ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

DIRECCIÓN DE POSGRADO Y FORMACIÓN CONTINUA

INFORME DE TRABAJO DE TITULACIÓN

PREVIA LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES Y SISTEMAS DISTRIBUIDOS

MODALIDAD:

PROYECTO DE INVESTIGACIÓN Y DESARROLLO

TEMA:

SEGURIDAD DE LA INFORMACIÓN DE INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS INFORMÁTICOS DEL GADM DEL CANTÓN CHONE BASADO EN LA NORMA ISO/IEC 27001

AUTOR:

JINNSON MANUEL MOREIRA ÁLVAREZ

TUTOR:

MGTR. LUIS CEDEÑO VALAREZO

CALCETA, SEPTIEMBRE 2019

DERECHOS DE AUTORÍA

JINNSON MANUEL MOREIRA ÁLVAREZ, declaro bajo juramento que el trabajo aquí escrito 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.

A través de la presente declaración cedo los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su Reglamento.

_____

JINNSON MANUEL MOREIRA ÁLVAREZ

CERTIFICACIÓN DE TUTOR

ING. LUIS CEDEÑO VALAREZO, Mg certifica haber tutelado el trabajo de titulación **SEGURIDAD DE LA INFORMACIÓN DE INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS INFORMÁTICOS DEL GADM DEL CANTÓN CHONE BASADO EN LA NORMA ISO/IEC 27001,** que ha sido desarrollada por **JINNSON MANUEL MOREIRA ALVAREZ**, previo a la obtención del título de Magister en Tecnología de la Información Mención en Redes y Sistemas Distribuidos, de acuerdo al **REGLAMENTO DE LA UNIDAD DE TITULACIÓN DE LOS PROGRAMAS DE POSGRADO** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

_____

MG. LUIS CEDEÑO VALAREZO.

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaramos que hemos **APROBADO** el trabajo de titulación **SEGURIDAD DE LA INFORMACIÓN DE INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS INFORMÁTICOS DEL GADM DEL CANTÓN CHONE BASADO EN LA NORMA ISO/IEC 27001**, que ha sido propuesto, desarrollado por **JINNSON MANUEL MOREIRA ALVAREZ**, previa la obtención de título de Magister en Tecnología de la Información mención en Redes y Sistemas Distribuidos, de acuerdo al **REGLAMENTO DE LA UNIDAD DE TITULACIÓN DE LOS PROGRAMAS DE POSGRADO** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

MGTR. GUSTAVO MOLINA GARZÓN

MIEMBRO

MGTR. SERGIO INTRIAGO BRIONES

MIEMBRO

DR. INF. MARLON NAVIA MENDOZA

PRESIDENTE

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que nos dio la oportunidad de una educación superior de calidad en la cual se han forjado nuestros conocimientos profesionales día a día.

Agradezco a los docentes que con su vocación de enseñanza y sus experiencias me nutrieron de conocimientos para que hoy pueda apretarles la mano y llamarlos colegas.

A mi tutor de tesis por su completo apoyo durante el desarrollo de este trabajo de titulación quien de manera desinteresada me prestó su ayuda y colaboró en la realización del presente trabajo. Le doy mis más infinitas gracias, estimado Ing. Luis Cedeño Valarezo, por la orientación, el seguimiento y la supervisión continúa del mismo, pero sobre todo por la motivación y el apoyo recibido en el transcurso de estos meses.

JINNSON MANUEL MOREIRA ÁLVAREZ

DEDICATORIA

El presente trabajo de investigación está dedicado principalmente a Dios, ya que gracias a su bondad tuve la fortaleza para seguir adelante en los días difíciles que se presentaron en el desarrollo del trabajo y en mi vida cotidiana.

A mis hijos, con su inmenso amor, son quienes me impulsan a la superación personal y académica en mi diario vivir.

También dedico con gran afecto esta investigación a mis padres, quienes me formaron como un ser íntegro, con valores y virtudes positivas que han servido para cumplir de manera honesta y responsable el desarrollo del trabajo.

De igual manera a la Escuela Superior Politécnica Agropecuaria de Manabí y con ella a mis maestros quienes han inculcado valores y conocimientos para seguir cumpliendo con éxito todo lo propuesto en mi vida académica.

JINNSON MANUEL MOREIRA ÁLVAREZ

CONTENIDO GENERAL

DERECHOS DE AUTORÍA ii
CERTIFICACIÓN DE TUTOR iii
APROBACIÓN DEL TRIBUNAL iv
AGRADECIMIENTO v
DEDICATORIA vi
CONTENIDO GENERAL vii
CONTENIDO DE TABLAS Y GRÁFICOS ix
RESUMEN x
ABSTRACT xi
CAPÍTULO I. ANTECEDENTES 1
1.1. PLANTEAMIENTO DEL PROBLEMA 1
1.2. JUSTIFICACIÓN 3
1.3. OBJETIVOS 4
1.3.1. OBJETIVO GENERAL 4
1.3.2. OBJETIVOS ESPECÍFICOS 4
1.4. IDEA A DEFENDER 4
CAPÍTULO II. REVISIÓN BIBLIOGRÁFICA 5
2.1. SEGURIDAD Y GESTIÓN DE LA INFORMACIÓN 5
2.2. INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS INFORMÁTICOS 7
2.3. ESTÁNDAR ISO/IEC 27001 9
2.4. METODOLOGÍA ANÁLISIS MODAL DE FALLOS Y EFECTOS (AMFE) 10
CAPÍTULO III. DESARROLLO METODOLÓGICO 12
3.1. OBJETIVO 1: DETERMINACIÓN LA SITUACIÓN ACTUAL EN EL ASPECTO DE SEGURIDAD DE LA INFORMACIÓN, RECURSOS, PROCESOS E INFRAESTRUCTURA DE TECNOLOGÍA Y SISTEMAS INFORMÁTICOS 12
3.2. OBJETIVO 2: EVALUACIÓN LOS RIESGOS, VULNERABILIDADES Y AMENAZAS QUE EXISTEN EN LOS SISTEMAS INSTITUCIONALES MEDIANTE LA METODOLOGÍA DE ANÁLISIS MODAL DE FALLOS Y EFECTOS (AMFE) 13
3.3. OBJETIVO 3: DISEÑO UN PLAN DE MEJORA DE LA SEGURIDAD INFORMÁTICA HACIA LA INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS INFORMÁTICOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN DE CHONE BASADOS EN LA NORMA ISO/IEC 27001 14

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN 15
4.1. RESULTADOS 15
4.1.1. OBJETIVO 1: DETERMINACIÓN LA SITUACIÓN ACTUAL EN EL ASPECTO DE SEGURIDAD DE LA INFORMACIÓN, RECURSOS, PROCESOS E INFRAESTRUCTURA DE TECNOLOGÍA Y SISTEMAS INFORMÁTICOS 15
4.1.2 OBJETIVO 2: EVALUACIÓN LOS RIESGOS, VULNERABILIDADES Y AMENAZAS QUE EXISTEN EN LOS SISTEMAS INSTITUCIONALES MEDIANTE LA METODOLOGÍA DE ANÁLISIS MODAL DE FALLOS Y EFECTOS (AMFE) 18
4.1.3. OBJETIVO 3: DISEÑO DE UN PLAN DE MEJORA DE LA SEGURIDAD INFORMÁTICA HACIA LA INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS INFORMÁTICOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN DE CHONE BASADOS EN LA NORMA ISO/IEC 27001 19
4.2. DISCUSIÓN 20
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 21
5.1. CONCLUSIONES 21
5.2. RECOMENDACIONES 22
BIBLIOGRAFÍA 23
ANEXOS 26
ANEXO 1 27
SOLICITUD APROBADA POR EL GADM CHONE PARA EL LEVANTAMIENTO DE INFORMACIÓN 27
ANEXO 2 29
CHECKLIST APLICADO AL DEPARTAMENTO TECNOLÓGICO DEL GADM CHONE BASADO EN LA NORMA ISO/IEC 27001:2013 29
ANEXO 3 42
VULNERABILIDADES ENCONTRADAS A TRAVÉS DE CHECKLIST BASADO EN LA NORMA ISO/IEC 27001:2013 42
ANEXO 4 48
MATRIZ DE ANÁLISIS MODAL, FALLOS Y EFECTOS (AMFE) PARA LA EVALUACIÓN DE LOS RIESGOS 48
ANEXO 5 63
PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMÁCIÓN Y DE LOS SITEMAS INFORMÁTICOS DEL GADM CHONE 63

CONTENIDO DE TABLAS Y GRÁFICOS

Cuadro 4. 1. Total de vulnerabilidades inventario activo 15
Cuadro 4. 2. Total de vulnerabilidades seguridad física 16
Cuadro 4. 3. Total de vulnerabilidades seguridad de los recursos humanos .. 16
Cuadro 4. 4. Total de vulnerabilidades Gestión de comunicación y de operación..... 16
Cuadro 4. 5. Total de vulnerabilidades control de acceso 17
Cuadro 4. 6. Total de vulnerabilidades cumplimento de la norma 17
Cuadro 4. 7. Porcentaje de Riesgo en cada componente de la norma ISO/IEC 27001:2013 19

Gráfico 4. 1. Total de vulnerabilidades 18

Figura 2. 1. Instalación con Infraestructura..... 8
Figura 2. 2. Diagrama de Infraestructura tecnológica..... 9

RESUMEN

El trabajo de titulación tuvo como finalidad la elaboración de un plan de Gestión para la Seguridad de la Información en la Infraestructura Tecnológica y Sistemas Informáticos del Gobierno Autónomo Descentralizado Municipal del Cantón Chone, basado en la Norma ISO/IEC 27001 para disminuir los riesgos en los sistemas de información institucional. La metodología aplicada fue consecución de objetivos, donde el primer objetivo se enfocó en la determinación de la situación actual de los procesos, recursos, información e infraestructura del departamento de TI a través de un checklist con preguntas estructuradas y basadas en los componentes de la norma aplicada, el segundo objetivo fue la evaluación de los riesgos en base a las vulnerabilidades encontradas con el objetivo anterior, para luego emplear la metodología Análisis Modal de Fallos y Efectos (AMFE), donde se identificó y evaluó el nivel de riesgos en cada componente, lo que permitió obtener las acciones de mitigación en aspectos de integridad, disponibilidad y confiabilidad de la información. El tercer objetivo se obtuvo de acuerdo con la información de los dos objetivos anteriores, a la cual se hizo un análisis general, dando como resultado un plan de gestión de seguridad de la información que plantea medidas de solución al departamento tecnológico objeto de estudio. Esta propuesta permite mejorar los aspectos de seguridad de TI mediante las correctivas necesarias para salvaguardar la integridad de sus datos.

PALABRAS CLAVES

Seguridad de la Información, Gestión de la información, AMFE, riesgos en seguridad de la información.

ABSTRACT

The purpose of the titling work was to prepare a Management Plan for Information Security in the Technological Infrastructure and Computer Systems of the Municipal Decentralized Autonomous Government of Chone Canton, based on the ISO / IEC 27001 Standard to reduce risks in the institutional information systems. The methodology applied was the achievement of objectives, where the first objective focused on determining the current situation of the processes, resources, information and infrastructure of the IT department through a checklist with structured questions based on the components of the standard applied, the second objective was the evaluation of the risks based on the vulnerabilities found with the previous objective, to then use the methodology Modal Analysis of Faults and Effects (AMFE), where the level of risks in each component was identified and evaluated, what allowed to obtain the mitigation actions in aspects of integrity, availability and reliability of the information. The third objective was obtained in accordance with the information of the two previous objectives, to which a general analysis was made, resulting in an information security management plan that proposes solution measures to the technological department under study. This proposal allows to improve the IT security aspects by means of the necessary corrections to safeguard the integrity of its data.

KEYWORDS

Information Security, Information Management, AMFE, risks in information security.

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO DEL PROBLEMA

Las organizaciones de hoy en día desean establecerse en un mercado globalizado y competitivo, pero deben de contar con una infraestructura que le permita interactuar con su entorno de manera adecuada, facilitándole la promoción, divulgación y/o prestación de sus productos o servicios a través de una plataforma tecnológica.

Los sistemas de información protegen a las organizaciones para que logren ventajas competitivas estratégicas sobre otras organizaciones y ayuden a la administración superior en el proceso de toma de decisiones, además, aportan a las organizaciones en la implementación oportuna de proyectos y la gestión efectiva de riesgos. (Nieves, 2017).

Molano (2017) manifiesta que teniendo en cuenta que en la actualidad las empresas utilizan las plataformas tecnológicas para la prestación de servicios o la comercialización de sus productos, se hace necesario la detección temprana de las vulnerabilidades que pueden afectar el normal desarrollo de las operaciones empresariales. Con el creciente uso del internet y la variedad de herramientas informáticas disponibles que facilitan el acceso fraudulento a las empresas, se presenta un aumento en la brecha de los controles que permiten un incremento de las amenazas a los sistemas de información (Vásquez y Cárdenas, 2015).

De acuerdo con lo mencionado la seguridad de la información es crucial para el éxito Institucional, y ha ganado cada vez más atención en el departamento de Tecnologías de Información y Comunicación (TIC) del Gobierno Autónomo Descentralizado Municipal (GADM) del Cantón Chone. Es así como desde hace algún tiempo se han implementado medidas de seguridad técnicas como

firewalls y control de acceso, también se ha establecido una política de seguridad para aclarar las rutinas en el manejo correcto de la información confidencial y los recursos de información.

Los requerimientos de la organización en el departamento ha generado la necesidad de desarrollar varios software para la institución tales como: sistema financiero, rentas, avalúos y catastros, tesorería, nómina de rol de pagos e inventarios de activos fijos, que por ser puntos relevantes para el municipio también estos se constituyen como procesos críticos en el nivel de seguridad que ellos deben de poseer, por tal razón es una preocupación para la entidad que estos sistemas de información no estén con la seguridad que requieren para su funcionalidad.

Este proyecto está basado legalmente bajo la LOTAIP (Ley Orgánica de Transparencia y Acceso a la Información Pública) en relación al artículo 13 donde estipula que las personas responsables o usuarios del archivo, están obligadas a adoptar medidas tecnológicas y organizativas, para garantizar la seguridad y confidencialidad de los datos personales, evitar adulteraciones, perdidas, consulta o acceso y tratamiento no autorizado y que permitan descubrir las desviaciones intencionales o no de información, ya sea que los registros provengan de la acción humana o del medio tecnológico usado.

Este proyecto lleva el fin de mejorar la seguridad de la información aplicando estándares internacionales y buenas prácticas que contribuirán a la salvaguarda del activo más importante de una organización como lo es la información que proporciona la entidad de Gobierno Autónomo Descentralizado Municipal del Cantón de Chone buscando la mejora en todos sus departamentos, la necesidad de que mejoren los servicios de la Municipalidad es lo que propicia al desarrollo de la presente investigación.

De acuerdo con lo antes mencionado, el autor se hace la siguiente interrogante: **¿De qué manera se puede mejorar la seguridad de la información para el GADM Chone?**

1.2. JUSTIFICACIÓN

El conjunto de debilidades y vulnerabilidades es parte de la realidad informática en todas las organizaciones por este motivo este trabajo de tesis conlleva a un diagnóstico de los procesos que se manejan en el Municipio para de esta manera contribuir con el cambio en la gestión de la seguridad de la información, ya sea innovando los softwares de sistemas informáticos para que superen las expectativas de los usuarios.

Basado el autor en el planteamiento del problema, también considera importante este trabajo de titulación para la seguridad de la información basada en la norma ISO 27001, ya que indica un diagnóstico actual de los procesos, infraestructura, aplicaciones y recursos con vulnerabilidades que pueden conllevar a riesgos como lograr pérdidas de información, ataques maliciosos en los sistemas de información, entre otros, de los cuales tomando las medidas correctivas y los ajustes necesarios según la norma establecida, contribuirá en la reducción de costos al mantener la seguridad a nivel tecnológico en el municipio, y de esta manera brindar una prestación de servicio segura a la comunidad sin afectar las actividades en las operaciones de la entidad.

Además, con el plan propuesto se busca el progreso de la institución con información disponible y segura, con alternativas de control que permitan la confidencialidad de los datos proporcionados y de esta manera conseguir que las debilidades Institucionales se conviertan en las fortalezas que mitiguen los posibles riesgos y coadyuven a la seguridad de toda la Información de los departamentos existentes.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Elaborar un plan de Gestión para la Seguridad de la Información en la Infraestructura Tecnológica y Sistemas Informáticos del Gobierno Autónomo Descentralizado Municipal del Cantón Chone basado en la Norma ISO/IEC 27001:2013 para disminuir los riesgos en los sistemas de información institucional.

1.3.2. OBJETIVOS ESPECÍFICOS

- Determinar la situación actual en el aspecto de seguridad de la Información, recursos, procesos e infraestructura de tecnología y sistemas Informáticos.

- Evaluar los riesgos, vulnerabilidades y amenazas que existen en los sistemas institucionales mediante la Metodología de Análisis Modal de Fallos y Efectos (AMFE)

- Diseñar un plan de mejora de la Seguridad Informática hacia la Infraestructura Tecnológica y Sistemas Informáticos del Gobierno Autónomo Descentralizado del Cantón de Chone basados en la Norma ISO/IEC 27001.

1.4. IDEA A DEFENDER

La elaboración de un Plan de Gestión para la Seguridad de la Información alineada con la norma ISO/IEC 27001:2013, permitirá disminuir los riesgos en la Infraestructura Tecnológica y Sistemas Informáticos del Gobierno Autónomo Descentralizado Municipal del Cantón Chone.

CAPÍTULO II. REVISIÓN BIBLIOGRÁFICA

2.1. SEGURIDAD Y GESTIÓN DE LA INFORMACIÓN

Según Hernández (2016) manifiesta que la definición de seguridad informática proviene de dos términos antes definidos, por ende, la seguridad informática son técnicas desarrolladas para proteger los equipos informáticos y la información de daños accidentales o intencionados.

La Seguridad de la Información se refiere a las metodologías y procesos, diseñados e implementados para proteger la información en medios electrónicos, medios impresos o cualquier otra forma de datos, ya sea información sensible, privada o confidencial del acceso no autorizado, uso, revelación, destrucción, modificación o interrupción (SANS, 2016; Montenegro, 2017).

Según afirma Gómez (2007) que la norma ISO 27001 del sistema de Gestión de la Garantía de Confidencialidad y garantía de la seguridad de la Información tiene relación con otras normas que conforman el modelo de gobierno y gestión de las Tecnologías de la Información y Comunicación (TIC) desarrollado por AENOR, basado en estándares aceptados mundialmente. Se puede decir que, gracias a este modelo, el Centro de Proceso de Datos y el resto de la organización comienzan a hablar el mismo lenguaje y a interconectarse de manera más natural y eficiente.

Ante un estudio realizado frente a Incidentes de Seguridad Informática se establece que los robos y atentados informáticos que utilizan la innovación tecnológica con fines delictivos cada vez son mayores, y no solo generan pérdidas económicas ya que su interés de manera actual se encuentra enfocado en el daño contra las personas, empresas y gobiernos (Mejía, 2015).

Un Sistema de Gestión de Seguridad de la Información (SGSI) preserva la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de un proceso de gestión del riesgo y brinda confianza acerca de la

gestión adecuada de los riesgos (Servicio Ecuatoriano de Normalización INEN, 2016; Montenegro, 2017). La metodología para implementar la gestión automatizada de controles de seguridad de la información es la combinación de varios métodos enfocados a la gestión de riesgos con un enfoque de automatización durante las etapas de operación, monitorización y revisión de un SGSI. Las tareas definidas en la fase de planificación, donde se incluye el análisis de riesgo como componente central, están destinadas a definir los objetivos de control para la determinación de controles automatizables (Cairo, 2016).

En los principios de la seguridad de la información, toda entidad o corporación debe tener claro que la Seguridad de la Información no es un producto que se puede comprar adquirir e instalar, sino que es un proceso. Por lo tanto, es un ciclo interactivo en el que se incluyen actividades como la valoración de riesgos, prevención, detección y respuesta ante incidentes de seguridad. Para poder alcanzar las actividades descritas en el apartado anterior, dentro del proceso de gestión de la seguridad de la información es necesario contemplar de la siguiente manera estos servicios o funciones de seguridad de la información:

Confidencialidad: Se trata de la cualidad que debe poseer un documento o archivo para que este sólo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.

De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y sólo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada. En el caso de un mensaje esto evita que exista una intercepción de éste y que pueda ser leído por una persona no autorizada (COIT, 2015).

Autenticación: La autenticación es la situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice. Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar

que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado. La autenticación en los sistemas informáticos habitualmente se realiza mediante un usuario o *login* y una contraseña o *password* (COIT, 2015).

Integridad: La Integridad de la Información es la característica que hace posible garantizar su exactitud y confiabilidad, velando para que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, de modo autorizado y mediante procesos autorizados. La integridad busca asegurar:

- Que no se realicen modificaciones por personas no autorizadas a los datos o procesos.
- Que no se realicen modificaciones no autorizadas por persona autorizada a los datos o procesos.
- Que los datos sean consistentes tanto interna como externamente (Burgos y Campos, 2008).

Disponibilidad: Se define como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia. Constantemente está recibiendo consultas, descargas a su sitio web, etc., por lo que siempre deberá estar disponible para sus usuarios (Burgos y Campos, 2008).

Los SGI deben estar en constante revisión de sus procesos, permitiendo agilizar de forma eficiente la información aplicando normas y estándares confiables y funcionales, creando un modelo propio de gestión para hacer de este un sistema eficiente.

2.2. INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS INFORMÁTICOS

Mediante una investigación desarrollada sobre la Infraestructura tecnológica y apropiación de las TIC afirma que “La infraestructura tecnológica comprende

los siguientes componentes: hardware, conectividad, soporte técnico, gastos y recursos digitales, que a la vez incluyen dos subcomponentes: software y recursos web" (Torres, 2010).

La infraestructura tecnológica en el GADM Chone puede estar constituida por elementos sólidos, que permitan llevar a cabo las funciones de gestión acordes a los requerimientos de la corporación municipal. Al mismo tiempo esta infraestructura debe poseer altos niveles de seguridad por la delicadeza de la información que maneja. En síntesis, una infraestructura tecnológica está compuesta por una parte de software y una parte de hardware, que en conjunto hacen posible una infraestructura tecnológica robusta y confiable.

En la figura 2.1 se muestra una infraestructura TI que utiliza puntos de acceso a la red mediante sistema inalámbrico en base a adaptadores que completen la función que necesiten, se van a utilizar computadoras con la misma rapidez que los conectados a un cable, la cual se conectará la red convencional y mediante los ordenadores se establece una conexión a un *switch* que tenga acceso internet y si es necesario en computadores portátiles.

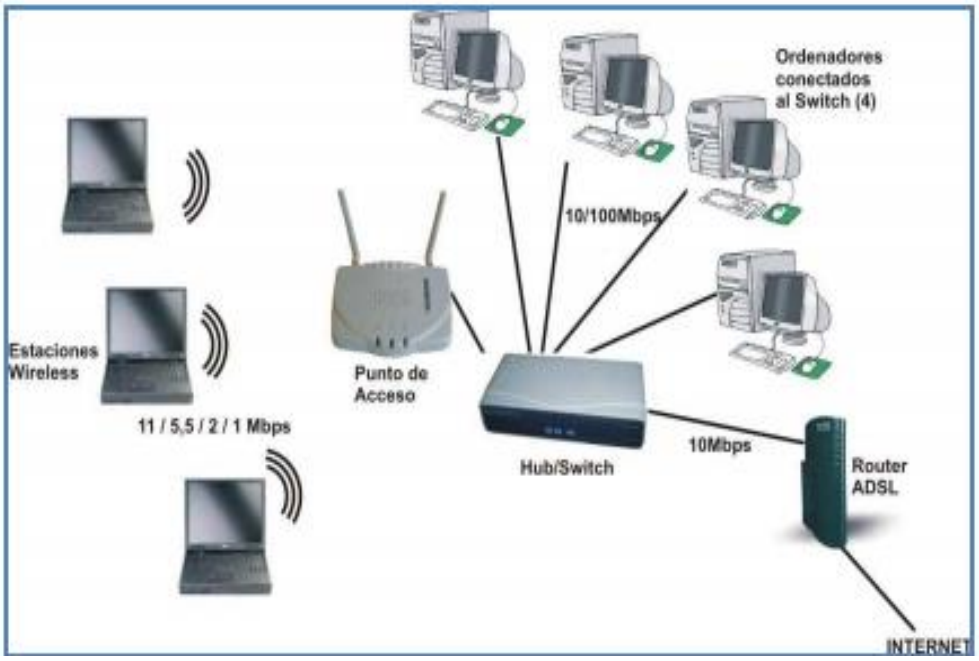


Figura 2. 1. Instalación con Infraestructura

Fuente: Cerón y Dávila (2013)

En la figura 2.2 se observa una infraestructura tecnológica implementada, se trata de una red redundante con *swichts* de *core* y fibra de conexión que permite obtener el internet en base un *router*, pasando el servidor y proveyendo internet a todos los ordenadores de la organización.

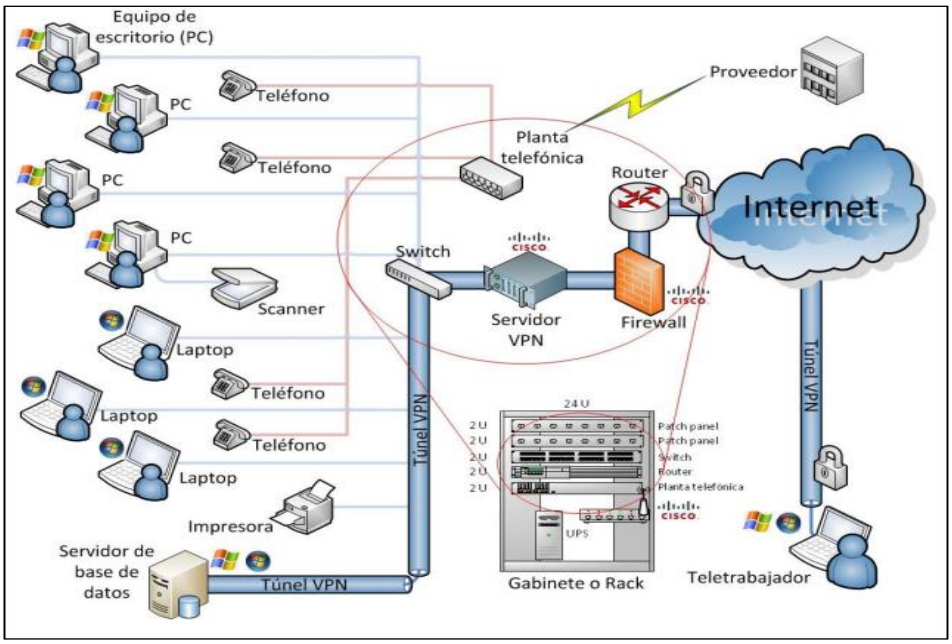


Figura 2. 2. Diagrama de Infraestructura tecnológica

Fuente: Munévar (2013)

2.3. ESTÁNDAR ISO/IEC 27001

Los estándares basados en la seguridad de la información están constituidos por la familia de estándares ISO/IEC 27000 E ISM3, normas dedicadas para la gestión de seguridad de la información implementadas en cualquier organización sin importar su magnitud o sector productivo (Andrade y Chávez, 2018).

Según afirma la Norma UNE-ISO/IEC 27001, “Un Sistema de Gestión de Seguridad de la Información (SGSI), es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Esto significa que se va a dejar de operar de una

manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización. Nos permitirá conocer mejor nuestra organización, cómo funciona y qué podemos hacer para que la situación mejore".

Si a la seguridad Informática se la mira desde esta óptica, se comprenderá la gran importancia que tiene dentro de cualquier empresa, sea esta pública o privada, porque a través de ella se puede resguardar lo más preciado y vulnerable que es su información.

La Norma ISO/IEC 27001 también proporciona un conjunto de recomendaciones sobre qué medidas debe tomar la empresa para asegurar los Sistemas de Información. Los objetivos de la seguridad recogen aquellos aspectos fundamentales que se deben analizar para conseguir un sistema seguro en cada una de las áreas que los agrupa. Para conseguir cada uno de estos objetivos la norma propone una serie de medidas o recomendaciones (controles) que son los que en definitiva se aplican para la gestión de riesgo analizado (Barragan, Góngora, & Martínez, 2011).

Evolución de ISO 27001.
Fuente: http://www.iso27000.es

2.4. METODOLOGÍA ANÁLISIS MODAL DE FALLOS Y EFECTOS (AMFE)

Esta metodología de Análisis Modal de Fallos y Efectos fue aplicada en una investigación en el proceso de prescripción, validación y dispensación de medicamentos, el mismo que llegó a la conclusión que "La aplicación del AMFE al proceso de prescripción, validación y dispensación de medicamentos, ha permitido identificar los puntos críticos, conocer las etapas en las que se pueden producir los errores, analizar las causas que los pueden provocar y los

efectos que estos tendrían en la seguridad del proceso, y establecer medidas para evitarlos o disminuirlos. Así mismo, les permitió iniciar en un proceso continuo de mejora de la calidad, lo que contribuirá a incrementar la seguridad del paciente" (Silveira, 2010).

De esta manera se ha considerado aplicar esta metodología para la búsqueda del análisis de los riesgos, la misma que tendrá las siguientes fases en el GADM del Cantón Chone:

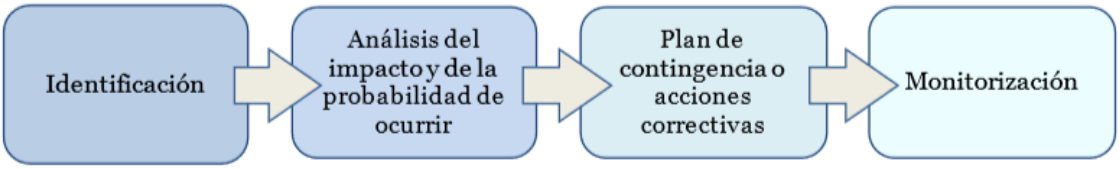


Figura 3. Fases de la Metodología AMFE.

Fuente: (García, 2018)

CAPÍTULO III. DESARROLLO METODOLÓGICO

Esta investigación se la efectuó en el Gobierno Autónomo Descentralizado Municipal del cantón Chone, departamento de Tecnología de la Información y Comunicación, para lo cual se realizó una solicitud al Señor alcalde la misma que fue aceptada (Anexo 1) con la finalidad de diseñar un plan de mejora en la Seguridad de Información de Infraestructura Tecnológica y Sistemas Informáticos basados en la Norma ISO/IEC 27001:2013. La metodología que se utilizó para esta investigación fue la de consecución de objetivos, donde el primer objetivo se desarrolló mediante la estructuración de un *checklist* basado en los componentes de la norma antes mencionada, lo que permitió conocer la situación actual en el área del departamento tecnológico del GADM Chone con respecto a recursos, procesos, información e infraestructura. Posterior a esto, para el segundo objetivo se empleó la metodología AMFE (Análisis Modal Fallos y Efectos) para la identificación, evaluación y análisis de los riesgos con respecto a vulnerabilidades y amenazas, de forma que se proporcionan medidas como acciones de mitigación y criterios de aceptación de acuerdo con los niveles de riesgos establecidos. Ya en el tercer objetivo se propone un plan de mejora aplicando la norma ISO 27001:2013 en la Infraestructura Tecnológica y Sistemas Informáticos.

3.1. OBJETIVO 1: DETERMINACIÓN LA SITUACIÓN ACTUAL EN EL ASPECTO DE SEGURIDAD DE LA INFORMACIÓN, RECURSOS, PROCESOS E INFRAESTRUCTURA DE TECNOLOGÍA Y SISTEMAS INFORMÁTICOS

Para el presente trabajo de investigación, fue necesario e imprescindible realizar la presentación de la solicitud de aprobación para el desarrollo de la investigación al director del departamento de tecnología de información y comunicación (TIC) como parte fundamental para la obtención de información de primera mano. Con el afán de recabar datos que refleje la situación actual de los Procesos de Seguridad de la Información en el GADM Chone, y con la

finalidad de realizar un diagnóstico inicial de la problemática, también se realizó un *checklist* al personal que labora en el departamento tecnológico, con información sensible de la institución, dichos cuestionarios permitieron la recolección de datos en forma dinámica y específica, permitiendo encausar los distintos problemas presentados en Gestión de la Seguridad de la Información.

Para cuantificar la situación actual del objeto de estudio se procedió a ponderar los *checklists* mediante la escala de *Likert* por el nivel de importancia que atribuye a la investigación permitiendo determinar los criterios de identificación y ponderación valorizados de la siguiente manera: **4** es un proceso que **Cumple**, **3** es **Cumple a medias**, 2 es **Cumple sin evidencia** y **1** es **No cumple** (Anexo 2A), dejando como más relevantes las críticas en intervalos del 1 al 3. Con base a las respuestas y evidencias obtenidas por parte del coordinador/director del Departamento Tecnológico, se pudo obtener resultados del cumplimiento de la norma aplicada con relación a los procesos, infraestructura, recursos e información del objeto de estudio.

3.2. OBJETIVO 2: EVALUACIÓN LOS RIESGOS, VULNERABILIDADES Y AMENAZAS QUE EXISTEN EN LOS SISTEMAS INSTITUCIONALES MEDIANTE LA METODOLOGÍA DE ANÁLISIS MODAL DE FALLOS Y EFECTOS (AMFE)

Para el cumplimiento de este objetivo, primeramente, se necesitó obtener los resultados del objetivo anterior. Una vez determinada la situación actual del objeto de estudio, se procedió a identificar las vulnerabilidades encontradas (Anexo 3: A, B, C, D, E, F, G) en el cumplimiento del *checklist* basados en los componentes de la norma ISO/IEC 27001:2013, para luego ser analizados y evaluados mediante la metodología AMFE (Anexo 4: A, B, C, D, E, F, G), clasificando por componente las vulnerabilidades y ponderando por Probabilidad, Impacto para obtener el Nivel de riesgos y de esta manera brindar acciones de mitigación y criterios de aceptación respectivamente para el departamento tecnológico del GADM Chone.

3.3. OBJETIVO 3: DISEÑO UN PLAN DE MEJORA DE LA SEGURIDAD INFORMÁTICA HACIA LA INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS INFORMÁTICOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN DE CHONE BASADOS EN LA NORMA ISO/IEC 27001

Siguiendo la metodología de investigación, para llevar a cabo este último objetivo, se consideraron los resultados del objetivo 1 y 2, de los cuales se elaboró el plan de Gestión para la Seguridad de la Información en la Infraestructura Tecnológica y Sistemas Informáticos del Gobierno Autónomo Descentralizado Municipal del Cantón Chone basado en la Norma ISO/IEC 27001 (Anexo 5) para disminuir los riesgos en los sistemas de información institucional, dando paso a la entrega del Plan al coordinador/director del departamento tecnológico de manera formal para su respectiva implementación, mejoras en los procesos y actividades que se realizan y cómo mitigar los posibles riesgos encontrados en la investigación.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

Los resultados obtenidos en este apartado contribuirán para el desarrollo de un plan de gestión de seguridad para el departamento tecnológico del GADM Chone, destacando cada resultado por objetivo planteado para esta investigación.

4.1.1. OBJETIVO 1: DETERMINACIÓN LA SITUACIÓN ACTUAL EN EL ASPECTO DE SEGURIDAD DE LA INFORMACIÓN, RECURSOS, PROCESOS E INFRAESTRUCTURA DE TECNOLOGÍA Y SISTEMAS INFORMÁTICOS

En el proceso de desarrollo de este objetivo se realizó una ponderación por cada componente de la norma ISO/IEC 27001:2013, evaluado mediante un checklist, de la cual se obtuvieron las siguientes vulnerabilidades de acuerdo con el cumplimiento de esta norma.

Cuadro 4. 1. Total de vulnerabilidades encontradas en el componente Inventario de Activo

Componente	Criterio	Nº de Vulnerabilidades (FA)	Frecuencia Relativa
INVENTARIO DE ACTIVO SG. NORMA ISO 27001	Cumple	0	0%
	Cumple A medias	3	43%
	Cumple sin evidencias	0	0%
	No cumple	4	57%
Total		**7**	**100%**

Elaboración: El autor

En el cuadro 4.1, son datos correspondientes al componente inventario de activo basados en la norma ISO 27001, donde se obtuvo en el criterio de **No cumple** un total de 4 vulnerabilidades correspondiente al 57%, siendo este el mayor porcentaje.

Cuadro 4. 2. Total de vulnerabilidades encontradas en el componente Seguridad Física

Componente	Criterio	Nº de Vulnerabilidades (FA)	Frecuencia Relativa
SEGURIDAD FISICA DEL ENTORNO SG. NORMA ISO 27001	Cumple	1	3%
	Cumple A medias	0	0%
	Cumple sin evidencias	22	73%
	No cumple	7	23%
Total		**30**	**100%**

Elaboración: El autor

En el cuadro 4.2, los datos corresponden al componente de seguridad física del entorno aplicando la norma ISO 27001, donde se obtuvo en el criterio **cumple sin evidencias** un total de 22 vulnerabilidades representados por el 73%.

Cuadro 4. 3. Total de vulnerabilidades encontradas en el componente Seguridad de los Recursos Humanos

Componente	Criterio	Nº de Vulnerabilidades (FA)	Frecuencia Relativa
SEGURIDAD DE LOS RECURSOS HUMANOS SG. NORMA ISO 27001	Cumple	2	22%
	Cumple A medias	1	11%
	Cumple sin evidencias	3	33%
	No cumple	3	33%
Total		**9**	**100%**

Elaboración: El autor

En el cuadro 4.3, los datos corresponden al componente seguridad de los recursos humanos basados en la norma ISO 27001, encontrando un total de 3 vulnerabilidades en el criterio de **Cumple sin evidencia** y 3 vulnerabilidades en el de **No cumple,** representados por el 33% respectivamente.

Cuadro 4. 4. Total de vulnerabilidades encontradas en el componente Gestión de comunicación y de operación

Componente	Criterio	Nº de Vulnerabilidades (FA)	Frecuencia Relativa
GESTION DE COMUNICACIÓN Y DE OPERACIÓN SG. NORMA ISO 27001	Cumple	1	6%
	Cumple A medias	0	0%
	Cumple sin evidencias	9	53%
	No cumple	7	41%
Total		**17**	**100%**

Elaboración: El autor

En el cuadro 4.4, los datos correspondientes al componente gestión de la comunicación y de operación basados en la norma ISO 27001, corresponden al

criterio **Cumple sin evidencia**, obteniendo un total de 9 vulnerabilidades, representados por el 53%.

Cuadro 4. 5. Total de vulnerabilidades encontradas en el componente Control de Acceso

Componente	Criterio	Nº de Vulnerabilidades (FA)	Frecuencia Relativa
CONTROL DE ACCESO SG. NORMA ISO 27001	Cumple	1	17%
	Cumple A medias	0	0%
	Cumple sin evidencias	3	50%
	No cumple	2	33%
Total		**6**	**100%**

Elaboración: El autor

En el cuadro 4.5, los datos correspondientes al componente control de acceso basados en la norma ISO 27001, el mayor número de vulnerabilidades esta sobre el criterio **Cumple sin evidencia,** representado por el 50%.

Cuadro 4. 6. Total de vulnerabilidades encontradas en el componente Cumplimento

Componente	Criterio	Nº de Vulnerabilidades (FA)	Frecuencia Relativa
CUMPLIMIENTO SG. NORMA ISO 27001	Cumple	0	0%
	Cumple A medias	0	0%
	Cumple sin evidencias	0	0%
	No cumple	2	100%
Total		**2**	**100%**

Elaboración: El autor

En el cuadro 4.6, los datos correspondientes al componente cumplimiento basados en la norma ISO 27001, se obtuvieron 2 vulnerabilidades sobre el criterio **No cumple**.

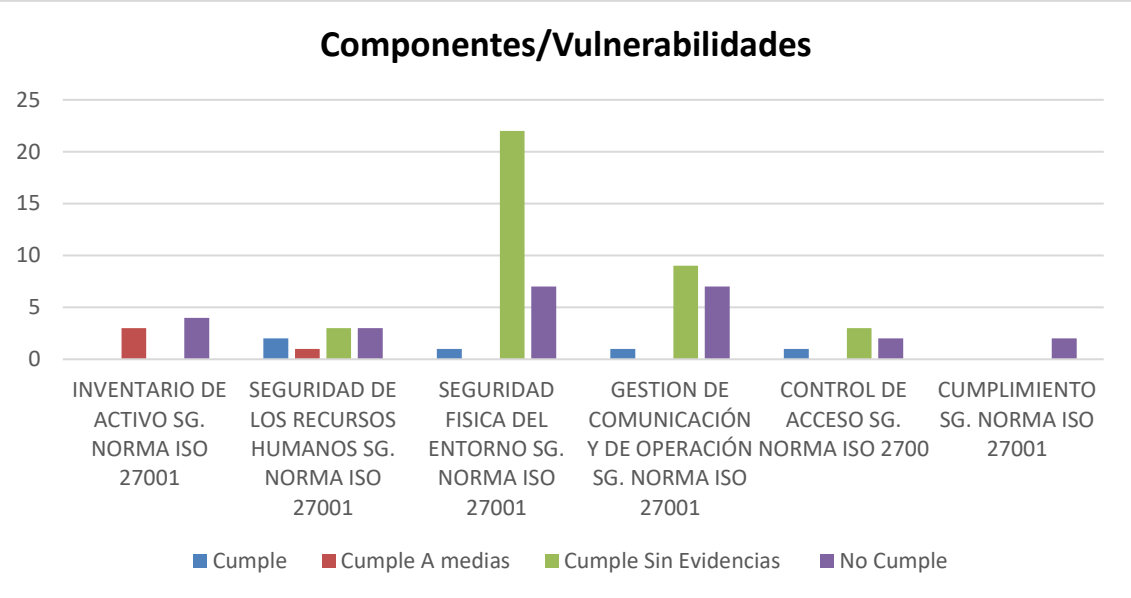


Gráfico 4. 1. Total de vulnerabilidades

En la gráfica 4.1, se puede observar que se encontraron 37 vulnerabilidades en el criterio "**Cumple sin evidencia**" en los componentes de seguridad física del entorno y gestión de la comunicación, seguido del "**No Cumple**" con 25 vulnerabilidades en los componentes antes mencionados adicionando el de cumplimiento, esto quiere decir que hay que llevar un mejor control al cumplimiento de la norma, y tener los respaldos de la documentación necesaria de los procesos para que se lleven estos de manera eficiente.

4.1.2 OBJETIVO 2: EVALUACIÓN LOS RIESGOS, VULNERABILIDADES Y AMENAZAS QUE EXISTEN EN LOS SISTEMAS INSTITUCIONALES MEDIANTE LA METODOLOGÍA DE ANÁLISIS MODAL DE FALLOS Y EFECTOS (AMFE)

El resultado de este objetivo se obtuvo empleando la matriz de riesgos Análisis Modal de Fallos y Efectos (AMFE), se pudo establecer por cada vulnerabilidad encontrada en el *Checklist* establecido con la Norma ISO/IEC 27001:2013, los riesgos, clasificados por cada componente de la norma aplicada, para una mejor compresión y adaptación (cuadro 4.7). (Anexo 4). Como se puede observar Seguridad de los Recursos Humanos es el componente que tiene el

mayor riesgo con el 46,03% y el componente Control de Acceso tiene un riesgo del 23,81%.

Cuadro 4. 7. Porcentaje de Riesgo en cada componente de la norma ISO/IEC 27001:2013

COMPONENTE	NIVEL DE RIESGO	RIESGOS IDENTIFICADOS EN MATRIZ AMFE	% DE RIESGO
Inventario de Activo	Critico	2	9,52%
	Alto	2	
	Medio	2	
	Bajo	0	
	TOTAL	6	
Seguridad de los Recursos Humanos	Critico	0	9,53%
	Alto	5	
	Medio	1	
	Bajo	0	
	TOTAL	6	
Seguridad Física del Entorno	Critico	6	46,03%
	Alto	8	
	Medio	10	
	Bajo	5	
	TOTAL	29	
Gestión de la Comunicación y Operación	Critico	3	23,81%
	Alto	10	
	Medio	2	
	Bajo	0	
	TOTAL	15	
Control de Acceso	Critico	3	7,94%
	Alto	2	
	Medio	0	
	Bajo	0	
	TOTAL	5	
Cumplimiento	Critico	1	3,17%
	Alto	1	
	Medio	0	
	Bajo	0	
	TOTAL	2	
TOTAL DE RIESGOS IDENTIFICADOS		63	100%

Elaboración: El autor

4.1.3. OBJETIVO 3: DISEÑO DE UN PLAN DE MEJORA DE LA SEGURIDAD INFORMÁTICA HACIA LA INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS INFORMÁTICOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN DE CHONE BASADOS EN LA NORMA ISO/IEC 27001

El resultado de este objetivo se obtuvo mediante la elaboración del Plan de Gestión de la seguridad de la información (Anexo 5), para mejorar los aspectos en los procesos, infraestructura, información del departamento tecnológico en el GAD Chone. Además, es importante mencionar que los resultados obtenidos para la elaboración de esta propuesta permitirán tomar acciones correspondientes a la gestión de la seguridad tomando en cuenta la criticidad de los riesgos para emitir medidas correctivas que coadyuven a salvaguardar la información.

4.2. DISCUSIÓN

Los beneficios que se obtienen en la implementación de un SGSI son varios, entre ellos está la toma de conciencia acerca de la necesidad de tratar la seguridad a nivel institucional, la identificación de las áreas de mejora y de control, también la aplicación de acciones correctivas oportunas y efectivas, permitiendo de esta manera brindar el apoyo al cumplimiento de leyes, regulaciones y normas nacionales y/o internacionales con respecto al tema de Seguridad de la Información y el manejo de los mismos, estableciendo bases confiables de conocimiento para la toma de decisiones y planeación de la gestión de seguridad (Bentacourt y Valverde, 2016).

Cada uno de los procesos que se han realizados, basados en la experiencia, no garantizan la seguridad de la información, y toma en cuenta que ésta es un activo de gran valor para la entidad por la cantidad de datos contables, donde se hace necesario una asesoría y seguimiento para la gestión de la seguridad de la información (Moyano y Suárez, 2017).

Por esto un sistema de Gestión de Seguridad de la Información logra generar sentido de pertinencia y compromiso con los temas vinculados a la seguridad, logrando la participación de los miembros de la organización en las diferentes etapas de su desarrollo. El autor de acuerdo con lo mencionado presenta un plan de gestión de seguridad de la información que aporta con medidas de control basados en la norma ISO/IEC 27001:2013 que permite mitigar los riesgos encontrados en los procesos, infraestructura, sistemas y recursos del departamento tecnológico del Municipio de Chone.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- La identificación de la situación actual de los procesos, recursos, infraestructura e información y requerimientos permitió evidenciar la cantidad de vulnerabilidades altas encontradas en la seguridad física del entorno y gestión de comunicación y operación (pág. 18) en la evaluación de la norma aplicada en los diferentes dominios, entre ella tenemos la carencia de documentos, procedimientos formales y guías para una buena gestión de la información y datos de clientes, empleados, entre otros.

- La identificación de las vulnerabilidades (Anexo 3) dio paso a la estimación de los riesgos por niveles: Crítico, Alto, Medio y Bajo, siendo estos evaluados y analizados, determinando las bases para la mejora continua de los procesos del SGSI mediante un plan de gestión que propone las correctivas necesarias para mitigar estos riesgos.

- El nivel de riesgo se determinó a través de la probabilidad e impacto que tenían las vulnerabilidades encontradas (Anexo 4), las mismas que están vinculadas con accesos no autorizados, fallos en los sistemas de gestión, robo, errores y omisiones, ataques internos y externos.

- De acuerdo con la evaluación de los riesgos y las directrices proporcionadas por la ISO/IEC 27001:2013 a través de sus componentes, se estableció el plan de gestión de seguridad de la información donde incluye:
  - ✓ Definición y comunicación de las políticas de seguridad del SGSI
  - ✓ Gestión de activos, responsables, activos de la información
  - ✓ La definición, asignación y comunicación de responsabilidades (Anexo 5).

5.2. RECOMENDACIONES

Se recomienda lo siguiente:

- Tomar en consideración la gestión de incidentes en la seguridad de la información, estableciendo responsabilidades y procedimientos para gestionar los eventos y debilidades de una manera efectiva una vez que hayan sido notificados.

- Disponer de información relevante acerca del estado de acciones preventivas y correctivas, desarrollo de los procesos y estado del cumplimiento de las políticas de seguridad de la información como cambios en el ambiente de la empresa, disponibilidad de recursos, condiciones regulatorias, legales o cambios técnicos.

- Adoptar la norma ISO 27001:2013 para la mejora continua de la seguridad de la información, ya que, a través de un plan de gestión de seguridad de la información, brinda acciones correctivas efectivas que aseguren la salvaguarda de los recursos y activos de la organización.

- Al GADM de Chone, la implementación del Plan de Sistema de Gestión de Seguridad de la Información, en el menor tiempo posible, que permita mitigar los riesgos que están expuestos los datos, los procesos que dan soporte a la operatividad del municipio, así como los sistemas y las redes que son bienes muy importantes para la entidad, y de esta manera brindar una mejora en la disponibilidad, integridad, confidencialidad de la información y la estabilidad de los procesos.

BIBLIOGRAFÍA

Andrade, J., & Chávez, C. (2018). Generación De Un Plan Para La Gestión Integral De Seguridad De La Información Basado En El Marco De La Norma ISO 27001 Y Las Mejores Prácticas De Seguridad De La Norma ISO 27002. Disponible en: http://repositorio.ug.edu.ec/handle/redug/32606

Barragan, I., Góngora, I., & Martínez, E. (2011). ISO/IEC 27001 en Ecuador. Disponible en: https://www.dspace.espol.edu.ec/bitstream/123456789/21546/2/manualtopico.pdf

Bentacourt, D. y Valverde D. (2016). Plan de Implementación de un SGSI. Disponible en: https://colabora.ife.org.mx/sites/SIGETIC/GpoTrabajo/Seguridad/Documentacin/Plan_Implementaci%C3%B3n_SGSI.pdf

Burgos, J., & Campos, P. G. (2008). Modelo Para Seguridad de la Información en TIC. En *EIG*. Vol. 488. pp. 234-253. Disponible en: http://ceur-ws.org/Vol-488/paper13.pdf.

Cairo, M. M. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. Revista Cubana de Ciencias Informaticas, versión On-line ISSN 2227-1899.

Cerón, S. & Dávila, B. (2013). Análisis de la Infraestructura tecnológica necesaria para emplear las TIC. Tesis en Telecomunicaciones mención Gestión empresarial. Guayaquil, Ecuador. Pp 1-199. Disponible en: http://repositorio.ucsg.edu.ec/bitstream/3317/1358/1/T-UCSG-PRE-TEC-ITEL-12.pdf

COIT (Colegio Oficial de Ingeniero de Telecomunicaciones). (2015). Implantación de un SGSI según la norma ISO 27001. Disponible en: https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf

García, C. (2018). Gestión de la Calidad, Riesgos y Evaluación. Tema 3: Herramientas Gestión y Evaluación (II)

Gómez, S. (2007). Seguridad en la Información. Obtenido de http://cybertesis.uni.edu.pe/bitstream/uni/9764/1/gomez_fs.pdf

Hernández, M. G. (2016). Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial. Escuela Superior Politécnica Del Litoral. Guayaquil.

Servicio Ecuatoriano de Normalización INEN. (2017). INEN-ISO/IEC 27002:2017. Norma Técnica Ecuatoriana. Tecnologías de la información - Técnicas de Seguridad - Código de práctica para los controles de seguridad de la información. Vol 1(2). Quito, Pichincha, Ecuador.

Mejía, J. (2015). Plan de Seguridad Informática en el departamento de Tecnologías de la Información y Comunicación de la UTB. Tesis de Ingeniería Informática. Babahoyo, Ecuador. Pp. 1-310. Disponible en: http://dspace.uniandes.edu.ec/bitstream/123456789/732/1/TUAMEIE012-2015.pdf

Montenegro , L. (2017). Propuesta metodológica para la evaluación de seguridad de usuarios de redes sociales con relación a ataques de ingeniería social. Cuenca: Universidad de Cuenca.

Molano, R. (2017). Estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma ISO 27001 en el área de TI para la empresa Market mix. Facultad de Ingeniería. Universidad Católica de Colombia. Bogotá, Colombia. Disponible en: repository.ucatolica.edu.co/bitstream/10983/15240/1/Esp%20Auditoria%20de%20sistemas.pdf

Moyano, L. & Suárez, y. (2017) Plan de implementación del SGSI basado en la norma ISO/IEC 27001:2013 para la empresa interfaces y soluciones. Tesis. Ingeniería Telemática. Universidad Distrital Francisco José de Caldas.

Múnevar, S. (2013). Diseño de una Infraestructura Tecnológica Funcional dentro de un Plan Piloto Propuesto Para La Implementación De Teletrabajo. Disponible en: https://repository.ean.edu.co/bitstream/handle/10882/6024/MunevarSantiago2013.pdf;sequence=7

Nieves, A. (2017). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?Sequence=1&isallowed=y

SANS Institute. (2016). Seguridad en los recursos de información. Disponible en: https://www.sans.org/information-security/

Silveira, E. D. (2010). Análisis modal de fallos y efectos del proceso de prescripción. Farmacia Hospitalaria , 31.

Torres, S. (2010). Obtenido de Infraestructura tecnológica y apropiación de las TIC en la Universidad Autónoma del Estado de Morelos.: http://www.scielo.org.mx/scielo.php?Pid=S0185-26982010000100006&script=sci_arttext

Vásquez, K. & Cárdenas M. (2015). Propuesta de Buenas Prácticas para Fortalecer los Controles de Prevención y Detección Temprana del Cibercrimen en las Empresas Colombianas. Pontificia Universidad Javeriana. Disponible en: https://repository.javeriana.edu.co/bitstream/handle/10554/18900/VasquezZarateKatyAlejandra2015.pdf?sequence=1&isAllowed=y

ANEXOS

ANEXO 1

SOLICITUD APROBADA POR EL GADM CHONE PARA EL LEVANTAMIENTO DE INFORMACIÓN

GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DEL CANTÓN CHONE

DIRECCION DE TALENTO HUMANO

OFICIO CHO19DTHMEMO-0054
Chone, junio 19 de 2019

Ingeniero
JINNSON MANUEL MOREIRA ÁLVAREZ
Presente. -

De mi consideración:

En atención a su Oficio S/N, fechado 27 de mayo de 2019, en el que solicita se le permita realizar el **TRABAJO DE TITULACIÓN** en el GADM Chone, bajo la modalidad de proyecto de investigación, el mismo que consiste en: **"SEGURIDAD DE LA INFORMACIÓN DE INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS INFÓRMATICOS DEL GADM DEL CANTON CHONE, BASADO EN LA NORMA ISO/IEC 27001".**

Al respecto, mediante MEMORANDO CHO-19-DTH-MEMO-0076, de fecha, Chone, mayo 30 de 2019, solicité al Subdirector de Tecnologías de la Información y Comunicación, analizar la viabilidad técnica de la petición hecha por usted.

El Ingeniero Luis Vera Palacios – Subdirector de Tecnologías de la Información y Comunicación, con Memorando N° CHO19-SDTIC-MEMO-0181, recibido en esta Dirección el 17 de junio del presente año, me informa que la petición de realizar su trabajo de titulación, es factible lo lleve a efecto en el área de Tecnologías de la Información y Comunicación.

Ante los antecedentes expuestos, comunico a usted que, a partir de la presente fecha, se puede acercar hasta la Subdirección de Tecnologías de la Información y Comunicación del GADM Chone, a realizar la investigación solicitada.

Particular que comunico a usted, para los fines consiguientes.

Cordialmente,

Ing. Janina Zambrano Alcívar
DIRECTORA DE TALENTO HUMANO
ELIVE

ANEXO 2

CHECKLIST APLICADO AL DEPARTAMENTO TECNOLÓGICO DEL GADM CHONE BASADO EN LA NORMA ISO/IEC 27001:2013

ANEXO 2A. Checklist aplicado y ponderado de acuerdo a la escala de Likert en el departamento de TI Municipio Chone

GAD DEL CANTON CHONE
CUESTIONARIO DE CONTROL INTERNO
Componente: INVENTARIO DE ACTIVO SG. NORMA ISO 27001
Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA: Departamento Tecnológico						
PREGUNTAS	**SI**	**NO**	**N/A**	**CALIFICACIÓN**	**PONDERACIÓN**	**OBSERVACIONES**
1) ¿Cuentan con un Plan Estratégico?		X		1	No cumple	
2) Se llevan los inventario de los activos en formatos físicos?		X		1	No cumple	
3) Se llevan los inventario de los activos en formatos electrónicos?		X		1	No cumple	
4) ¿Llevan los inventarios de los activos de soporte de hardware:				3	Cumple a medias	
a) Equipos Móviles (Smartphone, Tablet, celular, computadoras portátiles, etc.)	X					Se lo realiza en conjunto con Bodega
b) Equipos fijos (servidores, computadoras de escritorio, portátiles, etc.)	X					Se lo realiza en conjunto con Bodega
c)Periféricos de entrada (teclado, ratón, escáner, cámara digital, cámara web, etc.)	X					Se lo realiza en conjunto con Bodega
d) Periféricos de salida (monitor, audífonos, impresoras, proyector, etc.)	X					Se lo realiza en conjunto con Bodega

e) Periféricos y dispositivos de almacenamiento (disco duro portátil, disco flexible, grabador de discos, CD, DVD, Blu-Ray, Memoria USB, etc.)	X					
f) Periféricos de Comunicaciones (Tarjetas USB y tarjeta PCMCIA para redes inalámbricas: WiFi, Bluetooth, GPRS, HSDPA; tarjeta USB para redes alámbricas/inalámbricas de datos y telefonía, etc.)	X					
g) Tableros (de transferencia (bypass) de la unidad de energía (UPS); transferencia de salidas de energía, de transferencia automática de energía, etc.)	X					
h) Sistemas de control de acceso, de aire acondicionado, automático de extinción de incendios, etc.)	X					
5) ¿Llevan los inventarios de los activos de soporte de software?				1	No cumple	
a) Sistemas Operativos		X				
b) Software de servicio, mantenimiento, administración de : servidores, sistema de redes de datos, sistemas de almacenamiento, telefonía, sistemas de UPS, etc.		X				
c) Paquetes de software o software base (suite de ofimática, navegador de internet, mensajería instantánea, etc.)		X				

6) ¿Llevan los inventarios de los activos de soporte de redes?				2	Cumple sin evidencias	
a) Cable de Comunicaciones (Interfaces: RJ-45, RJ-11, etc.; Interfaz: RS232, USB, etc.; Panel de conexión, toma de red o puntos, etc.)		X				
b) Switches	X					
c) Router, Firewall, Controlador de red inalámbrica, etc.	X					
d) Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, etc.	X					
7) Existen activos o grupos de activos que no tienen custodios asignados?	X			2	Cumple a medias	

GAD DEL CANTON CHONE
CUESTIONARIO DE CONTROL INTERNO
Componente: SEGURIDAD DE LOS RECURSOS HUMANOS SG. NORMA ISO 27001
Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA: Departamento Tecnológico						
PREGUNTAS	**SI**	**NO**	**N/A**	**CALIFICACIÓN**	**PONDERACIÓN**	**OBSERVACIONES**
1) ¿Se socializan los procedimientos de mantenimiento preventivo, correctivo de los bienes: Hardware, Software y equipos de comunicación?	X			4	Cumple	Se lo realiza con personal del departamento de TI
2) ¿se responsabiliza al personal del mal uso y destrucción de los equipos tecnológicos asignados a su cargo?	X			4	Cumple	Se firmó acuerdos de confidencialidad

3) ¿El departamento tecnológico tiene delimitadas con claridad sus responsabilidades?	X			2	Cumple sin evidencias	
4) ¿Se han establecido objetivos para el departamento tecnológico?		X		1	No cumple	No se tiene un plan de seguridad estratégica
5) ¿Se han definido por escrito los objetivos del departamento tecnológico?		X		1	No cumple	
6) ¿El número de empleados que trabaja en el departamento de informática son los adecuados a las necesidades de este?	X			3	Cumple a medias	Por el momento hay 11
7) ¿Existen conflictos en el departamento tecnológico por la carga de trabajo?		X		1	No cumple	No hay conflicto pero desearían que se incremente el personal
8) La falta de cumplimiento de sus funciones es debido a:				2	Cumple sin evidencias	
a) falta de personal	X					
b) personal no capacitado carga de trabajo excesivas		X				Falta personal para cumplir con todas las tareas a cabalidad
c) por que realiza otras actividades		X				
d) otras razones		X				
9) ¿Se realiza la devolución de los activos de equipos tecnológicos del personal que finaliza su contrato de trabajo por escrito?	X			2	Cumple sin evidencias	

GAD DEL CANTON CHONE
CUESTIONARIO DE CONTROL INTERNO
Componente: SEGURIDAD FISICA DEL ENTORNO SG. NORMA ISO 27001
Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA: Departamento Tecnológico						
PREGUNTAS	**SI**	**NO**		**CALIFICACIÓN**	**PONDERACIÓN**	**OBSERVACIONES**
1) ¿Se ubican los equipos de repuestos y soportes a una distancia prudente para evitar daños en caso de desastre que afecten las instalaciones principales?	X			2	Cumple sin evidencia	
2) ¿se suministra y se ubica el equipo apropiado contra incendios?	X			2	Cumple sin evidencia	
3) ¿Se realizan mantenimientos de las instalaciones eléctricas y ups?	X			2	Cumple sin evidencia	
4) ¿Se realizan mantenimientos en los sistema y climatización y ductos de ventilación?	X			2	Cumple sin evidencia	
5) ¿Se adoptan controles para minimizar el riesgo de amenazas físicas, potenciales como robo, incendio, entre otras interferencias a las comunicaciones?	X			2	Cumple sin evidencia	
6) ¿ Se diseña y se aplica la protección física para trabajar en las áreas seguras?	X			2	Cumple sin evidencia	

7) ¿Se ubican o se protegen los equipos para reducir el riesgo debido a amenazas o peligros del entorno?	X			2	Cumple sin evidencia	
8) ¿Se monitorean las condiciones ambientales de temperatura y humedad?	X			2	Cumple sin evidencia	
9) ¿Se tiene protección contra descargas eléctricas en las edificaciones de la institución?	X			2	Cumple sin evidencia	
10) ¿Se disponen de filtros protectores en el suministro de energía y en las líneas de comunicación?	X			2	Cumple sin evidencia	
11) ¿Están los equipos tecnológicos protegidos contra fallas de suministro de energía?	X			2	Cumple sin evidencia	
12) ¿Se protege el cableado de la red contra la intersección o daño?	X			2	Cumple sin evidencia	
13) ¿Se separan los cables de energía de los cables de red?	X			2	Cumple sin evidencia	
14) ¿Se separan los cables de energía de los cables de red en el Data Center?	X			2	Cumple sin evidencia	
15) ¿Se llevan las normas locales e internacionales para la implementación de las redes?	X			2	Cumple sin evidencia	No se posee documentación de respaldo
16) ¿Se dispone de documentación, diseños/planos, y la distribución de conexiones de datos de redes inalámbricas y alámbricas?		X		2	Cumple sin evidencia	

17) ¿Se brindan mantenimientos periódicos a los equipos y dispositivos tecnológicos acuerdo a las especificaciones y recomendaciones del proveedor?		X		1	No cumple	Solo cuando es necesario
18) ¿Los mantenimientos de los equipos tecnológicos únicamente los realiza el personal calificado y autorizado?	X			2	Cumple sin evidencia	
19) ¿Se conservan los registros de los mantenimientos preventivos, correctivos o fallas relevantes o sospechosas?		X		1	No cumple	
20) ¿Se establecen controles de mantenimientos programados?		X		1	No cumple	
21) ¿Se llevan un registro de los mantenimientos preventivos y correctivos?		X		1	No cumple	
22) ¿Se custodian los equipos y medios que se encuentran fuera de las instalaciones de la institución?	X			4	Cumple	El custodio es el responsable de equipos fuera de las dependencias
23) ¿Se establece una cobertura adecuada de seguro para proteger los equipos que se encuentran fuera de las instalaciones de la institución?		X		1	No cumple	
24) ¿Existen controles de acceso a las redes inalámbricas de la institución?	X			2	Cumple sin evidencia	
25) ¿Existen controles de acceso a los servidores?	X			2	Cumple sin evidencia	

26) ¿ Se evalúan los dispositivos deteriorados que contengan información sensible antes de enviar a reparación?	X			2	Cumple sin evidencia	
27) ¿Que técnicas utilizan para borrar, destruir o sobrescribir la información sensible de un equipo reutilizado?	x			1	No cumple	
28) ¿Se tiene autorización previa para el retiro de cualquier equipo información o software	X			2	Cumple sin evidencia	Pero no se tiene documentado
29) ¿Se identifican a las personas autorizadas para el retiro de los activos de la institución?	X			2	Cumple sin evidencia	
30) ¿Se lleva un registro cuando el equipo o activo se ha retirado o cuando se ha devuelto	X			4	cumple	Se lo hace en conjunto con Bodega del GAD

GAD DEL CANTON CHONE
CUESTIONARIO DE CONTROL INTERNO
Componente: GESTION DE COMUNICACIÓN Y DE OPERACIÓN SG. NORMA ISO 27001
Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA: Departamento Tecnológico						
PREGUNTAS	**SI**	**NO**				**OBSERVACIONES**
1) ¿Se documenta el proceso de respaldo y restauración de la información?		X		1	No cumple	

2) ¿Se documentan las instrucciones para el manejo de errores y otras condiciones que pueden surgir mediante ejecución de tareas?		X		1	No cumple	
3) ¿Se documentan los procedimientos para el reinicio y recuperación del sistema en caso de fallas?		X		1	No cumple	
4) ¿Se planifica el proceso de cambio y se realiza la prueba correspondiente?		X		1	No cumple	
5) ¿Se establecen responsables y procedimientos formales de control de cambios en los equipos y software?		X		1	No cumple	
6) ¿Se aprueban de manera formal los cambios propuestos?		X		1	No cumple	
7) ¿Existen distribución de funciones y responsabilidades en el Departamento Tecnológico?	X			2	Cumple sin evidencias	
8) ¿Se realizan gestiones de capacidad futura para asegurar el desempeño requerido de los servicios y sistemas informáticos?	X			2	Cumple sin evidencias	
9) ¿Se prohíbe el uso de software no autorizado por la institución?	X			2	Cumple sin evidencias	
10) ¿Se instalan y actualizan periódicamente software de antivirus contra código malicioso?	X			2	Cumple sin evidencias	
11) ¿Se mantienen los sistemas operativos actualizados con las últimas versiones?	X			2	Cumple sin evidencias	

12) ¿ Existen políticas de respaldo de información el Departamento Tecnológico antes del mantenimiento?	X			4	Cumple	Se lo realiza cumpliendo estándares recomendados pero no se evidencia nada
13) ¿ Separan el área de redes con el área de mantenimiento?		X		1	No cumple	
14) ¿ Designan procedimientos y responsabilidades para la asistencia de equipos remotos?	X			2	Cumple sin evidencias	
15) ¿ Se realizan diseños antes de la implementación de una red?	X			2	Cumple sin evidencias	
16) ¿Revisan alertas o fallas del sistema operativo ?	X			2	Cumple sin evidencias	
17) ¿ Realizan cambios de configuración de los controles de seguridad del sistema operativo?	X			2	Cumple sin evidencias	

GAD DEL CANTON CHONE
CUESTIONARIO DE CONTROL INTERNO
Componente: CONTROL DE ACCESO SG. NORMA ISO 27001

Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA: Departamento Tecnológico						
PREGUNTAS	**SI**	**NO**				**OBSERVACIONES**
1) ¿Se identifican y se documentan los equipos que se encuentran en las redes?	X			4	Cumple	Se los identifica pero no se lleva control por escrito

2) ¿Se tiene documentada la identificación de los equipos que están permitidos, según la red que corresponda?	X			2	Cumple sin evidencia	
3) ¿Se implementan procedimientos para controlar la instalación de software en sistemas operativos?		X		1	No cumple	
4) ¿Se lleva un registro de auditoría de las actualizaciones de software que se realizan?		X		1	No cumple	
5) ¿Se tienen restricciones de cambios de paquetes de software?	X			2	Cumple sin evidencia	
6) ¿Se lleva un control de versiones para todas las actualizaciones de software?	X			2	Cumple sin evidencia	

GAD DEL CANTON CHONE
CUESTIONARIO DE CONTROL INTERNO
Componente: CUMPLIMIENTO SG. NORMA ISO 27001

Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA: Departamento Tecnológico						
PREGUNTAS	**SI**	**NO**				**OBSERVACIONES**

1) ¿Se tienen inventariadas todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para cada programa de software, servicio informático y toda información que utilice la institución?		X		1	No cumple	
2) ¿Se tiene conocimiento de todas las normas y leyes generales relacionadas a la gestión de datos e información electrónica?		X		1	No cumple	

ANEXO 3

VULNERABILIDADES ENCONTRADAS A TRAVÉS DE CHECKLIST BASADO EN LA NORMA ISO/IEC 27001:2013

ANEXO 3A. Vulnerabilidades en el componente Inventario de Activo

INVENTARIO DE ACTIVO SG. NORMA ISO 27001			
Vulnerabilidades			
Cumple	Cumple a medias	Cumple sin Evidencias	No Cumple
	Llevan los inventarios de los activos de soporte de hardware		Cuentan con un Plan Estratégico
	Llevan los inventarios de los activos de soporte de redes		Se llevan los inventario de los activos en formatos físicos
	Existen activos o grupos de activos que no tienen custodios asignados		Se llevan los inventario de los activos en formatos electrónicos
			Llevan los inventarios de los activos de soporte de software

Elaboración: El autor

ANEXO 3B. Vulnerabilidades en el componente Seguridad de los Recursos Humanos.

SEGURIDAD DE LOS RECURSOS HUMANOS SG. NORMA ISO 27001			
Vulnerabilidades			
Cumple	Cumple a medias	Cumple sin Evidencias	No Cumple
Se socializan los procedimientos de mantenimiento preventivo, correctivo de los bienes: Hardware, Software y equipos de comunicación	El número de empleados que trabaja en el departamento de informática son los adecuados a las necesidades de este	El departamento tecnológico tiene delimitadas con claridad sus responsabilidades	Se han establecido objetivos para el departamento tecnológico
Se responsabiliza al personal del mal uso y destrucción de los equipos tecnológicos asignados a su cargo		La falta de cumplimiento de sus funciones es debido a la falta de personal	Se han definido por escrito los objetivos del departamento tecnológico
		Se realiza la devolución de los activos de equipos tecnológicos del personal que finaliza su contrato de trabajo por escrito	Existen conflictos en el departamento tecnológico por la carga de trabajo

Elaboración: El autor

ANEXO 3C. Vulnerabilidades en el componente Seguridad Física del Entorno

SEGURIDAD FISICA DEL ENTORNO SG. NORMA ISO 27001			
Vulnerabilidades			
Cumple	Cumple a medias	Cumple sin Evidencias	No Cumple
Se lleva un registro cuando el equipo o activo se ha retirado o cuando se ha devuelto		Se ubican los equipos de repuestos y soportes a una distancia prudente para evitar daños en caso de desastre que afecten las instalaciones principales	Se brindan mantenimientos periódicos a los equipos y dispositivos tecnológicos acuerdo a las especificaciones y recomendaciones del proveedor
		Se suministra y se ubica el equipo apropiado contra incendios	Se conservan los registros de los mantenimientos preventivos, correctivos o fallas relevantes o sospechosas
		Se realizan mantenimientos de las instalaciones eléctricas y ups	Se establecen controles de mantenimientos programados
		Se realizan mantenimientos en los sistema y climatización y ductos de ventilación	Se llevan un registro de los mantenimientos preventivos y correctivos
		Se adoptan controles para minimizar el riesgo de amenazas físicas, potenciales como robo, incendio, entre otras interferencias a las comunicaciones	Se custodian los equipos y medios que se encuentran fuera de las instalaciones de la institución
		Se diseña y se aplica la protección física para trabajar en las áreas seguras	Se establece una cobertura adecuada de seguro para proteger los equipos que se encuentran fuera de las instalaciones de la institución
		Se ubican o se protegen los equipos para reducir el riesgo debido a amenazas o peligros del entorno	Que técnicas utilizan para borrar, destruir o sobrescribir la información sensible de un equipo reutilizado
		Se monitorean las condiciones ambientales de temperatura y humedad	
		Se tiene protección contra descargas eléctricas en las edificaciones de la institución	

		Se disponen de filtros protectores en el suministro de energía y en las líneas de comunicación	
		Están los equipos tecnológicos protegidos contra fallas de suministro de energía	
		Se protege el cableado de la red contra la intersección o daño	
		Se separan los cables de energía de los cables de red	
		Se separan los cables de energía de los cables de red en el Data Center	
		Se llevan las normas locales e internacionales para la implementación de las redes	
		Se dispone de documentación, diseños/planos, y la distribución de conexiones de datos de redes inalámbricas y alámbricas	
		Los mantenimientos de los equipos tecnológicos únicamente los realiza el personal calificado y autorizado	
		Existen controles de acceso a las redes inalámbricas de la institución	
		Existen controles de acceso a los servidores	
		Se evalúan los dispositivos deteriorados que contengan información sensible antes de enviar a reparación	
		Se tiene autorización previa para el retiro de cualquier equipo información o software	
		Se identifican a las personas autorizadas para el retiro de los activos de la institución	

Elaboración: El autor

ANEXO 3D. Vulnerabilidades en el componente Gestión de Comunicación y Operación

GESTION DE COMUNICACIÓN Y DE OPERACIÓN SG. NORMA ISO 27001			
Vulnerabilidades			
Cumple	Cumple a medias	Cumple sin Evidencias	No Cumple
Existen políticas de respaldo de información el Departamento Tecnológico antes del mantenimiento		Existen distribución de funciones y responsabilidades en el Departamento Tecnológico	Se documenta el proceso de respaldo y restauración de la información
		Se realizan gestiones de capacidad futura para asegurar el desempeño requerido de los servicios y sistemas informáticos	Se documentan las instrucciones para el manejo de errores y otras condiciones que pueden surgir mediante ejecución de tareas
		Se prohíbe el uso de software no autorizado por la institución	Se documentan los procedimientos para el reinicio y recuperación del sistema en caso de fallas
		Se instalan y actualizan periódicamente software de antivirus contra código malicioso	Se planifica el proceso de cambio y se realiza la prueba correspondiente
		Se mantienen los sistemas operativos actualizados con las últimas versiones	Se establecen responsables y procedimientos formales de control de cambios en los equipos y software
		Designan procedimientos y responsabilidades para la asistencia de equipos remotos	Se aprueban de manera formal los cambios propuestos
		Se realizan diseños antes de la implementación de una red	Separan el área de redes con el área de mantenimiento
		Revisan alertas o fallas del sistema operativo	
		Realizan cambios de configuración de los controles de seguridad del sistema operativo	

Elaboración: El autor

ANEXO 3E. Vulnerabilidades en el componente Control de Acceso

CONTROL DE ACCESO SG. NORMA ISO 27001			
Vulnerabilidades			
Cumple	Cumple a medias	Cumple sin Evidencias	No Cumple
Se identifican y se documentan los equipos que se encuentran en las redes		Se tiene documentada la identificación de los equipos que están permitidos, según la red que corresponda	Se implementan procedimientos para controlar la instalación de software en sistemas operativos
		Se tienen restricciones de cambios de paquetes de software	Se lleva un registro de auditoría de las actualizaciones de software que se realizan
		Se lleva un control de versiones para todas las actualizaciones de software	

Elaboración: El autor

ANEXO 3F. Vulnerabilidades en el componente Cumplimiento

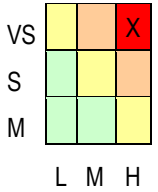
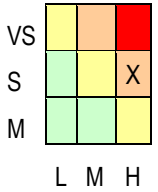
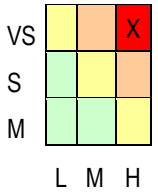
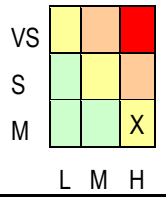
CUMPLIMIENTO SG. NORMA ISO 27001			
Vulnerabilidades			
Cumple	Cumple a medias	Cumple sin Evidencias	No Cumple
			Se tienen inventariadas todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para cada programa de software, servicio informático y toda información que utilice la institución
			Se tiene conocimiento de todas las normas y leyes generales relacionadas a la gestión de datos e información electrónica

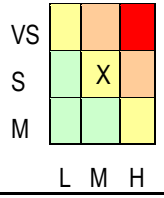
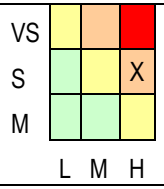
Elaboración: El autor

ANEXO 4

MATRIZ DE ANÁLISIS MODAL, FALLOS Y EFECTOS (AMFE) PARA LA EVALUACIÓN DE LOS RIESGOS

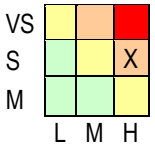
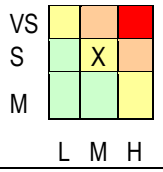
ANEXO 4A. Matriz de Riesgos basado en el componente Inventario de Activo según norma ISO/IEC 27001:2013

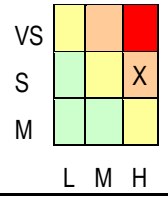
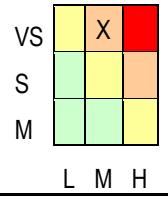
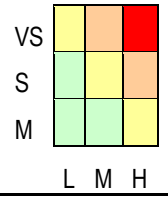
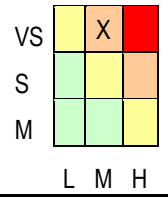
ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R.1.1.	No cuentan con un Plan Estratégico	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.1.1.1	Elaborar un PETI que contengas estrategias alineadas a los objetivos institucionales.	Continuidad del negocio.
R.1.2.	No se llevan los inventario de los activos en formatos físicos	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.1.2.1	Elaborar reportes de los activos que custodia el departamento TI tanto físico como digital	Constancia de los activos del departamento TI.
R.1.3.	No se llevan los inventarios de los activos de soporte de software	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.1.3.1	Realizar registros de inventario de activos que han tenido soporte cada 6 meses.	Registros actualizados
R.1.4.	Se llevan parcialmente los inventarios de los activos de soporte de hardware	Alto 3	Menor 1	Medio		Director/Coordinador TI	A.1.4.1	Cumplir en su totalidad el registro de soporte de los inventarios de activos de hardware	Registros actualizados

R.1.5.	Se llevan parcialmente los inventarios de los activos de soporte de redes	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.1.5.1	Cumplir en su totalidad el registro de soporte de los inventarios de activos de redes	Registros actualizados
R.1.6.	Existen activos o grupos de activos que en parte tienen custodios asignados y otros no.	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.1.6.1	Asignar a todos los equipos tecnológicos ya sea individual o grupal un custodio para la seguridad de los activos.	Mantener la normatividad en el inventario de activos.

Elaboración: El autor

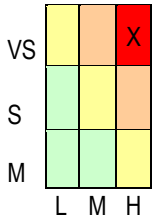
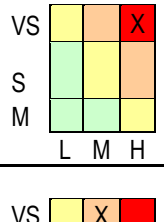
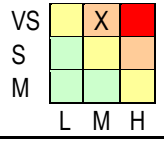
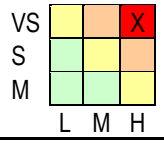
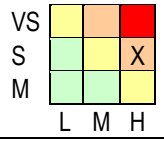
ANEXO 4B. Matriz de Riesgos basado en el componente Seguridad de los Recursos Humanos según norma ISO/IEC 27001:2013

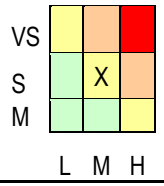
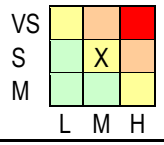
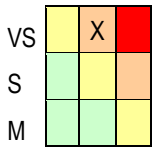
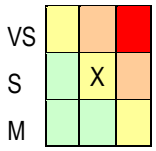
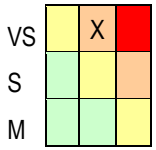
ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R. 2.1.	No se han establecido objetivos para el departamento tecnológico	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.2.1.1	Elaborar los objetivos del departamento para un mejor gobierno TI.	Planes, políticas y procedimientos del departamento TI.
R.2.2.	No se han definido por escrito los objetivos del departamento tecnológico	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.2.1.2	Aprobar mediante resolución por la máxima autoridad los objetivos del departamento TI y socializarlos con el resto del personal.	Integridad del departamento TI.

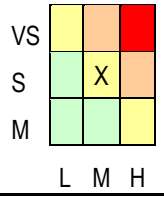
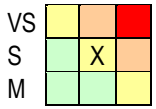
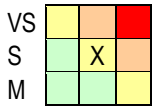
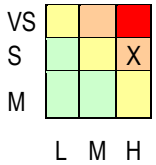
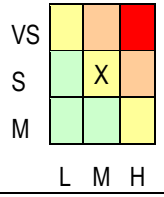
R.2.3	Existen conflictos en el departamento tecnológico por la carga de trabajo	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.2.1.3	El director de TI debe segregar funciones al personal que labora en el departamento	Ambiente laboral estable.
R.2.4.	El departamento tecnológico tiene delimitadas con claridad sus responsabilidades pero no hay un manual que lo evidencie.	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.2.1.4	Efectuar el manual de funciones de rol y responsabilidades para el departamento TI.	Mejorar el ambiente laboral.
R.2.5.	La falta de cumplimiento de sus funciones es debido a la falta de personal	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.2.1.5	Contratar personal capacitado en TI.	Mejorar el ambiente laboral.
R.2.6.	El número de empleados que trabaja en el departamento de informática no son en su totalidad los adecuados a las necesidades de este	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.2.1.6	Seleccionar a los empleados que tienen las capacidades necesarias para realizar las actividades que se manejan en departamento TI.	Capacidad laboral

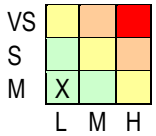
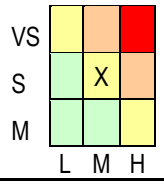
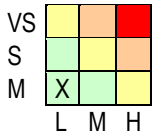
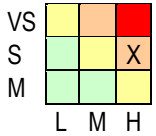
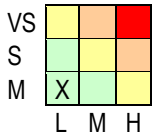
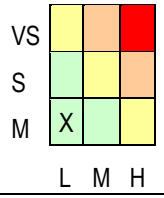
Elaboración: El autor

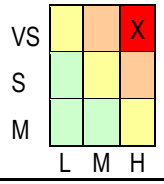
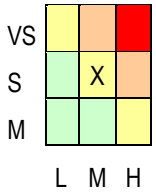
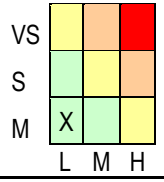
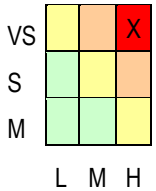
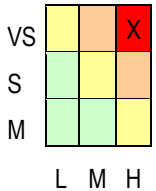
ANEXO 4C. Matriz de Riesgos basado en el componente Seguridad Física del Entorno según norma ISO/IEC 27001:2013

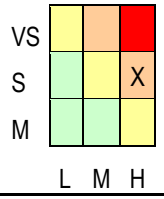
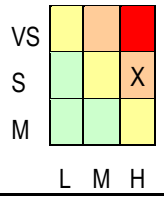
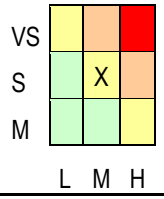
ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R.3.1	No se brindan mantenimientos periódicos a los equipos y dispositivos tecnológicos acuerdo a las especificaciones y recomendaciones del proveedor	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.3.1.1	Realizar mantenimientos periódicos de los equipos, dispositivos tecnológicos según las especificaciones y recomendaciones del proveedor	Mejora de los procesos
R.3.2.	No se conservan los registros de los mantenimientos preventivos, correctivos o fallas relevantes o sospechosas	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.3.2.1	Conservar en áreas seguras los registros de los mantenimientos preventivos y correctivos.	Mejora de los procesos
R.3.3.	No se establecen controles de mantenimientos programados	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.3.1	Establecer controles de mantenimientos programados cada 3 meses.	Control
R.3.4	No se llevan un registro de los mantenimientos preventivos y correctivos	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.3.4.1	Realizar registros de los mantenimientos correctivos y preventivos	Seguridad
R.3.5.	No se custodian los equipos y medios que se encuentran fuera de las instalaciones de la institución	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.5.1	Poner custodios a los equipos que están dentro y fuera de las instalaciones de la empresa.	Control

R.3.6.	No se establece una cobertura adecuada de seguro para proteger los equipos que se encuentran fuera de las instalaciones de la institución	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.3.6.1	Establecer una cobertura de seguro para proteger los equipos que están fuera de la institución	Control
R.3.7.	No se utilizan técnicas para borrar, destruir o sobrescribir la información sensible de un equipo reutilizado	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.3.7.1	Utilizar técnicas de borrado segura para información sensible	Ejecución
R.3.8.	Se ubican los equipos de repuestos y soportes a una distancia prudente para evitar daños en caso de desastre que afecten las instalaciones principales, pero no tienen el lugar adecuado para mantener los equipos en buen estado.	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.8.1	Mantener los equipos de repuestos en lugares que no puedan sufrir daños en caso de desastres y así mantenerlos en buen estado.	Seguridad
R.3.9.	No se evidencia que el equipo sea el apropiado contra incendios	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.3.9.1	Verificar que los equipos contra incendios sean los apropiados para TI.	Control
R.3.10.	Se realizan mantenimientos de las instalaciones eléctricas y ups sin llevar un control de registro de los fallos de los equipos.	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.10.1	Realizar registros de los mantenimientos para llevar detalladamente los fallos de los equipos.	Seguridad

R.3.11.	La unidad no posee alertas o fallas de los sistemas de información, sitios web, equipos tecnológicos.	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.3.11.1	Desarrollar un sistema de alertas o fallos para los sistemas de información	Control
R.3.12.	Se realizan mantenimientos en los sistema y climatización y ductos de ventilación pero no hay evidencia de registros de los mantenimientos.	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.3.12.1	Llevar los registros de mantenimientos en los sistemas y climatización y ductos de ventilación.	Control
R.3.13.	Se adoptan controles para minimizar el riesgo de amenazas físicas, potenciales como robo, incendio, entre otras interferencias a las comunicaciones, pero no hay evidencia de los registros de control.	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.3.13.1	Realizar registros de control de riesgos para minimizar amenazas físicas, robo, incendio, interferencia.	Control
R.3.14.	Se diseña y se aplica la protección física para trabajar en las áreas seguras, pero no se evidencia	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.14.1	Elaborar un diseño de seguridad y protección física de las áreas seguras	Ejecución
R.3.15.	No se evidencia la ubicación o la protección de los equipos para reducir el riesgo debido a amenazas o peligros del entorno	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.3.15.1	Ubicar los equipos en lugares seguros para reducir el riesgo de peligros del entorno	Seguridad

R.3.16.	Se monitorean las condiciones ambientales de temperatura y humedad, pero no hay reportes de control	Bajo 1	Menor 1	Bajo		Área de TI asignada por Director/Coordinador TI	A.3.16.1	Controlar la temperatura ambiental y la humedad para que los equipos no sufran daños o deterioros en su funcionalidad	Seguridad
R.3.17.	No se evidencia la protección contra descargas eléctricas en las edificaciones de la institución	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.3.17.1	Mantenerlas edificaciones de la institución seguras contra descargas eléctricas	Seguridad
R.3.18.	Se disponen de filtros protectores en el suministro de energía y en las líneas de comunicación, sin evidencia	Bajo 1	Menor 1	Bajo		Área de TI asignada por Director/Coordinador TI	A.3.18.1	Colocar filtros protectores el suministro de energía y en las líneas de comunicación	Seguridad
R.3.19.	Están los equipos tecnológicos protegidos contra fallas de suministro de energía, sin evidencia	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.19.1	Proteger los equipos tecnológicos contra fallas de energía	Seguridad
R.3.20.	Se protege el cableado de la red contra la intersección o daño, sin evidencia de control	Bajo 1	Menor 1	Bajo		Área de TI asignada por Director/Coordinador TI	A.3.20.1	Proteger el cableado de la red para que no sufra daños o deterioro	Seguridad
R.3.21.	Se separan los cables de energía de los cables de red, no se evidencia	Bajo 1	Menor 1	Bajo		Área de TI asignada por Director/Coordinador TI	A.3.21.1	Separar los cables de energía de los cables de red	Seguridad

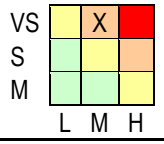
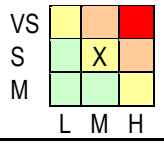
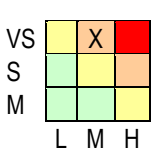
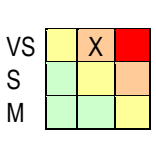
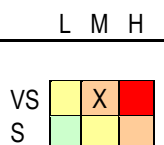
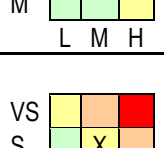
R.3.22.	Se llevan las normas locales e internacionales para la implementación de las redes, parcialmente	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.3.22.1	Adoptar la norma de CGE 410-09 TI.	Mejorar la seguridad
R.3.23.	Se dispone de documentación, diseños/planos, y la distribución de conexiones de datos de redes inalámbricas y alámbricos, no están disponibles	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.3.23.1	Tener toda la información en documentos, diseños, planos, distribución de red	Control
R.3.24.	Los mantenimientos de los equipos tecnológicos únicamente los realiza el personal calificado y autorizado, sin evidencia	Bajo 1	Menor 1	Bajo		Área de TI asignada por Director/Coordinador TI	A.3.24.1	El personal que da mantenimiento a los equipos debe estar capacitado y autorizado para dar el soporte	Control
R.3.25.	Existen controles de acceso a las redes inalámbricas de la institución, sin evidencia de control de acceso a las redes	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.3.25.1	Realizar el control de acceso a las redes inalámbricas de la institución.	E
R.3.26.	Existen controles de acceso a los servidores, sin evidencias de control	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.3.26.1	Efectuar controles de acceso a los servidores	Seguridad

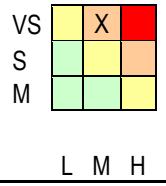
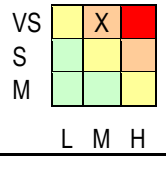
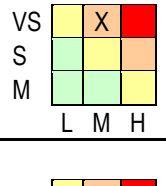
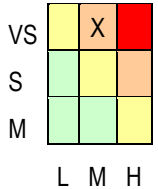
R.3.27.	Se evalúan los dispositivos deteriorados que contengan información sensible antes de enviar a reparación, no hay registros	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.27.1	Realizar la evaluación de equipos deteriorados que contengan información sensible	Control
R.3.28.	Se tiene autorización previa para el retiro de cualquier equipo información o software, sin evidencia de acta de entrega y recepción de equipos.	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.28.1	Para retirar un equipo informático se debe contar con el permiso previo del director de TI..	Control
R.3.29.	Se identifican a las personas autorizadas para el retiro de los activos de la institución, sin credenciales de autorización.	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.3.29.1	El retiro de activos de la institución debe ser hecha formalmente a través de actas de entrega-recepción, e identificando la persona quien lo va a retirar.	Seguridad

Elaboración: El autor

ANEXO 4D. Matriz de Riesgos basado en el componente Gestión de Comunicación y Operación según norma ISO/IEC 27001:2013

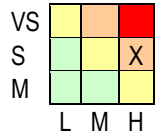
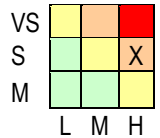
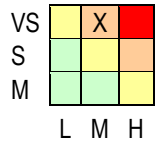
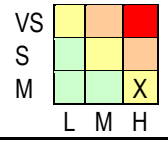
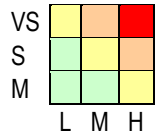
ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R. 4.1.	No se documenta el proceso de respaldo y restauración de la información	Alto 3	Muy Grave 3	Critico	VS S M / L M H — X en (VS, H)	Director/Coordinador TI	A.4.1.1	Documentar el proceso de respaldo y restauración de la información	Control
R.4.2.	No se documentan las instrucciones para el manejo de errores y otras condiciones que pueden surgir mediante ejecución de tareas	Alto 3	Muy Grave 3	Critico	VS S M / L M H — X en (VS, H)	Director/Coordinador TI	A.4.2.1	Documentar los errores y otras fallas que se presentan en la ejecución de tareas	Control
R.4.4.	No se documentan los procedimientos para el reinicio y recuperación del sistema en caso de fallas	Alto 3	Muy Grave 3	Critico	VS S M / L M H — X en (VS, H)	Director/Coordinador TI	A.4.4.1	Documentar los procedimientos para el inicio y recuperación del sistema en caso de fallos.	Control
R.4.5.	No se planifica el proceso de cambio y se realiza la prueba correspondiente	Medio 2	Muy Grave 3	Alto	VS S M / L M H — X en (S, H)	Director/Coordinador de TI - Áreas asignadas	A.4.5.1	Elaborar una planificación de los cambios que se realizan en cada prueba	Ejecución
R.4.6.	No se establecen responsables y procedimientos formales de control de cambios en los equipos y software	Alto 3	Grave 2	Alto	VS S M / L M H — X en (VS, M)	Director/Coordinador de TI - Áreas asignadas	A.4.6.1	Establecer la formalidad en los cambios de equipos y software estableciendo un responsable	Ejecución

R.4.7.	No se aprueban de manera formal los cambios propuestos	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.4.7.1	Aprobar los cambios para que haya formalidad en el proceso	Ejecución
R.4.8.	No se separan el área de redes con el área de mantenimiento	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.4.8.1	Todas las areas del departamento deben estar separadas	Seguridad
R.4.9.	Existen distribución de funciones y responsabilidades en el Departamento Tecnológico, pero no se evidencia el plan	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.4.9.1	Designar funciones de acuerdo al perfil del empleado TI, a través del manual de funciones y responsabilidades	Control
R.4.10.	Se realizan gestiones de capacidad futura para asegurar el desempeño requerido de los servicios y sistemas informáticos, pero no hay informes de desempeño	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.4.10.1	Elaborar indicadores de desempeño de los servicios y sistemas informáticos	Control
R.4.11.	No se evidencia la prohibición del uso de software no autorizado por la institución	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.4.11.1	Mantener la seguridad y control del uso de software no autorizado	Control y seguridad
R.4.12.	Se instalan y actualizan periódicamente software de antivirus contra código malicioso, no hay programa de registros	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.4.12.1	Realizar programas de actualización periódica de antivirus contra código malicioso	Seguridad

R.4.13.	Designan procedimientos y responsabilidades para la asistencia de equipos remotos, no hay manual de funciones y responsabilidades, solo lo hacen al azar.	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.4.13.1	Designar responsabilidades para la asistencia de equipos remotos de acuerdo al manual de procedimientos	Control
R.4.14.	No se realizan diseños antes de la implementación de una red	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.4.14.1	Realizar los diseños de red antes de su implementación	Seguridad de Redes
R.4.15.	No se revisan alertas o fallas del sistema operativo	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.4.15.1	Revisar periódicamente las fallas o alertas del sistema operativo	Ejecución
R.4.16.	No se realizan cambios de configuración de los controles de seguridad del sistema operativo	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.4.16.1	Configurar los controles de seguridad del sistema operativo	Seguridad y Control

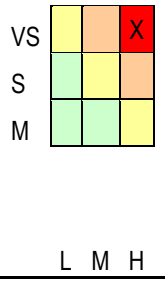
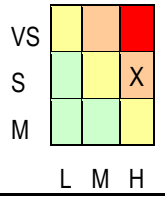
Elaboración: El autor

ANEXO 4E. Matriz de Riesgos basado en el componente Control de Acceso según norma ISO/IEC 27001:2013

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R.5.1.	No se implementan procedimientos para controlar la instalación de software en sistemas operativos	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.5.1.1	Elaborar los procedimientos para el control y uso de software.	Antivirus
R.5.2.	No se lleva un registro de auditoría de las actualizaciones de software que se realizan	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.5.2.1	Elaborar una lista de los controles de auditoria que se hacen en la actualización del software.	Control
R.5.3.	Se tiene documentada la identificación de los equipos que están permitidos, según la red que corresponda, pero no se evidencia	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.5.3.1	Realizar la documentación de identificación de los equipos permitidos, según la red a la que pertenecen.	Registros documental
R.5.4.	No se tienen restricciones de cambios de paquetes de software, sin evidencia	Alto 3	Menor 1	Medio		Director/Coordinador TI	A.5.4.1	Restringir los cambios de paquetes de software	Seguridad
R.5.5.	Se lleva un control de versiones para todas las actualizaciones de software, pero no hay registros	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.5.5.1	Realizar el reporte de versiones actualizadas de software.	Control

Elaboración: El autor

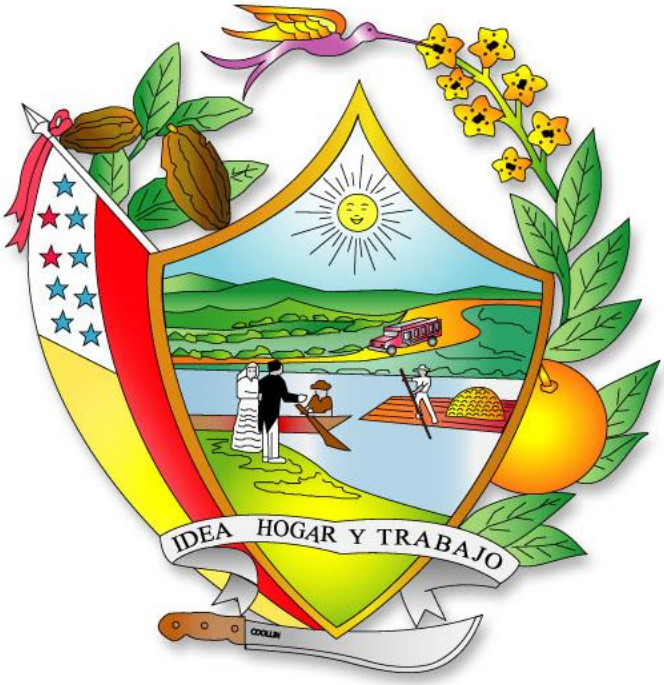
ANEXO 4F. Matriz de Riesgos basado en el componente Cumplimiento según norma ISO/IEC 27001:2013

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R.6.1.	No se tienen inventariadas todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para cada programa de software, servicio informático y toda información que utilice la institución	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.6.1.1	Adoptar la norma de Contraloría General del Estado 410-09 de TI, normas internacionales ISO 27001 para asegurar la información, buenas prácticas para el gobierno TI.	Normativa para la seguridad de la información
R.6.2.	No se tiene conocimiento de todas las normas y leyes generales relacionadas a la gestión de datos e información electrónica	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.6.2.1	Capacitar al personal y al Director TI sobre las leyes que se están rigiendo para la gestión de información	Regulación de la normativa

Elaboración: El autor

ANEXO 5

PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMÁCIÓN Y DE LOS SITEMAS INFORMÁTICOS DEL GADM CHONE



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPIO CHONE

PLAN DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SISTEMAS INFORMÁTICOS

Junio 2019

CONTENIDO

1. INTRODUCCIÓN 4
2. ALCANCE 5
3. OBJETIVOS 5
3.1. OBJETIVO GENERAL 5
3.2. OBJETIVOS ESPECÍFICOS 5
4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) 6
5. NORMA ISO/IEC 27001 6
6. GLOSARIO DE TÉRMINOS 7
7. ANÁLISIS DE VULNERABILIDADES CON ISO/IEC 27001:2013 8
8. ANÁLISIS DE RIESGO CON LA METODOLOGÍA AMFE 10
9. POLÍTICAS DE SEGURIDAD 25
9.1.MEDIDAS DE CONTROL MEDIANTE POLITICAS DE SEGURIDAD 26
9.1.1. POLITICA DE SEGURIDAD FISICA Y DEL ENTORNO 26
9.1.2. POLITICA DE GESTIÓN DE COMUNICACIÓN Y OPERACIÓN . 27
9.1.3. POLITICA DE CONTROL DE ACCESO 28
9.1.4. POLITICAS DE CUMPLIMIENTO 29
10. RESPONSABLES 29
11. CONCLUSIONES Y RECOMENDACIONES 30
11.1. CONCLUSIONES 30
11.2. RECOMENDACIONES 30
BIBLIOGRAFIA 32
ANEXOS 34

CONTENIDO DE TABLAS Y GRAFICOS

Tabla 1. Definición de términos..... 7
Tabla 2. Total de vulnerabilidades en los diferentes componentes de la norma ISO/IEC 27001:2013 9
Tabla 3. Matriz de Riesgos basado en el componente Inventario de Activo según norma ISO/IEC 27001:2013 12
Tabla 4. Matriz de Riesgos basado en el componente Seguridad de los Recursos Humanos según norma ISO/IEC 27001:2013 13
Tabla 5. Matriz de Riesgos basado en el componente Seguridad Física del Entorno según norma ISO/IEC 27001:2013 15
Tabla 6. Matriz de Riesgos basado en el componente Gestión de Comunicación y Operación según norma ISO/IEC 27001:2013..... 20
Tabla 7. Matriz de Riesgos basado en el componente Control de Acceso según norma ISO/IEC 27001:2013 23
Tabla 8. Matriz de Riesgos basado en el componente Cumplimiento según norma ISO/IEC 27001:2013 24
Tabla 9. % de Nivel de Riesgos basado en los componentes según norma ISO/IEC 27001:2013 25

1. INTRODUCCIÓN

La finalidad de este documento es detallar un plan de mejora de Gestión de Seguridad de la Información y sistemas informáticos, que permita optimizar aspectos de seguridad, disponibilidad y confidencialidad en los procesos, recursos, infraestructura y sistemas de información, a través de la descripción de medidas de seguridad que deben ser adoptados según la Norma ISO/IEC 27001:2013.

Este plan detalla las vulnerabilidades que se presentan en los diferentes componentes que tiene la norma aplicada con el checklist, previamente examinados y ponderados, mediante la escala de Likert y la aplicación de una matriz de riesgos según la metodología Análisis Modal de Fallos y Efectos (AMFE), donde se presenta cada una de estas vulnerabilidades por componente, y a su vez determina el nivel de riesgo y el criterio de mitigación.

Además, este Plan de Mejora de seguridad de la información, se procura socializarlo con el GADM Chone, que previa aprobación, fue parte de este trabajo de investigación. Este documento emite medidas estratégicas que aprueben la mejora de los procesos, recursos, infraestructura y sistemas de información donde se encontraron los posibles riesgos que presentan las vulnerabilidades y de esta manera se puedan mitigar y prever eventos maliciosos o sospechosos en la seguridad de la información.

2. ALCANCE

Este plan de mejora abarca lo siguiente:

- Análisis de las vulnerabilidades de los procesos, recursos, infraestructura y sistemas de información aplicando la norma ISO/IEC 27001:2013.
- Identificación y evaluación de los riesgos mediante la metodología AMFE.
- Análisis de los riesgos encontrados en el cumplimiento de la Norma aplicada.
- Medidas de Seguridad para mitigar los riesgos encontrados.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Efectuar un plan de Gestión para la Seguridad de la Información en la Infraestructura Tecnológica y Sistemas Informáticos del Gobierno Autónomo Descentralizado Municipal del Cantón Chone basado en la Norma ISO/IEC 27001:2013 para disminuir los riesgos en los sistemas de información institucional.

3.2. OBJETIVOS ESPECÍFICOS

- Identificar las vulnerabilidades de Seguridad en los procesos, recursos, infraestructura y sistemas de información, basados en el estándar ISO/IEC 27001:2013.
- Analizar los riesgos en aspectos de seguridad, disponibilidad y confidencialidad encontrados en la matriz AMFE.
- Plantear medidas estratégicas preventivas y correctivas que permitan optimizar la seguridad de la información en el GADM Chone.

4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

SGSI: es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. **ISMS** es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, entre otros de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración (ISO, 2014).

Según Del Valle y Chilán (2014) manifiestan que la seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta toda la estructura de la seguridad de la información:

- ✓ **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- ✓ **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- ✓ **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

5. NORMA ISO/IEC 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001:2013 (Nieves, 2017).

6. GLOSARIO DE TÉRMINOS

Tabla 1. Definición de términos

TÉRMINOS	DEFINICIÓN
Dato informático	Toda representación de hechos, información o conceptos expresados de cualquier forma que se presente a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función (MISP y MDN, 2015).
Componentes	Es como se encuentra dividida o clasificada las áreas de aplicación de la Ciberseguridad (Martínez, 2016).
Estrategia	Es una estructura orgánica que se integra en el marco del Sistema de Seguridad Nacional.
Evaluación de riesgos	Es una gestión que se lleva a cabo en las organizaciones para determinar los riesgos efectuados en aspectos de seguridad, disponibilidad y confidencialidad de la información (Rozo, 2016).
Información	Información denominamos al conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado (Guerra, 2017).
Informática	INFORMÁTICA es la ciencia que estudia el tratamiento automático y racional de la información (UCLA, s.f.).
Infraestructuras de tecnología	Es el conjunto de hardware y software sobre el que se asientan los diferentes servicios que la Universidad necesita tener en funcionamiento para poder llevar a cabo toda su actividad, tanto docente como de investigación o de gestión interna (UOC, s.f.).
Medidas de protección	Las medidas de protección son aquellas actitudes y decisiones, a fin de hacer efectivo el cuidado y protección de algo (García, 2017).
Mitigación de riesgos	La mitigación de riesgos sirve para aplicar acciones que permitan reducir la vulnerabilidad a ciertos peligros (García, 2017).

Plan de mejora	Sirve para priorizar las iniciativas más importantes para cumplir con los objetivos y metas que has marcado (Grau, 2019).
Niveles de vulnerabilidad	Se refiere a la poca o inexistente de riesgo.
Norma ISO/iec27001:2013	Es un estándar para la seguridad de la información que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) (López y Ruiz, 2012).
Política de Seguridad	La Política de Seguridad está orientada a gestionar eficazmente la seguridad de la información tratada por las áreas que se encuentran expuestas a amenaza, vulnerabilidades y posibles riesgos de ataques (Enagas, 2019).
Responsables	Ser capaz de tomar decisiones conscientemente, llevar a cabo conductas que persigan mejorarse a uno mismo y/o ayudar a los demás (Sanchéz, 2018).
Riesgos	El riesgo es la probabilidad de que una amenaza se convierta en un desastre.
Seguridad	La seguridad es un estado en el cual los peligros y las condiciones que pueden provocar daños de tipo físico, psicológico o material son controlados para preservar la salud y el bienestar de los individuos y de la comunidad (INSPQ, s.f.).
TICs	Tecnología de la información y comunicaciones.
Vulnerabilidades	La vulnerabilidad es la incapacidad de resistencia cuando se presenta un fenómeno amenazante, o la incapacidad para reponerse después de que ha ocurrido un desastre o riesgos (Carvajal, 2017).
Sistema informático	Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa (MISP y MDN, 2015).

Elaboración: El autor

7. ANÁLISIS DE VULNERABILIDADES CON ISO/IEC 27001:2013

Una vulnerabilidad es un punto débil en la seguridad de un sistema informático. A través de ésta se pueden presentar amenazas que pongan en peligro la confidencialidad e integridad de la información; haciendo un análisis para identificar el tipo y el nivel de cada vulnerabilidad se considera qué tan posible es que las vulnerabilidades se exploten para causar algún daño a los activos. Esto te permitirá conocer el nivel de riesgo. Por ejemplo, una vulnerabilidad alta puede permitir que una persona externa controle el sistema (TSI, 2016).

Los estándares ISO/IEC siempre entregan directrices para dar soluciones a las vulnerabilidades, las mismas que deben buscarse, implementarse y, cuando una solución no es posible o factible, los controles deben ser puestos en su lugar. Este enfoque debe aplicarse con carácter prioritario por lo que las vulnerabilidades que presentan mayor riesgo se abordan en primer lugar.

Para la evaluación de las vulnerabilidades, se aplicaron checklists con los componentes de la norma ISO/IEC 27001:2013, con el fin de verificar el cumplimento según las directrices de esta norma en el sistema de gestión de seguridad de la información. Con los datos obtenidos se pudo identificar las vulnerabilidades, las mismas que fueron ponderadas y clasificadas de acuerdo a la escala de Likert, tomando 4 ítems y considerando solamente 3 de ellos para esta investigación (No Cumple, Cumple sin evidencias y Cumple a medias), para después con ello realizar la matriz AMFE.

De esta manera teniendo un poco claro lo que es una vulnerabilidad, y el proceso de identificación y evaluación de las mismas, este documento se enfocó en mostrar los resultados del total de vulnerabilidades obtenidas en el cumplimiento de la norma ISO/IEC 27001:2013 mediante un checklist aplicado con los componentes seleccionados, para luego ponderarlas y analizarlas, mostrándose en la **tabla 2** lo siguiente:

Tabla 2. Total de vulnerabilidades en los diferentes componentes de la norma ISO/IEC 27001:2013

Componente	Vulnerabilidades			
	Cumple	Cumple A medias	Cumple Sin Evidencias	No Cumple
INVENTARIO DE ACTIVO SG. NORMA ISO 27001	0	3	0	4
SEGURIDAD DE LOS RECURSOS HUMANOS SG. NORMA ISO 27001	2	1	3	3
SEGURIDAD FISICA DEL ENTORNO SG. NORMA ISO 27001	1	0	22	7
GESTION DE COMUNICACIÓN Y DE OPERACIÓN SG. NORMA ISO 27001	1	0	9	7
CONTROL DE ACCESO SG. NORMA ISO 2700	1	0	3	2
CUMPLIMIENTO SG. NORMA ISO	0	0	0	2

27001				
Total	5	4	37	25

Elaboración: El autor

Observando la tabla 2, se puede determinar que el mayor número de 22 vulnerabilidades recae sobre el criterio “Cumple sin evidencia” en los componentes de seguridad física del entorno y gestión de la comunicación, seguido del “No Cumple” en el componente ante mencionado 7 vulnerabilidades, de igual manera en gestión de comunicación y operación, esto quiere decir que hay que llevar un mejor control al cumplimiento de la norma, y tener los respaldos de la documentación necesaria de los procesos para que se lleven estos de manera eficiente.

8. ANÁLISIS DE RIESGO CON LA METODOLOGÍA AMFE

Una vez identificadas las vulnerabilidades en los componentes que maneja la norma ISO/IEC 27001:2013 se empleó la metodología Análisis Modal de Fallos y Efectos (AMFE), la cual especifica las vulnerabilidades encontradas, y de esta manera identificar y evaluar los riesgos por componente al cual pertenecen cada vulnerabilidad. Esta matriz se aplicó al cumplimiento de la Norma antes mencionada cubriendo los componentes de Inventarios de Activos, Seguridad de los Recursos Humanos, Seguridad Física del entorno, Gestión de comunicación y operación, Control de Acceso y Cumplimiento, como se puede apreciar en las **tablas 3**, **4, 5, 6, 7** y **8**, para luego determinar el nivel de riesgo que tienen estas vulnerabilidades encontradas.

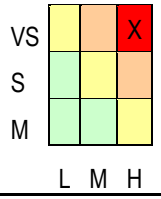
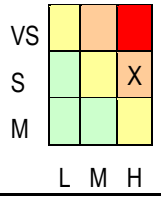
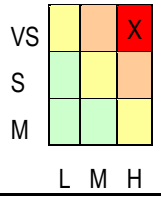
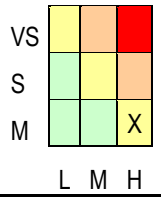
Mediante esta matriz se constituyeron parámetros como, Identificador del riesgo, descripción de la vulnerabilidad, probabilidad, impacto, nivel de riesgo, la acción de mitigación y su criterio de aceptación, que servirán para prever los posibles riesgos a ataques o al mal uso de la información en el GADM Chone. Es importante destacar que se consideraron los siguientes parámetros para determinar el nivel de riesgo:

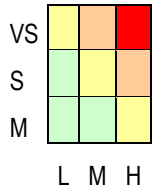
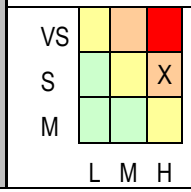
- **Probabilidad:** Alto, Medio y Bajo.

- **Impacto:** Muy Grave, Grave y Menor
- **Nivel de riesgo**: Crítico, Medio y Bajo de las vulnerabilidades.

Una vez que se obtuvo el nivel de riesgo se emiten criterios de mitigación y el responsable directo para la respectiva mitigación y criterios de aceptación.

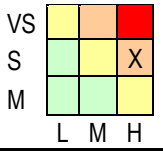
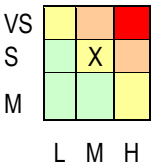
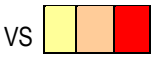
Tabla 3. Matriz de Riesgos basado en el componente Inventario de Activo según norma ISO/IEC 27001:2013

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R.1.1.	No cuentan con un Plan Estratégico	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.1.1.1	Elaborar un PETI que contengas estrategias alineadas a los objetivos institucionales.	Continuidad del negocio.
R.1.2.	No se llevan los inventario de los activos en formatos físicos	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.1.2.1	Elaborar reportes de los activos que custodia el departamento TI tanto físico como digital	Constancia de los activos del departamento TI..
R.1.3.	No se llevan los inventarios de los activos de soporte de software	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.1.3.1	Realizar registros de inventario de activos que han tenido soporte cada 6 meses.	Registros actualizados
R.1.4.	Se llevan parcialmente los inventarios de los activos de soporte de hardware	Alto 3	Menor 1	Medio		Director/Coordinador TI	A.1.4.1	Cumplir en su totalidad el registro de soporte de los inventarios de activos de hardware	Registros actualizados
R.1.5.	Se llevan parcialmente los	Medio	Grave	Medio		Director/Coordinador	A.1.5.1	Cumplir en su totalidad el	Registros

	inventarios de los activos de soporte de redes	2	2			TI		registro de soporte de los inventarios de activos de redes	actualizados
R.1.6.	Existen activos o grupos de activos que en parte tienen custodios asignados y otros no.	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.1.6.1	Asignar a todos los equipos tecnológicos ya sea individual o grupal un custodio para la seguridad de los activos.	Mantener la normatividad en el inventario de activos.

Elaboración: El autor

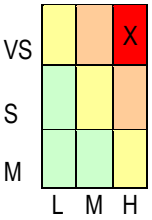
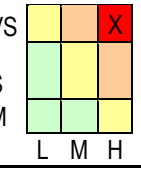
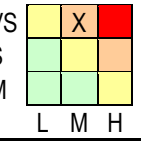
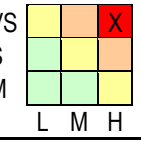
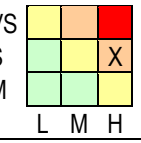
Tabla 4. Matriz de Riesgos basado en el componente Seguridad de los Recursos Humanos según norma ISO/IEC 27001:2013

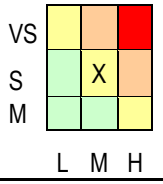
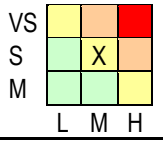
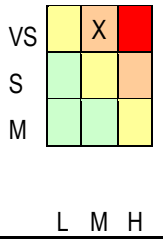
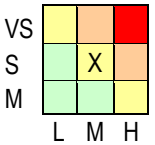
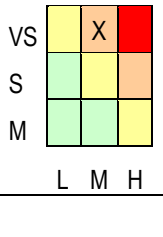
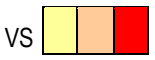
ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R. 2.1.	No se han establecido objetivos para el departamento tecnológico	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.2.1.1	Elaborar los objetivos del departamento para un mejor gobierno TI.	Planes, políticas y procedimientos del departamento TI.
R.2.2.	No se han definido por escrito los objetivos del departamento tecnológico	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.2.1.2	Aprobar mediante resolución por la máxima autoridad los objetivos del departamento TI y socializarlos con el resto del personal.	Integridad del departamento TI.
R.2.3	Existen conflictos en el departamento tecnológico por	Alto	Grave	Alto		Director/Coordinador de TI - Áreas	A.2.1.3	El director de TI debe segregar funciones al	Ambiente laboral estable.

	la carga de trabajo				S M L M H X	asignadas		personal que labora en el departamento	
		3	2						
R.2.4.	El departamento tecnológico tiene delimitadas con claridad sus responsabilidades pero no hay un manual que lo evidencie.	Medio	Muy Grave	Alto	VS S M L M H X	Director/Coordinador de TI - Áreas asignadas	A.2.1.4	Efectuar el manual de funciones de rol y responsabilidades para el departamento TI.	Mejorar el ambiente laboral.
		2	3						
R.2.5.	La falta de cumplimiento de sus funciones es debido a la falta de personal	Alto	Grave	Alto	VS S M L M H	Director/Coordinador de TI - Áreas asignadas	A.2.1.5	Contratar personal capacitado en TI.	Mejorar el ambiente laboral.
		3	2						
R.2.6.	El número de empleados que trabaja en el departamento de informática no son en su totalidad los adecuados a las necesidades de este	Medio	Muy Grave	Alto	VS S M L M H X	Director/Coordinador de TI - Áreas asignadas	A.2.1.6	Seleccionar a los empleados que tienen las capacidades necesarias para realizar las actividades que se manejan en departamento TI.	Capacidad laboral
		2	3						

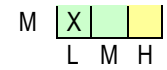
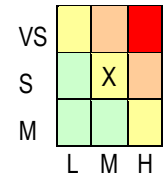
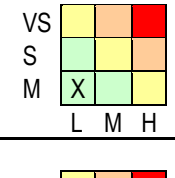
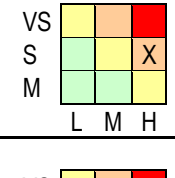
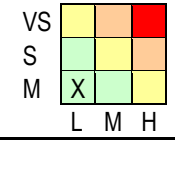
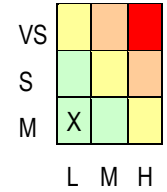
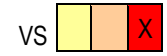
Elaboración: El autor

Tabla 5. Matriz de Riesgos basado en el componente Seguridad Física del Entorno según norma ISO/IEC 27001:2013

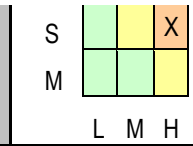
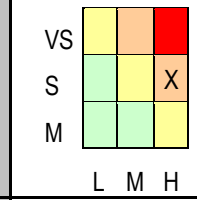
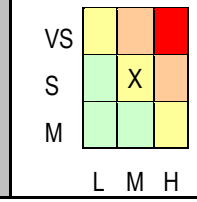
ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R.3.1	No se brindan mantenimientos periódicos a los equipos y dispositivos tecnológicos acuerdo a las especificaciones y recomendaciones del proveedor	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.3.1.1	Realizar mantenimientos periódicos de los equipos, dispositivos tecnológicos según las especificaciones y recomendaciones del proveedor	Mejora de los procesos
R.3.2.	No se conservan los registros de los mantenimientos preventivos, correctivos o fallas relevantes o sospechosas	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.3.2.1	Conservar en áreas seguras los registros de los mantenimientos preventivos y correctivos.	Mejora de los procesos
R.3.3.	No se establecen controles de mantenimientos programados	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.3.1	Establecer controles de mantenimientos programados cada 3 meses.	Control
R.3.4	No se llevan un registro de los mantenimientos preventivos y correctivos	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.3.4.1	Realizar registros de los mantenimientos correctivos y preventivos	Seguridad
R.3.5.	No se custodian los equipos y medios que se encuentran fuera de las instalaciones de la institución	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.5.1	Poner custodios a los equipos que están dentro y fuera de las instalaciones de la empresa.	Control
R.3.6.	No se establece una	Medio	Grave	Medio		Director/Coordinador	A.3.6.1	Establecer una cobertura de	Control

	cobertura adecuada de seguro para proteger los equipos que se encuentran fuera de las instalaciones de la institución					TI		seguro para proteger los equipos que están fuera de la institución	
		2	2						
R.3.7.	No se utilizan técnicas para borrar, destruir o sobrescribir la información sensible de un equipo reutilizado	Medio	Grave	Medio		Director/Coordinador TI	A.3.7.1	Utilizar técnicas de borrado segura para información sensible	Ejecución
		2	2						
R.3.8.	Se ubican los equipos de repuestos y soportes a una distancia prudente para evitar daños en caso de desastre que afecten las instalaciones principales, pero no tienen el lugar adecuado para mantener los equipos en buen estado.	Medio	Muy Grave	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.8.1	Mantener los equipos de repuestos en lugares que no puedan sufrir daños en caso de desastres y así mantenerlos en buen estado.	Seguridad
		2	3						
R.3.9.	No se evidencia que el equipo sea el apropiado contra incendios	Medio	Grave	Medio		Director/Coordinador TI	A.3.9.1	Verificar que los equipos contra incendios sean los apropiados para TI.	Control
		2	2						
R.3.10.	Se realizan mantenimientos de las instalaciones eléctricas y ups sin llevar un control de registro de los fallos de los equipos.	Medio	Muy Grave	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.10.1	Realizar registros de los mantenimientos para llevar detalladamente los fallos de los equipos.	Seguridad
		2	3						
R.3.11.	La unidad no posee alertas o fallas de los sistemas de	Medio	Grave	Medio		Director/Coordinador TI	A.3.11.1	Desarrollar un sistema de alertas o fallos para los	Control

	información, sitios web, equipos tecnológicos.				S M L M H			sistemas de información	
		2	2						
R.3.12.	Se realizan mantenimientos en los sistema y climatización y ductos de ventilación pero no hay evidencia de registros de los mantenimientos.	Medio	Grave	Medio	VS S M L M H	Director/Coordinador TI	A.3.12.1	Llevar los registros de mantenimientos en los sistemas y climatización y ductos de ventilación.	Control
		2	2						
R.3.13.	Se adoptan controles para minimizar el riesgo de amenas físicas, potenciales como robo, incendio, entre otras interferencias a las comunicaciones, pero no hay evidencia de los registros de control.	Medio	Grave	Medio	VS S M L M H	Director/Coordinador TI	A.3.13.1	Realizar registros de control de riesgos para minimizar amenazas físicas, robo, incendio, interferencia.	Control
		2	2						
R.3.14.	Se diseña y se aplica la protección física para trabajar en las áreas seguras, pero no se evidencia	Medio	Muy Grave	Alto	VS S M L M H	Director/Coordinador de TI - Áreas asignadas	A.3.14.1	Elaborar un diseño de seguridad y protección física de las áreas seguras	Ejecución
		2	3						
R.3.15.	No se evidencia la ubicación o la protección de los equipos para reducir el riesgo debido a amenazas o peligros del entorno	Medio	Grave	Medio	VS S M L M H	Director/Coordinador TI	A.3.15.1	Ubicar los equipos en lugares seguros para reducir el riesgo de peligros del entorno	Seguridad
		2	2						
R.3.16.	Se monitorean las condiciones ambientales de temperatura y humedad, pero	Bajo	Menor	Bajo	VS S	Área de TI asignada por Director/Coordinador	A.3.16.1	Controlar la temperatura ambiental y la humedad para que los equipos no	Seguridad

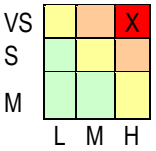
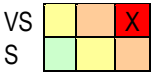
	no hay reportes de control	1	1			TI		sufran daños o deterioros en su funcionalidad	
R.3.17.	No se evidencia la protección contra descargas eléctricas en las edificaciones de la institución	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.3.17.1	Mantenerlas edificaciones de la institución seguras contra descargas eléctricas	Seguridad
R.3.18.	Se disponen de filtros protectores en el suministro de energía y en las líneas de comunicación, sin evidencia	Bajo 1	Menor 1	Bajo		Área de TI asignada por Director/Coordinador TI	A.3.18.1	Colocar filtros protectores el suministro de energía y en las líneas de comunicación	Seguridad
R.3.19.	Están los equipos tecnológicos protegidos contra fallas de suministro de energía, sin evidencia	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.19.1	Proteger los equipos tecnológicos contra fallas de energía	Seguridad
R.3.20.	Se protege el cableado de la red contra la intersección o daño, sin evidencia de control	Bajo 1	Menor 1	Bajo		Área de TI asignada por Director/Coordinador TI	A.3.20.1	Proteger el cableado de la red para que no sufra daños o deterioro	Seguridad
R.3.21.	Se separan los cables de energía de los cables de red, no se evidencia	Bajo 1	Menor 1	Bajo		Área de TI asignada por Director/Coordinador TI	A.3.21.1	Separar los cables de energía de los cables de red	Seguridad
R.3.22.	Se llevan las normas locales e internacionales para la	Alto	Muy Grave	Critico		Director/Coordinador TI	A.3.22.1	Adoptar la norma de CGE 410-09 TI.	Mejorar la seguridad

	implementación de las redes, parcialmente				S M L M H				
		3	3						
R.3.23.	Se dispone de documentación, diseños/planos, y la distribución de conexiones de datos de redes inalámbricas y alámbricos, no están disponibles	Medio	Grave	Medio	VS S X M L M H	Director/Coordinador TI	A.3.23.1	Tener toda la información en documentos, diseños, planos, distribución de red	Control
		2	2						
R.3.24.	Los mantenimientos de los equipos tecnológicos únicamente los realiza el personal calificado y autorizado, sin evidencia	Bajo	Menor	Bajo	VS S M X L M H	Área de TI asignada por Director/Coordinador TI	A.3.24.1	El personal que da mantenimiento a los equipos debe estar capacitado y autorizado para dar el soporte	Control
		1	1						
R.3.25.	Existen controles de acceso a las redes inalámbricas de la institución, sin evidencia de control de acceso a las redes	Alto	Muy Grave	Critico	VS X S M L M H	Director/Coordinador TI	A.3.25.1	Realizar el control de acceso a las redes inalámbricas de la institución.	E
		3	3						
R.3.26.	Existen controles de acceso a los servidores, sin evidencias de control	Alto	Muy Grave	Critico	VS X S M L M H	Director/Coordinador TI	A.3.26.1	Efectuar controles de acceso a los servidores	Seguridad
		3	3						
R.3.27.	Se evalúan los dispositivos deteriorados que contengan	Medio	Muy Grave	Alto	VS	Director/Coordinador de TI - Áreas	A.3.27.1	Realizar la evaluación de equipos deteriorados que	Control

	información sensible antes de enviar a reparación, no hay registros	2	3			asignadas		contengan información sensible	
R.3.28.	Se tiene autorización previa para el retiro de cualquier equipo información o software, sin evidencia de acta de entrega y recepción de equipos.	Alto / 3	Grave / 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.28.1	Para retirar un equipo informático se debe contar con el permiso previo del director de TI..	Control
R.3.29.	Se identifican a las personas autorizadas para el retiro de los activos de la institución, sin credenciales de autorización.	Medio / 2	Grave / 2	Medio		Director/Coordinador TI	A.3.29.1	El retiro de activos de la institución debe ser hecha formalmente a través de actas de entrega-recepción, e identificando la persona quien lo va a retirar.	Seguridad

Elaboración: El autor

Tabla 6. Matriz de Riesgos basado en el componente Gestión de Comunicación y Operación según norma ISO/IEC 27001:2013

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R. 4.1.	No se documenta el proceso de respaldo y restauración de la información	Alto / 3	Muy Grave / 3	Critico		Director/Coordinador TI	A.4.1.1	Documentar el proceso de respaldo y restauración de la información	Control
R.4.2.	No se documentan las instrucciones para el manejo de errores y otras condiciones	Alto	Muy Grave	Critico		Director/Coordinador TI	A.4.2.1	Documentar los errores y otras fallas que se presentan en la ejecución	Control

	que pueden surgir mediante ejecución de tareas	3	3		M L M H			de tareas	
R.4.4.	No se documentan los procedimientos para el reinicio y recuperación del sistema en caso de fallas	Alto 3	Muy Grave 3	Critico	VS S M L M H	Director/Coordinador TI	A.4.4.1	Documentar los procedimientos para el inicio y recuperación del sistema en caso de fallos.	Control
R.4.5.	No se planifica el proceso de cambio y se realiza la prueba correspondiente	Medio 2	Muy Grave 3	Alto	VS S M L M H	Director/Coordinador de TI - Áreas asignadas	A.4.5.1	Elaborar una planificación de los cambios que se realizan en cada prueba	Ejecución
R.4.6.	No se establecen responsables y procedimientos formales de control de cambios en los equipos y software	Alto 3	Grave 2	Alto	VS S M L M H	Director/Coordinador de TI - Áreas asignadas	A.4.6.1	Establecer la formalidad en los cambios de equipos y software estableciendo un responsable	Ejecución
R.4.7.	No se aprueban de manera formal los cambios propuestos	Medio 2	Muy Grave 3	Alto	VS S M L M H	Director/Coordinador de TI - Áreas asignadas	A.4.7.1	Aprobar los cambios para que haya formalidad en el proceso	Ejecución
R.4.8.	No se separan el área de redes con el área de mantenimiento	Medio 2	Grave 2	Medio	VS S M L M H	Director/Coordinador TI	A.4.8.1	Todas las areas del departamento deben estar separadas	Seguridad
R.4.9.	Existen distribución de funciones y responsabilidades en el Departamento Tecnológico, pero no se	Medio 2	Muy Grave 3	Alto	VS S M	Director/Coordinador de TI - Áreas asignadas	A.4.9.1	Designar funciones de acuerdo al perfil del empleado TI, a través del manual de funciones y	Control

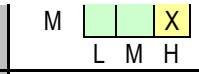
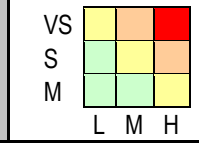
	evidencia el plan				L M H			responsabilidades	
R.4.10.	Se realizan gestiones de capacidad futura para asegurar el desempeño requerido de los servicios y sistemas informáticos, pero no hay informes de desempeño	Medio 2	Muy Grave 3	Alto	VS S M X L M H	Director/Coordinador de TI - Áreas asignadas	A.4.10.1	Elaborar indicadores de desempeño de los servicios y sistemas informáticos	Control
R.4.11.	No se evidencia la prohibición del uso de software no autorizado por la institución	Medio 2	Muy Grave 3	Alto	VS S M X L M H	Director/Coordinador de TI - Áreas asignadas	A.4.11.1	Mantener la seguridad y control del uso de software no autorizado	Control y seguridad
R.4.12.	Se instalan y actualizan periódicamente software de antivirus contra código malicioso, no hay programa de registros	Medio 2	Grave 2	Medio	VS S X M L M H	Director/Coordinador TI	A.4.12.1	Realizar programas de actualización periódica de antivirus contra código malicioso	Seguridad
R.4.13.	Designan procedimientos y responsabilidades para la asistencia de equipos remotos, no hay manual de funciones y responsabilidades, solo lo hacen al azar.	Medio 2	Muy Grave 3	Alto	VS S M X L M H	Director/Coordinador de TI - Áreas asignadas	A.4.13.1	Designar responsabilidades para la asistencia de equipos remotos de acuerdo al manual de procedimientos	Control
R.4.14.	No se realizan diseños antes de la implementación de una red	Medio 2	Muy Grave 3	Alto	VS S M X L M H	Director/Coordinador de TI - Áreas asignadas	A.4.14.1	Realizar los diseños de red antes de su implementación	Seguridad de Redes
R.4.15.	No se revisan alertas o fallas del sistema operativo	Medio 2	Muy Grave 3	Alto	VS S M X	Director/Coordinador de TI - Áreas asignadas	A.4.15.1	Revisar periódicamente las fallas o alertas del sistema operativo	Ejecución

					L M H				
R.4.16.	No se realizan cambios de configuración de los controles de seguridad del sistema operativo	Medio 2	Muy Grave 3	Alto	VS S M L M H	Director/Coordinador de TI - Áreas asignadas	A.4.16.1	Configurar los controles de seguridad del sistema operativo	Seguridad y Control

Elaboración: El autor

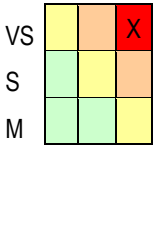
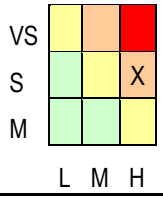
Tabla 7. Matriz de Riesgos basado en el componente Control de Acceso según norma ISO/IEC 27001:2013

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R.5.1.	No se implementan procedimientos para controlar la instalación de software en sistemas operativos	Alto 3	Grave 2	Alto	VS S M L M H	Director/Coordinador de TI - Áreas asignadas	A.5.1.1	Elaborar los procedimientos para el control y uso de software.	Antivirus
R.5.2.	No se lleva un registro de auditoría de las actualizaciones de software que se realizan	Alto 3	Grave 2	Alto	VS S M L M H	Director/Coordinador de TI - Áreas asignadas	A.5.2.1	Elaborar una lista de los controles de auditoria que se hacen en la actualización del software.	Control
R.5.3.	Se tiene documentada la identificación de los equipos que están permitidos, según la red que corresponda, pero no se evidencia	Medio 2	Muy Grave 3	Alto	VS S M L M H	Director/Coordinador de TI - Áreas asignadas	A.5.3.1	Realizar la documentación de identificación de los equipos permitidos, según la red a la que pertenecen.	Registros documental
R.5.4.	No se tienen restricciones de cambios de paquetes de software, sin evidencia	Alto	Menor	Medio	VS S	Director/Coordinador TI	A.5.4.1	Restringir los cambios de paquetes de software	Seguridad

		3	1						
R.5.5.	Se lleva un control de versiones para todas las actualizaciones de software, pero no hay registros	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.5.5.1	Realizar el reporte de versiones actualizadas de software.	Control

Elaboración: El autor

Tabla 8. Matriz de Riesgos basado en el componente Cumplimiento según norma ISO/IEC 27001:2013

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R.6.1.	No se tienen inventariadas todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para cada programa de software, servicio informático y toda información que utilice la institución	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.6.1.1	Adoptar la norma de Contraloría General del Estado 410-09 de TI, normas internacionales ISO 27001 para asegurar la información, buenas prácticas para el gobierno TI.	Normativa para la seguridad de la información
R.6.2.	No se tiene conocimiento de todas las normas y leyes generales relacionadas a la gestión de datos e información electrónica	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.6.2.1	Capacitar al personal y al Director TI sobre las leyes que se están rigiendo para la gestión de información	Regulación de la normativa

Elaboración: El autor

Con estos datos se obtuvo el resultado del Nivel de Riesgo basado en los componentes de la norma aplicada en la investigación, mostrando en la tabla 9 el porcentaje de los riesgos según su nivel.

Tabla 9. % de Nivel de Riesgos basado en los componentes según norma ISO/IEC 27001:2013

COMPONENTE	NIVEL DE RIESGO	RIESGOS IDENTIFICADOS EN MATRIZ AMFE	% DE RIESGO
Inventario de Activo	Critico	2	**9,52%**
	Alto	2	
	Medio	2	
	Bajo	0	
	TOTAL	**6**	
Seguridad de los Recursos Humanos	Critico	0	**9,53%**
	Alto	5	
	Medio	1	
	Bajo	0	
	TOTAL	**6**	
Seguridad Física del Entorno	Critico	6	**46,03%**
	Alto	8	
	Medio	10	
	Bajo	5	
	TOTAL	**29**	
Gestión de la Comunicación y Operación	Critico	3	**23,81%**
	Alto	10	
	Medio	2	
	Bajo	0	
	TOTAL	**15**	
Control de Acceso	Critico	3	**7,94%**
	Alto	2	
	Medio	0	
	Bajo	0	
	TOTAL	**5**	
Cumplimiento	Critico	1	**3,17%**
	Alto	1	
	Medio	0	
	Bajo	0	
	TOTAL	**2**	
TOTAL DE RIESGOS IDENTIFICADOS		**63**	**100%**

Elaboración: El autor

9. POLÍTICAS DE SEGURIDAD

Las políticas de seguridad deben conformar un conjunto de normas y recomendaciones sobre cómo se llevarán a cabo los siguientes temas:

- **Organización de la seguridad:** Establecer un marco gerencial para controlar su implementación.
- **Seguridad del personal:** Reducir riesgos de error humano.
- **Seguridad física y ambiental:** Impedir accesos no autorizados.
- **Gestión de las comunicaciones y las operaciones:** Garantizar el funcionamiento correcto y seguro de las instalaciones de telecomunicaciones.
- **Control de Acceso:** Controlar el acceso lógico a la información.
- **Desarrollo y Mantenimiento de los sistemas:** Medidas de seguridad en los sistemas de información.
- **Administración de la continuidad del negocio:** Proteger los procesos críticos.
- **Cumplimiento:** Impedir infracciones y violaciones de las normas internas y externas (Del Valle y Rodríguez, 2014).

9.1. MEDIDAS DE CONTROL MEDIANTE POLITICAS DE SEGURIDAD

Las siguientes medidas de control están planteadas para mitigar los riesgos a corto plazo, considerando los componentes de mayor nivel de criticidad de los riesgos encontrados como son: Seguridad física y del entorno, Gestión de la comunicación y operación, Control de acceso y cumplimiento.

9.1.1. POLITICA DE SEGURIDAD FISICA Y DEL ENTORNO

- **Medidas de Control en Seguridad Física**

  ✓ Crear medidas de control físicas alrededor de las oficinas del GADM Chone y de las instalaciones de procesamiento de información.

  ✓ Utilizar perímetros de seguridad (pared, puertas de acceso, biométrico, oficina de recepción) para salvaguardar las áreas que contienen activos primordiales como equipos de redes, abastecimiento de energía eléctrica, aire acondicionado y otro sector importante

considerada como crítica para que haya el funcionamiento adecuado de los sistemas de información.

- **Medidas de control de acceso físico**

  ✓ Elaborar bitácoras de registros de las personas que piden audiencia a las áreas protegidas para el registro de fecha y horario de entrada y salida.

  ✓ Controlar el límite del acceso a la información clasificada y a las instalaciones con activos importantes, salvo que tengan acceso autorizado.

  ✓ Determinar un período para examinar los derechos de acceso para áreas protegidas, documentando las actualizaciones realizadas.

  ✓ Examinar cada seis meses los registros de acceso de las áreas protegidas.

- **Medidas de Control de Mantenimiento de Equipo**

  ✓ Llevar un programa de tareas de mantenimiento preventivo con descripciones recomendadas por los proveedores y autorización del Coordinador Técnico TI.

  ✓ Llevar un registro de los mantenimientos correctivos con detalles de los cambios físicos (disco duro, routers, tarjetas de memoria, entre otros) y lógicos (sistema operativo, configuraciones, entre otros) de los equipos que han sufrido algún daño.

  ✓ Mantener el inventario de activos tecnológicos actualizado que permita brindar el mantenimiento preventivo respectivo.

  ✓ Elaborar un registro que genere un reporte de todas las fallas o eventos reales de todos los mantenimientos preventivos y correctivos que se realizan en el GADM Chone.

9.1.2. POLITICA DE GESTIÓN DE COMUNICACIÓN Y OPERACIÓN

- **Medidas de control en documentación de los procedimientos operativos**

✓ Especificaciones para el manejo de los errores o fallas que se pueden dar en la ejecución de tareas.
✓ Personal de soporte inmediato destinado para asistir las dificultades operativas o técnicas imprevistas.
✓ En caso de producir fallos en el sistema documentar el reinicio del sistema y los procedimientos de recuperación del mismo.
✓ Instalación y mantenimiento de equipos de redes y computación.
✓ Resguardo de información.
✓ Gestión de servicios y de incidentes de seguridad donde se realizan las actividades del GADM Chone.

- **Medidas de control para el manejo de incidentes**

✓ Establecer todos los posibles incidentes relacionados a la seguridad.
✓ Implementar controles formalizados de las acciones de recuperación.
✓ Con respecto a la violación de la seguridad y corrección de fallas es necesario la presencia del Coordinador técnico de TI o los directivos del área para tratar estos incidentes ocurridos.

9.1.3. POLITICA DE CONTROL DE ACCESO

- **Medidas de control en la administración de acceso de usuarios**

✓ A través de procedimientos otorgar los permisos para acceder a los sistemas, daos y servicios de información.

- **Medidas de control en el registro de usuarios**

✓ Emplear identificadores de usuarios únicos, con el objeto de identificar usuarios para evitar múltiples perfiles de acceso de un mismo usuario.
✓ Verificar el acceso que tiene el usuario para ver qué rol tiene y si cumple con la política de seguridad del municipio.

✓ Emitir un documento donde se especifique los derechos de acceso a los usuarios.

✓ Mantener una bitácora de todas las personas que utilizan el servicio.

9.1.4. POLITICAS DE CUMPLIMIENTO

- **Medidas de control para el cumplimiento de la política de seguridad**

✓ Cada área tiene un responsable, el cual es encargado de la correcta implementación, cumplimiento de las normas o estándares y procedimientos de seguridad establecidos dentro de su competencia**.**

✓ La realización de las revisiones periódicas de todas las áreas del departamento TI, las debe efectuar el responsable de seguridad informática, quien garantiza el cumplimiento de las normas aplicadas en cada área.

- **Medidas de control en la sanción prevista por incumplimiento**

✓ Todo aquel que viole las políticas de seguridad será sancionado administrativamente de acuerdo a los dispuesto por las normas que regulan al personal.

✓ En las políticas internas de la empresa debe existir un referente al incumplimiento y demás normativas especificas aplicables donde la sanción puede ser ejecutada mediante un acto administrativo.

10. RESPONSABLES

La persona responsable de llevar a cabo la implementación de este plan de mejora de SGSI es el Director de TI, designando a su vez las tareas correspondientes para el cumplimiento de estas medidas de control en las diferentes áreas del departamento TI del GADM Chone.

11. CONCLUSIONES Y RECOMENDACIONES

11.1. CONCLUSIONES

- La información es el activo primordial en cualquier institución, por lo tanto, su seguridad es la responsabilidad de todos dentro de la entidad, la misma que debe estar documentada con manuales, políticas y/o procedimientos aprobados por la máxima autoridad para el buen uso de los activos del Municipio.

- La identificación y la evaluación de los riesgos determinados en la matriz AMFE permitió tomar medidas de control en los componentes de mayor criticidad de riesgo y establecerlas en este plan de mejora para la mitigación de los mismos.

- Esta propuesta coadyuva a la sensibilización sobre seguridad de la información, permitiendo efectuar ambientes del buen uso y manejo de los activos de información.

11.2. RECOMENDACIONES

- Para una mayor y mejor seguridad de la información, el Municipio puede implementar este plan de mejora que entrega medidas de control para los riesgos de mayor criticidad encontrados.
- De la misma manera, al ser aplicada y legalizada por el GADM Chone, ser socializada y concientizada por el personal del departamento TI, para de esta forma obtener una seguridad robusta de los activos de información más importantes para la entidad.
- Es importante también tomar en consideración las normativas o buenas prácticas para la seguridad de los activos de la información, adoptando las

directrices de la Norma ISO/IEC 27001:2013 y de esta manera llevar un mejor control en la seguridad.

BIBLIOGRAFIA

Carvajal. (2017). Definición de ciberseguridad y riesgo. Disponible en: https://www.icemd.com/digital-knowledge/articulos/definicion-ciberseguridad-riesgo/

Del Valle, C. & Chilán, L. (2014) Análisis para la integración de un sistema de gestión de seguridad de la información (SGSI) ISO-27001 Utilizando OSSIM para empresa industrial. Tesis Ingeniería en Sistemas. Universidad Politécnica Salesiana sede Guayaquil. Guayaquil, Ecuador. Pp. 1-155

Enagas. (2019). Politicas de ciberseguridad. Disponible en: https://www.enagas.es/stfls/ENAGAS/Documentos/Politicas/Pol%C3%ADtica%20de%20ciberseguridad%20nf.pdf

García. (2017). Marco Legal - Formas o modalidades legales para operar. Disponible en: http://www.contactopyme.gob.mx/guiasempresariales/guias.asp?s=10&g=4&sg=27

García. (2017). Prevención y mitigación en Gestión de Riesgos de origen natural. Disponible en: https://www.ealde.es/gestion-de-riesgos-prevencion-mitigacion-natural/

Grau. (2019). Los 5 paso para crear el plan de acción definitivo. Disponible en: https://agustingrau.com/plan-de-accion/

Guerra. (2017). Significado de Información. Disponible en: https://www.significados.com/informacion/

INSPQ. (s.f.). Definición del concepto de seguridad. Disponible en: https://www.inspq.qc.ca/es/centro-collaborador-oms-de-quebec-para-la-promocion-de-la-seguridad-y-prevencion-de-traumatismos/definicion-del-concepto-de-seguridad

ISO (International Estándar Organization). (2014). Sistema de Gestión para Seguridad de la Información (SGSI) 27001:2013. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

Martínez. (2016). Ciberseguridad una Guía de supervición. Disponible en: https://auditoresinternos.es/uploads/media_items/guia-supervision-ciberseguridad-fabrica-pensamiento-iai.original.pdf

MISP, & MDN. (2015). Disponible en: Base de una política nacional de ciberseguridad: https://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf

Nieves, A. (2017). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2013. Tesis Ingeniería en seguridad de la información. Colombia. Pp. 1-37.

Rozo. (2016). GESTION DE SEGURIDAD DE LA INFORMACION EN LA INSTITUCIÓN EDUCATIVA LEÓN XIII DEL MUNICIPIO DE SOACHA. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/659/Rozo%20Suarez%20Proyecto%20trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Sanchéz. (2018). Responsabilidad: ¿Qué es? Concepto y claves para ser más responsable. Disponible en: https://blog.cognifit.com/es/responsabilidad/

TSI (Técnico en Seguridad de la Información). (2016). Vulnerabilidades informáticas. Disponible en: https://capacitateparaelempleo.org/assets/4aq4l6q.pdf

UCLA. (s.f.). IMPORTANCIA DE LA INFORMATICA. Disponible en: http://www.ucla.edu.ve/dac/Departamentos/coordinaciones/informaticai/documentos/Resumen%20tema2.pdf

UOC. (s.f.). Infraestructura tecnológica. Disponible en: https://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/index.html

ANEXOS

ANEXO 1

CHECKLIST APLICADOS EN EL DEPARTAMENTO TI DEL GADM CHONE BASADOS EN LOS COMPONENTES DE LA NORMA ISO/IEC 27001:2013

GAD DEL CANTON CHONE
CUESTIONARIO DE CONTROL INTERNO
Componente: INVENTARIO DE ACTIVO SG. NORMA ISO 27001
Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA: Departamento Tecnológico						
PREGUNTAS	**SI**	**NO**	**N/A**	**CALIFICACIÓN**	**PONDERACIÓN**	**OBSERVACIONES**
1) ¿Cuentan con un Plan Estratégico?		X		1	No cumple	
2) Se llevan los inventario de los activos en formatos físicos?		X		1	No cumple	
3) Se llevan los inventario de los activos en formatos electrónicos?		X		1	No cumple	
4) ¿Llevan los inventarios de los activos de soporte de hardware:				3	Cumple a medias	
a) Equipos Móviles (Smartphone, Tablet, celular, computadoras portátiles, etc.)	X					Se lo realiza en conjunto con Bodega
b) Equipos fijos (servidores, computadoras de escritorio, portátiles, etc.)	X					Se lo realiza en conjunto con Bodega
c)Periféricos de entrada (teclado, ratón, escáner, cámara digital, cámara web, etc.)	X					Se lo realiza en conjunto con Bodega
d) Periféricos de salida (monitor, audífonos, impresoras, proyector, etc.)	X					Se lo realiza en conjunto con Bodega
e) Periféricos y dispositivos de almacenamiento (disco duro portátil, disco flexible, grabador de discos, CD, DVD, Blu-Ray, Memoria USB, etc.)	X					
f) Periféricos de Comunicaciones (Tarjetas USB y tarjeta PCMCIA para redes inalámbricas: WiFi, Bluetooth, GPRS, HSDPA; tarjeta USB para redes alámbricas/inalámbricas de datos y telefonía, etc.)	X					

g) Tableros (de transferencia (bypass) de la unidad de energía (UPS); transferencia de salidas de energía, de transferencia automática de energía, etc.)	X					
h) Sistemas de control de acceso, de aire acondicionado, automático de extinción de incendios, etc.)	X					
5) ¿Llevan los inventarios de los activos de soporte de software?				1	No cumple	
a) Sistemas Operativos		X				
b) Software de servicio, mantenimiento, administración de : servidores, sistema de redes de datos, sistemas de almacenamiento, telefonía, sistemas de UPS, etc.		X				
c) Paquetes de software o software base (suite de ofimática, navegador de internet, mensajería instantánea, etc.)		X				
6) ¿Llevan los inventarios de los activos de soporte de redes?				2	Cumple sin evidencias	
a) Cable de Comunicaciones (Interfaces: RJ-45, RJ-11, etc.; Interfaz: RS232, USB, etc.; Panel de conexión, toma de red o puntos, etc.)		X				
b) Switches	X					
c) Router, Firewall, Controlador de red inalámbrica, etc.	X					
d) Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, etc.	X					
7) Existen activos o grupos de activos que no tienen custodios asignados?	X			2	Cumple a medias	

GAD DEL CANTON CHONE
CUESTIONARIO DE CONTROL INTERNO
Componente: SEGURIDAD DE LOS RECURSOS HUMANOS SG. NORMA ISO 27001
Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA: Departamento	

Tecnológico						
PREGUNTAS	**SI**	**NO**	**N/A**	**CALIFICACIÓN**	**PONDERACIÓN**	**OBSERVACIONES**
1) ¿Se socializan los procedimientos de mantenimiento preventivo, correctivo de los bienes: Hardware, Software y equipos de comunicación?	X			4	Cumple	Se lo realiza con personal del departamento de TI
2) ¿se responsabiliza al personal del mal uso y destrucción de los equipos tecnológicos asignados a su cargo?	X			4	Cumple	Se firmó acuerdos de confidencialidad
3) ¿El departamento tecnológico tiene delimitadas con claridad sus responsabilidades?	X			2	Cumple sin evidencias	
4) ¿Se han establecido objetivos para el departamento tecnológico?		X		1	No cumple	No se tiene un plan de seguridad estratégica
5) ¿Se han definido por escrito los objetivos del departamento tecnológico?		X		1	No cumple	
6) ¿El número de empleados que trabaja en el departamento de informática son los adecuados a las necesidades de este?	X			3	Cumple a medias	Por el momento hay 11
7) ¿Existen conflictos en el departamento tecnológico por la carga de trabajo?		X		1	No cumple	No hay conflicto pero desearían que se incremente el personal
8) La falta de cumplimiento de sus funciones es debido a:				2	Cumple sin evidencias	
a) falta de personal	X					
b) personal no capacitado carga de trabajo excesivas		X				Falta personal para cumplir con todas las tareas a cabalidad
c) por que realiza otras actividades		X				
d) otras razones		X				

9) ¿Se realiza la devolución de los activos de equipos tecnológicos del personal que finaliza su contrato de trabajo por escrito?	X			2	Cumple sin evidencias	

GAD DEL CANTON CHONE
CUESTIONARIO DE CONTROL INTERNO
Componente: SEGURIDAD FISICA DEL ENTORNO SG. NORMA ISO 27001
Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA: Departamento Tecnológico						
PREGUNTAS	**SI**	**NO**		**CALIFICACIÓN**	**PONDERACIÓN**	**OBSERVACIONES**
1) ¿Se ubican los equipos de repuestos y soportes a una distancia prudente para evitar daños en caso de desastre que afecten las instalaciones principales?	X			2	Cumple sin evidencia	
2) ¿se suministra y se ubica el equipo apropiado contra incendios?	X			2	Cumple sin evidencia	
3) ¿Se realizan mantenimientos de las instalaciones eléctricas y ups?	X			2	Cumple sin evidencia	
4) ¿Se realizan mantenimientos en los sistema y climatización y ductos de ventilación?	X			2	Cumple sin evidencia	
5) ¿Se adoptan controles para minimizar el riesgo de amenazas físicas, potenciales como robo, incendio, entre otras interferencias a las comunicaciones?	X			2	Cumple sin evidencia	
6) ¿ Se diseña y se aplica la protección física para trabajar en las áreas seguras?	X			2	Cumple sin evidencia	
7) ¿Se ubican o se protegen los equipos para reducir el riesgo debido a amenazas o peligros del entorno?	X			2	Cumple sin evidencia	
8) ¿Se monitorean las condiciones ambientales de temperatura y humedad?	X			2	Cumple sin evidencia	

9) ¿Se tiene protección contra descargas eléctricas en las edificaciones de la institución?	X			2	Cumple sin evidencia	
10) ¿Se disponen de filtros protectores en el suministro de energía y en las líneas de comunicación?	X			2	Cumple sin evidencia	
11) ¿Están los equipos tecnológicos protegidos contra fallas de suministro de energía?	X			2	Cumple sin evidencia	
12) ¿Se protege el cableado de la red contra la intersección o daño?	X			2	Cumple sin evidencia	
13) ¿Se separan los cables de energía de los cables de red?	X			2	Cumple sin evidencia	
14) ¿Se separan los cables de energía de los cables de red en el Data Center?	X			2	Cumple sin evidencia	
15) ¿Se llevan las normas locales e internacionales para la implementación de las redes?	X			2	Cumple sin evidencia	No se posee documentación de respaldo
16) ¿Se dispone de documentación, diseños/planos, y la distribución de conexiones de datos de redes inalámbricas y alámbricas?		X		2	Cumple sin evidencia	
17) ¿ Se brindan mantenimientos periódicos a los equipos y dispositivos tecnológicos acuerdo a las especificaciones y recomendaciones del proveedor?		X		1	No cumple	Solo cuando es necesario
18) ¿Los mantenimientos de los equipos tecnológicos únicamente los realiza el personal calificado y autorizado?	X			2	Cumple sin evidencia	
19) ¿Se conservan los registros de los mantenimientos preventivos, correctivos o fallas relevantes o sospechosas?		X		1	No cumple	
20) ¿Se establecen controles de mantenimientos programados?		X		1	No cumple	
21) ¿Se llevan un registro de los mantenimientos preventivos y correctivos?		X		1	No cumple	

22) ¿Se custodian los equipos y medios que se encuentran fuera de las instalaciones de la institución?	X			4	Cumple	El custodio es el responsable de equipos fuera de las dependencias
23) ¿Se establece una cobertura adecuada de seguro para proteger los equipos que se encuentran fuera de las instalaciones de la institución?		X		1	No cumple	
24) ¿Existen controles de acceso a las redes inalámbricas de la institución?	X			2	Cumple sin evidencia	
25) ¿Existen controles de acceso a los servidores?	X			2	Cumple sin evidencia	
26) ¿Se evalúan los dispositivos deteriorados que contengan información sensible antes de enviar a reparación?	X			2	Cumple sin evidencia	
27) ¿Que técnicas utilizan para borrar, destruir o sobrescribir la información sensible de un equipo reutilizado?	x			1	No cumple	
28) ¿Se tiene autorización previa para el retiro de cualquier equipo información o software	X			2	Cumple sin evidencia	Pero no se tiene documentado
29) ¿Se identifican a las personas autorizadas para el retiro de los activos de la institución?	X			2	Cumple sin evidencia	
30) ¿Se lleva un registro cuando el equipo o activo se ha retirado o cuando se ha devuelto	X			4	cumple	Se lo hace en conjunto con Bodega del GAD

GAD DEL CANTON CHONE
CUESTIONARIO DE CONTROL INTERNO
Componente: GESTION DE COMUNICACIÓN Y DE OPERACIÓN SG. NORMA ISO 27001
Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA: Departamento Tecnológico						
PREGUNTAS	**SI**	**NO**				**OBSERVACIONES**
1) ¿Se documenta el proceso de respaldo y restauración de la información?		X		1	No cumple	

2) ¿Se documentan las instrucciones para el manejo de errores y otras condiciones que pueden surgir mediante ejecución de tareas?		X		1	No cumple	
3) ¿Se documentan los procedimientos para el reinicio y recuperación del sistema en caso de fallas?		X		1	No cumple	
4) ¿Se planifica el proceso de cambio y se realiza la prueba correspondiente?		X		1	No cumple	
5) ¿Se establecen responsables y procedimientos formales de control de cambios en los equipos y software?		X		1	No cumple	
6) ¿Se aprueban de manera formal los cambios propuestos?		X		1	No cumple	
7) ¿Existen distribución de funciones y responsabilidades en el Departamento Tecnológico?	X			2	Cumple sin evidencias	
8) ¿Se realizan gestiones de capacidad futura para asegurar el desempeño requerido de los servicios y sistemas informáticos?	X			2	Cumple sin evidencias	
9) ¿Se prohíbe el uso de software no autorizado por la institución?	X			2	Cumple sin evidencias	
10) ¿Se instalan y actualizan periódicamente software de antivirus contra código malicioso?	X			2	Cumple sin evidencias	
11) ¿Se mantienen los sistemas operativos actualizados con las últimas versiones?	X			2	Cumple sin evidencias	
12) ¿Existen políticas de respaldo de información el Departamento Tecnológico antes del mantenimiento?	X			4	Cumple	Se lo realiza cumpliendo estándares recomendados pero no se evidencia nada
13) ¿Separan el área de redes con el área de mantenimiento?		X		1	No cumple	
14) ¿Designan procedimientos y responsabilidades para la asistencia de equipos remotos?	X			2	Cumple sin evidencias	

15) ¿Se realizan diseños antes de la implementación de una red?	X			2	Cumple sin evidencias	
16) ¿Revisan alertas o fallas del sistema operativo ?	X			2	Cumple sin evidencias	
17) ¿Realizan cambios de configuración de los controles de seguridad del sistema operativo?	X			2	Cumple sin evidencias	

GAD DEL CANTON CHONE
CUESTIONARIO DE CONTROL INTERNO
Componente: CONTROL DE ACCESO SG. NORMA ISO 27001

Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA: Departamento Tecnológico						
PREGUNTAS	**SI**	**NO**				**OBSERVACIONES**
1) ¿Se identifican y se documentan los equipos que se encuentran en las redes?	X			4	Cumple	Se los identifica pero no se lleva control por escrito
2) ¿Se tiene documentada la identificación de los equipos que están permitidos, según la red que corresponda?	X			2	Cumple sin evidencia	
3) ¿Se implementan procedimientos para controlar la instalación de software en sistemas operativos?		X		1	No cumple	
4) ¿Se lleva un registro de auditoría de las actualizaciones de software que se realizan?		X		1	No cumple	
5) ¿Se tienen restricciones de cambios de paquetes de software?	X			2	Cumple sin evidencia	
6) ¿Se lleva un control de versiones para todas las actualizaciones de software?	X			2	Cumple sin evidencia	

GAD DEL CANTON CHONE
CUESTIONARIO DE CONTROL INTERNO
Componente: CUMPLIMIENTO SG. NORMA ISO 27001

Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de

procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.						
ÁREA AUDITADA: Departamento Tecnológico						
PREGUNTAS	**SI**	**NO**				**OBSERVACIONES**
1) ¿Se tienen inventariadas todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para cada programa de software, servicio informático y toda información que utilice la institución?		X		1	No cumple	
2) ¿Se tiene conocimiento de todas las normas y leyes generales relacionadas a la gestión de datos e información electrónica?		X		1	No cumple	