Activo de Inf.
1	Muy Baja	No se genera ningún impacto negativo	No se genera ningún impacto negativo	No se genera ningún impacto negativo
2	Baja	Impacta negativamente de manera leve	Impacta negativamente de manera leve	Impacta negativamente de manera leve
3	Media	Impacta negativamente	Impacta negativamente	Impacta negativamente
4	Alta	Impacta negativamente a la entidad	Impacta negativamente a la entidad	Impacta negativamente a la entidad

Ilustración 12: Nivel de valoración de los activos; Autor: Propio.

- *Valoración de la probabilidad*

  La probabilidad es la posibilidad de ocurrencia de algún evento no deseado en cuanto a la seguridad de la información.

  A continuación, se visualiza un gráfico con el rango de valoración de la probabilidad.

Probabilidad		Descripción
Raro	1	Probabilidad de ocurrencia Muy Baja
Improbable	2	Probabilidad de ocurrencia Baja
Posible	3	Probabilidad de ocurrencia Media
Probable	4	Probabilidad de ocurrencia Alta

Ilustración 13: Valoración de la Probabilidad por nivel; Autor: Propio.

Para la valoración de los riesgos se toma en cuenta la tabla 1, en el cual se define el nivel de riesgo, los valores expuestos son tomados en base a la formula Riesgo= Valor de activo* Probabilidad de amenaza.

Tabla 1: Intervalo para determinar en nivel de riesgo; Autor: Propio

Intervalo para determinar el nivel de Riesgo		
Valor Mínimo	Valor Máximo	Nivel de Riesgo
1	6	Bajo
7	9	Medio
10	16	Alto

En base a los niveles de valoración del activo y del riesgo, se realiza una matriz de riesgo, en el cual se define todos los activos a ser analizados y las posibles amenazas a las que pueden estar expuestas tal como se visualiza en la Ilustración Nª 14 de acuerdo a los cálculos realizados, se determina que existen activos críticos las cuales deben ser protegidos mediante un tratamiento e implementación de controles.

Matriz De analisis de riesgo					Probabilidad de Amenaza [1= Insignificante; 2= Bajo ; 3= Medio; 4= Alta]							
Activos	Dimensión			Magnitud de Daño: 1= Insignifacante 2= Bajo 3= Medio 4= Alto	Compromiso de las funciones	Compromiso de la informacion	Acciones no autorizadas	Daño Fisico	Eventos Naturales	Fallas Tecnicas	Perdida de los Servicios Esenciales	Fallos no intencionados
	Confidencialidad	Integridad	Disponibilidad		2	4	2	3	2	3	4	2
CPU, NEGRO, serie MXL1411J6Z	1	1	2	4	8	16	8	12	8	12	16	8
Alimentador de corriente estuche negro marca TARGUS	1	1	2	4	8	16	8	12	8	12	16	8
UPS-APC-4B1035P18177	1	1	2	4	8	16	8	12	8	12	16	8
Servidor doble nucleo core 2 DUO 2,93 GHZ	1	1	1	3	6	12	6	9	6	9	12	6
Licencia windows 7 Pro, 32 bit	1	1	1	3	6	12	6	9	6	9	12	6
Regulador CDP serial N0 100123-0570171	1	1	2	4	8	16	6	9	6	9	12	6
Lecttro biometrico motorola	1	1	1	3	6	12	6	9	6	9	12	6
Scanner Epson Worforce DS-560-26PPM	1	0	1	2	4	8	8	6	4	6	8	4
Regulador de voltaje THOR	1	1	1	3	6	12	6	9	6	9	12	6
Servidor HP con dos tragetas de red SERVER HP, proliant DL360E-Gen 8 -7-2 k - Sata 1TB 657739	1	1	2	4	8	16	8	12	8	12	16	8
Lincencia de Checkpoit	1	1	2	4	8	16	8	12	8	12	16	8
Servidor, intel XEON E5-2609, 1.9 MHZ 32MB memoria, disco de 300, GB, 4T, DVD ROOM - POWEREDGE R430	1	1	2	4	8	16	8	12	8	12	16	8
Disco Duro externo Toshiba	1	1	1	3	6	12	6	9	6	9	6	6
SINAT - Sistema Nacional de Administracion	1	1	2	4	8	16	8	12	8	12	16	8
Equipo de Computo CPU INTEL CELERON-4 GB- 1TB-2.0 GHZ, QC PASS	1	1	1	3	6	12	6	9	6	9	12	6
Impresora Multifuncion wifi Epson L395	1	1	1	3	6	12	6	9	6	9	12	6
"Monitor SONY BRAVIA de 32", Modelo KDL-32R429B/SERIAL	1	0	1	2	4	8	4	6	4	6	8	4
Computador XTRATECH CORE I3 memoria de 4GB, disc de 1 TERA, LECTOR DVD + lector de memoria	1	1	2	4	8	16	8	12	8	12	16	8

Ilustración 14: Matriz de riesgo; Autor: Propio

Las políticas o controles de seguridad ayudan a reducir, mitigar los riesgos, es decir busca implementar acciones para gestionar los riesgos que se puedan presentar, no solo en los activos antes mencionados, sino en toda el área administrativa, financiera, RRHH, tecnológico etc., con las que cuenta una organización, para el desarrollo de la misma se toma como guía la norma ISO/IEC 27002, para la implementación de los controles pertinentes.

CAPITULO IV

PROPUESTA

4.1 Título de la Propuesta

"MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL GAD INTERCULTURAL DE EL TAMBO".

4.2 La Organización

4.2.1 Misión, Visión

Misión

"El GADMICET, es el facilitador del buen vivir con enfoque cultural, a través de los servicios públicos y comunitarios de calidad con transparencia, honestidad y vocación de servicio a los ciudadanos que son los pilares de la seguridad municipal." (EL Gobierno Autonomo Decentralizado Municipal Intercultural Comunitario Tambo-GADMICET, 2014)

Visión

"Un referente de la administración pública municipal del ecuador hacia el sumakKawsay; en donde lo intercultural, el trabajo comunitario la responsabilidad ciudadana son prácticas irreversibles de los actores territoriales." (EL Gobierno Autonomo Decentralizado Municipal Intercultural Comunitario Tambo-GADMICET, 2014).

4.2.2 Manual de políticas

Manual de Políticas de seguridad de la información

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL INTERCULTURAL
EL TAMBO - GADMIET

Elaborado Por: Carlos Chimborazo

CAÑAR - ECUADOR
2021- 2022

INTRODUCCIÓN

El Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo (GADMIET) establece la información como el activo más importante para el manejo de la entidad el cual permite el desarrollo continuo de la misión y el cumplimiento de los objetivos estratégicos. Razón por la cual, surge la necesidad de determinar políticas que ayuden a proteger la confidencialidad, integridad y la disponibilidad de la información.

Con la evolución de nuevas tecnologías de la información los GAD optan por servicios tecnológicos para optimizar sus procesos, el uso y el manejo inadecuado de estas tecnologías han ocasionado problema a las organizaciones ya que son vulnerables a las amenazas que se presentan en el medio, las mismas que pueden convertirse en riesgo y afectar enormemente la integridad de la información.

El objetivo del desarrollo del presente manual es establecer las políticas que integran el sistema de gestión de seguridad de la información SGSI para el Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo, las mismas deben ser socializados y adaptados por los funcionarios y todo el personal que presten servicios al GADMIET, el desarrollo de estas políticas están orientadas y basadas en los controles y requisitos identificados en el estándar ISO/IEC 27001 y la guía de buenas prácticas ISO 27002.

Las políticas descritas en el presente manual se constituyen como parte fundamental para el cumplimiento misional de la entidad, y se convierte en una base para la implantación de los controles, procedimientos para la mejora de la organización, por ende, es deber de los funcionarios del GADMIET velar por el cumplimiento de las políticas definidas en el presente documento y no realizar actividades que vayan en contra de los mismos.

OBJETIVO

Establecer las políticas de la seguridad de la información para el Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo, con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información.

ALCANCE

El presente documento define las políticas de seguridad de la información las cuales cubren todos los aspectos administrativos y de control que deben ser cumplidos por los funcionarios que laboren en el GADMIET, con la finalidad de mantener una apropiada protección de la información.

ESTRUCTURA ORGANIZACIONAL

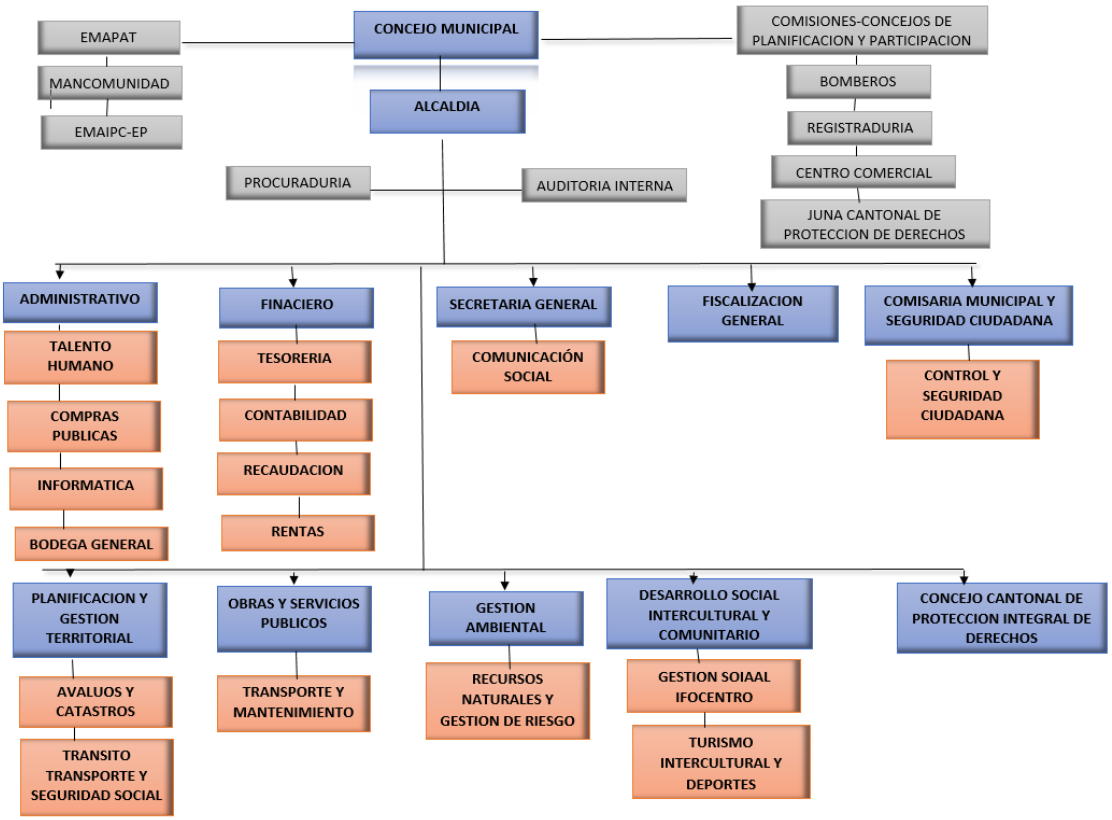


Ilustración 15: Estructura Organizacional - GADMIET; Autor: Propio.

MARCO CONCEPTUAL

Seguridad de la Información: La seguridad de la información es la protección de la integridad, disponibilidad y confidencialidad de la información, según el nivel requerido para los objetivos de negocio de la empresa. [1]

Sistema de Gestión de la seguridad de la información (SGSI): Frente a la dependencia de los sistemas de información y al crecimiento de las amenazas existentes, se hace necesario para las organizaciones establecer un Sistema de 1gestion de Seguridad de la Información. Hay que tener en cuenta una premisa fundamental: la seguridad no es un producto, es un proceso; por tanto, la seguridad no puede comprarse, pero puede gestionarse. [1]

Activos de información: Los activos de información son cualquier componente sean esta (humanos, tecnológicos, software, documental o de infraestructura) que soportan uno o más procesos de negocios de cualquier organización que ameritan ser protegidos para el funcionamiento del mismo. [5]

Políticas de Seguridad: El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de una organización, y en particular al involucrado directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados. [8]

ISO: Organización Internacional de Normalización, Es una agrupación de organizaciones nacionales de normalización el cual tiene como objetivo establecer, proporcionar y gestionar estándares las cuales pueden ser implementados para la mejora de las organizaciones.

Norma ISO/IEC 27001: La norma establece los requisitos que debe cumplir un SGSI (sistema de Gestión de la Seguridad de la Información) para su certificación en términos de procesos de seguridad a nivel organizativo. [9]

Norma ISO/IEC 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, esta norma no es certificable. Contiene 35 objetivos de control y 114 controles agrupados en 14 dominios. [10]

RESPONSABILIDAD Y CUMPLIMIENTO DEL MANUAL

Teniendo en cuenta que el presente manual es solo una propuesta para el GADMIET, se definen algunas responsabilidades en caso de existir aplicabilidad de la misma.

- La alta gerencia del GADMIET es el encargado de apoyar el proceso de implementación de las políticas de seguridad de la información.
- El encargado del departamento de TIC es responsable de realizar un seguimiento de la implementación de las políticas, supervisar al personal a su cargo para garantizar que les dé debido cumplimiento y brindar apoyo cuando sea necesario.
- El departamento de TIC demostrara compromiso en la divulgación de este manual de políticas a todos los funcionarios de la institución.
- El departamento de TIC tiene la obligación de verificar periódicamente el cumplimiento de las políticas de seguridad de la información.
- También se le designa la responsabilidad al departamento de TIC, para su debida revisión del presente manual, ya sea por actualización o mejoras.

Regulación

Las políticas descritas en el presente documento deberán ser conocidas, acepadas y cumplidas por todo el personal del GADMIET. El incumplimiento de las mismas se considerará un incidente de seguridad, que de acuerdo con el caso podrá dar lugar a un proceso disciplinario interno para los funcionarios.

1. **POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADMIET**

Toda información manejada en el Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo es considerado activo de gran valor, ya que gracias a ello se hace posible la prestación de servicio a la ciudadanía del cantón El Tambo y sus alrededores, de la misma manera ayuda en la toma de decisiones para posibles mejoras de la municipalidad o el cantón.

Todo funcionario que tenga responsabilidad sobre los recursos del procesamiento de información del GADMIET deben tener en cuenta los lineamientos contenidos en el presente manual, con el fin de mantener la confidencialidad, integridad y disponibilidad de la información de su dependencia.

Las políticas de seguridad de la información propuestas para el GADMIET se fundamentan en los dominios y objetivos de control de la norma internacional ISO 27001:2013.

El personal encargado de la seguridad de la información tiene la potestad de aplicar este manual o en su defecto a ser necesario modificar las políticas según revisiones en un tiempo determinado.

1.1. POLÍTICAS DE SEGURIDAD

1.1.1. Directrices de la dirección en seguridad de la información

La alta gerencia del GADMIET debe apoyar la seguridad de la información, con el debido cumplimiento de las leyes y reglamentos adecuados.

1.1.1.1. Conjunto de políticas para la seguridad de la información

Las políticas deberán ser definidas en base a las necesidades identificadas en el análisis de riesgo, las cuales debe estar aprobadas y comunicadas a todo el personal involucrado ya sea interna o externa a la institución.

1.1.1.2. Revisión de las políticas para la seguridad de la información

Mediante este control se da un seguimiento para verificar que las políticas de seguridad de la información sean definidas, implementadas, que se cumpla con su debida revisión y actualización.

1.2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

1.2.1. Organización Interna GADMIET

- El Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo junto con el departamento de TIC deben establecer un diseño de seguridad de la información en donde se encuentre contemplado los roles y responsabilidades que consideren necesarios para la gestión de la seguridad de la información.
- El departamento de TIC debe mantener contacto con organizaciones externas relacionadas con la seguridad de la información que de una u otra manera aporten a la gestión de riesgos que pueden ser identificados.

- El desarrollo de nuevos proyectos del GADMIET en cuanto a la seguridad deben contemplar una gestión de riesgos, con la finalidad de identificar los riesgos y definir su tratamiento.
- También se pone a consideración de alinear las políticas de seguridad de la información contenida en el presente manual en futuros proyectos a desarrollarse.

1.2.1.1. Asignación de responsabilidades para la seguridad de la información.

Cada activo de información del GADMIET debe poseer un dueño quien deberá velar por su seguridad, de la misma manera los dueños de la información son los únicos responsables de afirmar que la información manejada dentro de la institución cuente con las políticas para su respectiva protección y así mantener la confidencialidad, integridad y privacidad de la información.

1.2.1.2. Contactos con las Autoridades

Los encargados de la seguridad deberán mantener contacto con las autoridades especializadas en dicha área, que ayuden a solucionar inconvenientes surgidas en cuanto a la seguridad de la información de la institución.

1.2.1.3. Seguridad de la información en la gestión de proyectos

Para la gestión de nuevos proyectos dentro del GADMIET se deberá tomar en cuenta o hacer partícipe al área de la seguridad de la información, basado en ello se podrá analizar y evaluar los riesgos inherentes, por lo que se convierte en un pilar fundamental para la ejecución de la misma.

1.2.1.4. Teletrabajo

El departamento de TIC deberá garantizar que las conexiones de teletrabajo se efectúan de forma segura, es decir que toda información en uso se encuentre seguro, también deberán contar con todos los softwares necesarios para protegerla de los ataques.

1.3. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

1.3.1. Antes de la Contratación

1.3.1.1. Investigación de antecedentes

Los candidatos previos a ocupar un cargo en el municipio deberán pasar por un proceso de investigación y verificación de antecedente, esto en base a las leyes, reglamentos vigentes en el GADMIET.

1.3.1.2. Términos y Condiciones de contratación

Los candidatos a ocupar un puesto en la institución deberán firmar un contrato en donde se especifique los acuerdos de seguridad, en el que se les informara la existencia de políticas contenidas en el presente Manual y las responsabilidades otorgadas por la institución en relación a la seguridad de la información. Dicho contrato deberá estar archivada con los demás documentos de contratación.

1.3.2. Durante la contratación

Asegurarse que todo empleado que labore en la entidad, conozca sus responsabilidades de seguridad y las mimas estén en correcto cumplimiento.

1.3.2.1. Responsabilidades de gestión

El departamento de TIC debe instruir la importancia de la seguridad de la información a todo el personal involucrado del GADMIET, de la misma manera incitar a la toma

de conciencia de sus responsabilidades de seguridad desde el ingreso hasta su retiro y el cumplimiento de las políticas, normas y estándares establecidos.

1.3.2.2. Concienciación, educación y capacitación en seguridad de la información

La alta gerencia en conjunto con el departamento de TIC deberá organizar charlas, capacitaciones relacionadas a la seguridad de la información, la misma que se puede llevar a cabo de manera anual y en caso de existir actualizaciones regulares de las políticas y demás procedimientos el programa de capacitación se lo realizará constantemente.

Los empleados que hagan uso de la información en base a su cargo en la institución, deberán cumplir con lo indicado en el presente manual y asistir a las charlas y capacitaciones que se efectúen.

1.3.3. Cese o cambio de puesto de trabajo

Cada empleado debe estar informado de las responsabilidades que deben cumplir en caso de cambio o abandono de puesto de trabajo. El líder o jefe de departamento está en la obligación de dar a conocer al departamento de Recursos Humanos, el cambio o abandono del puesto de los empleados, de manera qué se pueda tomar una decisión.

1.4. GESTIÓN DE ACTIVOS

1.4.1. Responsabilidad sobre los Activos

Identificar los activos tanto del departamento de TIC como de la institución en general, estos activos deberán ser asignados a un personal responsable, documentados, inventariados y clasificados según sea necesario.

1.4.1.1. Inventario de Activos

Cada jefe de departamento deberá generar un inventario de activos de información para su respectiva área a la que este laborando, el responsable de dichos activos deberá clasificarlas respectivamente ya sea basándose en su valor, riesgos de pérdida o los requerimientos legales que estas requieran.

1.4.1.2. Propiedad de los activos

El departamento de TIC deberá realizar la respectiva inspección al inventario de activos de información, en caso de existir actualizaciones o se requiera establecer las responsabilidades sobre cada una de ellas.

Los activos de información deben ser utilizados por toda la institución de acuerdo con las políticas determinadas en el presente manual o normativas establecidas en la institución con la finalidad de evitar el impacto en los mismos.

1.4.1.3. Devolución de los activos

Todo funcionario al culminar o abandonar el puesto de trabajo, debe devolver todos los activos de información entregados al momento de ocupar su cargo. Se deberá firmar un acta de entrega por ambas partes al momento de la devolución.

1.4.2. Clasificación de la Información

La entidad definirá los niveles más apropiados para clasificar su información, de acuerdo a su importancia y el departamento de TIC será el encargado de determinar los controles necesarios para su protección, con el fin de preservar la confidencialidad, integridad y disponibilidad de dichos activos.

1.4.2.1. Directrices de clasificación

Para cumplir con la clasificación respectiva de la información se cuenta con las siguientes prioridades.

Publica: Información compartida a todos los usuarios de la municipalidad.

Uso Interno: Información netamente institucional.

Información confidencial: Información de interés solo por departamentos.

1.4.2.2. Manipulación de Activos

Todo Activo de información clasificada debe contener los siguiente:

Nombre del activo de información, proceso a la que se encuentra inmerso, nivel de sensibilidad.

El jefe del departamento de TIC podrá determinar el nivel de clasificación en caso de existir clasificados los mimos activos en niveles diferentes.

1.4.3. Manejo de los soportes de almacenamiento

La institución establecerá procedimientos necesarios para el manejo de los soportes de almacenamiento, evitando la divulgación o eliminación de la información almacenada.

1.5. CONTROL DE ACCESO

1.5.1. Requisitos del negocio para el control de acceso

El departamento de TIC bebe restringir el acceso a terceras personas a instalaciones de procesamiento de información.

1.5.1.1. Políticas de control de acceso

La municipalidad garantizara la implementación y el correcto funcionamiento de mecanismos de seguridad física, controles para el acceso físico, escenarios medioambientales requeridas y necesarias para el buen funcionamiento de las

plataformas tecnológicas, de manera que se pueda controlar las amenazas físicas, accesos no autorizados.

1.5.1.2. Control de acceso a las redes y servicios asociados

El departamento de TIC debe controlar el acceso a la red de la institución, mediante la implementación de mecanismos de identificación y autentificación que eviten los accesos no autorizados a la red.

Los usuarios externos y funcionarios de la institución que deseen que los equipos electrónicos personales tengan acceso a la red de la entidad, deben cumplir con todos los requisitos para su debida autentificación.

1.5.2. Gestión de acceso de usuarios

1.5.2.1. Gestión de altas y bajas en el registro de usuarios

Se debe establecer por el departamento de TIC, los procedimientos que afirmen la eliminación o bloqueo de privilegios de acceso a los sistemas y servicios de información. Se debe asegurar de la misma manera la inhabilitación o eliminación de usuarios que tengan asignados tales recursos tecnológicos.

1.5.2.2. Gestión de los derechos de acceso con privilegios especiales.

Los usuarios que tengan el acceso a los servicios tecnológicos, serán responsables en el uso de dichos servicios, ya que es su obligación salvaguardar la información a las cuales se tiene acceso autorizado. Mantener en secreto las claves de acceso asignado a estos servicios.

1.5.3. Responsabilidades del usuario

1.5.3.1. Uso de información confidencial para la autenticación

Todo usuario autorizado para el acceso a los recursos tecnológicos de la institución es responsable de las operaciones realizadas en las mismas. Por ende, la identificación de cada usuario debe ser determinada de forma única y segura.

1.5.4. Control de acceso a sistemas y aplicaciones

1.5.4.1. Restricción del acceso a la información

Todo usuario que labore dentro de la institución y terceras personas a las cuales se les fue asignado las credenciales para el acceso a los servicios de red, deben ser responsables en el uso que les den a esos recursos.

Toda persona que ingresa a las instalaciones y sobre todo la infraestructura tecnológica del GADMIET, debe contar con un identificador único y personalizado.

1.5.4.2. Procedimientos seguros de inicio de sesión

El departamento de TIC debe implementar mecanismos necesarios para proteger los servicios tecnológicos de los ataques forzosos en los intentos de inicio de sesión, cada denegación en intentos de inicio de sesión deberá visualizar un mensaje de advertencia indicando que no tiene los permisos necesarios para accedes a dichos servicios.

1.5.4.3. Gestión de contraseñas de usuario

Al crear una contraseña deben contar con lo siguiente:

Las claves o contraseñas deberán tener un nivel aceptable de complejidad, compuestas por mínimo 8 a 10 caracteres alfanuméricos, no deben ser palabras que sean de información personal.

Es recomendable cambiar la clave de acceso a la red y demás sistemas de información cada cierto tiempo.

El departamento de TIC debe implementar controles para bloquear el acceso a la red después de 3 intentos fallidos de ingreso de la contraseña.

1.6. SEGURIDAD FÍSICA Y AMBIENTAL

1.6.1. Áreas Seguras

La institución debe implementar mecanismos de seguridad física, para evitar el acceso no autorizado a las instalaciones, controlar las amenazas externas e internas de origen físico, para garantizar la seguridad de las áreas de cualquier factor de riesgo.

1.6.1.1. Protección contra amenazas externas y ambientales

La institución debe contar con sistemas de control ambiental de temperatura, humedad, detección de incendios, sistemas de descarga eléctrica, sistemas de vigilancia, monitoreo y alarmas en caso de presentarse manifestaciones de fenómenos climáticos que puedan provocar daños a las instalaciones.

El departamento o personal encargado de los centros de procesamiento de datos y centros de cableado de la institución, debe vigilar que todo el recurso de la plataforma tecnológica, se encuentren resguardados contra fallas o paralización eléctrica. También deberán realizar mantenimientos y pruebas de funcionalidad de UPS.

1.6.2. Seguridad de los equipos

1.6.2.1. Emplazamiento y protección de equipos

Todo funcionario de la municipalidad ara uso de los equipos tecnológicos asignados únicamente para el cargo que desempeña en la entidad.

Todos los recursos tecnológicos de la institución deben contar con mecanismos de seguridad física para protegerlo contra amenazas de acceso no autorizado, ambientales para evitar daños o perdida de los activos.

1.6.2.2. Seguridad del cableado

El departamento de TIC debe contar con un modelo de croquis con lo que respecta a las conexiones de cableado, para facilitar la identificación de los elementos conectados y evitar desconexiones erróneas. Garantizar que los centros de cableado se encuentren aislados de las áreas que corran riesgo de inundación e incendios.

1.6.2.3. Mantenimiento de los equipos

El departamento de TIC o técnicos autorizados bebe ser los únicos en realizar los servicios de mantenimiento y reparación de los equipos informáticos de la entidad.

Todo empleado que maneje información relevante para el funcionamiento de la institución deberá realizar un Backup de dicha información, en caso de deterioro de los equipos informáticos.

1.7. SEGURIDAD EN LAS OPERATIVA

1.7.1. Responsabilidades y procedimientos de operación

El departamento de TIC debe contar con la debida documentación de los procedimientos relacionados con la operación y administración de los sistemas de información de la entidad. Evitar las interferencias a la información de la institución y el acceso no autorizado a las infraestructuras tecnológicas.

1.7.2. Protección contra códigos maliciosos

1.7.2.1. controles contra el código malicioso

Todo equipo de cómputo de la institución debe contar con una licencia de antivirus actualizado, el cual garantice la protección de la información, mediante el uso de software de antivirus se debe realizar un chequeo en un tiempo determinado para verificar que los archivos contenidos en dichos equipos se encuentren libre de virus y protegidos ante ataques de software malicioso.

El personal del GADMIET en caso de sospechas de virus en los equipos, deberán suspender las tareas realizadas e informar al departamento de TIC, para su respectiva limpieza y eliminación del virus.

1.7.3. Copias de seguridad

1.7.3.1. Copias de seguridad de la información

La institución en conjunto con el departamento de TIC es responsable de la ejecución de copias de respaldo y almacenamiento de su información confidencial, estableciendo las operaciones necesarias y definiendo las estrategias a seguir para el cumplimiento de estas actividades.

El departamento de TIC es responsable de garantizar la integridad física de los respaldos, en caso de robo, destrucción o perdida, deberá contar con procedimientos necesarios para el debido cumplimiento.

1.7.4. Registro de actividades y supervisión

1.7.4.1. Registro de gestión de eventos de actividad

La institución y el área de TIC son los responsables de llevar a cabo el proceso de revisión del uso que le dan los funcionarios a los recursos de los sistemas

tecnológicos, el departamento de TIC definirá el tiempo que crea conveniente realizar el monitoreo de los registros de auditoría sobre los aplicativos donde se ejecutan los procesos de la institución.

1.7.4.2. Protección de los registros de información

Todos los registros de auditoria generados en la entidad deberán ser protegidos y accedidos solo por el personal autorizado, con el fin de preservar la integridad y disponibilidad de los mismos.

1.7.5. Control de Software en explotación

1.7.5.1. Instalación del software en sistemas en producción

El departamento de TIC será el encargado de elegir a un personal responsables el cual se encargará de llevar un control adecuado de las instalaciones de software en los equipos informáticos de la institución, al presentarse nuevas versiones de software se deberá realizar pruebas de actualización para certificar el correcto funcionamiento de los sistemas de información y demás herramientas de software que se ejecutan en dichos equipos.

1.7.6. Gestión de la vulnerabilidad técnica

1.7.6.1. Gestión de las vulnerabilidades técnicas

La institución en conjunto con el departamento de TIC se encargará de realizar un monitoreo de todos los sistemas y aplicaciones en un tiempo determinado para detectar vulnerabilidades que puedan materializar una amenaza y provocar un riesgo crítico para la organización, con el fin de poder mitigar dichas vulnerabilidades.

1.7.6.2. Restricción sobre la instalación de software

Todo software que se desee instalar en los equipos informáticos de la institución, deberá ser con la debida autorización del departamento de TIC o solicitar al mismo departamento a que se realice la instalación respectiva.

1.8. SEGURIDAD EN LAS TELECOMUNICACIONES

1.8.1. Gestión de seguridad en las redes

1.8.1.1. Controles de Red

El departamento de TIC en conjunto con la dirección de la institución implementará mecanismos de seguridad para evitar posibles amenazas que puedan afectar las instalaciones de procesamiento de información de la institución, de igual modo salvaguardará la integridad, confidencialidad de la información que se remite a través de las redes de datos.

De la misma manera el departamento de TIC deberá implementar controles para la reducción de riego que se puedan presentar en la información transportada por la red, todos los servicios, protocolos y puertos autorizados en la red de la institución deberán ser documentados respectivamente.

1.8.2. Intercambio de información con partes externas

1.8.2.1. Políticas y procedimiento de intercambio de información

Para el intercambio de información, la institución deberá establecer acuerdos de confidencialidad de información con personas o entidades externas que ejerzan dicho proceso. El departamento de TIC garantizará la seguridad y protección de información en el momento del intercambio o transferencia.

1.8.2.2. Mensajería electrónica

El departamento de TIC deberá velar por la seguridad de la mensajería electrónica, ya que al ser un servicio indispensable en el intercambio de información de la institución con sus usuarios es importante que el intercambio este cifrado, para evitar riesgo de suplantación la identificación de cada usuario deberá ser generado de forma segura es decir que los usuarios y contraseñas deben enviarse y almacenarse cifrados.

1.9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

1.9.1. Gestión de incidentes de seguridad de la información y mejoras.

1.9.1.1. Responsabilidades y procedimientos.

Los funcionarios de la entidad promoverán el reporte de incidentes que sean relacionados con la seguridad de la información, en el cual, estarán inmerso cualquier tipo de almacenamiento de información, tanto físicos como lógicos. Con lo que respecta al tratamiento de los mismos el GADMIET asignara un responsable calificado para el tratamiento de los incidentes de seguridad de la información, quienes deberán investigar y solucionar los incidentes reportados.

El personal designado por el GADMICET, será el único autorizado para reportar incidentes de seguridad ante la autoridad

1.9.1.2. Notificación de los eventos de seguridad de la información

Los empleados del GADMIET que manejen a su cargo información de gran importancia deberán informar de manera urgente al departamento de TIC, los incidentes de seguridad que se identifiquen, con el fin de que esto lleguen a materializarse.

1.10. CUMPLIMIENTO

1.10.1. Cumplimiento de los requisitos legales y contractuales

1.10.1.1. Identificación de la legislación aplicable

El departamento de TIC debe contar con documentación de los requisitos legales y contractuales de la seguridad de la información aplicables a la institución.

La institución en conjunto con el departamento de TIC, deberán garantizar el cumplimiento de las legislaciones de seguridad de la información, como el derecho de autor y propiedad intelectual, de modo que todo software que se manejan en la municipalidad se encuentre protegidos por dichas legislaciones y requiera licencia de uso.

1.10.1.2. Protección de los registros de la organización

La alta gerencia del GADMIET debe mantener actualizado los requisitos legales y contractuales de la organización, con el fin de evitar pérdidas, destrucción o falsificación de dichos registros.

1.10.1.3. Protección de datos y privacidad de la información personal

La institución velará por la seguridad de la información personal de todos los funcionarios y usuarios que se encuentren registrados y almacenados en la base de datos de la institución, dicha información será utilizada para funciones propias de la entidad.

1.10.2. Revisiones de la seguridad de la información

1.10.2.1. Revisión independiente de la seguridad de la información

La institución y el departamento de TIC deben llevar acabo revisiones periódicas de las políticas de seguridad de la información, para generar actualizaciones si en caso lo amerite. Los controles que se establezcan deberán ser las que corresponde a la

norma con la que fue desarrollado el presente manual la ISO 27001 y la guía de buenas prácticas ISO 27002.

1.10.2.2. Cumplimiento de las políticas y normas de seguridad

El departamento de tecnología de información y comunicación (TIC) debe velar por el debido cumplimiento del manual de políticas de seguridad de la información, en caso de violación de políticas de seguridad, la institución tomara acciones según el caso lo requiera.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Con el desarrollo de este proyecto, se logró identificar el estado actual del Gobierno Autónomo Descentralizado Municipal Intercultural Comunitario el Tambo en relación con la gestión de seguridad de la información, para ello se planteó una encuesta con los controles de la ISO 27002, en el cual se puedo estimar el porcentaje de cumplimiento en un 50% de acuerdo a los 14 dominios de seguridad, cabe mencionar que existieron controles se su porcentaje de cumplimiento fuero el 0%.

En los resultados del parámetro del cumplimiento actual del departamento de TI, se pudo constatar que los puntos más débiles son la falta de políticas de seguridad, lo que conlleva a una falta de revisión y verificación del cumplimiento.

Las encuestas planteadas en base a la norma ISO 27001 permitiendo desarrollar una propuesta de manual de políticas de seguridad de la información, ajustadas a los resultados obtenidos en el diagnostico previamente realizado, obteniendo todas las particularidades necesarias del departamento de TI del GADMICET, con el fin de valorar los riesgos y amenazas, construyendo un manual basado en las necesidades de la municipalidad.

El manual de Seguridad de la información desarrollado en este trabajo necesita actualización según el caso lo requiera, la implementación de este manual depende del apoyo de la alta gerencia y personal del departamento de TIC del GADMICET ya que serán los encargados de su difusión y acatamiento del mismo.

Recomendaciones

- Se recomienda que en un futuro se desarrollen otros proyectos tomado como referencia a lo expuesta en el presente trabajo.
- Se recomienda revisar la documentación del manual de políticas al menos una vez por año con el fin de mantener la eficacia de las políticas ya que pueden darse cambios en los requerimientos de seguridad de manera que este documento se encuentre actualizado.
- Se recomienda al departamento de TIC del GADMICET controlar el cumplimiento del presente manual para un mejor desempeño de las políticas.
- Capacitar a todo el personal de la institución sobre las políticas de seguridad de la información, para que sean conscientes de sus obligaciones y sanciones en caso de incumplimiento de dichas políticas

REFERENCIAS

Aguilera Lopez, P. (2010). *Seguridad Informatica* . Editex.

Aguilera López, P. (s.f.). *Seguridad informática.* Editex.

AREITIO BERTOLIN, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Paraninfo.

Cabrera Cubas, H. P. (Noviembre de 2018). *https://repositorio.upeu.edu.pe/.* Obtenido de https://repositorio.upeu.edu.pe/bitstream/handle/UPEU/1542/Henry_Tesis_Licenciatura_2018.pdf?sequence=5&isAllowed=y

CASTRO GIL , M. A., DÍAZ ORUETA, G., ALZÓRRIZ ARMENDÁRIZ, I., & SANCRISTÓBAL RUIZ, E. (2014). *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES.* Madrid.

EL Gobierno Autonomo Decentralizado Municipal Intercultural Comunitario Tambo-GADMICET. (01 de 01 de 2014). *docplayer.es.* Obtenido de https://docplayer.es/16931446-El-gobierno-autonomo-descentralizado-municipal-intercultural-comunitario-el-tambo-gadmicet-considerando.html

Escuela Tecnologica Instituto Tecnico Cnetral. (01 de 02 de 2021). *etitc.edu.co.* Recuperado el 21 de 09 de 2021, de https://www.etitc.edu.co/archives/calidad/GSI-MA-01.pdf

Francisco, L. C. (01 de 01 de 2019). *dspace.uce.edu.ec.* Obtenido de http://www.dspace.uce.edu.ec/bitstream/25000/18451/1/T-UCE-0011-ICF-122.pdf

Galisteo Pradillo, I. (2014). *MF0975_2 - Técnicas de recepción y comunicación.* ELEARNING S.L.

INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR. (01 de 10 de 2014). *portal.icetex.gov.co.* Recuperado el 2021

de 09 de 2021, de https://portal.icetex.gov.co/Portal/docs/default-source/documentos-el-icetex/biblioteca/manuales-de-la-entidad/manual-de-pol%C3%ADticas-de-seguridad-de-la-informaci%C3%B3n.pdf?sfvrsn=2

ISO 27000. (01 de 01 de 2005). *iso27000.es*. Recuperado el 19 de 08 de 2021, de https://www.iso27000.es/iso27000.html

Lema Pazmiño, G. X. (2017). *http://dspace.udla.edu.ec/.* Obtenido de http://dspace.udla.edu.ec/bitstream/33000/7650/3/UDLA-EC-TIRT-2017-06.pdf

Lorena, C. A. (s.f.). Seguridad informática y seguridad de la informacion. Colombia.

Miguel Pérez, J. C. (2015). *Protección de Datos y Seguridad de la Información.* Madrid: RA-MA S.A.

Orellana, R. V. (01 de 01 de 2017). *repositorio.uide.edu.ec.* Obtenido de https://repositorio.uide.edu.ec/bitstream/37000/1746/1/T-UIDE-1142.pdf

Sánchez Garreta, J. S. (2003). *Ingeniería de proyectos informáticos: actividades y procedimientos.* Publicacions de la Universitat Jaume I.

Veiga, J. M. (2020). *Perito Judicial en Seguridad física y lógica de un sistema de información.* José Manuel Ferro Veiga,.

ANEXOS

Anexo 1: Anteproyecto

Trabajo de Titulación

Tema:

Manual de Políticas de Seguridad de la Información basado en la norma ISO 27001 en el Gad Intercultural de El Tambo.

Unidad Académica

Tecnologías de la Información y la Comunicación

Carrera

Ingeniera de Sistemas

Alumno

Carlos Francisco Chimborazo Quizhpi

Tutor:

Ing. Cristian Flores

Abril – Agosto-2021

Cañar, 08 de marzo de 2021

Ingeniero
Leopoldo Pauta Ayabaca, Msc.
DECANO DE LA UNIDAD ACADÉMICA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Ciudad.

Yo**, CARLOS FRANCISCO CHIMBORAZO QUIZHPI** con número de identificación **0302362645**, alumno de la carrera de Ingeniería de Sistemas, solicito por su intermedio a Consejo Directivo la aprobación del tema de tesis **"MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL GAD INTERCULTURAL DE EL TAMBO",** proponiendo como tutor de la misma al Ing. Cristian Flores Urgilés, el tema propuesto está considerado su desarrollo en décimo ciclo, ya que estaré matriculada en la Unidad de Titulación.
Por la atención que Ud. y el Honorable Consejo Directivo le brinden a la presente, anticipo

mis sentimientos de consideración y estima para cada uno de Uds.

Atentamente;

SR. CARLOS FRANCISCO CHIMBORAZO QUIZHPI
Estudiante de Ingeniería de Sistemas, extensión Cañar
CI: 0302362645

Anexo: Formato del Anteproyecto.

A. TÍTULO
Manual de Políticas de Seguridad de la Información basado en la norma ISO 27001 en el Gad intercultural de El Tambo

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	Analítica de Datos	
		Ingeniería de Software	
		Algoritmos computacionales	
		Inteligencia de negocios	
		Gobierno de TI	
		Auditoria y Seguridad Informática	X
		Simulación	

C. PLANTEAMIENTO DEL PROBLEMA
Hoy en día el tema de la seguridad informática ha despertado gran un gran interés en las organizaciones ya que la información o datos viene siendo el activo más importante de aseguramiento. Las entidades u organizaciones han sufrido constantes ataques informáticos estos pueden ser usuarios internos o externos a las entidades. Con el uso y el manejo inadecuado de las tecnologías han ocasionado problema a las organizaciones ya que son vulnerables a las amenazas que se presentan en el medio, las mismas que pueden convertirse en riesgo y afectar enormemente la integridad de la información. La implementación de un manual de políticas de información en las municipalidades permite optimizar la seguridad de la información en la entidad. Es por esto que se pretende diseñar un manual de políticas de seguridad de la información para el Gad intercultural de El Tambo la que permita proteger y conservar la

información de la entidad. El manual de políticas será debidamente documentado, puesto en conocimiento de los empleados de la entidad será de uso obligatorio

D. OBJETIVO GENERAL

Diseñar un Manual de Políticas de Seguridad de la Información para el Gad intercultural de El Tambo basado en la norma ISO/IEC 27001:2013 con el fin de garantizar la confidencialidad, integridad de la información existente en el departamento de TI.

E. OBJETIVOS ESPECÍFICOS

1. Realizar un estudio teórico con los temas relacionados a la investigación.
2. Realizar un el levantamiento y análisis de información para determinar el diagnóstico de la situación actual de la seguridad de información y de amenazas, vulnerabilidades y riesgos relacionados a la información del área de TI en el Gad intercultural de El Tambo en base a la norma ISO/IEC27001:2013.
3. Elaborar un manual de políticas de seguridad de la información en base a la norma ISO/IEC 27001:2013 para el Gad intercultural de El Tambo

F. JUSTIFICACIÓN

La seguridad de la información es un proceso en el que se da cabida a un creciente número de elementos: aspectos tecnológicos, de gestión-organizacionales, de recursos humanos, de índole económica, de negocio, de tipo legal, de cumplimiento, etc; abarcando no solo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medioambientales, humanos, etc [4]

Un nivel de protección total de la información es prácticamente imposible, por lo que un sistema de gestión de la seguridad de la información debe garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización. [4]

Es por esto que se propone realizar un manual de políticas de información para el Gad intercultural El Tambo con la finalidad de especificar el manejo y uso adecuado de las tecnologías para obtener un mayor grado de ventajas que brindan estas herramientas y sobre todo, la integridad de la información.

G. ALCANCE

El alcance de la presente investigación tiene como finalidad el diseño de un manual de políticas de la seguridad de información basado en la norma ISO/IEC27001:2013 para el Gad intercultural de El Tambo con el objetivo de establecer los lineamientos necesarios que mejoren la gestión de la seguridad de la información y garanticen la integridad de la información.

H. CONCEPTOS RELACIONADOS

Seguridad de la Información

La seguridad de la información es la protección de la integridad, disponibilidad y confidencialidad de la información, según el nivel requerido para los objetivos de negocio de la empresa. [3]

Seguridad Informática

No existe una definición estricta de lo que se entiende por Seguridad Informática, puesto que esta abarca múltiples y muy diversas áreas relacionadas con los SI. Tampoco es único el objetivo de la seguridad informática: la confidencialidad, la integridad y la disponibilidad. [4]

Sistema de Gestión de la seguridad de la información (SGSI)

Frente a la dependencia de los sistemas de información y al crecimiento de las amenazas existentes, se hace necesario para las organizaciones establecer un Sistema de 1gestion de Seguridad de la Información. Hay que tener en cuenta una premisa fundamental: la seguridad no es un producto, es un proceso; por tanto, la seguridad no puede comprarse, pero puede gestionarse. [3]

Políticas de Seguridad

El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de una organización, y en particular al involucrado directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados. [4]

Norma ISO/IEC 27001

La norma establece los requisitos que debe cumplir un SGSI (sistema de Gestión de la Seguridad de la Información) para su certificación en términos de procesos de seguridad a nivel organizativo. [6]

I. TRABAJOS RELACIONADOS

Existen varios autores que han desarrollado diversos estudios de investigación sobre el tema, cuyos resultados han generado una guía a tomarse en consideración. A continuación, se mencionan algunos de ellos:

Un estudio similar realizado en la Universidad Internacional SEK de la facultad de Arquitectura e Ingenierías, proyecto de investigación, presentado por el estudiante Henry Percy Cabrera Cubas que lleva el título "DISEÑO DE UNA POLÍTICAS EN LA NORMA ISO 27001, PARA MEJORAR LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE FLORIDA -BOGARA - AMAZONA", donde recomienda realizar talleres, programas de capacitación de seguridad

de la información más seguido, y especialmente al personal nuevo que ingresa; pero primero debemos implementar el programa de seguridad para los administrativos, jefes de cada área administrativa, liego trabajadores, y a todo el personal eterno que brinda servicios. [7]

Esta investigación será de ayuda para profundizar las bases teóricas y tener en cuenta los controles y dominios que presenta la norma ISO 27001, las mismas que serán utilizadas en el desarrollo de esta investigación.

Otro estudio similar realizado en la Universidad de las Américas, de la facultad de Ingeniería y Ciencias Agropecuarias por el estudiante Gustavo Xavier Lema Pazmiño con título "DISEÑO DE LAS BUENAS PRÁCTICAS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN NORMAS ISO 27001 PARA LA DIRECCIÓN GENERAL DE AVIACIÓN CIVIL", la presente tesis describe una investigación referente a un mejoramiento de los procesos de seguridad, políticas y mejoras del área técnica de la Dirección Aviación Civil del Ecuador (DGAC), por ello se ha generado una evaluación y análisis de la información obtenida para verificar la vulnerabilidad existente en la red de datos, así como también evidencia la falla en los procesos que se generan en dicha institución. [8]

En base a este proyecto se podrá determinar las vulnerabilidades, los riesgos que pueden afectar a los sistemas, determinar los procesos críticos las cuales necesiten de la implementación de controles para su que la información se encuentre protegida.

J. METODOLOGÍA

El método que se va a utilizar en este trabajo investigativo será descriptivo ya que se hará una recolección de información de la metodología a utilizarse, para mejorar la gestión de la seguridad de la información. Las fases que se desarrollaran son las siguientes:

1. **Identificación y delimitación del problema**

   En esta fase de identifican con las personas y departamentos que se van a trabajar del Gad intercultural El Tambo para determinar la situación actual de la Gestión de Seguridad de la Información.

2. **Elaboración y construcción de los instrumentos**

   Para la recolección de la información se elabora una entrevista, encuestas a las personas encargadas del área de TI del Gad intercultural El Tambo. También se obtendrá información de libros digitales, artículos, etc, documentos relacionados l tema de investigación.

   Se construye un plan de evaluación de seguridad de la información en base a la norma ISO/IEC27001:2013

3. **Observación y registro de datos**

   Se tabula la información recolectada de las encuestas, entrevistas realizadas al departamento de TI, en donde se determina si existe un documento donde se estipulé sobre la protección de la información.

4. **Decodificación y categorización de la información**

   Utilizando como guía los controles de la norma ISO 27001 y en base a los resultados obtenidos de las encuestas se identificar a que está expuesta la información critica el Gad intercultural El Tambo.

5. Análisis

Para el análisis se toma el resultado de la etapa cuatro, en la que se determina que dominios de la norma ISO27001:2013 se incluirán en el diseño del manual de políticas de seguridad de la información.

K. CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD	MES I				MES II				MES III				IV				V				
		S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	MEDIOS DE VERIFICACIÓN
1	**Segundo objetivo** Realizar un estudio teórico con los temas relacionados a la investigación.																					
	-Buscar y seleccionar sobre las metodologías sobre las políticas de información																					-Documentos pdf Que contenga las fases de la metodología.
2	**Segundo objetivo** Realizar un el levantamiento y análisis de información para determinar el diagnóstico de la situación actual de la seguridad de información y de amenazas, vulnerabilidades y riesgos relacionados a la información del área de TI en el Gad intercultural de El Tambo en base a la norma ISO/IEC27001:2013.																					
	-Aplicar las encuestas y entrevistas al personal de TI. -Aplicar un análisis en base a los dominios de la ISO27001																					-Documento con las respectivas respuestas. -Documento con el análisis en base a la ISO27001
3	**Tercer Objetivo** Elaborar un manual de políticas de seguridad de la información en base a la norma ISO/IEC 27001:2013 para el Gad intercultural de El Tambo																					
	-Desarrollo de un manual de políticas																					Elaboración del Documento de Políticas de información

L. DECLARACIÓN FINAL
Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES	
DIRECTOR:	Cristian Flores Urgilés
ESTUDIANTE 1	Carlos Francisco Chimborazo Quizhpi

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	Cañar
Fecha:	08/03/02021

Firmas:

Nombre: Cristian Flores Urgilés CC:0301638375 **Director del Proyecto**	Nombre: Carlos Chimborazo Q. C.C.: 0302362645 **Estudiante / Egresado**

O. APROBACIÓN	
Firmas:	
Nombre: CC: **Primer Par Revisor**	Nombre: C.C.: **Segundo Par Revisor**

P. REFERENCIAS

AGUILERA LOPEZ, P. (2010). *SEGURIDAD INFORMATICA* . EDITEX.

Aguilera López, P. (s.f.). *Seguridad informática.* Editex.

AREITIO BERTOLIN, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Paraninfo.

Cabrera Cubas, H. P. (Noviembre de 2018). *https://repositorio.upeu.edu.pe/.* Obtenido de https://repositorio.upeu.edu.pe/bitstream/handle/UPEU/1542/Henry_Tesis_Licenciatura_2018.pdf?sequence=5&isAllowed=y

Campoverde-Molina, M., & Valverde, L. (2019). Accessibility analysis of the web portals of the educational institutions in Cuenca, Ecuador. *Revista Cátedra, 2*(2), 55-75.

CARPENTIER, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Barcelona: Ediciones ENI.

CASTRO GIL , M. A., DÍAZ ORUETA, G., ALZÓRRIZ ARMENDÁRIZ, I., & SANCRISTÓBAL RUIZ, E. (2014). *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES.* Madrid.

EL Gobierno Autonomo Decentralizado Municipal Intercultural Comunitario Tambo-GADMICET. (01 de 01 de 2014). *docplayer.es.* Obtenido de https://docplayer.es/16931446-El-gobierno-autonomo-descentralizado-municipal-intercultural-comunitario-el-tambo-gadmicet-considerando.html

Escuela Tecnologica Instituto Tecnico Cnetral. (01 de 02 de 2021). *etitc.edu.co.* Recuperado el 21 de 09 de 2021, de https://www.etitc.edu.co/archives/calidad/GSI-MA-01.pdf

Francisco, L. C. (01 de 01 de 2019). *dspace.uce.edu.ec.* Obtenido de http://www.dspace.uce.edu.ec/bitstream/25000/18451/1/T-UCE-0011-ICF-122.pdf

Galisteo Pradillo, I. (2014). *MF0975_2 - Técnicas de recepción y comunicación.* ELEARNING S.L.

García-Moran, J. P. (2014). *Hacking y Seguridad en Internet.* Madrid: RA-MA.

INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR. (01 de 10 de 2014). *portal.icetex.gov.co.* Recuperado el 2021 de 09 de 2021, de https://portal.icetex.gov.co/Portal/docs/default-source/documentos-el-

icetex/biblioteca/manuales-de-la-entidad/manual-de-pol%C3%ADticas-de-seguridad-de-la-informaci%C3%B3n.pdf?sfvrsn=2

ISO 27000. (01 de 01 de 2005). *iso27000.es*. Recuperado el 19 de 08 de 2021, de https://www.iso27000.es/iso27000.html

Lema Pazmiño, G. X. (2017). *http://dspace.udla.edu.ec/.* Obtenido de http://dspace.udla.edu.ec/bitstream/33000/7650/3/UDLA-EC-TIRT-2017-06.pdf

Lopez, D. (s.f.). *Internet. la Red Con Mayusculas. E-book.* Madrid: MAD-Eduforma.

Lorena, C. A. (s.f.). Seguridad informática y seguridad de la informacion. Colombia.

MARTÍNEZ VALVERDE, J. F., & ROJAS RUIZ, F. (2017). *Comercio digital internacional.* Madrid: Ediciones Paraninfo, S.A.

Medina Cartuche, V. H., & Yunga Rodriguez, S. E. (2017). *http://dspace.espoch.edu.ec.* Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/3321/1/98T00049.pdf

Miguel Pérez, J. C. (2015). *Protección de Datos y Seguridad de la Información.* Madrid: RA-MA S.A.

Orellana, R. V. (01 de 01 de 2017). *repositorio.uide.edu.ec.* Obtenido de https://repositorio.uide.edu.ec/bitstream/37000/1746/1/T-UIDE-1142.pdf

Oropeza Gorocica, E. (Noviembre de 2006). *https://repositorio.tec.mx.* Obtenido de https://repositorio.tec.mx/handle/11285/567256

Pilla Yanzapanta, J. C. (2019). *https://repositorio.uisek.edu.ec/.* Obtenido de https://repositorio.uisek.edu.ec/bitstream/123456789/3601/1/DISE%c3%91O%20DE%20UNA%20POL%c3%8dTICA%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%c3%93N%20PARA%20EL%20%c3%81REA%20DE%20TECNOLOG%c3%8dA%20DE%20LA%20INFORMACI%c3%93.pdf

Sánchez Garreta, J. S. (2003). *Ingeniería de proyectos informáticos: actividades y procedimientos.* Publicacions de la Universitat Jaume I.

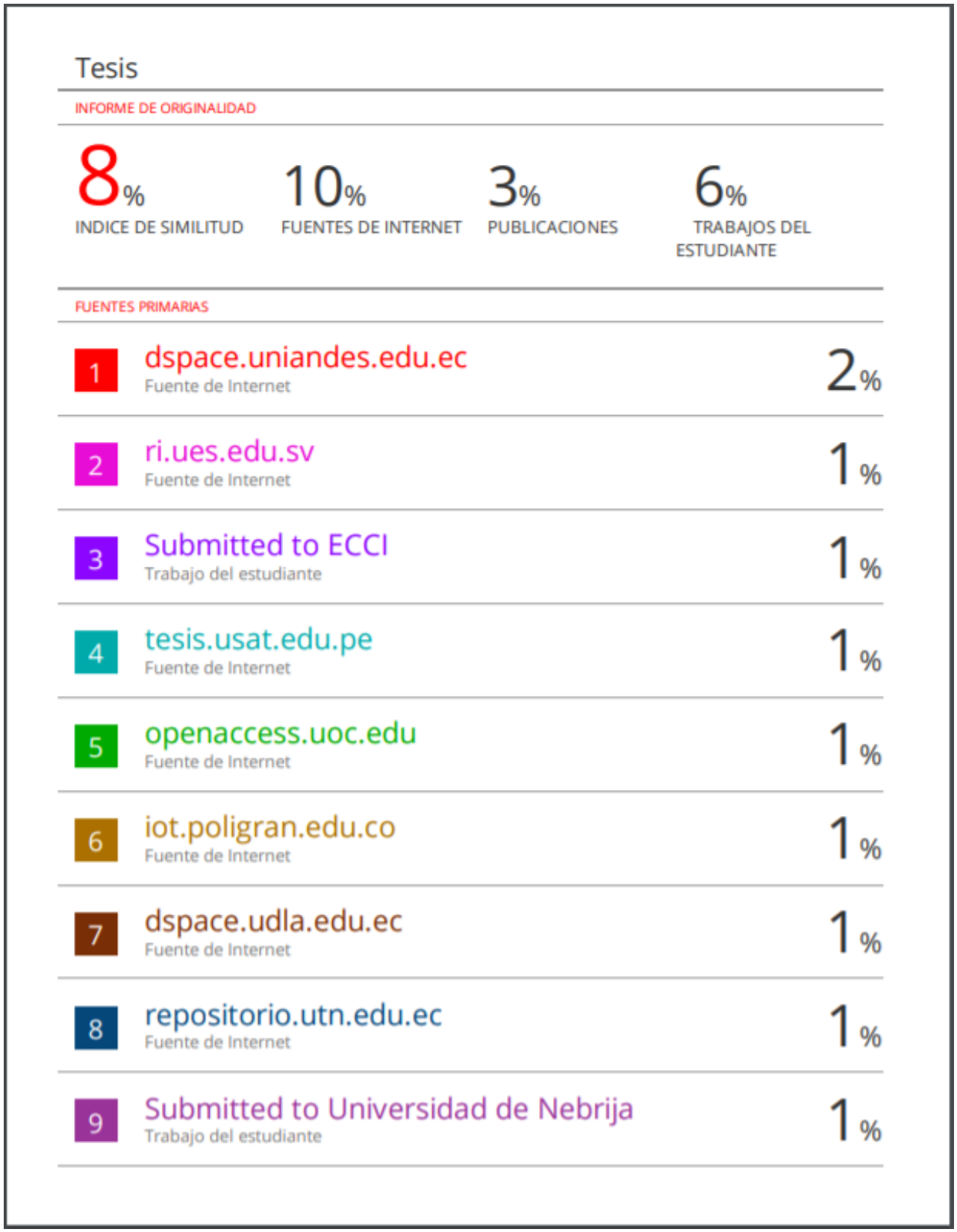
Simbaña-Gallardo, V., & Luján-Mora, S. (2018). Instructions about the manuscript structureof Revista Cátedra. *Revista Cátedra, 1*(1), 36-52.

Universidad Católica de Cuenca. (2020). *Directrices para autores/as*. Obtenido de https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/about/submissions

Anexo 2:

	GOBIERNO AUTONOMO DESCENTRALIZADO INTERCULTURAL DEL CANTÓN CAÑAR	**Código:** S001		
		Fecha: 00/00/2021		
		Versión: 01		
		Pagina:		
PREGUNTAS CLASIFICADAS POR DOMINIOS.				
Dominios - ISO 27002	**ENCUESTA**	**SI**	**NO**	**En Proceso**
Políticas de la Seguridad	¿Existe en su organización un documento que contenga las políticas de seguridad de la información?		**X**	
	¿Considera Usted que este documento es suficiente y apropiadamente difundido y comunicado a todos los miembros de la organización?		**X**	
	¿El documento de seguridad es revisado periódicamente y en caso de ocurrencia de eventos significativos?		**X**	
	¿El personal del GADMICET tiene conocimiento sobre las políticas de seguridad de la información?		**X**	
Aspectos organizativos de la Seguridad de la Información.	¿Existe un comité de gestión de seguridad que proponga o de soporte a las iniciativas de seguridad?		**X**	
	¿En la institución se ha contratado personal con conocimientos en materia de seguridad de la información?		**X**	
	¿Están claramente definidas los responsables, roles, y responsabilidades de la protección y aplicación de procesos de seguridad de todos los activos claves de la organización?		**X**	
	¿Están establecidos contactos y acuerdos de cooperación con organizaciones para el manejo de asuntos de seguridad?		**X**	
	¿Se realizan auditorias de seguridad independientes a la implantación de las políticas de seguridad de la información de la organización?		**X**	
	¿Se establecen contratos formales de seguridad cuando recursos de tecnologías de información de su organización serán accedidos y/o manejados por terceros?		**X**	

Seguridad Ligada a los Recursos Humanos.	¿Se cuenta con alguna política en la que se establezca que, en caso de abandono del puesto de trabajo de algún empleado se devuelva el equipamiento, así como también se elimine completamente los derechos de acceso (Acceso a información confidencial, Acceso a sistema)?	**X**		
	¿Se firman acuerdos de confidencialidad entre la organización y cada empleado como parte de los términos y condiciones de su trabajo?	**X**		
	¿Se educa y entrena a los empleados adecuadamente en las políticas y procedimientos de seguridad de la organización?		**X**	
	¿Conocen los empleados los procedimientos para reportar amenazas, riesgos, sospechas u ocurrencias de: incidentes de seguridad, debilidades en sistemas o servicios e incorrecto funcionamiento de aplicaciones/software?		**X**	
	¿Están definidos los procesos disciplinarios para sancionar a aquellos empleados que incurran en violaciones a las políticas y procedimientos de seguridad de la información de la organización?		**X**	
Gestión de Activos.	¿Se dispone de inventario de activos asociados a los recursos del tratamiento de la información tales como: recursos de información (bases de datos, documentación de sistemas, manuales de usuario), recursos de software (software de aplicaciones, sistemas operativos, herramientas de desarrollo, etc.), activos físicos (equipamiento informático, dispositivos móviles, pen drives, mobiliario, etc.) y servicios (servicios informáticos y de comunicaciones, calefacción,			**X**
	¿Existen esquemas o directrices para la clasificación de la información de la organización de acuerdo al grado de protección que deban recibir		**X**	
	¿Están definidos los controles de protección asociados al grado de protección que deba recibir cada activo de información?		**X**	
	¿Están definidos los procedimientos para el etiquetado y manejo de activos de información de acuerdo con el esquema de clasificación concebido por la organización?		**X**	
	¿Se protege los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización?		**X**	



Tesis

INFORME DE ORIGINALIDAD

8%	10%	3%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	dspace.uniandes.edu.ec Fuente de Internet	2%
2	ri.ues.edu.sv Fuente de Internet	1%
3	Submitted to ECCI Trabajo del estudiante	1%
4	tesis.usat.edu.pe Fuente de Internet	1%
5	openaccess.uoc.edu Fuente de Internet	1%
6	iot.poligran.edu.co Fuente de Internet	1%
7	dspace.udla.edu.ec Fuente de Internet	1%
8	repositorio.utn.edu.ec Fuente de Internet	1%
9	Submitted to Universidad de Nebrija Trabajo del estudiante	1%

Excluir citas	Activo	Excluir coincidencias	< 1%
Excluir bibliografía	Activo		

Universidad Católica de Cuenca

INFORME

Oficio Nro.: UCACUE-CAT-2021-0065-UT
Cañar, 23 de noviembre de 2021

Asunto: Trabajo de titulación

Señora Ingeniera
Ruth Andrade
BIBLIOTECARIA DE LA UNIVESIDAD CATOLICA DE CUENCA, EXTENSIÓN CAÑAR
Presente

De mi consideración

Reciba un cordial y afectuoso saludo, el éxito en las funciones que acertadamente viene desempeñando a favor de la Universidad.

El motivo de la presente es hacerle conocer que el estudiante, **Sr. Carlos Francisco Chimborazo Quizhpi,** ha concluido su trabajo de titulación que lleva por nombre "**MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN LAS NORMAS ISO 27001 EN EL GAD INTERCULTURAL DE EL TAMBO**", por lo cual autorizo subir la información al repositorio institucional.

Aprovecho la ocasión para reiterarle éxitos en el desempeño de sus funciones.

Atentamente,
DIOS, PATRIA, CULTURA Y DESARROLLO
"AÑO JUBILAR, QUICUAGÉSIMO ANIVERSARIO FUNDACIONAL"

Universidad Católica de Cuenca | SISTEMAS DE LA INFORMACIÓN
DIRECCIÓN DE CARRERA

Ing. Julio Jhovanny Santacruz Espinoza
DIRECTOR DE CARRERA DE INGENIERÍA DE SISTEMAS DE LA UNIVERSIDAD CATÓLICA DE CUENCA - EXTENSIÓN CAÑAR

Elaborado por:	Ing. José Carrillo Z.	
Aprobado por:	Ing. José Carrillo Z.	

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Carlos Francisco Chimborazo Quizhpi portador de la cedula de ciudadanía N.° 0302362645. En calidad de autor y titular de los derechos patrimoniales del trabajo de titulación "**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL GAD INTERCULTURAL DE EL TAMBO.**" de conformidad a lo establecido en el articulo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconoce a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Catoliza de Cuenca, para que realice la publicación de este trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el articulo 144 de la Ley Organiza de Educación Superior.

Cañar, 29 de noviembre del 2021.

F:.....

Carlos Francisco Chimborazo Quizhpi

CI: 0302362645