



UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E
INDUSTRIAL
CARRERA DE INGENIERÍA EN SISTEMAS
COMPUTACIONALES E INFORMÁTICOS

TEMA:

PLAN DE CONTINGENCIA INFORMÁTICO PARA EL ÁREA DE TI EN
BASE A LA NORMA DE CALIDAD ISO 27001:2013 PARA LA FUNDACIÓN
CULTURAL Y EDUCATIVA AMBATO - UNIDAD EDUCATIVA ATENAS.

Trabajo de Titulación. Modalidad: Proyecto de Investigación, presentado previo
la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

ÁREA: Administrativas Informáticas.

LÍNEA DE INVESTIGACIÓN: Administración de Recursos.

AUTOR: Burgos Gordón Christian Andrés.

TUTOR: Ing. Julio Balarezo, PhD.

Ambato - Ecuador

Agosto - 2020

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Titulación con el tema: “PLAN DE CONTINGENCIA INFORMÁTICO PARA EL ÁREA DE T I EN BASE A LA NORMA DE CALIDAD ISO 27001:2013 PARA LA FUNDACIÓN CULTURAL Y EDUCATIVA AMBATO - UNIDAD EDUCATIVA ATENAS”, desarrollado bajo la modalidad Proyecto de Investigación por el señor Burgos Gordón Christian Andrés, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, agosto 2020



Firmado electrónicamente por:
**JULIO ENRIQUE
BALAREZO LOPEZ**

Ing. Julio Balarezo, PhD.

TUTOR

AUTORÍA

El presente Proyecto de Investigación titulado: “PLAN DE CONTINGENCIA INFORMÁTICO PARA EL ÁREA DE TI EN BASE A LA NORMA DE CALIDAD ISO 27001:2013 PARA LA FUNDACIÓN CULTURAL Y EDUCATIVA AMBATO - UNIDAD EDUCATIVA ATENAS” es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, agosto 2020



Burgos Gordón Christian Andrés

CC:1804577169

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Burgos Gordón Christian Andrés, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación titulado “PLAN DE CONTINGENCIA INFORMÁTICO PARA EL ÁREA DE TI EN BASE A LA NORMA DE CALIDAD ISO 27001:2013 PARA LA FUNDACIÓN CULTURAL Y EDUCATIVA AMBATO - UNIDAD EDUCATIVA ATENAS”, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta del Tribunal.

Ambato, agosto 2020



Firmado electrónicamente por:
**ELSA PILAR
URRUTIA**

Ing. Pilar Urrutia, Mg.

PRESIDENTA DEL TRIBUNAL



Firmado electrónicamente por:
**CARLOS ISRAEL
NUNEZ MIRANDA**



Firmado electrónicamente por:
**DENNIS VINICIO
CHICAIZA
CASTILLO**

Ing. Dennis Chicaiza, Mg.
DOCENTE CALIFICADOR

Ing. Carlos Núñez, Mg.
DOCENTE CALIFICADOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, agosto 2020



Burgos Gordón Christian Andrés

CC:1804577169

AUTOR

DEDICATORIA

El presente proyecto lo dedico en primer lugar a Dios, quien me dio la inteligencia, fortaleza y constancia durante mi carrera ayudándome a superar cada dificultad que se presentaba.

A mis padres Andrés Burgos y Mercedes Gordón que fueron mi principal apoyo en mi educación, con sus ejemplos y enseñanzas de superación inculcándome a saber perseguir mis objetivos y llegar a ser un profesional.

A mis amigos y compañeros que en su momento me brindaron apoyo y con quienes superábamos cada obstáculo durante la carrera apoyándonos mutuamente.

Además le dedico a una persona muy especial Andreina, que llegó a mi vida de que estaba cursando la mitad de mi carrera, por su apoyo y amor incondicional que me brinda siempre motivándome a conseguir mis objetivos.

Burgos Gordón Christian Andrés

AGRADECIMIENTO

Agradezco a la Universidad Técnica de Ambato en especial a la Facultad de Ingeniería en Sistemas, Electrónica e Industrial la cual me dio la oportunidad para formarme profesionalmente.

A cada uno de los docentes de los diferentes niveles de la carrera de Ingeniería en Sistemas Computacionales e Informáticos, que con sus enseñanzas y apoyo logré terminar mi formación académica.

Al personal que forma parte de la Unidad Educativa Atenas que me apoyo dándome apertura tanto para realizar mis prácticas preprofesionales, ayudándome a desarrollar mis conocimientos ya en el campo laboral y en este punto mi proyecto de investigación.

Gracias a mi tutor Ing. Julio Balarezo por ser una excelente persona y compartir sus conocimientos que fueron fundamentales para la elaboración y culminación del presente trabajo de investigación.

Burgos Gordón Christian Andrés

ÍNDICE

APROBACIÓN DEL TUTOR	ii
AUTORÍA	iii
APROBACIÓN DEL TRIBUNAL DE GRADO	iv
DERECHOS DE AUTOR	v
DEDICATORIA	vi
AGRADECIMIENTO	vii
RESUMEN EJECUTIVO	xiii
ABSTRACT	xiv
CAPÍTULO 1 MARCO TEÓRICO	1
1.1 Antecedentes Investigativos	1
1.2 Objetivos	3
CAPÍTULO 2 METODOLOGÍA	4
2.1 Materiales	4
2.1.1 Humanos	4
2.1.2 Institucionales	4
2.1.3 Otros	4
2.2 Métodos	8
2.2.1 Evaluación de riesgos informáticos	11
2.2.1.1 Riesgos de Seguridad y Privacidad de la Información	12
2.2.1.2 Riesgos de Ciberseguridad	13
2.2.1.3 Valoración de Activos	13
2.2.1.4 Análisis de Riesgo	15
2.2.2 Modalidad de la investigación	18
2.2.3 Recolección de información	18

2.2.4	Procesamiento y análisis de datos	19
2.2.5	Desarrollo del proyecto	19
CAPÍTULO 3 RESULTADOS Y DISCUSIÓN		20
3.1	Análisis y discusión de los resultados	20
3.1.1	Desarrollo de la propuesta	20
3.1.2	Planificación	20
3.1.3	Alcance	20
3.1.4	Diagnóstico de la situación actual	21
3.1.5	Direccionamiento Estratégico de la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas	22
3.1.6	Políticas de seguridad	22
3.1.7	Ubicación geográfica	28
3.1.8	Departamentos de la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas	29
3.1.9	Activos de información	31
3.1.10	Red de datos	31
3.1.11	Cuarto de telecomunicaciones	34
3.1.12	Descripción de los equipos de red	34
3.1.13	Activos de software	35
3.1.14	Activos de hardware	37
3.1.15	Servicios del departamento informático	42
3.1.16	Personal	42
3.1.17	Evaluación de riesgos y escenarios de contingencia	43
3.1.18	Evaluación de los Activos de la Fundación Cultural y Educativa Ambato – Unidad Educativa Atenas	44
3.1.19	Evaluación de las amenazas	45
3.1.20	Matriz de contingencia	47
3.1.21	Identificación de controles preventivos	49
3.1.22	Formación de grupos y asignación de roles en caso de una contingencia	49
3.1.23	Priorización de recursos tecnológicos	50
3.1.24	Declaración de Aplicabilidad	51
3.1.25	Estado y aplicabilidad de los controles de seguridad de la información ISO 27001:2013	52
3.1.26	Métricas y resultados de la evaluación de los controles ISO 27001:2013 - Anexo A	67
3.2	Diseño del plan de contingencia informático	68

CAPÍTULO 4 CONCLUSIONES Y RECOMENDACIONES	95
4.1 Conclusiones	95
4.2 Recomendaciones	96
Bibliografía	97
Anexos	99

ÍNDICE DE TABLAS

2.1	Valoración de Activos.	14
2.2	Probabilidad de Ocurrencia.	16
2.3	Prioridades de Evaluación del Impacto.	17
3.1	Direccionamiento Estratégico UEA	22
3.2	Amenazas naturales y antrópicas en la parroquia de Izamba	28
3.3	Activos de Información.	31
3.4	Redes de Comunicación de la Unidad Educativa Atenas.	32
3.5	Activos Físicos de Red.	34
3.6	Activos de Software Personal Administrativo.	35
3.7	Activos de Software Dpto. Sistemas.	35
3.8	Activos de Software Dpto. Contabilidad.	36
3.9	Activos de Software Personal Docente.	36
3.10	Activos de Software Dpto. Marketing.	37
3.11	Activos de Software Dpto. Diseño.	37
3.12	Activos de Hardware Dpto. Administrativos.	38
3.13	Activos de Hardware Área de Colegio.	39
3.14	Activos de Hardware Área de Escuela.	40
3.15	Activos de Hardware Área de Inicial.	41
3.16	Activos de Hardware Área de Artes.	41
3.17	Activos de Hardware Área del Bar.	42
3.18	Evaluación de Suspensión de Principales Servicios de la UEA	42
3.19	Personal del Dpto. de Sistemas de la Unidad Educativa Atenas.	43
3.20	Valoración de los Activos de la Unidad Educativa Atenas.	44
3.21	Evaluación de las Amenazas a los Activos de la UEA.	46
3.22	Evaluación de las Amenazas a Activos Físicos.	48
3.23	Roles y Responsabilidades en Caso de una Contingencia.	50
3.24	Requerimientos de Seguridad de los Activos de la UEA.	51
3.25	Estado y Aplicabilidad de los Controles ISO 27001:2013.	53
3.26	Valoración de los Controles SGSI.	67
3.27	Escenarios de Contingencia	88

ÍNDICE DE FIGURAS

2.1	Recursos Utilizados	4
2.2	Proceso de un Sistema de Información	5
2.3	Pasos del Método Delphi	10
2.4	Niveles de Madurez de SW-CMM.	11
2.5	Proceso para la Gestión de Riesgos.	12
2.6	Niveles de Riesgo.	17
3.1	Diagrama de Proceso Respaldo de Información.	24
3.2	Diagrama de Proceso Mantenimiento de Hardware y Software. . .	27
3.3	Vista Satelital Ubicación Geográfica de la Unidad Educativa Atenas.	29
3.4	Organigrama Institucional UEA.	30
3.5	Topología Física de la Red UEA.	33
3.6	Dominios Anexo “A” de ISO 27001:2013	52
3.7	Estado Global del SGSI.	68
3.8	Flujograma ante el fallo en los servicios de comunicaciones entre cliente – servidor de la UEA.	89
3.9	Flujograma ante el fallo crítico en un servidor del cuarto de telecomunicaciones.	90
3.10	Flujograma ante el corte del suministro eléctrico.	91
3.11	Flujograma ante perdida de la conectividad a internet	92
3.12	Flujograma para la restauración del cuarto de servidores	93
3.13	Flujograma ante la ausencia parcial o total del personal en el área de tecnologías de la información.	94

RESUMEN EJECUTIVO

Un plan de contingencia informático es un conjunto de actividades que nos permiten realizar acciones para minimizar los riesgos en caso de algún desastre de origen natural o humano, manteniendo la operatividad de las actividades a un mínimo nivel hasta recuperar la totalidad de los sistemas y recursos, en la actualidad la información de cualquier empresa o institución es prioridad, en conjunto con los procesos y sistemas informáticos los cuales son considerados como sus activos más importantes debiendo protegerlos y garantizar su confiabilidad, disponibilidad e integridad para de esta manera mantener una excelente imagen institucional.

El constante avance de las Tecnologías de la Información y Comunicación, ha conllevado también al incremento de las amenazas para los activos informáticos que se aprovechan de las vulnerabilidades causando incidentes informáticos dando como resultado la detención parcial o total de los procesos y actividades normales que desarrolla una entidad, por tal razón se debe contar con un plan de contingencia informático actualizado y así poder evitar o minimizar los efectos de los incidentes informáticos garantizando la continuidad operativa de la institución y la integridad de sus datos.

El presente proyecto de investigación, plantea el Diseño de un Plan de Contingencia Informático en base a la norma de calidad ISO 27001:2013 para la Unidad Educativa Atenas, evaluando cada una de las amenazas y vulnerabilidades a los que se encuentran expuestos sus principales activos informáticos. Este plan permitirá la recuperación ante cualquier eventualidad que pueda afectar la continuidad de las actividades de la institución, reduciendo el impacto producido, ya que detalla las acciones a tomar antes, durante o después de la materialización de las amenazas, realizando la restauración de los equipos y actividades a su estado inicial, evitando la pérdida de información valiosa para la unidad educativa.

PALABRAS CLAVES: amenazas, riesgo, disponibilidad, integridad, confiabilidad, ISO 27001, plan de contingencia informático.

ABSTRACT

A computer contingency plan is a set of activities that allow us to carry out actions to minimize risks in the event of a disaster of natural or human origin, keeping the operation of the activities at a minimum level until recovering all the systems and resources, At present, the information of any company or institution is a priority, together with the computer processes and systems which are considered as its most important assets, and must protect them and guarantee their reliability, availability and integrity in order to maintain an excellent institutional image.

The constant advance of Information and Communication Technologies, has also led to the increase in threats to computer assets that exploits vulnerabilities causing computer incidents resulting in partial or total arrest of normal processes and activities that develops a entity, for this reason you must have an updated computer contingency plan and thus be able to avoid or minimize the effects of computer incidents guaranteeing the operational continuity of the institution and the integrity of your data.

This research project proposes the Design of a Computer Contingency Plan based on the quality standard ISO 27001: 2013 for the Athens Education Unit, evaluating each of the threats and vulnerabilities to which its main IT assets are exposed . This plan will allow recovery in the event of any eventuality that may affect the continuity of the institution's activities, reducing the impact produced, since it details the actions to be taken before, during or after the materialization of the threats, by restoring the equipment. and activities to their initial state, avoiding the loss of valuable information for the educational unit.

KEYWORDS: threats, risk, availability, integrity, reliability, ISO 27001, computer contingency plan.

CAPÍTULO 1

MARCO TEÓRICO

1.1. Antecedentes Investigativos

Revisado archivos investigativos desde de las fuentes bibliográficas de Internet se ha encontrado los siguientes trabajos:

“Implementación del primer Sistema de Gestión de Seguridad de la Información, en el Ecuador, certificado bajo la norma ISO 27001:2005”. Elaborado por José Alfonso Aranda Segovia trabajo realizado en Guayaquil - Ecuador en el año 2009, en cuyas conclusiones menciona lo siguiente:

La norma ISO 27001 está orientada al tratamiento de la seguridad de la información mediante la gestión del riesgo, tanto para sus activos como para sus procesos; esto garantiza que ante recursos limitados las inversiones sean bien focalizadas, para lograr ello se necesita de la concientización de la compañía ya que es un pilar fundamental de esta norma, por lo cual las organizaciones deben ingeniosamente buscar y adoptar mecanismos que permitan que se despierte un interés y compromiso por parte de todos los empleados. Además al tener implantado un SGSI certificado bajo la norma ISO 27001:2005 no significa contar con seguridad máxima en la información de la organización sino que esto representa que la empresa cumple con los requerimientos y mejores prácticas establecidas en dicha norma para que su SGSI actual funcione correctamente y además pueda evolucionar hacia la sofisticación.[1]

“Plan de contingencia para la unidad de sistemas y tecnología de información del Gobierno Autónomo Descentralizado Antonio Ante en base a la norma ISO/IEC 27001”. Elaborado por Karina Alexandra Méndez Luna realizado en Ibarra - Ecuador en el año 2015, en cuyas conclusiones menciona lo siguiente:

El desarrollo del diseño de un plan de contingencia informático permite conocer las vulnerabilidades latentes en infraestructura de red y servicios dentro de la institución, y pone a consideración de las autoridades los respectivos correctivos

mediante la identificación, evaluación de los riesgos y escenarios de contingencia en los activos considerados críticos para la institución se realizó en base a perfiles de amenazas, considerando el impacto ocasionado si llegan a materializarse los riesgos, Se definen recomendaciones para el control y administración de la red de la institución que permitan asegurar la operatividad de la red al mínimo de su capacidad con la finalidad de minimizar pérdidas económicas y de reputación. De tal manera que una institución provista de un plan de contingencia informático va a estar preparada para eventos inesperados, tomar medidas oportunas y soluciones eficientes.[2]

“Diseño de un Plan de Contingencia del Sistema de Información para la entidad ITRC”. Elaborado por Héctor Alfonso Acosta Ramírez realizado en Bogota - Colombia, en cuyas conclusiones menciona lo siguiente:

En el análisis de riesgos siguiendo los pasos de la metodología ‘MAGERIT’ se encontró precisamente la necesidad de un plan de contingencia que le permita a la Entidad estar preparada en caso de siniestros que comprometan el normal funcionamiento del sistema de información a la vez que la red de información se requiere la aplicación de mayores controles, se plantearon las actividades que se ejecutaran para recuperar todos los procesos en el sitio principal y también en el sitio alterno. Este proyecto es de gran ayuda para la Agencia ITRC porque permite tener el plan de contingencia con el cual se está preparado en caso de eventualidades.[3]

En el centro de informática de la empresa de Acensa, C. A, la cual implemento un modelo de un plan de contingencia para posibles pérdidas de información, ya que mantiene información de clientelas en diferentes sectores de Venezuela, en esta información se maneja la cantidad de personas en un edificio y en qué departamento se encuentra, además la empresa se encarga de la programación y mantenimiento de los ascensores y en el equipo de informática guardan los sistemas de programación, es por ello que decidieron la creación del plan de contingencia y tener un respaldo de información ante una pérdida de la misma.[4]

1.2. Objetivos

General

- Diseñar un plan de contingencia informático para el área de TI en base a la norma de calidad ISO 27001:2013 para la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas.

Específicos

1. Analizar los servicios informáticos que ofrece la institución al personal tanto interno como externo.
2. Identificar las vulnerabilidades que se presentan en la infraestructura tecnológica de la fundación.
3. Establecer nivel de impacto que puede ocasionar la falla de los servicios en el establecimiento.
4. Proponer un plan de contingencia informático basado en la norma ISO 27001:2013 de acuerdo a la evaluación realizada en la institución

CAPÍTULO 2

METODOLOGÍA

2.1. Materiales

2.1.1. Humanos

- Docente Tutor de Tesis.
- Personal Administrativo y Analistas del Departamento de Sistemas de la Unidad Educativa Atenas.
- Autor del Proyecto.

2.1.2. Institucionales

- Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas.
- Laboratorios de Cómputo y Servicio de Internet de la UEA.
- Biblioteca y Repositorios Virtuales de la Universidad Técnica de Ambato.
- Acceso a Internet.

2.1.3. Otros

Figura 2.1: Recursos Utilizados

Nº.	Detalle	Unidad	Cantidad	Valor Unitario	Valor Total
1	Internet	mensual	5	\$ 38,00	\$ 190,00
2	Servicio eléctrico	mensual	5	\$ 15,00	\$ 75,00
3	Carpetas	c/u	3	\$ 1,00	\$ 3,00
4	Impresiones	c/u	400	\$ 0,05	\$ 20,00
5	Copias	c/u	400	\$ 0,03	\$ 12,00
6	Lápices	c/u	2	\$ 0,50	\$ 1,00
7	Borrador	c/u	1	\$ 0,30	\$ 0,30
8	Esferos	c/u	2	\$ 0,75	\$ 1,50
9	Laptop	c/u	1	\$ 850,00	\$ 850,00
10	Transporte	mensual	5	\$ 40,00	\$ 200,00
Subtotal					\$ 1.352,80
Imprevistos(10%)					\$ 135,28
TOTAL					\$ 1.488,08

Fuente: Elaborado por el Investigador

Plan de contingencia: El plan de contingencia es un conjunto de procesos que tienen como principal objetivo restablecer las actividades normales llevadas a cabo en una institución que son automatizados por los sistemas informáticos, de igual manera permite la ejecución de normativas y acciones básicas a la solución de una eventualidad, por causa de un incidente externo o interno, su finalidad es de colocar en marcha nuevamente el sistema de trabajo.[5][6]

Objetivo de un plan de contingencia: El objetivo es permitir que una organización vuelva a sus actividades cotidianas tan pronto como sea posible después de un acontecimiento imprevisto.[7]

Un sistema informático: “Es un conjunto de elementos que hace posible el tratamiento automático de la información” [8], también se puede decir que es un conjunto de partes o recursos formados por el hardware, software y las personas que lo emplean, que se relacionan entre sí para almacenar y procesar información, esto es propio de en instituciones que necesitan almacenar y tener sistemas de apoyo para el respaldo de información.

En la figura 2.2 podemos apreciar de manera gráfica el proceso que realiza el sistema de información.

Figura 2.2: Proceso de un Sistema de Información



Fuente: [9].

1. Entrada: captura de datos tanto desde el interior como del exterior del sistema de información.
2. Procesamiento: convertir datos e información de una manera más significativa para el negocio.
3. Salida: transferir la información ya procesada a los usuarios para que desarrollen sus actividades diarias.

Seguridad activa: La seguridad activa tiene como objetivo proteger y evitar posibles daños en los sistemas informáticos, por esa razón se debe tomar recursos necesarios para evitar posibles problemas utilizando técnicas en el uso adecuado de contraseñas, que podamos añadirles símbolos numéricos, letras mayúsculas , minúsculas, encriptaciones de datos entre otros.

Seguridad pasiva: La seguridad pasiva tiene como finalidad el de minimizar los efectos negativos causados por un accidente, un usuario o malware. Por tanto para prevenir cualquier inconveniente se debe realizar un análisis del uso de hardware adecuado contra accidentes y averías, también se pueden utilizar copias de seguridad de los datos y del sistema operativo.

Seguridad física y lógica: La seguridad física son los procedimientos y tareas físicas cuyo objetivo es proteger al sistema tangible de los peligros físicos del ambiente, de personas entre otros. La seguridad lógica en cambio tiene que ver mas con la protección directa de los datos y de la información intangible de la empresa.[10]

Seguridad informática: “La seguridad informática se le define como el conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que puedan llegar a afectarlo”. [11]

Objetivo de la seguridad informática: El objetivo principal de la seguridad informática es el de proteger los recursos informáticos valiosos de la organización, entre ellas el hardware y software, a través de la implantación de ciertas medidas adecuadas de protección, la seguridad informática permite a la empresa alcanzar sus metas, protegiendo sus activos financieros, sistemas entre otros.[11]

Control de Calidad: Es el conjunto de técnicas y actividades de acción operativa que se utilizan, actualmente, para evaluar los requisitos que se deben cumplir con estándares respecto de la calidad del producto o servicio.

Norma ISO: Se denomina a un conjunto de normas en las que se establecen los diferentes modelos de aseguramiento de calidad, facilitando así la coordinación y unificación de las normas internacionales e incorporando la idea de estandarización logrando beneficios para los productores y compradores de bienes y servicios, existen dos organismos a nivel mundial: [11]

- ISO (International Organization for Standardization, Organización Internacional para la Estandarización) organismo internacional dedicado a desarrollar reglas de normalización en diferentes campos como la informática.
- IEC (International Electrotechnical Commission) organismo que publica normas de estandarización en el ámbito de la electrónica.

Un activo: “Es un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización”. [10] Como parte de los activos se considera a la información, los datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones y recursos humanos.

Amenaza: “Se define como cualquier circunstancia o evento con el potencial de afectar negativamente a las operaciones de la organización, las amenazas pueden ser accidentales o de manera intencional”. Se clasifican en:

- Desastres naturales: terremotos, incendios, inundaciones o filtraciones de agua.
- Desastres por falla de servicios: fallas en el sistema de energía, ventilación y en el sistema de seguridad, en la red de datos, los equipos de networking y servidores.
- Fallas por terceros: errores humanos, denegación de servicios, software malicioso virus informáticos, vandalismos, espionajes, suspensión en el procesamiento de información. [5]

Vulnerabilidad: “Es una debilidad o defecto de un sistema de información en sus procedimientos de seguridad” [6], arquitectura, implementación o en los controles de seguridad que podrían ser explotados por una amenaza para eludir los sistemas de seguridad y acceder de manera no autorizada a la información. [12]

Políticas de seguridad: Las políticas de seguridad implican informar a los usuarios, trabajadores y personal de dirección, de los requisitos obligatorios para proteger la información de la organización, debe especificar también los mecanismos a través de los cuales estos requisitos puedan ser conocidos.

Eventos controlables: Cuando al identificarlos se pueden tomar acciones preventivas que disminuyan el impacto y minimicen su ocurrencia.

Eventos no controlables: Sucesos impredecibles que solo se pueden tomar acciones para minimizar el impacto.

ISO 9001:2015: Es una norma ISO internacional que se aplica a los Sistemas de Gestión de Calidad de organizaciones públicas y privadas, independientemente de su tamaño o actividad empresarial. Se trata de un método de trabajo excelente para la mejora de la calidad de los productos y servicios, así como de la satisfacción del cliente.[13]

2.2. Métodos

El presente trabajo de investigación se centra en conocer la problemática que surge al no contar con un plan de contingencia informático ya que con el mismo podríamos mitigar los riesgos de pérdida de información tanto por factores internos como externos. Para reconocer los diferentes riesgos ejecutaremos las siguientes metodologías y modalidades:

Sistema de gestión de seguridad de la información: Es un conjunto de políticas de administración de la información enmarcadas dentro de la norma ISO/IEC 27001:2013, la misma que utiliza una organización para establecer objetivos en cuanto a la seguridad de la información y alcanzarlos, basándose en un enfoque de gestión del riesgo y de mejora continua.[14]

ISO/IEC 27001:2013: Es la norma donde se contienen los requisitos para implementar y mejorar un Sistema de Gestión de Seguridad de la Información; tiene sus orígenes en una publicación del Departamento de Comercio e Industria (DTI), donde se establecía un código de mejores prácticas para la administración de la seguridad de la información.[15]

Ventajas de la implantación de un plan de contingencia informático basado en la Norma ISO/IEC 27001:2013

- Disminuir el riesgo, y reducción de gastos asociados.
- Reducir la incertidumbre de conocer los riesgos e impactos asociados.
- Mejora constante de la gestión de seguridad de la información.
- Garantizar la continuidad del negocio.
- Aumento de competitividad mejorando la imagen corporativa.

- Incremento de confianza.
- Aumento de la rentabilidad, que derive del control de riesgos.
- Cumplir la legislación vigente relacionada a la seguridad de la información.
- Aumentar las oportunidades de negocio.
- Reducir los costos asociados a los incidentes.
- Mejorar la participación de los usuarios en la gestión de la seguridad.
- Integración con distintos sistemas de gestión como la norma ISO 9001.
- Mejorar los procesos y servicios prestados.[16]

Metodología Octave: Operationally Critical Threats Assets and Vulnerability Evaluation. Es un método de evaluación y de gestión de los riesgos en base a tres principios Confidencialidad, Integridad y Disponibilidad, para garantizar la seguridad de los sistema de información.

Existen 3 versiones de la metodología OCTAVE

- La versión original de OCTAVE
- La versión para pequeñas empresa OCTAVE-S
- La versión simplificada de la herramienta OCTAVE-ALLEGRO

En el presente proyecto se usara la versión OCTAVE-S, mismo que fue desarrollado para ser implementado en organizaciones pequeñas de 100 personas o menos utilizando un proceso un poco más reducido que el original OCTAVE, pero con los mismos resultados.[17]

Características:

- Requiere un grupo de 3 a 5 personas que conozcan a plenitud el desarrollo de la empresa, para recopilar información sobre los activos informáticos mas importantes, los requisitos de seguridad, las amenazas y las prácticas de seguridad.
- Solo realiza un barrido de manera superficial a la infraestructura informática.[18]

Las fases con las que trabaja esta metodología son:

1. Identificación de los principales activos informáticos.
2. Determina cuales de los activos identificados son los más críticos para el éxito de la organización.
3. Valoración de cada activo, en base a los tres principios de la metodología.
4. Identificar las amenazas que pueden interferir con el cumplimiento de los procesos y actividades de la organización.
5. Determina la probabilidad de que las amenazas puedan ocurrir y el impacto que conllevaría esto para la organización.
6. Realiza una valoración del riesgo, determinando en que nivel de ocurrencia se encuentra cada amenaza.
7. Finalmente, desarrolla un plan de mitigación de riesgos tomando los niveles altos y críticos.[19]

Método delphi: “Es un método de estructuración de un proceso de comunicación con expertos de forma grupal, que es efectivo a la hora de permitir a un grupo de individuos como un todo, tratar un problema complejo”. [20] Este método consta de seis pasos definidos para lograr los resultados requeridos.

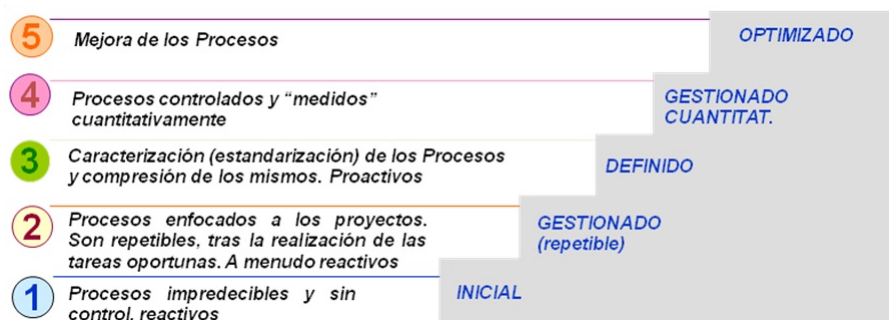
Figura 2.3: Pasos del Método Delphi



Fuente: [21].

Capability Maturity Model: Modelo de Madurez de la Capacidad (CMM), es un modelo de calidad que proporciona un marco de trabajo a las organizaciones para guiar sus actividades por las mejores prácticas de producción. Dirige su enfoque a la mejora de procesos en una organización, estudia los procesos de desarrollo y produce una evaluación de la madurez de la organización según una escala de cinco niveles (inicial, repetible, definido, gestionado y optimizado).[22]

Figura 2.4: Niveles de Madurez de SW-CMM.



Fuente: [23].

2.2.1. Evaluación de riesgos informáticos

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la "Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias".[24]

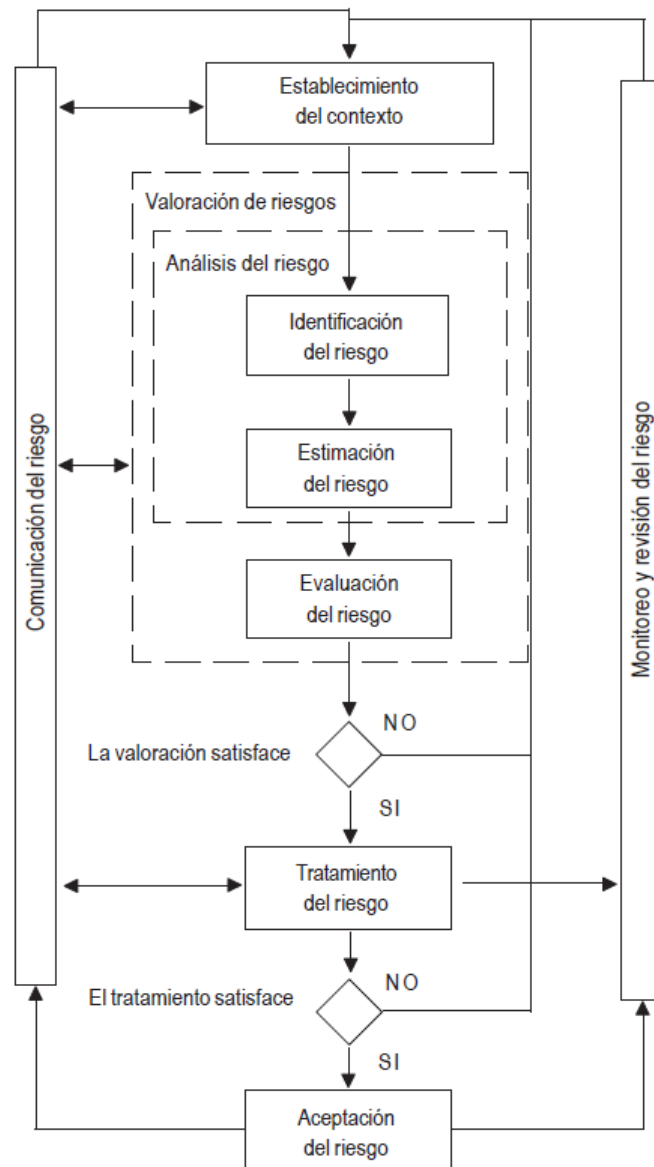
Los riesgos que pueden afectar a la institución se deben evaluar regularmente, por lo que servirá como guía de referencia NTC-ISO 27005, que nos proporciona pautas para la seguridad de la información a través de una serie de métodos y ejemplos para de esta manera poder realizar una evaluación de riesgos en sus sistemas y componentes de información.

Pasos de la metodología El proceso de gestión de riesgos conlleva una metodología en base a la ISO 27005, esta se compone de las siguientes etapas:

- a) Identificación de riesgos.
- b) Evaluar los riesgos en términos de impacto y probabilidad de ocurrencia.
- c) Establecer un orden adecuado de prioridad en el tratamiento de los riesgos.

- d) Definir la designación de roles de trabajo y obligaciones al personal en caso de emergencia.
- e) Realizar un monitoreo continuo de los riesgos.[25]

Figura 2.5: Proceso para la Gestión de Riesgos.



Fuente: [26].

2.2.1.1. Riesgos de Seguridad y Privacidad de la Información

Riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.

De acuerdo con lo descrito en la norma GTC-ISO/IEC 27035, un incidente de seguridad de la información está definido como “Evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y vulnerar la seguridad” .[27]

2.2.1.2. Riesgos de Ciberseguridad

Riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dada su naturaleza dinámica incluye también aspectos relacionados con el entorno físico. Estos riesgos tienen una relación directa con los principios de la Seguridad de la Información y se clasifican teniendo en cuenta los siguientes grupos:

Pérdida de la confidencialidad. Pérdida de la propiedad de la información que impide su divulgación a individuos, entidades o procesos no autorizados.

Pérdida de la integridad. Pérdida de la propiedad de contar con información exacta y completa, o que pudo haber sido sin ser manipulada o alterada por personas o procesos no autorizados.

Pérdida de la disponibilidad. Pérdida de la cualidad o condición de la información de encontrarse a disposición de quienes requieran acceder a ella, ya sean personas, procesos o aplicaciones.[28]

2.2.1.3. Valoración de Activos

Para la valoración de los activos se procede a definir una escala de valoración para cada uno de los activos presentes en la institución, tomando como referencia el cuadro de valoración de la ISO27001 en la cual se expresan tanto valores cuantitativos como cualitativos para cada uno de los niveles a ser evaluados en aspectos de Disponibilidad, Integridad y Confidencialidad. En conjunto con el departamento de sistemas se hará uso de la tabla 2.1 de valoración de activos.

Tabla 2.1: Valoración de Activos.

VALORACIÓN DE LOS ACTIVOS				
Valor	Nivel	Disponibilidad	Integridad	Confidencialidad
4	Critico	La información, instalaciones y recursos siempre debe estar disponibles. Su pérdida es considerada como catastrófica para la Institución.	Toda información, instalación o recurso donde la integridad es importante y debe garantizarse. Su pérdida sería catastrófica.	Abarca toda información, instalación o recurso calificado como de uso confidencial. Solo puede ser utilizado con autorización explícita
3	Alto	Toda información, instalación o recurso cuya disponibilidad puede estar detenida por algunas horas.	Abarca toda información, instalación o recurso en el cual la integridad es muy importante y debe garantizarse.	Toda información, instalación o recurso calificado como de uso restringido. Solo puede ser utilizado por personal autorizado.
2	Medio	Toda información, instalación o recurso cuya disponibilidad puede estar detenida por 24 horas máximo.	Todo recurso, información o instalación en el cual la integridad es de importancia media y debe garantizarse.	Información, instalación o recurso calificado como de uso semi- restringido. Solo puede ser utilizado por personal interno.
1	Bajo	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por 48 horas máximo.	Este nivel abarca toda información, instalación o recurso en el cual la integridad no es muy importante, pero debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso interno. Solo puede ser utilizado por personal interno o usuarios/clientes.

Fuente: ISO27001, Tomada de la Investigación de [2].

Entre los criterios que tomo en cuenta para la respectiva asignación del nivel de valoración de activos constan los siguientes:

- El valor económico que representa cada uno de los activos de la institución.
- El nivel de consideración que el activo tiene pérdida de disponibilidad, integridad, confidencialidad.
- El impacto que puede generar para la institución los daños de los activos o posible suspensión de los servicios.

Dichos parámetros son mencionados en la investigación de [2], los cuales fueron tomados para evaluar cada uno de los activos con los que cuenta la institución, de esta manera asignando los niveles conforme a la disponibilidad, integridad y confidencialidad de los mismos.

2.2.1.4. Análisis de Riesgo

En general el análisis de riesgos es el proceso en el cual se estima la probabilidad de que ocurra un evento no deseado que conlleve consecuencias en la seguridad de la información. Es muy importante realizar este proceso dentro de la institución ya que permite identificar los activos, controles de seguridad, para de esta manera conocer los criterios para la elaboración de un Plan de Contingencias que permite prevenir y mitigar riesgos, con lo cual se lograría afrontar diferentes eventos con eficacia así minimizando los daños y logrando en el menor tiempo posible la recuperación evitando grandes pérdidas para la institución.

a) Probabilidad de Riesgo. La probabilidad de que ocurra una amenaza debe establecerse en qué circunstancias el activo tendrá valor o necesitará protección [25]. Se determinará en función de las estadísticas recopiladas en toda la administración, también se tendrá en cuenta lo siguiente:

- Lo importante que es el activo para la institución.
- El nivel de ocurrencia que posee la vulnerabilidad en el activo.
- La susceptibilidad técnica que la vulnerabilidad se materialice.

b) Evaluación de Probabilidad de Riesgo. Es el proceso con el que se identifica la frecuencia con la que ocurren las amenazas, los activos afectados y las vulnerabilidades; a su vez los criterios de riesgo establecidos se comparan con los riesgos estimados de esta manera, se determinará el nivel de importancia del riesgo. El riesgo se evalúa contemplando tres elementos básicos:

1. Estimado del valor de los activos de riesgo.
2. Probabilidad de ocurrencia del riesgo.
3. Valoración del riesgo de los activos.[25]

En la tabla 2.2 se define los valores cuantitativos y cualitativos los cuales van a ser asignados a cada una de las vulnerabilidades encontradas. De acuerdo a su nivel de ocurrencia.

Tabla 2.2: Probabilidad de Ocurrencia.

NIVEL	PROBABILIDAD	VALOR	DESCRIPCIÓN
4	Muy Frecuente	76-100%	Eventos repetitivos
3	Frecuente	51-75%	Eventos aislados
2	Ocasional	26-50%	Sucede alguna vez
1	Remoto	0-25%	Improbable que suceda

Fuente: Tomado de [29], adaptado por el investigador.

c) Impacto del Riesgo. El impacto es la medida del daño en el activo derivado de la materialización de una amenaza, puede afectar de inmediato a más de un activo en la institución, o puede conducir a la pérdida de información en el futuro, resultando en una pérdida financiera.[25]

Existen varios criterios para evaluar el impacto a causa de los diferentes riesgos. Depende de cada organización definir las consideraciones necesarias para llevar a cabo esta actividad, se tomó a consideración criterios muy importantes para la institución para de esta manera elaborar la tabla de evaluación de impacto entre los cuales tenemos:

- El nivel de impacto para la institución en caso de cualquier daño o interrupción de los procesos de gran importancia.
- La valoración de la importancia de los activos institucionales.
- Las vulnerabilidades que existen tanto a nivel lógico como físico.
- Los datos y servicios que son de uso tanto interior como exterior en la institución.
- El valor monetario para la institución en caso de sufrir algún daño, interrupción o falla en sus principales servicios.

Tabla 2.3: Prioridades de Evaluación del Impacto.

IMPACTO	VALOR	DESCRIPCIÓN
Bajo	1	Cuando no afectan las actividades y los sistemas principales trabajan de forma normal.
Medio	2	Cuando los daños son parciales y se dan en los sistemas, no afecta a las operaciones.
Alto	3	Cuando se ven afectadas de manera directa las operaciones y funciones, los usuarios y los sistemas informáticos.
Critico	4	Pérdida de información crítica, daños severos en los equipos, Suspensión de funciones

Fuente: Tomado de [29], adaptado por el investigador.

d) Determinación del Riesgo. Para determinar el riesgo de un sistema, se lleva a cabo a través del impacto de las amenazas en el valor de cada uno de los activos más relevantes para la institución y la probabilidad de ocurrencia.

Para desarrollar el plan de contingencia, se deben tener en cuenta los riesgos que son altamente probables y que tienen un fuerte impacto en la institución. En la figura 2.6 podemos observar el nivel de riesgo.

Figura 2.6: Niveles de Riesgo.

PROBABILIDAD	4	A	A	C	C
	3	M	M	A	C
	2	B	M	M	A
	1	B	B	M	A
		1	2	3	4
	IMPACTO				

Fuente: Tomado de [29], adaptado por el investigador.

- El rojo nos indica los riesgos críticos. (C)
- El naranja no indica que son riesgos altos. (A)
- El amarillo son riesgos medios. (M)
- El verde no indica los riesgos bajos. (B)

2.2.2. Modalidad de la investigación

Modalidad bibliográfica: Este método va a permitir a la investigación un análisis de definiciones y contextos los cuales serán extraídos de investigaciones previas, referentes al tema con la finalidad de dar un aporte teórico, lo que permitirá ser de base y complemento investigativo de diferentes autores que han expresado diferentes conclusiones del problema.

Modalidad de campo: La presente modalidad es considerada ya que es necesario acudir al lugar de los hechos, donde son desarrolladas todas las actividades de control de información por parte del departamento de sistemas de la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas, lo que generara una recolección de datos reales aportando información específica a la investigación.

Modalidad aplicada: El presente proyecto se basa en una investigación aplicada ya que en el mismo se plasma todos los conocimientos adquiridos durante los semestres de formación académica para de esta manera poder proponer soluciones a los problemas que se detecten en cuanto a la seguridad de la información, elaborando un plan de contingencia informático cuyo objetivo principal es mitigar los riesgos y garantizar la disponibilidad, integridad y confidencialidad de la información valiosa para la institución.

2.2.3. Recolección de información

Las personas que proporcionaran información serán: Administrativos y Analistas del departamento de sistemas de la institución, se verificará el cumplimiento de las políticas establecidas en la Unidad Educativa Atenas en cuanto a seguridad de la información basándose en la Norma ISO 27001:2013. De esta manera se logrará saber en que situación se encuentra actualmente todos los activos tecnológicos de la misma.

Para esto se utilizará técnicas como la observación de campo, la encuesta y entrevista especialmente al personal que se encuentra a cargo del departamento de sistemas. Además se hará uso de fuentes de internet basándose en libros, tesis, documentos técnicos, etc. Para así cumplir con cada uno de los objetivos planteados.

2.2.4. Procesamiento y análisis de datos

Procesamiento y análisis de la información. Lo primero que se realizará al recopilar la información, será seleccionar los datos que se requiere para el desarrollo del proyecto los mismos que será analizados en relación con el problema y para poder establecer las conclusiones respectivas asegurando que los datos sean lo más reales posibles.

Plan de análisis e interpretación de resultados. El análisis de los resultados se realizará desde el punto de vista descriptivo y estadístico, proceso que permite realizar la interpretación adecuada basada en el marco teórico, relacionado las variables de la investigación y la propuesta lo que servirá para establecer las conclusiones y recomendaciones.

2.2.5. Desarrollo del proyecto

Para el desarrollo del presente proyecto se planearon las siguientes tareas a ejecutarse y así obtener el Plan de Contingencia Informático para el Área de TI en base a la Norma de Calidad ISO 27001:2013 para la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas.

- Análisis de la situación actual de la institución y sus políticas.
- Identificar los recursos tecnológicos, aplicaciones y consumos de servicios.
- Emplear técnicas de recolección de información en el departamento de sistemas.
- Revisión de la organización en cuanto a seguridad de la información.
- Evaluar el sistema de gestión de la seguridad de la información en la institución.
- Analizar las vulnerabilidades en la seguridad de la información.
- Plantear soluciones prácticas a la resolución de las vulnerabilidades detectadas.
- Diseño del plan de contingencia basado en la norma de calidad ISO 27001:2013.

CAPÍTULO 3

RESULTADOS Y DISCUSIÓN

3.1. Análisis y discusión de los resultados

3.1.1. Desarrollo de la propuesta

El presente capítulo expone de una manera detallada las fases para la elaboración de un Plan de Contingencia Informático para el área de TI en base a la norma de calidad ISO 27001:2013 para la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas. Conformado de la siguiente forma: Alcance del Plan de Contingencia, Diagnostico inicial de la institución respecto a los recursos informáticos que actualmente mantiene, Escenarios de contingencia, Evaluación de los riesgos e Identificación de controles que ayuden a disminuir los riesgos.

3.1.2. Planificación

En la actualidad todas las instituciones ya sean publicas o privadas deben poseer un Plan de Contingencia Informático para de este modo y en base al mismo poder afrontar cualquier eventualidad que pueda afectar el rendimiento de las actividades que se realizan normalmente, de esta manera la institución debe estar involucrada con los planes de prevención, ejecución y recuperación ante factores internos o externos como tenemos desastres, interrupción de servicios, etc.

3.1.3. Alcance

El diseño del Plan de Contingencia Informático incluye los sistemas de información, equipos, infraestructura de red, el mismo se presentó al Jefe del Departamento de Sistemas de la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas, en lo cual consta la elaboración de este Plan de Contingencia no se realizara el desarrollo de la fase de pruebas y validación del Plan de Contingencia, tampoco se implementará el mismo, por consiguiente queda a cargo de las autoridades y del Departamento de Sistemas de la Institución Educativa una vez dado por finalizado el presente proyecto de titulación proceder al desarrollo del mismo.

3.1.4. Diagnóstico de la situación actual

La Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas, en la actualidad posee una red de datos la misma que es administrada y gestionada por el Departamento de Sistemas. Cuenta con una infraestructura tecnológica conformada por una red LAN la misma que fue mejorada en los últimos meses por la cual se transmite gran cantidad de información diariamente, la misma que no posee suficientes mecanismos de seguridad que garanticen la integridad de la información.

El Departamento de Sistemas cuentan con mecanismos básicos de seguridad de la información como: el acceso mediante clave a la información con la protección de Windows, la autenticación de los usuarios mediante clave de acceso a la información de los servidores, también se realiza respaldos de la información más relevante en el Google Drive una vez al día; los mismos no son suficientes para responder a eventualidades como desastres naturales, interrupción o falla de servicios.

La Unidad Educativa está en constante cambio tanto en sus activos de hardware y software, por tal motivo es de suma importancia analizar continuamente los riesgos que conllevarían a pérdidas críticas de información, en este punto se debería establecer un nivel de prioridad de recuperación de los activos más importantes dentro de la institución, de la misma forma verificar periódicamente el estado tanto de los servicios y comunicaciones dentro de la red, de esta manera mejorar las restricciones y controles de acceso a la información.

Con el diseño de un Plan de Contingencia Informático se planteara opciones de recuperación de información y servicios basados en su previo análisis, de esta manera se lograra un nivel de disponibilidad aceptable de la red mientras se consigue restablecer los servicios completamente luego de haber sido afectados por un incidente.

3.1.5. Direccionamiento Estratégico de la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas

Tabla 3.1: Direccionamiento Estratégico UEA

Direccionamiento Estratégico de la UEA	
Misión	Creemos y aprendamos juntos, fortaleciendo nuestro principios y valores, desarrollando las capacidades y habilidades de nuestra comunidad, de forma crítica y creativa para contribuir a un mundo mejor.
Visión	Somos la organización responsable de la formación de personas felices e íntegras, con conciencia social y capacidades para triunfar.
Valores	<ul style="list-style-type: none"> • RESPECTO: Es un derecho inalienable de todo ser humano. Reconocemos nuestra individualidad y valoramos la de los demás. • VERDAD: Hablamos y actuamos de manera coherente con nuestra conciencia y nuestras convicciones personales, siendo auténticos y valientes. • SOLIDARIDAD: Extendemos la mano voluntariamente a quien lo necesita, sintiendo como algo propio el sufrimiento de nuestro prójimo, permitiéndonos crecer como personas íntegras. • RESPONSABILIDAD: Hacemos lo que tenemos que hacer en el momento oportuno, sin que nadie nos lo recuerde y asumimos las consecuencias de nuestras decisiones.
Política de Calidad	Educamos y formamos jóvenes competentes, responsables y de servicio. Trabajamos para la satisfacción de nuestros clientes internos y externos mediante el cumplimiento de requisitos, la innovación de procesos, una organización efectiva, personal especializado y comprometido, una infraestructura adecuada y la participación de la familia.

Fuente: Elaboración propia a partir de la página oficial UEA:
<https://www.atenas.edu.ec/atenas/>

3.1.6. Políticas de seguridad

Las siguientes políticas y procesos de seguridad de la información son tomados de documentos certificados y aprobados dentro de la Unidad Educativa Atenas los mismos que son usados para el correcto uso tanto de las de redes de comunicación, dispositivos de hardware y software de esta manera garantizar que la información no sea exteriorizada.

Para el uso de la infraestructura física de comunicaciones.

1. No está permitido intervenir las redes de cableado, instalando cables no suministrados por Sistemas, cortando o empalmado cables, desprendiendo marcaciones de tomas, puertas o ductos, golpeando o forzando tubos y/o canaletas.

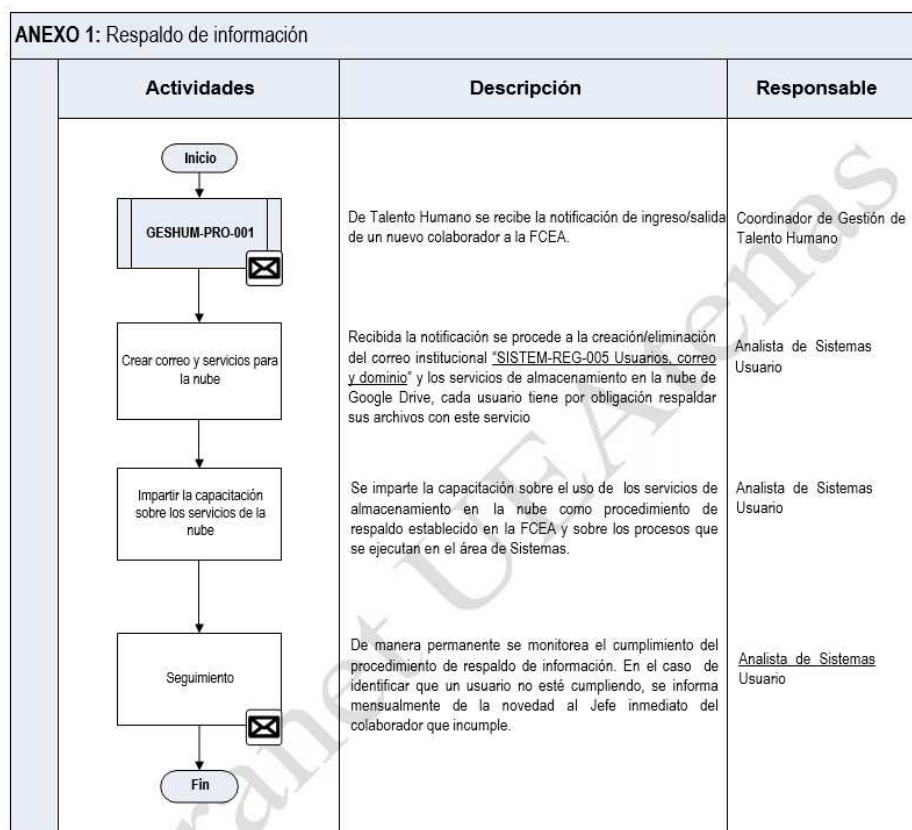
2. Tampoco está permitida la instalación de cables, derivaciones a través de conectores en “T” o cualquier tipo de derivación de voz o de datos por parte de los usuarios.
3. No se permite la instalación de ningún servicio que intervenga directamente el cableado que alimenta las tomas. Sin excepción, las conexiones deberán ser realizadas por personal autorizado.

La violación de cualquiera de estas normas podrá causar al usuario la cancelación de la cuenta de correo electrónico, la suspensión indefinida de todos los servicios de red y demás sanciones contempladas en los reglamentos de la Fundación Cultural y Educativa Ambato.

Respaldo de información

1. Se considera respaldos de Prioridad Alta únicamente a información almacenada en Base de Datos y código fuente de aplicaciones implantadas en la institución.
2. Una vez por semana se respalda la información con un nivel de importancia alta (Base de Datos, Código Fuente).
3. Cada usuario es responsable de respaldar su información, Sistemas se responsabiliza de mantener disponible el servicio de respaldo según sea el caso, para ello cada usuario recibe al menos dos capacitaciones sobre los sistemas de respaldo después de su entrada a la FCEA.
4. Si la PC no permite instalar el aplicativo el usuario debe ubicar sus archivos en la nube a través de la Web, vía Internet con un navegador, preferiblemente Google Chrome.
5. Para los cargos definidos por Rector y Gerencia Administrativa Financiera el área de Sistemas hará respaldos en HDD o DVD.
6. Las contraseñas de administrador de red únicamente las poseerá el departamento de Sistemas, en el caso de los laboratorios se utilizará una contraseña local la misma que no deberá estar almacenada de forma física.

Figura 3.1: Diagrama de Proceso Respaldo de Información.



Fuente: Documentos de procesos del Dpto. Sistemas Unidad Educativa Atenas.

Sobre el uso de computadoras en las estaciones de trabajo

1. La Fundación Cultural y Educativa Ambato hará la entrega formal del equipo de cómputo en funcionamiento, con el respectivo software instalado, de acuerdo con la actividad del usuario.
2. Los recursos de computación se deben usar exclusivamente para propósitos relacionados con la educación.
3. Sólo los encargados del área de Sistemas puede llevar a cabo cualquier tipo de mantenimiento tanto de hardware como de software y de la configuración de acceso a la red.
4. El usuario debe reportar cualquier tipo de daño en el equipo a los encargados del área de Sistemas por medio de un correo electrónico.
5. Toda persona a cargo de uno o varios equipos de cómputo es responsable luego de su uso, dejar apagado correctamente cada uno de sus componentes (CPU, Monitor, Parlantes, Impresora, Proyector).

6. Los encargados del departamento de Sistemas por autorización de Dirección Ejecutiva, se reserva el derecho de revisar en cualquier computador y sin previo aviso el tráfico de internet, software instalado y la información almacenada en cada uno de ellos, para verificar el cumplimiento de las políticas establecidas y aplicar las consecuencias que corresponda.
7. El uso de impresoras es estrictamente para trabajos relacionados con la institución. El personal de la Fundación Cultural y Educativa Ambato NO debe imprimir archivos personales o que no tengan relación con la actividad institucional.
8. No se permite a los usuarios:
 - Retirar el computador o sus accesorios de las instalaciones de la Fundación Cultural y Educativa Ambato
 - Comer o ingerir bebidas mientras esté junto al computador.
 - Pegar calcomanías, notas, recordatorios o cualquier tipo de adornos a los equipos

Sobre el uso de portátiles y celulares

1. Todo usuario podrá acceder a los servicios de red (internet, correo electrónico) desde su computador personal o celular previo el registro de la MAC Address de su WiFi en Sistemas.
2. El usuario es responsable de su equipo, mantenimiento y buen uso de su computador o celular.
3. No se permite el uso de CHAT en ningún horario y bajo ninguna aplicación (Página web, ICQ, Messenger, Skype, Trillian, etc).
4. Los usuarios no deben descargar archivos de música, videos ya sea por medio de programas P2P, Torrent, etc. Esto se gestionará en Sistemas.
5. El Usuario no debe instalar ningún programa para escuchar emisoras de radio o ver televisión por internet (Winamp, Real Audio, Music Match, Oozio Player, BWV, etc).
6. El usuario NO debe entrar en páginas web con contenido pornográfico.

7. No debe utilizarse el internet para realizar llamadas locales, nacionales, internacionales (Dialpad, Net2phone, Freephone, etc).
8. No se permite navegar en redes Sociales ya sea por servidores seguros (<https://>), usando Proxys Anónimos.
9. En el caso en que se detecte un mal uso de internet en equipos personales se procederá a la suspensión definitiva del servicio de internet.

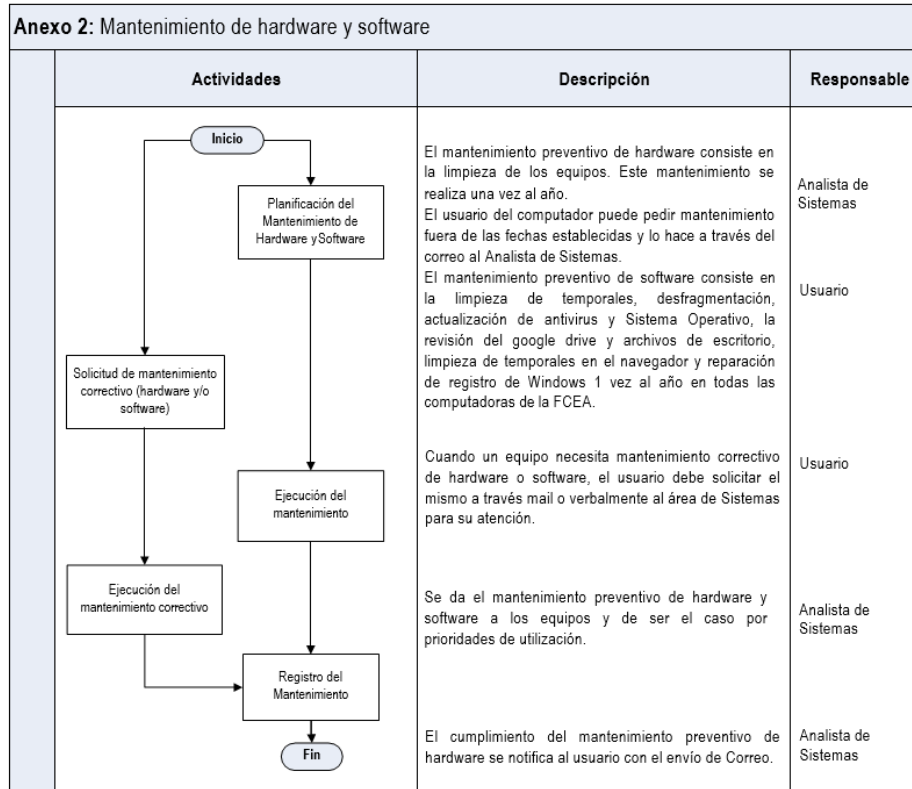
En el caso en que se detecte un mal uso de internet en equipos de la institución se procederá a definir alguna medida restrictiva de uso de la red en conjunto con Jefe inmediato, Coordinación y/o Gerente Administrativo Financiero.

Mantenimiento de hardware y software

Asegurar la disponibilidad de los equipos mediante el oportuno y efectivo mantenimiento del hardware y software de computadoras, servidores y equipos electrónicos.

1. Una vez al año se realiza un mantenimiento preventivo al hardware de los equipos, este consiste en la limpieza interior de las CPU para eliminar las partículas de polvo así como el resto de equipos donde sea posible hacer dicha limpieza. Hay equipos como los monitores, mouse, entre otros que no requieren este tipo de limpieza o no es posible realizarla.
2. De forma aleatoria se deberá hacer mantenimiento preventivo de software en todas las computadoras una vez al año.
3. El área de Sistemas dará solución con un mantenimiento correctivo lo antes posible según la carga de trabajo, disponibilidad de recursos y capacidad de solución.

Figura 3.2: Diagrama de Proceso Mantenimiento de Hardware y Software.



Fuente: Documentos de procesos del Dpto. Sistemas Unidad Educativa Atenas.

Sobre el uso de correo electrónico

La Fundación Cultural y Educativa Ambato asignará una cuenta de correo electrónico a profesores y personal administrativo. Dicha cuenta es personal e intransferible.

En el caso de correo electrónico NO está permitido:

1. Atentar contra la integridad de la institución
2. Enviar correo tipo SPAM, es decir “Correo Basura”, relacionado con falsos virus, con publicidad de empresas, cadenas de mensajes, etc.
3. Enviar correo masivo de su cuenta personal (usuario@atenas.edu.ec). Esto se gestionará a través de Sistemas previa autorización de Rectorado.
4. Usar la cuenta de correo electrónico de otro usuario o entregar a un tercero la contraseña propia.
5. Leer, borrar, copiar o modificar mensajes de correo electrónico de otras personas, sin su autorización.

6. Iniciar o continuar cadenas de mensajes pues estas tienden a congestionar innecesariamente la red.

3.1.7. Ubicación geográfica

El cantón Ambato como toda la región interandina está ubicado en un sector de influencia y propenso a varios fenómenos naturales los cuales pueden influir tanto a nivel local, cantonal, provincial y nacional.

Peligros sísmicos: Ambato se encuentra en un área de alta incidencia sísmica y de actividad volcánica. Izamba no verifica fallas importantes, por lo que no se ha denotado eventos importantes hasta la fecha.

Peligros volcánicos: En la parroquia Izamba se puede observar un fenómeno de peligro volcánico en lo concerniente a la rivera del río Cutuchi por la incidencia volcánica del volcán Cotopaxi. La incidencia es baja y de poca afectación para la parroquia dentro del sector poblado.

Peligros naturales: Izamba no está exento a peligros naturales ya que por ser una parroquia bordeada y asentada en parte montañosa esta propensa a deslizamientos de tierras, en la parte donde existe agua natural.[30]

Tabla 3.2: Amenazas naturales y antrópicas en la parroquia de Izamba

Amenazas	Ubicación	Ocurrencia
<i>Amenazas Naturales</i>		
Volcánica	Riveras del río Ambato y río Cutuchi	Baja
Sísmica	Todo el territorio de Izamba	Moderada
Sequía	Todo el territorio de Izamba	Moderada
Helada	Todo el territorio de Izamba	Baja incidencia
<i>Amenazas antrópicas</i>		
Quema	Todo el territorio de Izamba	Mediana
Erosión	Todo el territorio de Izamba	Mediana
Contaminación	Riveras del río Ambato y río Cutuchi, quebradas, relleno sanitario, minas pétreas, aguas de regadío,	Alta

Fuente: Cartografía base 1:50000 IGM
Elaborado por: Equipo Técnico Plan de Desarrollo y Ordenamiento Territorial
Izamba (PDyOT 2015)

La Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas se encuentra ubicada en la ciudad de Ambato, entre la Calle Gabriel Román s/n y Av. Pedro Vásconez Yacupamba, Izamba. La ubicación está especificada en las siguientes coordenadas; latitud: 1°13'18.8" S y longitud: 78°34'58.9" W.

Figura 3.3: Vista Satelital Ubicación Geográfica de la Unidad Educativa Atenas.




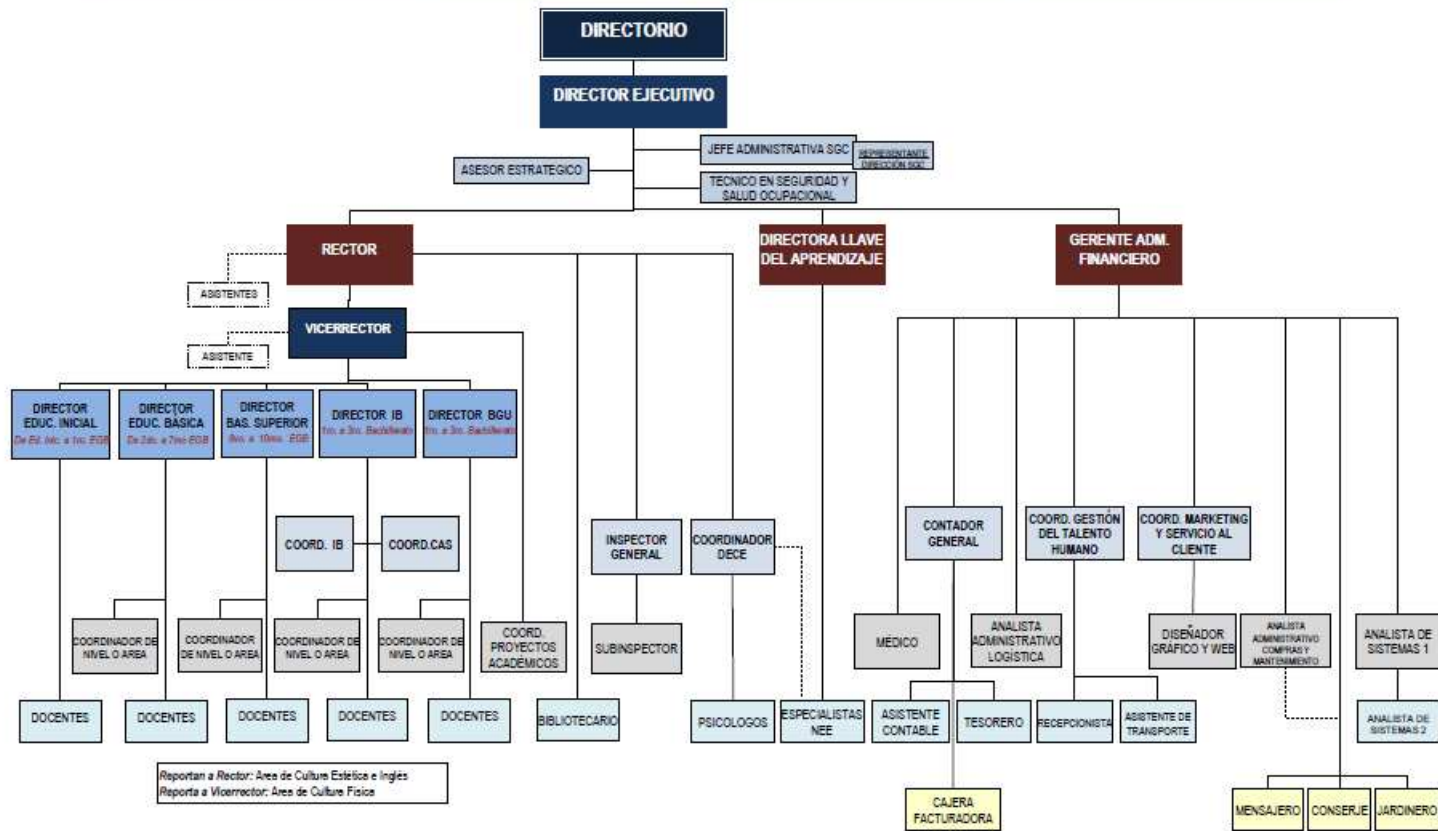
Fuente: Página Google Maps.

3.1.8. Departamentos de la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas

En el cantón Ambato se encuentra ubicada la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas que está conformada por varios departamentos, cada uno de estos desempeña funciones importantes los cuales permiten brindar un servicio educativo de calidad formando a los niños y jóvenes de nuestra ciudad con conciencia social y capacidades para triunfar.

Figura 3.4: Organigrama Institucional UEA.

	ORGANIGRAMA FCEA - Unidad Educativa Atenas	Código: REVER-DOG-002
		Fecha de Elaboración: 12 de Diciembre del 2007
		Fecha Última Aprobación: 07 de mayo de 2019
		Revisión: 028
Elaborado: Patricia Aguiyase	Revisado: Patricia Aguiyase	Aprobado: José Cuesta v. - Director Ejecutivo



Fuente: Unidad Educativa Atenas.

3.1.9. Activos de información

La información es uno de los activos más importantes para la institución por lo cual se debe contar con un almacenamiento adecuado y respaldos de la misma ya sea en forma impresa, de forma digital, o en los servidores principales que se encuentran en el cuarto de telecomunicaciones y así en caso de ataques de terceras personas poder evitar pérdidas y daños irreparables.

En la tabla 3.3 se describe el tipo de servidor que posee la institución el mismo que se encuentra virtualizado en 3 servidores en los cuales se alojan los sistemas y la base de datos, también se detalla el sistema operativo con el cual cuenta cada uno.

Tabla 3.3: Activos de Información.

HP PROLAIN DL360 9ºgeneración	AD - Active Directory	- Minerva - Active Directory	Windows Server 2012
	BDD - Base de Datos (SQL Server 2012)	- Control Bussiness	Windows Server 2012
	APP – Aplicaciones	- Biométrico - Wamp Server (Intranet)	Windows Server 2012
FISICO	VIRTUALIZADO	SOFTWARE	SISTEMA OPERATIVO

Fuente: Información recopilada del Dpto. de Sistemas de la Unidad Educativa Atenas.

3.1.10. Red de datos

La Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas, para su conexión a los servicios de internet e intranet cuentan con una red interna cableada y una inalámbrica para brindar conexión tanto a los administrativos, docentes y estudiantes. Poseen un enlace de 100 Mbps el cual abastece de manera eficaz cubriendo toda el área de la institución.

Tabla 3.4: Redes de Comunicación de la Unidad Educativa Atenas.

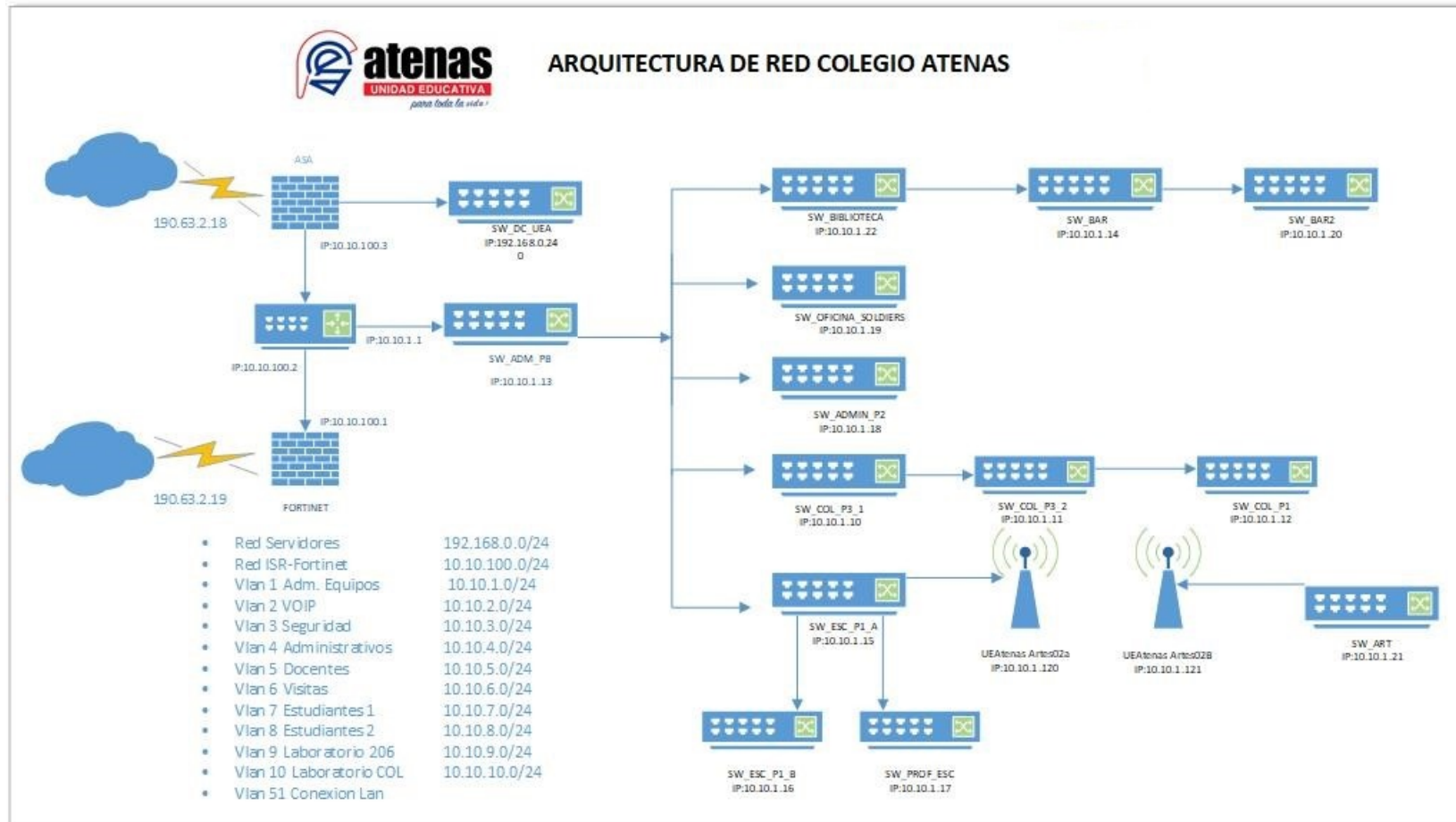
RED	DESCRIPCION
Red Local	Es la red cableada categoría 5a y 6a, es una red totalmente plana.
Red Wireless	Es la red inalámbrica de la institución, los puntos de acceso se encuentran distribuidos en diferentes espacios, ubicados estratégicamente para dar acceso a todo el personal de la Unidad Educativa Atenas.

Fuente: Información recopilada del Dpto. de Sistemas de la Unidad Educativa Atenas.

En la Institución se encuentra configurada una red cableada con topología estrella, de esta manera todos los departamentos de la misma se encuentran conectadas a un servidor principal, esta topología se la usa de manera frecuente en las redes LAN ya que entre las ventajas que presenta tenemos si una estación de trabajo deja de funcionar el resto de la red continua en funcionamiento normalmente, además que es de fácil configuración ya sea para agregar o quitar una estación de trabajo sin afectar al resto de equipos.

El servicio de internet se lo obtiene a través del proveedor movistar el cual suministra el servicio a través de fibra óptica de 6 hilos, la red existente es de clase C, es una red totalmente plana. En la figura 3.5 Podemos apreciar la configuración y topología de la red que posee la Unidad Educativa Atenas.

Figura 3.5: Topología Física de la Red UEA.



Fuente: Unidad Educativa Atenas.

3.1.11. Cuarto de telecomunicaciones

El área de Servidores es de 1x3m2 el mismo que cuenta con 2 racks de piso de 38 unidades cada uno para el alojamiento de los distintos equipos de networking, entre los dispositivos que podemos encontrar en los mismos tenemos: un Path Core de 48 puertos de categoría 6, un switch Cisco de 48 puertos el cual está configurado para el área de Administración, un switch Cisco en el cual se aloja el Data Center, un Cisco ASA-5520 Series para controlar la seguridad de las aplicaciones, también cuentan con una central telefónica de VoIP de 8 puertos, un UPS para la protección en caso de fallas eléctricas, poseen también dos Dvrs para todas las cámaras de vídeo vigilancia de la institución, adicional tienen dos amplificadores para el sistema de altavoces, además cuentan con dos sistemas de aire acondicionado para lograr un cuarto frío.

3.1.12. Descripción de los equipos de red

Los diferentes equipos que forman parte del cuarto de telecomunicaciones en la actualidad dentro de la Unidad Educativa Atenas son de gama media y alta. A continuación en la tabla 3.5 se detallan los equipos que comprenden la parte activa de la red de la Unidad Educativa Atenas.

Tabla 3.5: Activos Físicos de Red.

CANTIDAD	DESCRIPCIÓN	ESTADO
5	Pares de conexión de fibra óptica	activo
1	Patch Cord 48 puertos, Categoría 6	activo
8	Switch Cisco 48 puertos, catalyst 3750 v2 series	activo
1	Switch Cisco 48 puertos, catalyst 3750 E-series	activo
1	Firewall Cisco ASA 5520 Series (ASP)	activo
1	Central Telefónica de VoIP 8 puertos, GrandStream	activo
1	Servidor HP Prolain DL360 9ª generación	activo
1	Servidor HP AiO400r Intel xeon	activo
1	CPU – Servidor AMD	activo
1	Cisco 2900 series	activo
1	HP A-MSR 900 Router IF 812A	activo
1	Cisco 1900 Series	activo
1	Transceiver TP LINK N/C 100 CM	activo
3	Dvrs HikVision	activo
1	Firewall Fortinet 90 D	activo
1	Patch Panel 24 puertos, Categoría 6	activo
1	Switch Nexxt 16 puertos (no configurable)	activo
1	Switch 4210, 26 puertos	activo
1	Switch leviton 24 puertos, Categoría 5	activo
3	Switch Nexxt 12 puertos (no configurable)	activo
1	Patch Core 24 puertos, Categoría 5	activo
2	Aires acondicionados Ecox y LG	activo

Fuente: Información recopilada del cuarto de telecomunicaciones de la UEA.

3.1.13. Activos de software

En las siguientes tablas se detallan el tipo de software que es usado en los diferentes departamentos de la institución acorde a las funciones desempeñadas en cada uno, la mayoría de software utilizado posee su respectiva licencia, también cuentan con software Open Source, Libre o a su vez aplicaciones desarrolladas por el Departamento de Sistemas de la institución tomando en cuenta las necesidades de los usuarios.

Tabla 3.6: Activos de Software Personal Administrativo.

PERSONAL ADMINISTRATIVO	
APLICACIÓN	DESCRIPCIÓN
Sistema operativo Windows 10	Equipo licenciado
Windows Defender Antivirus	Antivirus de sistema operativo
Adobe Reader	Libre
Microsoft Office	Equipo con licencia
Firefox	OpenSource
Google Chrome	OpenSource
Google Drive Institucional	OpenSource
Ccleaner	Libre

Fuente: Información recopilada del Área de Administrativos de la Unidad Educativa Atenas.

Tabla 3.7: Activos de Software Dpto. Sistemas.

DEPARTAMENTO DE SISTEMAS	
APLICACIÓN	DESCRIPCIÓN
Sistema operativo Windows 10	Equipos licenciados
Windows Defender Antivirus	Antivirus de sistema operativo
Adobe Reader	Libre
Microsoft Office	Equipos con licencia
Firefox	OpenSource
Google Chrome	OpenSource
Google Drive Institucional	OpenSource
Ccleaner	Libre
VMware & vSphere Client	Libre
Datacard ID Works Designer	Propietario
Nero	Libre
iVMS-4200 Client (cámaras)	Libre
VLC	OpenSource
AnyDesk	Libre
TeamViwer	Libre
PHP	OpenSource
WampServer	OpenSource
Html5	OpenSource

Fuente: Información recopilada del Dpto. de Sistemas de la Unidad Educativa Atenas.

Tabla 3.8: Activos de Software Dpto. Contabilidad.

DEPARTAMENTO DE CONTABILIDAD	
APLICACIÓN	DESCRIPCIÓN
Sistema operativo Windows 10	Equipo licenciado
Windows Defender Antivirus	Antivirus de sistema operativo
Adobe Reader	Libre
Microsoft Office	Equipo con licencia
Firefox	OpenSource
Google Chrome	OpenSource
Google Drive Institucional	OpenSource
Ccleaner	Libre
Control Bussiness	Software de contabilidad
Dimm SRI	OpenSource

Fuente: Información recopilada del Dpto. de Contabilidad de la Unidad Educativa Atenas.

Tabla 3.9: Activos de Software Personal Docente.

PERSONAL DOCENTE	
APLICACIÓN	DESCRIPCIÓN
Sistema operativo Windows 10	Equipo licenciado
Windows Defender Antivirus	Antivirus de sistema operativo
Adobe Reader	Libre
Microsoft Office	Equipo con licencia
Firefox	OpenSource
Google Chrome	OpenSource
Google Drive Institucional	OpenSource
Ccleaner	Libre
Nota: Mediante solicitud del usuario final el departamento de sistemas podrá instalar software solicitado siempre que este sea software que tenga licencia libre entre ellos tenemos: java, virtual box, geogebra, libros digitales para el uso del personal docente, etc.	

Fuente: Información recopilada de los PC's del Personal Docente de la Unidad Educativa Atenas.

Tabla 3.10: Activos de Software Dpto. Marketing.

DEPARTAMENTO DE MARKETING (Atención al cliente) Y DISEÑO	
APLICACIÓN	DESCRIPCIÓN
Sistema operativo Windows 10	Equipo licenciado
Windows Defender Antivirus	Antivirus de sistema operativo
Microsoft Office	Equipo con licencia
Google Chrome	OpenSource
Google Drive Institucional	OpenSource
Ccleaner	Libre
Camtasia Studio 9	Licencia de Prueba
Adobe Audition	Licencia de Prueba
Adobe Illustrator	Licencia de Prueba
aTube Catcher	Libre
VLC	OpenSource
Mp3 Gain	Libre

Fuente: Información recopilada del Dpto. de Marketing de la Unidad Educativa Atenas.

Tabla 3.11: Activos de Software Dpto. Diseño.

DEPARTAMENTO DE MARKETING Y DISEÑO (Diseño Gráfico)	
APLICACIÓN	DESCRIPCIÓN
MacOS Mojave, versión 10.14	Equipo licenciado
OS X El Capitan, versión 10.11.6	Equipo licenciado
Microsoft Office	Equipo con licencia
Firefox	OpenSource
Google Chrome	OpenSource
Google Drive Institucional	OpenSource
Adobe Reader	Libre
Adobe Illustrator	Licencia de Prueba
Photoshop	Licencia de Prueba
IDesigner	Licencia de Prueba
IPremier	Licencia de Prueba

Fuente: Información recopilada del Dpto. de Diseño de la Unidad Educativa Atenas.

3.1.14. Activos de hardware

La institución educativa se encuentra dividida por departamentos para los administrativos y aulas para el área de educación en sus diferentes niveles, los cuales poseen activos físicos con respecto a tecnología, en las siguientes tablas se puede apreciar los diferentes componentes tecnológicos que posee cada departamento.

Tabla 3.12: Activos de Hardware Dpto. Administrativos.

ÁREA DE ADMINISTRATIVOS			
DEPARTAMENTO	CPU	DESCRIPCIÓN	OTROS DISPOSITIVOS
Rector	1	HP Intel Core i7-7700 CPU 3.60 GHz	1 Teléfono IP GrandStream 1 Epson L380
Vicerrector	1	Intel Core i5-8400 CPU 2.80GHz	1 Teléfono IP GrandStream 1 Epson L210
Departamento de Sistemas	3	HP Intel Core 2 Quad CPU 2.83 GHz (Auxiliar Sistemas) HP Intel Core i5-4460 CPU 3.20 GHz HP Intel Core i7-7700 CPU 3.60 GHz	2 Teléfonos IP GrandStream 1 Epson L375
Marketing	1	HP Intel Core i5-8400 CPU 2.80 GHz	1 Teléfono IP GrandStream 1 Epson Workforce 615
Proveeduría	1	Pentium Dual- Core CPU E5800 3.2 GHZ	1 Teléfono IP GrandStream 2 Fotocopiadora Ricoh MP 5002
Recepción	2	Intel Core i3-6100 CPU 3.70GHz Intel Core i5-8400 CPU 2.80GHz	2 Teléfonos IP GrandStream
Coordination de Proyectos Académicos	2	Pentium Dual-Core CPU E5200 2.50GHz Intel Core2 Quad CPU Q9500 2.83GHz	2 Teléfonos IP GrandStream
Soldiers	2	Intel Core i3-7100 CPU 3.90 GHz Intel Pentium Dual CPU E2160 2.20 GHz	1 Teléfono IP GrandStream
Llave del Aprendizaje	4	HP AMD Athlon 7550 Dual Core 2500 MHz Intel Core i3-2100 CPU 3.10 GHz Intel Core i3-7100 CPU 3.90 GHz Intel Core i3-7100 CPU 3.90 GHz	3 Teléfonos IP GrandStream
Mensajería	1	Biostar, Intel Core i3-6100 CPU 3.70 GHz	
Contador y Auxiliar	2	LG, Intel Core i3-7100 CPU 3.90 GHz HP Pentium Dual-Core CPU E5800 3.20 GHz	2 Teléfonos IP GrandStream 1 Epson L3150 1 Epson L375
Tesorería	2	HP Pentium Dual-Core CPU E5800 3.20 GHz	1 Teléfono IP GrandStream 1 Epson L395
Diseño	2	iMac Retina 5k, 27-inch, Late 2015 Intel Core i5 CPU 3.3 GHz iMac 21.5-inch, Mid 2011 Intel Core i5 CPU 3.3 GHz	1 Teléfono IP GrandStream 1 Epson L3150
Administración BAR	1	Intel Pentium Dual CPU E2180 2.00 GHz	1 Teléfono IP GrandStream 1 Epson L6170
Secretaria Escuela	1	HP Intel Core i3-7100 CPU 3.90 GHz	1 Teléfono IP GrandStream
Jefe Gestión de Calidad	1	HP Intel Core i5-8400 CPU 2.80 GHz	1 Teléfono IP GrandStream 1 Epson L380
Talento Humano y Auxiliar	2	HP Intel Core i5-8500 CPU 2,80 GHz Intel Core i3-7100 CPU 3.90 GHz	1 Teléfono IP GrandStream 1 Epson L220
Biblioteca	1	AMD Athlon 7550 Dual Core 2.50 GHz	1 Teléfono IP GrandStream 1 Fotocopiadora Ricoh MP 5002

Fuente: Información recopilada del Dpto. de Administrativos de la Unidad Educativa Atenas.

Tabla 3.13: Activos de Hardware Área de Colegio.

ÁREA DE COLEGIO			
DEPARTAMENTO \ AULA	CPU	DESCRIPCIÓN	OTROS DISPOSITIVOS
PRIMER PISO			
C101	1	HP Pentium Dual-Core CPU E5800 3.20 GHz	1 Proyector Epson Powerlite S12+
C102	1	HP Pentium Dual-Core CPU E5800 3.20 GHz	1 Proyector Epson Powerlite S12+
C103	1	Intel Core i3-7100 CPU 3.90 GHz	1 Proyector Epson Powerlite S12+
C104	1	HP Pavilion, AMD Athlon 7550 Dual-Core CPU 2.5 GHz	1 Proyector Epson Powerlite S12+
C105	1	HP Pentium Dual-Core CPU E5800 3.20 GHz	1 Proyector Epson Powerlite S12+
C106	1	Pentium Dual-Core CPU E5200 2.50 GHz	1 Proyector Epson Powerlite S12+
C107	1	HP Intel Core 2 Quad CPU Q9500 2.83 GHz	1 Proyector Epson Powerlite S12+
C108 \ DECE	1\4	HP Intel Core 2 Quad CPU Q9500 2.83 GHz	3 Teléfonos IP GrandStream 1 Epson L210
SEGUNDO PISO			
C201	1	Pentium Dual-Core CPU E5300 2.60 GHz	
C202	1	HP Intel Core i3-3240 CPU 3.40 GHz	1 Proyector Epson Powerlite S12+
C203	1	HP Pentium Dual-Core CPU E5800 3.20 GHz	1 Proyector Epson Powerlite S12+
C204	1	AMD Athlon 7550 Dual-Core CPU 2.50 GHz	1 Proyector Epson Powerlite S12+
C205 \ SECRETARIA	1\3	HP Pentium Dual-Core CPU E5800 3.20 GHz	3 Teléfonos IP GrandStream 1 Epson L220
C206	1	HP Pentium Dual-Core CPU E5800 3.20 GHz	1 Proyector Epson Powerlite S12+
C207	1	HP Intel Core 2 Quad CPU Q9500 2.83 GHz	1 Proyector Epson Powerlite S12+
C208	1	HP Pentium Dual-Core CPU E5800 3.20 GHz	1 Proyector Epson Powerlite S12+
C209	1	HP Pavilion, AMD Athlon 7550 Dual-Core CPU 2.5 GHz	
TERCER PISO			
C301 \ INSPECCION GENERAL	2	HP Intel Core i3-3240 CPU 3.40 GHz Dell Intel Core i5-7200 CPU 2.50 GHz	1 Teléfono IP GrandStream 1 Epson L220
C302	1	HP Intel Core 2 Quad CPU Q9500 2.83 GHz	1 Proyector Epson Powerlite S12+
C303	1	HP Intel Core 2 Quad CPU Q9500 2.83 GHz	1 Proyector Epson Powerlite S12+
C304	1	HP Pavilion, AMD Athlon 7550 Dual-Core CPU 2.5 GHz	1 Proyector Epson Powerlite S12+
C305	1	HP Intel Pentium Dual-Core CPU 2180 2.00 GHz	1 Proyector Epson Powerlite S12+
C300 \ DIRECTORA	3	HP Pentium Dual-Core CPU E5800 2.60 GHz HP Pentium Dual-Core CPU E5800 3.20 GHz Dell Intel Core i5-7200 CPU 2.50 GHz	3 Teléfonos IP GrandStream 1 Epson L355
C307	1	HP Intel Pentium Dual-Core CPU 2180 2.00 GHz	1 Proyector Epson Powerlite S12+
C308	1	HP Pentium Dual-Core CPU E5700 3.00 GHz	1 Proyector Epson Powerlite S12+
C309 \ LAB. COMPUTACION	1	COMPAC Pentium Dual-Core CPU E5400 2.70 GHz	1 Teléfono IP GrandStream 1 Proyector Epson Powerlite S12+
C310	1	BIOSTAR Intel Core i3-6100 CPU 3.70 GHz	1 Proyector Epson Powerlite S12+

Fuente: Información recopilada del Edificio de Colegio de la Unidad Educativa Atenas.

Tabla 3.14: Activos de Hardware Área de Escuela.

ÁREA DE ESCUELA			
DEPARTAMENTO \ AULA	CPU	DESCRIPCIÓN	OTROS DISPOSITIVOS
PRIMER PISO			
E101	1	HP Intel Core 2 Quad CPU Q9500 2.83GHz	1 Proyector Epson Powerlite S12+
E102	1	COMPAC Pentium Dual-Core CPU E5500 2.80 GHZ	1 Proyector Epson Powerlite S12+
E103	1	LG Intel Pentium Dual CPU E2200 2.4 GHz	1 Proyector Epson Powerlite S12+
E104	1	HP Pentium Dual-Core CPU E5800 3.20GHz	1 Teléfono IP GrandStream
E105	1	COMPAC Pentium Dual-Core CPU E5500 2.80 GHZ	1 Proyector Epson Powerlite S12+
E106	1	HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.56 GHz	1 Proyector Epson Powerlite S12+
E107	1	HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.56 GHz	1 Proyector Epson Powerlite S12+
E108	1	Pentium Dual-Core CPU E5300 2.60GHz	1 Proyector Epson Powerlite S12+
SEGUNDO PISO			
E201	1	HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.56 GHz	1 Proyector Epson Powerlite S12+
E202	1	HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.56 GHz	1 Proyector Epson Powerlite S12+
E203	1	HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.56 GHz	1 Proyector Epson Powerlite S12+
E204	1	HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.56 GHz	1 Proyector Epson Powerlite S12+
E205 \ CULT. FISICA E INGLES	3	HP Intel Core 2 Quad CPU Q9500 2.83 GHz HP Intel Core 2 Quad CPU Q9500 2.83 GHz HP Intel Core 2 Quad CPU Q9500 2.83 GHz	
E206 LAB. COMPUTACION	1	HP Pentium Dual-Core CPU E5800 3.20GHz	1 Teléfono IP GrandStream 1 Proyector Epson Powerlite S12+
E207	1	HP Pentium ADM Athlon 7550 Dual-Core 2.56 GHz	1 Proyector Epson Powerlite S12+
E208	1	Pentium Dual-Core CPU E5300 2.60GHz	1 Proyector Epson Powerlite S12+
E209	1	HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.56 GHz	1 Proyector Epson Powerlite S12+

Fuente: Información recopilada del Edificio de Escuela de la Unidad Educativa Atenas.

Tabla 3.15: Activos de Hardware Área de Inicial.

ÁREA DE INICIAL			
DEPARTAMENTO \ AULA	CPU	DESCRIPCIÓN	OTROS DISPOSITIVOS
Medico	1	Intel Pentium Dual CPU E2180 2.00 GHz	1 Teléfono IP GrandStream
P102	1	LG Intel Pentium Dual CPU E2180 2.00 GHz	1 Proyector Epson Powerlite S12+
P103	1	HP Pentium Dual-Core E5800 3.20 GHz	1 Proyector Epson Powerlite S12+
P104	1	Intel Core i3-7100 CPU 3.90GHz	1 Proyector Epson Powerlite S12+
P105	1	HP Pentium Dual-Core E5800 3.20 GHz	1 Proyector Epson Powerlite S12+
P106	1	HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.5 GHz	1 Proyector Epson Powerlite S12+
P107	1	HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.5 GHz	1 Proyector Epson Powerlite S12+
P108	1	HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.5 GHz	1 Proyector Epson Powerlite S12+
P109	1	Pentium Dual-Core CPU E5300 2.60 GHz	1 Proyector Epson Powerlite S12+
P110	1	HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.5 GHz	1 Proyector Epson Powerlite S12+
P111	1	Intel Pentium Dual CPU E2180 2.00 GHz	1 Proyector Epson Powerlite S12+
P112	1	BIOSTAR Pentium Dual-Core CPU E5200 2.50 GHz	1 Proyector Epson Powerlite S12+
P113	1	VTECK Pentium Dual-Core CPU E5400 2.70 GHz	1 Proyector Epson Powerlite S12+
P114\ Directora	1	HP Intel Core i5 CPU 2.5 GHz	1 Teléfono IP GrandStream 1 Epson L350
P115	1	Pentium Dual-Core CPU E5300 2.60 GHz	

Fuente: Información recopilada del Area de Inicial de la Unidad Educativa Atenas.

Tabla 3.16: Activos de Hardware Área de Artes.

ÁREA DE ARTES			
DEPARTAMENTO \ AULA	CPU	DESCRIPCIÓN	OTROS DISPOSITIVOS
T105	1	HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.5 GHz	1 Teléfono IP GrandStream
T104	1	HP Intel Core 2 Quad CPU Q9500 2.83 GHz	
T103	1	HP Pentium Dual-Core CPU E5800 3.2 GHz	1 Teléfono IP GrandStream
MUSICA	2	Intel Pentium Dual-Core CPU E2180 2.0 GHz	1 Teléfono IP GrandStream
		Pentium Dual-Core CPU E5800 3.20 GHz	1 Proyector Epson Powerlite S12+

Fuente: Información recopilada del Edificio de Artes de la Unidad Educativa Atenas.

Tabla 3.17: Activos de Hardware Área del Bar.

ÁREA DE BAR			
DEPARTAMENTO \AULA	CPU	DESCRIPCIÓN	OTROS DISPOSITIVOS
BAR	3	HP Intel Core 2 Quad CPU Q9500 2.83 GHz	1 Teléfono IP GrandStream
		HP Pavilion AMD Athlon 7550 Dual-Core CPU 2.5 GHz	
		Intel Core i5-9400F CPU 2.4 GHz	

Fuente: Información recopilada en el Área del Bar Unidad Educativa Atenas.

3.1.15. Servicios del departamento informático

Principales

El costo por hora en los servicios que el departamento de sistemas administra en la institución, se asignó de acuerdo a valores por suspensión de servicio o el costo por cambio de equipos a causa de daños físicos.

Tabla 3.18: Evaluación de Suspensión de Principales Servicios de la UEA

Servicios Informáticos	Probabilidad	Impacto	Riesgo	Costo por hora de suspensión
Escolástico Idukay	2	2	M	\$ 850
Telefonía IP	2	3	M	\$ 500
Cámaras IP	2	1	B	\$ 450
Internet	2	4	A	\$ 2500
Intranet	1	3	M	\$ 7000
Correo electrónico institucional	2	2	M	\$ 2500

Fuente: Información recopilada cuarto de telecomunicaciones UEA.

Otros

- Respaldo de datos (Backups diarios de información).
- Implantación de sistemas operativos de cliente y de servidor.
- Desarrollo de sistemas de información y páginas web.
- Mantenimiento de servicios de red y servidores.

3.1.16. Personal

Actualmente en el Departamento de Sistemas de la institución trabajan 2 personas, en la tabla 3.19 se detallan las funciones que cada uno realiza diariamente y su cargo correspondiente.

Tabla 3.19: Personal del Dpto. de Sistemas de la Unidad Educativa Atenas.

CARGO	ENCARGADO	DESCRIPCIÓN
Analista de Sistemas 1	Juan Carlos Calvache	<ul style="list-style-type: none"> - Planifica, coordina, dirige y elabora estudios sobre funcionamiento y organización del Área de Sistemas. - Determina normas, sistemas y procedimientos necesarios en la Institución. - Propone, elabora, coordina e implanta nuevo software necesarios en la institución. - Supervisa el trabajo del analista 2 y determina plazos para el cumplimiento de éste. - Coordina y/o desarrolla herramientas tecnológicas intermedias que suplan necesidades específicas de la institución, garantizando su funcionamiento y aplicabilidad al proceso en el cual se vayan a utilizar.
Analista de Sistemas 2	Ing. Franklin Edmundo Escobar	<ul style="list-style-type: none"> - Administra el correo electrónico de la institución, garantizando su buen funcionamiento y velando por que los usuarios hagan uso correcto de sus servicios. - Mantiene en perfecto funcionamiento la red y los servidores de la institución. - Realiza periódicamente el proceso de respaldo de datos, garantizando el cuidado de la información que se maneja en la institución. - Verifica el cumplimiento de los requisitos ISO que apliquen a los procesos en los que interviene. - Cumple las otras funciones que le asigne su jefe inmediato.

Fuente: Información recopilada del Dpto. de Sistemas de la Unidad Educativa Atenas.

3.1.17. Evaluación de riesgos y escenarios de contingencia

La Fundación Cultural y Educativa Ambato – Unidad Educativa Atenas con el pasar de los años ha ido implementando más personal como maestros y estudiantes dando como resultado una ampliación de la infraestructura tecnológica, por tal motivo se decidió cambiar la estructura de la red para optimizarla y obtener una mayor eficacia en la misma, por lo cual se procede a efectuar un análisis de riesgos y amenazas para de esta manera poder desarrollar un plan de contingencia informático el cual nos permitirá mitigar todos los posibles riesgos detectados para que no afecten las actividades diarias de la institución.

De acuerdo a la ISO-27001:2013 y de manera conjunta con el jefe de Departamento de Sistemas de la institución, analizando las actividades que se realizan diariamente se obtuvieron los siguientes criterios para la evaluación de los riesgos:

1. Se evaluarán los activos en cuanto a disponibilidad, confidencialidad e integridad de sus operaciones.
2. Se realizará una evaluación de amenazas.
3. Se evaluará las vulnerabilidades a las que están expuestos.
4. Se analizará cada uno de los activos que podrían verse afectados con la interrupción de este proceso.

3.1.18. Evaluación de los Activos de la Fundación Cultural y Educativa Ambato – Unidad Educativa Atenas

La evaluación y análisis de los activos de la institución se los realizara tomando como base tres aspectos principales como son: Disponibilidad (D), Integridad (I), Confidencialidad (C). Todos los activos no están sometidos a esta evaluación bajo los criterios mencionados, de esta manera en caso de no cumplir con algún aspecto se lo representa con un guion medio (-). Acorde a la tabla 2.1 (Valoración de activos) en esta se explica los criterios tomados a consideración para realizar la evaluación de los activos en la tabla 3.20.

Tabla 3.20: Valoración de los Activos de la Unidad Educativa Atenas.

CANT.	DESCRIPCIÓN	V.PROPIO			V.ACUMULADO
		D	I	C	
1	BDD Base de Datos - Control Bussiness	4	3	4	3,7
1	Active Directory - Wamp Server - Minerva	3	3	3	3
1	Aplicaciones - Wamp Server - Intranet	4	4	4	4
1	HP PROLAIN DL360 9ª generación	4	4	4	4
8	Switch Cisco 48 puertos, catalyst 3750 v2 series	3	4	3	3,3
1	Firewall Cisco ASA 5520 Series (ASP)	3	-	3	3
1	Central Telefónica de VoIP 8 puertos, GrandStream	4	3	2	3
1	Cisco 2900 series	2	-	-	2
1	HP A-MSR 900 Router IF 812A	3	-	-	3
1	Firewall Fortinet 90 D	4	4	4	4
1	Ups - Cuarto Telecomunicaciones	4	-	-	4
1	Switch 4210, 26 puertos	4	-	-	4
6	Laptops	3	-	-	3
90	Computadores de escritorio completos	3	-	-	3
17	Impresoras	1	-	-	1
2	Aires acondicionados - Cuarto Telecomunicaciones	4	-	-	4
	Infraestructura de Red	4	-	-	4
	Red Wireless -WIFI	4	-	-	4
	Red local -LAN	4	-	-	4

Fuente: Información recopilada en la Unidad Educativa Atenas.

De acuerdo a los resultados obtenidos mediante encuestas, observación y conforme a la presente valoración de activos los cuales son considerados de alta importancia para la institución se obtuvo los siguientes resultados:

1. La base de datos que almacena toda la información de la institución.
2. El servidor principal el cual esta virtualizado y facilita ser usado como servidor de aplicaciones con la intranet y active directory con el sistema minerva.
3. El control business software del departamento de contabilidad es de suma importancia para la institución ya que en el mismo se encuentran almacenados los datos de las cuentas, sistema de facturación, ingresos y egresos, la Unidad Educativa Atenas es privada por lo cual la falla o perdida de información de esta BDD acarrearía una perdida cuantiosa para la institución.
4. Los servidores que ayudan a desarrollar de manera continua las actividades diarias con los servicios de correo electrónico, archivos, web y VoIP.
5. La estructura de red con un cableado estructurado categoría 5a y 6a mediante el cual toda la institución se encuentra intercomunicada con todos sus departamentos.
6. El cuarto de telecomunicaciones con sus respectivas instalaciones eléctricas, sistemas de backups, protecciones en caso de falla o cortes de energía, y aire acondicionado.
7. Todos los equipos de networking que conforman el cuarto de telecomunicaciones.
8. Cada uno de los CPU de los administrativos y docentes de la institución.

3.1.19. Evaluación de las amenazas

La evaluación de las amenazas se realizará de acuerdo al análisis de cada una de las vulnerabilidades que han sido detectadas en los diferentes activos que tiene un nivel crítico, conforme a la tabla 2.2 se definirá la probabilidad de ocurrencia de cada una de las mismas. Por lo cual consideramos varios criterios:

- Lo importante que es el activo para la institución.
- El nivel de ocurrencia que posee la vulnerabilidad en el activo.

- La susceptibilidad técnica que la vulnerabilidad se materialice.

Tabla 3.21: Evaluación de las Amenazas a los Activos de la UEA.

Nro.	AMENAZA	ACTIVO	VULNERABILIDAD	PROBABILIDAD
1	Desastres naturales \Terremotos	Cuarto de Telecomunicaciones	Información almacenada en un solo lugar	Remoto
2	Incendio		Sobrecargas en el sistema eléctrico	Remoto
3	Interrupción de servicios		Falla en el software o hardware	Ocasional
4	Avería de origen físico o lógico		Periodos de limpieza no definidos	Ocasional
5	Corte del suministro eléctrico	Equipos de Networking	Inestabilidad de voltaje	Frecuente
6	Humedad\ Fallo de servicios de comunicaciones		Falta de mantenimiento en los equipos de enfriamiento	Frecuente
7	Desgaste\ Daños físicos		Muchos años de servicio de los equipos	Frecuente
8	Errores del administrador	Servidores	Ineficaz conexión de los cables de red	Ocasional
9	Espionaje remoto		Flujo de contraseñas sin autorización	Ocasional
10	Fallas de Software		Errores de compilación	Ocasional
11	Difusión de software dañino (virus)		Trafico de información sin protección	Frecuente
12	Ingeniería Social		Personas mal intencionadas (Ataques)	Remoto
13	Fallas de energía	PC	Averías en las fuentes de alimentación de los equipos	Ocasional
14	Fallas en el Hardware		Equipos con falta de mantenimiento	Ocasional
15	Fallas en el Software		Falta de pruebas en el software	Ocasional
16	Caída del sistema por agotamiento de recursos		Utilización errónea de aplicaciones de software	Ocasional
17	Códigos maliciosos		Descarga y uso no controlado de software	Ocasional

18	Errores físicos	Red de Datos	La infraestructura de red de cat 6e no cumple con las normas y estándares	Ocasional
19	Ataques a los principales servicios		No existe segmentación de la red	Remoto
20	Presencia de interferencias electromagnéticas		Fallas en el diseño de red	Remoto
21	Intercepción de información		Las líneas de comunicación con falta de protección	Ocasional
22	Modificación o alteración de la información		El envío de tráfico sensible a través de la red es inseguro	Ocasional
23	Incumplimiento de los objetivos del departamento	Estructura organizacional	Falta de personal en el departamento informático	Remoto
24	Abuso y acceso a páginas no autorizadas		Falta de monitoreo de los recursos de procesamiento de la red	Remoto
25	Negación de servicios		Faltan procedimientos de identificación y evaluación de riesgos.	Ocasional
26	Interrupción de servicios		Falta de planes de continuidad	Frecuente
27	Descuido mal uso del servicios		Falta políticas sobre el uso de correo electrónico	Remoto
28	Negación de servicios	Información	Saturación de las BBDD	Ocasional
29	Modificación o alteración de información		Errores de duplicidad	Ocasional
30	Ingeniería social		Falta de cultura de la seguridad de la información	Ocasional
31	Accesos no autorizados		Falta de controles para la habilitación de servicios	Ocasional
32	Suplantación de identidad	Software	Falta de mecanismos de identificación y autenticación de usuario	Ocasional

Fuente: Información recopilada del Dpto. de Sistemas de la Unidad Educativa Atenas.

3.1.20. Matriz de contingencia

La tabla 3.22 pertenece a la evaluación de los activos físicos tecnológicos, el valor de la probabilidad se lo toma acorde a la tabla 2.2 en sus valores cuantitativos conjuntamente con la previa evaluación de las amenazas, el impacto es evaluado mediante la tabla 2.3 tomando el valor conforme a su descripción, el nivel de riesgo

se encuentran acorde a la figura 2.6 en sus valores de probabilidad e impacto, la clasificación de los posibles eventos a materializarse se usa una nomenclatura: (C) para eventos controlables y (NC) para cada uno de los eventos no controlables.

Tabla 3.22: Evaluación de las Amenazas a Activos Físicos.

Nro.	Amenaza	Probabilidad	Impacto	Riesgo	Categoría
Activo: Cuarto de Telecomunicaciones					
1	Desastres naturales \Terremotos	1	4	A	NC
2	Incendio	1	4	A	NC
3	Interrupción de servicios	2	3	M	C
4	Avería de origen físico o lógico	2	3	M	NC
Activos: Equipos de Networking y Red de Datos					
5	Corte del suministro eléctrico	3	4	C	NC
6	Humedad\Fallo de servicios de comunicaciones	3	3	A	C
7	Desgaste\ Daños físicos	3	3	A	C
18	Errores físicos	2	2	M	C
21	Interceptación de información	2	3	M	C
Activo: Equipos de Almacenamiento (servidores)					
8	Errores del administrador	2	2	M	C
9	Espionaje remoto	2	3	M	C
10	Fallas de software	2	3	M	C
11	Difusión de software dañino (virus)	3	3	A	C

Activo: PCs. Hardware y Software					
13	Fallas de energía	2	3	M	NC
14	Fallas en el Hardware	2	3	M	C
15	Fallas en el Software	2	2	M	C
16	Caída del sistema por agotamiento de recursos	2	3	M	C
17	Códigos maliciosos	2	3	M	C
32	Suplantación de identidad	2	1	B	NC

Activo: Información					
28	Negación de servicios	2	3	M	C
29	Modificación o alteración de información	2	3	M	C
30	Ingeniería social	2	2	M	NC
31	Accesos no autorizados	2	3	M	C

Fuente: Información recopilada del Dpto. de Sistemas de la UEA.

3.1.21. Identificación de controles preventivos

En esta fase es esencial implementar la asignación de roles y responsabilidades en el departamento de sistemas ya que los mismos serán los encargados de cumplir con tareas específicas para solucionar problemas en caso de presentarse una emergencia.

3.1.22. Formación de grupos y asignación de roles en caso de una contingencia

Para establecer un equipo que actué en caso de una contingencia, en primer lugar se debe contar con un coordinador principal este debe ser responsable de informar el progreso diario en la recuperación y si es necesario, inmediatamente comunicar a la persona responsable del plan general de contingencias.

La Tabla 3.23 describe los roles y responsabilidades los cuales cada uno de los miembros del departamento de sistemas deben desarrollar para recuperarse ante una emergencia. (Plan de contingencia informático).

Tabla 3.23: Roles y Responsabilidades en Caso de una Contingencia.

ROLES	PUESTO	RESPONSABILIDADES
Coordinador principal	Analista de Sistemas 1	Encargado de la toma de prontas decisiones en caso de alguna emergencia.
		Organiza e implementa las fases para la ejecución del plan de contingencia de una manera eficaz.
		Evaluar cada uno de los sistemas que se encuentran en un estado crítico acorde al tipo de evento que se ha suscitado.
		Ejecución de pruebas cuando se realiza una nueva configuración de sistemas
		Mantener un inventario actualizado de los equipos de telecomunicaciones, PCs, software, impresoras, faxes, etc.
		Responsable de dar por concluida la declaración de contingencia
Coordinador de sistemas	Analista de Sistemas 2	Responsable de los procedimientos en los cuales la eventualidad haya afectado la red de comunicación, los servicios de internet, correo electrónico o daño a los dispositivos del cuarto de telecomunicaciones.
		Realizar pruebas de funcionamiento en caso de que los servicios sufran alguna interrupción parcial o total.
		Encargado de mantener actualizadas las copias de seguridad.
		Mantener las copias de seguridad de forma segura en una ubicación externa.
		Determinar las características necesarias de los equipos para dar continuidad a las operaciones.
		Responsable de restablecer el servicio a la brevedad posibles sea cual sea el daño en los equipos

Fuente: Elaborado por el investigador.

3.1.23. Priorización de recursos tecnológicos

Después de identificar los riesgos de seguridad en la matriz de contingencia, se determinaron los requisitos necesarios para mejorar la seguridad de la información de cada activo. En la tabla 3.24 se menciona el activo conjuntamente con las posibles soluciones para mejorar los requerimientos de seguridad.

Tabla 3.24: Requerimientos de Seguridad de los Activos de la UEA.

ACTIVO	REQUERIMIENTOS
Centro de Datos	Debe haber un manual de contingencia en caso de errores o desastres en los sistemas principales ubicados en el interior como: Wamp Server (intranet), Active Directory, Sistema Biométrico, etc. Para la reanudación inmediata de actividades.
Equipos de Networking y Red de datos	<ul style="list-style-type: none"> • Siempre debe estar disponible porque por aquí se transfiere mucha información para ser almacenada en los servidores • Se debe mantener procedimientos de control de acceso, ciberseguridad y protección contra desastres. • Debe tener una copia de seguridad de todas las configuraciones de los dispositivos de red. • El manejo de los dispositivos solo puede ser realizado por personal capacitado
Servidores	<p>Estos dispositivos de almacenamiento contienen una gran cantidad de información importante la institución. Por esta razón, siempre deben estar activos y disponibles.</p> <ul style="list-style-type: none"> • Deben tener políticas de autenticación basadas en perfiles de usuario. • La información almacenada en estos dispositivos solo puede acceder o modificar el personal autorizado, ya que deben ser altamente confiables y completos. • Debe tener procedimientos de recuperación de respaldos de la información que residan en los servidores.
Software	<ul style="list-style-type: none"> • Debe tener un alto nivel de disponibilidad. • Deben contar con procedimientos de contingencias • Solo personal autorizado y debidamente capacitado puede tener acceso a estos sistemas • Los datos ingresados a través de estos sistemas deben tener integridad.
PCs	<ul style="list-style-type: none"> • Son los principales medios de trabajo de los empleados de la institución, por lo que deben funcionar correctamente para realizar sus actividades diarias. • Deben tener un software antivirus o freezarlas para evitar daños debido a códigos maliciosos. • Deben ser utilizados exclusivamente para actividades laborales.
Información	<ul style="list-style-type: none"> • Debe haber procedimientos para realizar copias de seguridad, de esta manera respaldar toda la información importante de la institución. • Se debe almacenar las copias de seguridad en lugares y servidores seguros fuera de las instalaciones principales de la institución.

Fuente: Elaborado por el investigador.

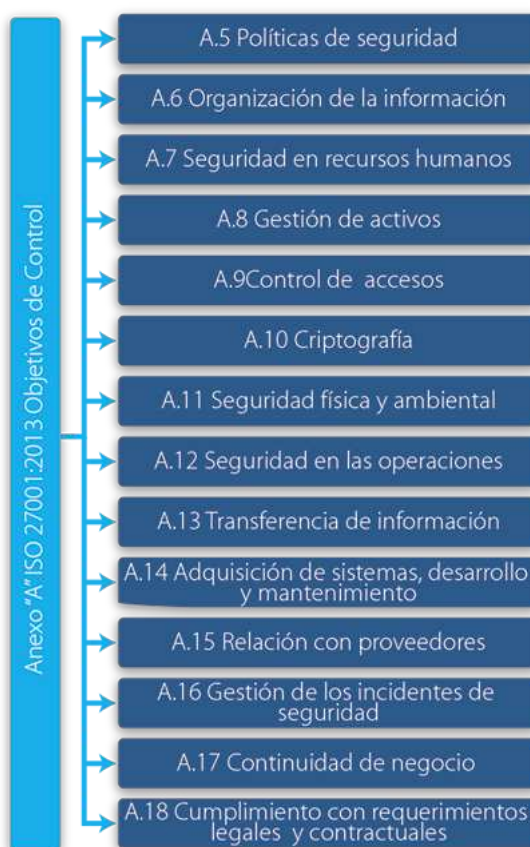
3.1.24. Declaración de Aplicabilidad

En este punto, conocemos los activos de la institución, hemos evaluado las amenazas y desarrollamos la matriz de contingencia. Es hora de evaluar en qué medida la institución cumple con las buenas prácticas de seguridad.

La ISO/IEC 27001 es una norma de seguridad de la información la cual posee un conjunto de 114 controles agrupados en 35 objetivos de control, en su versión 2013. EL anexo A se usa generalmente como referencia para la implementación de medidas de protección de la información en la misma se detallan y verifica los controles relevantes para su aplicabilidad a la situación actual de la institución.

Respaldándonos en el modelo de madurez de capacidades (CMM) que es una metodología para analizar el grado de madurez con la que cuenta la institución, en cuanto a la implementación del sistema de gestión de seguridad de la información (SGSI). En esta fase el objetivo principal es evaluar el nivel de madurez de la seguridad en la institución, en lo que respecta a los 114 controles planeados por la ISO/IEC 27001:2013. En resumen, los dominios a analizar se detallan en la figura 3.6.

Figura 3.6: Dominios Anexo “A” de ISO 27001:2013



Fuente: [11].

3.1.25. Estado y aplicabilidad de los controles de seguridad de la información ISO 27001:2013

Tabla 3.25: Estado y Aplicabilidad de los Controles ISO 27001:2013.

ISO/IEC 27001:2013	Estado	No Aplicable	Justificación
A.5. Política de la seguridad de la información.			
A5.1 Directrices de gestión de la seguridad de la información			
A5.1.1 Políticas para la seguridad de la información	Inicial		Se debe plantear un conjunto de políticas de seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado al personal y las partes interesadas.
A5.1.2 Revisión de las políticas para la seguridad de la información	Inicial		Las políticas de seguridad de la información deben revisarse periódicamente para garantizar su idoneidad y eficacia.
A.6. Organización de la seguridad de la información			
A6.1 Organización interna			
A6.1.1 Roles y responsabilidades en seguridad de la información	Inicial		Todas las responsabilidades de seguridad de la información deben definirse y asignarse.
A6.1.2 Segregación de tareas	Definido		Las tareas y áreas en conflicto deben estar separadas para reducir la posibilidad de modificación no autorizada o mal uso de los activos de la organización.
A6.1.3 Contacto con las autoridades	Optimizado		Se debe mantener una comunicación adecuada con el departamento de sistemas ya que los mismos están a cargo de la seguridad de la información.
A6.1.4 Contacto con grupos de interés especial	Definido		Debe tener una relación con las partes interesadas u otros foros, asociaciones profesionales relacionados con la seguridad.
A6.1.5 Seguridad de la información en la gestión de proyectos	Inicial		Independientemente del tipo de proyecto, los problemas de seguridad de la información deben abordarse en la gestión del proyecto.
A6.2 Los dispositivos móviles y el teletrabajo			
A6.2.1 Política de dispositivos móviles	Administrado		Se deben implementar políticas y medidas de seguridad para gestionar los riesgos que conlleva el uso de dispositivos móviles.
A6.2.2 Teletrabajo	Administrado		Se deben implementar políticas de seguridad para proteger la información a la que se accede mediante teletrabajo.

A.7. Seguridad relativa a los recursos humanos			
A7.1 Antes del empleo			
A7.1.1 Investigación de antecedentes	Administrado		La verificación de antecedentes de todos los solicitantes para un puesto debe realizarse de acuerdo con las leyes, regulaciones y principios éticos relevantes.
A7.1.2 Términos y condiciones del empleo	Administrado		Los empleados y contratistas deben tener responsabilidades de seguridad de la información con la institución.
A7.2 Durante el empleo			
A7.2.1 Responsabilidades de gestión	Administrado		La dirección debe exigir a todos los empleados y administrativos que utilicen la seguridad de la información de acuerdo con las políticas establecidas en la organización.
A7.2.2 Concienciación, educación y capacitación en seguridad de la información	Administrado		Todo el personal de la institución debe recibir capacitación y actualización sobre las políticas y procedimientos de seguridad de la información para que puedan ejercer su cargo.
A7.2.3 Proceso disciplinario	Administrado		Debe haber un proceso de comunicación formal para tomar medidas contra los empleados que violen la seguridad de la información.
A7.3 Finalización del empleo o cambio en el puesto de trabajo			
A7.3.1 Responsabilidades ante la finalización o cambio	Administrado		Las responsabilidades y obligaciones de la seguridad de la información son válidas aun cuando el empleado ya no trabaje en la institución.

A.8. Gestión de activos			
A8.1 Responsabilidad sobre los activos			
A8.1.1 Inventario de activos	Administrado		Se deben identificar los activos relacionados con la información y se debe desarrollar y mantener un inventario actualizado de estos activos.
A8.1.2 Propiedad de los activos	Administrado		Los activos incluidos en el inventario deben pertenecer a la institución y a cargo del departamento de sistemas para garantizar un control y uso adecuado.
A8.1.3 Uso aceptable de los activos	Definido		Se deben implementar reglas para el uso de los activos asociados con información e instalaciones de procesamiento de datos.
A8.1.4 Devolución de activos	Administrado		Al final del contrato, todos los empleados y usuarios externo deben devolver los activos de información de los cuales son responsables a la institución.
A8.2 Clasificación de la información			
A8.2.1 Clasificación de la información	Administrado		La información debe clasificarse de acuerdo con los requisitos legales, valor, criticidad y la sensibilidad a la divulgación o modificación no autorizada.
A8.2.2 Etiquetado de la información	Inicial		Se deben realizar procedimientos de etiquetado de información de acuerdo con el esquema de clasificación de información establecido por la institución.
A8.2.3 Manipulado de la información	Administrado		Los procedimientos de gestión de activos deben implementarse y garantizar que solo el personal autorizado tenga acceso a ellos.
A8.3 Manipulación de los soportes			
A8.3.1 Gestión de soportes extraíbles	Inexistente		Los procedimientos de gestión de medios extraíbles deben implementarse para mantener la confidencialidad de la información.
A8.3.2 Eliminación de soportes	Administrado		Cuando ya no se necesitan medios de soporte, deben eliminarse de manera segura mediante procedimientos formales.
A8.3.3 Soportes físicos en tránsito		X	Los medios que contienen información deben estar protegidos contra el acceso no autorizado, mal uso o daños durante el transporte.

A.9. Control de acceso			
A9.1 Requisitos de negocio para el control de acceso			
A9.1.1 Política de control de acceso	Definido		Se debe establecer políticas de control de acceso para garantizar la seguridad de la información en base a los requisitos de la institución.
A9.1.2 Acceso a las redes y a los servicios de red	Administrado		A los usuarios solo se les debe permitir el acceso a la red y a los servicios de red a través de reglas prohibiéndoles donde no están específicamente autorizados.
A9.2 Gestión de acceso de usuario			
A9.2.1 Registro y baja de usuario	Optimizado		Se debe implementar un proceso formal de registro de usuarios con una identificación de usuario única para administrar el acceso a la información.
A9.2.2 Provisión de acceso de usuario	Inicial		Se debe implementar un proceso para el acceso de usuarios para de esta manera asignar o revocar el acceso a todos los sistemas y servicios de la institución.
A9.2.3 Gestión de privilegios de acceso	Administrado		La asignación y el uso de derechos de acceso privilegiado deben ser restringidos y controlados.
A9.2.4 Gestión de la información secreta de autenticación de los usuarios	Repetible		La distribución de información secreta de autenticación debe controlarse a través de un proceso de gestión formal.
A9.2.5 Revisión de los derechos de acceso de usuario	Desconocido		Los propietarios de activos deben verificar periódicamente el acceso de los usuarios.
A9.2.6 Retirada o reasignación de los derechos de acceso	Optimizado		El acceso de todos los empleados y usuarios externos a la información debe ser revocado al final del contrato.
A9.3 Responsabilidades del usuario			
A9.3.1 Uso de la información secreta de autenticación	Administrado		Se debe exigir a los usuarios que cumplan con las políticas de la institución con respecto al uso de información secreta de autenticación.

A9.4 Control de acceso a sistemas y aplicaciones			
A9.4.1 Restricción del acceso a la información	Administrado		El acceso a la información y a las funciones de los sistemas se debe restringir para de esta manera evitar que personas ajenas a la institución obtengan información.
A9.4.2 Procedimientos seguros de inicio de sesión	Administrado		El acceso a los sistemas y aplicaciones en la institución debe controlarse mediante un proceso de conexión segura.
A9.4.3 Sistema de gestión de contraseñas	Administrado		Los sistemas de gestión de contraseñas deben garantizar contraseñas cifradas y de alta calidad.
A9.4.4 Uso de utilidades con privilegios del sistema	Administrado		El uso de programas que puedan anular el control de los sistemas y aplicación debe restringirse y controlarse.
A9.4.5 Control de acceso al código fuente de los programas	Administrado		El acceso al código fuente del programa debe estar restringido.
A.10. Criptografía			
A10.1 Controles criptográficos			
A10.1.1 Política de uso de los controles criptográficos		X	Debería existir una política de protección de la información mediante controles criptográficos.
A10.1.2 Gestión de claves		X	Se deben implementar políticas relacionadas con el uso, protección y caducidad de las claves criptográficas.

A.11. Seguridad física y del entorno			
A11.1 Áreas seguras			
A11.1.1 Perímetro de seguridad física	Repetible		Los límites de seguridad deben definirse para proteger las áreas que procesan o contienen información confidencial o importante.
A11.1.2 Controles físicos de entrada	Inicial		Las áreas seguras deben estar protegida por controles para garantizar que solo el personal autorizado tenga acceso.
A11.1.3 Seguridad de oficinas, despachos y recursos	Inexistente		Se deben aplicar medidas de seguridad a las oficinas e instalaciones para mantener la confidencialidad e integridad de la información.
A11.1.4 Protección contra las amenazas externas y ambientales	Inicial		Se debe desarrollar planes de gestión de riesgos para desastres naturales, ataques maliciosos o accidentes para evitar que la institución pierdan información valiosa.
A11.1.5 El trabajo en áreas seguras	Desconocido		Se deben utilizar procedimientos para trabajar en áreas seguras para garantizar la confidencialidad de la información.
A11.1.6 Áreas de carga y descarga		X	Las áreas de despacho y carga donde pueden ingresar personas no autorizadas deben controlarse, si es posible aislarlas de las instalaciones de procesamiento de información.
A11.2 Seguridad de los equipos			
A11.2.1 Emplazamiento y protección de equipos	Optimizado		Los equipos deben ubicarse de manera estratégica para que se pueda reducir el riesgo de amenazas, riesgos ambientales y también la posibilidad de acceso no autorizado.
A11.2.2 Instalaciones de suministro	Optimizado		Los equipos principales debe estar protegidos por un UPS contra cortes de energía u otras interrupciones causadas en el servicio eléctrico.
A11.2.3 Seguridad del cableado	Optimizado		Las líneas de energía y telecomunicaciones deben estar protegidas contra interceptaciones, interferencias o daños.
A11.2.4 Mantenimiento de los equipos	Optimizado		Los equipos deben mantenerse adecuadamente para garantizar su disponibilidad e integridad, y no causen pérdida de información a futuro.

A11.2.5 Retirada de materiales propiedad de la empresa	Administrado		Ningún dispositivo, información o software puede retirarse de su sitio sin autorización previa.
A11.2.6 Seguridad de los equipos fuera de las instalaciones	Administrado		Deben aplicarse medidas de seguridad a los activos fuera de la institución, teniendo en cuenta los diferentes riesgos de trabajar fuera de la misma.
A11.2.7 Reutilización o eliminación segura de equipos	Optimizado		Todos los equipos que contengan medios de almacenamiento o cualquier información confidencial deben ser verificados para su eliminación o sobrescritura antes de desecharlos o reutilizarlos.
A11.2.8 Equipo de usuario desatendido	Administrado		Los empleados deben asegurarse de que sus dispositivos no supervisados estén completamente protegidos por contraseñas para evitar la pérdida de información.
A11.2.9 Política de puesto de trabajo despejado y pantalla limpia	Optimizado		Se debe establecer políticas de escritorio y pantalla limpios para los papeles y medios de almacenamiento extraíbles en el procesamiento de información.
A.12. Seguridad de las operaciones			
A12.1 Procedimientos y responsabilidades operacionales			
A12.1.1 Documentación de procedimientos operacionales	Optimizado		Los procedimientos operativos deben documentarse y ponerse a disposición de todos los usuarios que los necesiten.
A12.1.2 Gestión de cambios	Administrado		Los cambios en la institución, instalaciones y sistemas de procesamiento de información que afectan la seguridad de la información deben ser monitoreados.
A12.1.3 Gestión de capacidades	Optimizado		El uso de los recursos debe ser monitoreado y ajustado para garantizar el rendimiento requerido del sistema.
A12.1.4 Separación de los recursos de desarrollo, prueba y operación		X	El desarrollo, las pruebas y los entornos operativos deben estar separados para reducir el riesgo de acceso no autorizado al entorno operacional.

A12.2 Protección contra el software malicioso (malware)			
A12.2.1 Controles contra el código malicioso	Optimizado		Se deben implementar controles de detección, prevención y recuperación para proteger la información de código malicioso.
A12.3 Copias de seguridad			
A12.3.1 Copias de seguridad de la información	Optimizado		Se deben hacer copias de seguridad de la información, software e imágenes de los sistemas y probarse regularmente para garantizar que la información esté disponible en caso de un incidente
A12.4 Registros y supervisión			
A12.4.1 Registro de eventos	Repetible		Los registros de eventos relacionados con la seguridad de la información deben mantenerse y revisarse periódicamente para proporcionar soluciones más efectivas.
A12.4.2 Protección de la información del registro	Administrado		Las instalaciones y la información de registro deben estar protegidas contra cambios y acceso no autorizado.
A12.4.3 Registros de administración y operación	Definido		Las actividades del administrador y del operador del sistema deben registrarse y verificarse regularmente.
A12.4.4 Sincronización del reloj	Optimizado		Los relojes de todos los sistemas de procesamiento de información en la institución deben sincronizarse con una única fuente de referencia de tiempo
A12.5 Control del software en explotación			
A12.5.1 Instalación del software en explotación	Administrado		Los instalación de software en los sistemas operativos debe estar controlada para así precautelar el acceso a información importante.
A12.6 Gestión de la vulnerabilidad técnica			
A12.6.1 Gestión de las vulnerabilidades técnicas	Definido		Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información, y tomar las medidas apropiadas para tratar el riesgo asociado.
A12.6.2 Restricción en la instalación de software	Administrado		Se debe implementar políticas de instalación de software por parte de los usuarios.

A12.7 Consideraciones sobre la auditoría de sistemas de información			
A12.7.1 Controles de auditoría de sistemas de información	Administrado		Los requisitos y actividades de auditoría que implican la revisión de los sistemas de información deben planificarse cuidadosamente para minimizar la interrupción de los procesos de la institución.
A.13. Seguridad de las comunicaciones			
A13.1 Gestión de la seguridad de las redes			
A13.1.1 Controles de red	Administrado		La red debe ser administrada y controlada para proteger la información en sistemas y aplicaciones.
A13.1.2 Seguridad de los servicios de red	Administrado		Independientemente de si el servicio es proporcionado interna o externamente, el mecanismo de seguridad debe determinarse e incluirse en el acuerdo de servicio de red.
A13.1.3 Segregación en redes	Administrado		Se deben realizar una segmentación de red para una mejor organización por departamentos en la institución.
A13.2 Intercambio de información			
A13.2.1 Políticas y procedimientos de intercambio de información	Administrado		Deben existir políticas para proteger la transmisión de información mediante el uso de todo tipo de medios de comunicación.
A13.2.2 Acuerdos de intercambio de información	Administrado		El acuerdo debe abordar el tema de la transferencia segura de información con partes externas de la institución.
A13.2.3 Mensajería electrónica	Repetible		La información contenida en los mensajes electrónicos debe estar debidamente protegida.
A13.2.4 Acuerdos de confidencialidad o no revelación	Inexistente		Los requisitos de confidencialidad o no divulgación para la protección de la información deben revisarse y documentarse periódicamente.

A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información			
A14.1 Requisitos de seguridad en los sistemas de información			
A14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	Administrado		La seguridad de la información debe aplicarse a nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A14.1.2 Asegurar los servicios de aplicaciones en redes públicas	Administrado		La información involucrada en la red pública debe estar protegida contra fraudes, revelaciones o modificaciones no autorizadas.
A14.1.3 Protección de las transacciones de servicios de aplicaciones	Administrado		La información involucrada en las transacciones de servicio de aplicaciones debe protegerse para evitar la transferencia incompleta, divulgación o reproducción de mensajes no autorizados.
A14.2 Seguridad en el desarrollo y en los procesos de soporte			
A14.2.1 Política de desarrollo seguro	Administrado		Las reglas de desarrollo de software y sistema deben establecerse y aplicarse al desarrollo dentro de la institución.
A14.2.2 Procedimiento de control de cambios en sistemas	Administrado		Los cambios en los sistemas dentro del ciclo de desarrollo de software y sistemas deben realizarse dentro de la institución.
A14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Definido		Al cambiar las plataformas y sistemas operativos, se sugiere que se verifique y pruebe las aplicaciones para asegurarse de que no afecten la seguridad de la información.
A14.2.4 Restricciones a los cambios en los paquetes de software	Definido		Los cambios a los paquetes de software deben ser desaconejados, todos los cambios deben ser estrictamente controlados.
A14.2.5 Principios de ingeniería de sistemas seguros	Definido		Es necesario establecer principios para la organización de sistemas seguros utilizándolos en la implementación de sistemas de información.
A14.2.6 Entorno de desarrollo seguro	Definido		La institución debe establecer entornos de desarrollo seguros para las tareas de desarrollo e integración a lo largo del ciclo de vida de desarrollo de software.

A14.2.7 Externalización del desarrollo de software	Optimizado		La institución debe supervisar la actividad de desarrollo de los sistemas subcontratados.
A14.2.8 Pruebas funcionales de seguridad de sistemas	Administrado		Durante el proceso de desarrollo, se deben realizar pruebas funcionales y de seguridad.
A14.2.9 Pruebas de aceptación de sistemas	Administrado		Para nuevos sistemas de información, actualizaciones y nuevas versiones, se deben establecer procedimientos de prueba.
A14.3 Datos de prueba			
A14.3.1 Protección de los datos de prueba	Definido		Los datos de prueba deben seleccionarse, protegerse y controlarse cuidadosamente.
A.15. Relación con proveedores			
A15.1 Seguridad en las relaciones con proveedores			
A15.1.1 Política de seguridad de la información en las relaciones con los proveedores	Inexistente		Los requisitos de seguridad de la información deben acordarse y documentarse para mitigar los riesgos asociados con el acceso del proveedor a los activos de la institución.
A15.1.2 Requisitos de seguridad en contratos con terceros	Definido		Se deben establecer políticas de seguridad de la información con cada proveedor que puedan tener acceso a la infraestructura de TI de la institución.
A15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	Inexistente		Los acuerdos con proveedores deben abordar los riesgos asociados con la cadena de suministro de productos y servicios de TIC.
A15.2 Gestión de la provisión de servicios del proveedor			
A15.2.1 Control y revisión de la provisión de servicios del proveedor	Administrado		La institución debe monitorear y revisar regularmente los servicios prestados por los proveedores.
A15.2.2 Gestión de cambios en la provisión del servicio del proveedor	Administrado		Los cambios en los servicios prestados por los proveedores deben gestionarse, teniendo en cuenta la importancia de la información de la institución y la reevaluación de los riesgos.

A.16. Gestión de incidentes de seguridad de la información			
A16.1 Gestión de incidentes de seguridad de la información y mejoras			
A16.1.1 Responsabilidades y procedimientos	Definido		Deben establecerse responsabilidades para garantizar una respuesta efectiva y adecuada a los incidentes de seguridad de la información.
A16.1.2 Notificación de los eventos de seguridad de la información	Definido		Los eventos de seguridad de la información se deben informar al departamento del sistema para una gestión adecuada lo antes posible.
A16.1.3 Notificación de puntos débiles de la seguridad	Administrado		Todos los empleados que utilizan servicios y sistemas de información deben estar obligados a informar cualquier debilidad en la seguridad de la información en los mismos.
A16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	Definido		Los incidentes de seguridad de la información deben evaluarse y decidir si se clasifican como incidentes de seguridad de la información.
A16.1.5 Respuesta a incidentes de seguridad de la información	Optimizado		Las respuestas a incidentes de seguridad deben responderse de acuerdo con los procedimientos documentados.
A16.1.6 Aprendizaje de los incidentes de seguridad de la información	Optimizado		El conocimiento adquirido en la resolución de incidentes de seguridad de la información debe usarse para reducir la ocurrencia o impacto de futuros incidentes.
A16.1.7 Recopilación de evidencias	Administrado		La institución debe definir y aplicar procedimientos para identificar y recopilar información que pueda servir como evidencia.

A.17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio			
A17.1 Continuidad de la seguridad de la información			
A17.1.1 Planificación de la continuidad de la seguridad de la información	Inicial		La institución debe planificar la continuidad de la gestión de la seguridad de la información en situaciones adversas, como durante una crisis o desastre.
A17.1.2 Implementar la continuidad de la seguridad de la información	Administrado		La institución debe establecer y mantener procesos para garantizar la continuidad de la seguridad de la información en situaciones adversas.
A17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Repetible		La institución debe revisar periódicamente los controles de continuidad de la seguridad de la información implementados para garantizar que sean válidos y efectivos en situaciones adversas.
A17.2 Redundancias			
A17.2.1 Disponibilidad de los recursos de tratamiento de la información	Definido		Las instalaciones de procesamiento de información deben mantener un procesamiento continuo para cumplir con los requisitos de disponibilidad.

A.18. Cumplimiento			
A18.1 Cumplimiento de los requisitos legales y contractuales			
A18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Definido		La institución debe documentar y mantener actualizados los requisitos legales y reglamentarios relevantes para cada sistema de información.
A18.1.2 Derechos de Propiedad Intelectual (DPI)	Administrado		Se deben implementar procedimientos para garantizar el cumplimiento de los derechos de propiedad intelectual y el uso de productos de software con licencia.
A18.1.3 Protección de los registros de la organización	Optimizado		Los registros deben estar protegidos contra pérdida, destrucción o acceso no autorizado de acuerdo con el reglamento de la institución .
A18.1.4 Protección y privacidad de la información de carácter personal	Definido		La privacidad y la protección de los datos personales deben garantizarse de acuerdo con las normas pertinentes.
A18.1.5 Regulación de los controles criptográficos		X	Se deben utilizar controles criptográficos, de conformidad con todos los acuerdos.
A18.2 Revisiones de la seguridad de la información			
A18.2.1 Revisión independiente de la seguridad de la información	Definido		Para la gestión de la seguridad de la información se debe revisar los objetivos de control, políticas y procedimientos en intervalos planificados o cuando ocurran cambios significativos.
A18.2.2 Cumplimiento de las políticas y normas de seguridad	Definido		Los directores deben revisar periódicamente el cumplimiento de los procedimientos de seguridad de la información en cada área de la institución.
A18.2.3 Comprobación del cumplimiento técnico	Definido		Los sistemas de información deben verificarse regularmente para determinar el cumplimiento de las políticas y estándares de seguridad de la información.

Fuente: Elaborado por el Investigador.

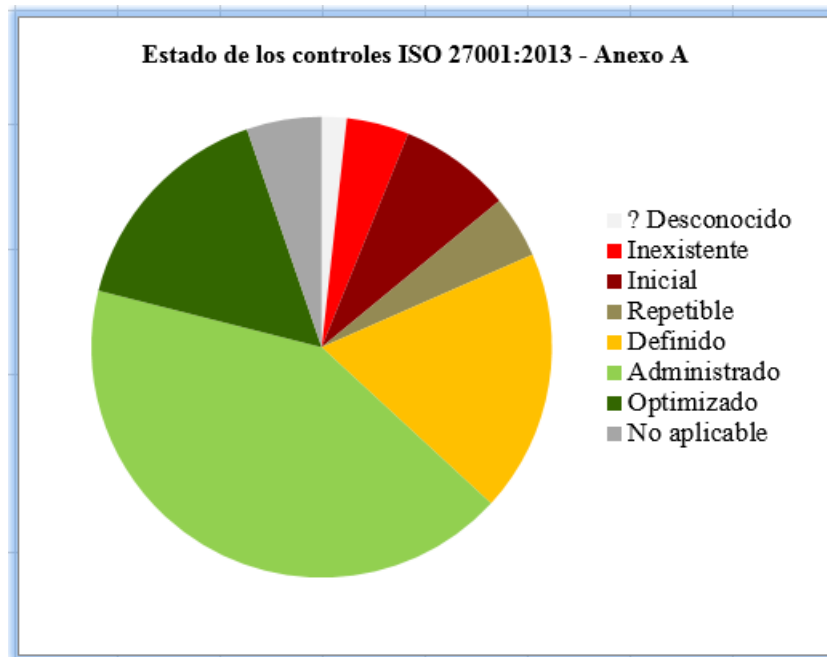
3.1.26. Métricas y resultados de la evaluación de los controles ISO 27001:2013 - Anexo A

Tabla 3.26: Valoración de los Controles SGSI.

Estado	Significado	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	2%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	4%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	8%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	4%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni por la Dirección.	18%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	42%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	16%
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	5%
Total		100%

Fuente: Métricas del modelo de madurez de capacidades (CMM), adecuación Investigador.

Figura 3.7: Estado Global del SGSI.



Fuente: Elaborado por el Investigador.

3.2. Diseño del plan de contingencia informático

Para diseñar el plan de contingencia informático es de vital importancia establecer cada uno de los pasos necesarios los cuales permitirán ya sea minimizar o evitar que ocurran eventos o incidentes que acarren la paralización parcial o total de los servicios críticos que son parte de los sistemas de información y comunicación.

Los cuales son fundamentales para la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas, de tal manera que este plan se establece con la finalidad de restablecer las actividades y servicios ante los riesgos que a continuación se detallan en el menor tiempo posible, logrando minimizar el impacto e interrupción de las actividades diarias de la institución.

MANUAL DE PROCEDIMIENTOS PARA EL DEPARTAMENTO DE
SISTEMAS DE LA UEA

CONTENIDO

OBJETO

ALCANCE

DEFINICIONES

REFERENCIAS

RESPONSABILIDADES

DESCRIPCIÓN DE LAS AMENAZAS

PLAN DE CONTINGENCIA INFORMÁTICO

OBJETO

Dar continuidad a las operaciones en la Unidad Educativa Atenas con la mayor prontitud posible posterior a haber sucedido una situación de contingencia.

ALCANCE

El presente manual de procedimientos es aplicable al departamento de Sistemas de la Unidad Educativa Atenas, en el cual se detallan procedimientos de recuperación que beneficiaran a toda la institución en caso de alguna falla, interrupción o desastre en el área informática.

Se considera los siguientes puntos:

1. Restablecimiento de los sistemas y equipos que son indispensables para la continuidad de las actividades de la institución.
2. Rehabilitación de los componentes principales de la red de comunicación.
3. El departamento de sistemas tiene como responsabilidad:
 - Mantener el correcto funcionamiento y dar soporte a la red local.
 - Contactarse con los proveedores de servicios externos conforme se requiera.

- Planificar la inducción del personal nuevo para que lleven a cabo sus nuevas funciones.
- Notificar las políticas de uso de los equipos y sistemas de información para evitar situaciones de desastre.

Además está considerado:

- Procedimientos de evacuación del personal de la institución.

DEFINICIONES

Sistemas de información: Es el conjunto en el cual se agrupan personas, equipos y procesos, que mediante mecanismos ordenados tienen como fin recibir datos y producir información, para que de esta manera puedan ser recuperados y procesados fácilmente.

Plan de respaldo: Está compuesto por todos los procedimientos y medidas preventivas para de esta manera garantizar que las actividades se reanuden antes de que ocurran amenazas. El plan de respaldo es el más importante, puede mitigar y disminuir la posibilidad de un desastre.

Plan de recuperación: Se detallan las estrategias y acciones a seguir después de haberse controlado la amenaza, Este plan tiene como objetivo principal restablecer los equipos, actividades y servicios de TI a su estado óptimo ante cualquier eventualidad.

Activo: Es todo aquello que tiene un cierto valor para la institución, y por lo tanto debe protegerse.

Confidencialidad: Se refiere a la garantía de que la información será protegida y únicamente estará accesible para el personal autorizado, y estará bajo reglas que limitan el acceso a la misma.

Disponibilidad: Es la capacidad de garantizar que todos los usuarios autorizados tengan el acceso tanto a la información y los recursos en todo momento y cada vez que lo requieran.

Integridad: El objetivo es proteger la información y evitar transmisiones o modificaciones sin autorización, la información debe ser válida y precisa.

Incidente: Es aquello que de manera inesperada se materializa interponiéndose en el transcurso normal de las actividades de una institución, por ejemplo tenemos falla el sistema eléctrico, accesos no autorizados, ingeniería social, códigos maliciosos, robo y borrado de información, etc.

Interrupción de servicios: Es la suspensión de manera temporal o total de un proceso vital de la institución.

Evento: Es un hecho que se ha dado de manera inesperada ya sea en un servicio, sistema o red de comunicación por una posible violación de las políticas de seguridad de la información dentro de las actividades normales en una empresa o institución.

Riesgo: Es la probabilidad de que una amenaza se materialice causando pérdidas de información o interrupción de servicios.

Servidores: Es un ordenador físico el cual proporciona acceso a los archivos y servicios a las máquinas cliente.

Red: Es el medio por el cual una empresa o institución está interconectada a través de dispositivos, con el fin de intercambiar información y compartir recursos ya sea interna o externamente.

REFERENCIAS Norma ISO/IEC 27001:2013

RESPONSABILIDADES

Coordinador Administrativo:

- Organizar reuniones con los responsables del departamento de sistemas, para examinar cada una de las medidas de seguridad si son las adecuadas para proteger los activos informáticos de mayor importancia para la institución.
- Debe notificar los inconvenientes que observe tanto en los procesamientos, servicios contratados y cumplimiento de las operaciones diarias de la institución.

- Debe coordinar capacitaciones por parte de los encargados del área de sistemas en cuanto a la seguridad de la información y la protección de la integridad de los equipos en caso de situaciones de contingencia, dirigido para los diferentes jefes de los departamentos y docentes de la institución.
- Trabajar conjuntamente con el coordinador principal y de sistemas aplicando los lineamientos de seguridad, para reanudar inmediatamente las actividades de la institución ante la ocurrencia de un riesgo.
- Tiene la responsabilidad de llevar un documento con el historial de todos los incidentes informáticos que ha sufrido la institución, además de las actualizaciones en los sistemas y equipos informáticos.

Coordinador Principal: Es el encargado de la ejecución, supervisión y designación de actividades a cada miembro del grupo de contingencia, así como también de cada una de las tareas relacionadas a su área de alcance entre las cuales consta:

- Realizar las pruebas necesarias en los sistemas en caso de nuevas configuraciones en los equipos.
- Debe verificar el correcto funcionamiento de los servicios y la red de comunicación.
- Verificar el óptimo funcionamiento de los sistemas considerados críticos.
- Optimizar recursos.

Coordinador de Sistemas: Es el responsable de ejecutar las tareas asignadas por el coordinador principal, también tiene a su cargo los procedimientos en los cuales la eventualidad haya afectado a la red de comunicación, servicio, o daños en los dispositivos del cuarto de telecomunicaciones. Adicional a esto lo siguiente:

- Restablecer los servicios de la manera más rápida posible sin importar el daño que se haya presentado en los equipos.
- Brindar mantenimiento y soporte a los dispositivos de cada una de las dependencias de la institución.
- Debe mantener actualizadas y en un lugar seguro las copias de seguridad.

DESCRIPCIÓN DE LAS AMENAZAS

a) Desastres Naturales / Terremotos

Si los desastres naturales fueran de magnitudes bajas y no causan fuertes daños en la estructura del edificio de administrativos que es donde se encuentra el cuarto de telecomunicaciones, no se verían afectados de ninguna manera los dispositivos que almacenan la información importante, sin embargo para asegurar la integridad del personal que labora en la institución se procedería a evacuar hasta que se evalué las instalaciones y el reingreso sea seguro. El impacto que tendría para la Unidad Educativa Atenas sería mínimo ya que las actividades se paralizarían solamente por unas horas.

Al contrario si los desastres naturales ocurren en magnitudes mayores se interrumpiría por un tiempo mas prolongado las actividades en la institución, sufriría daños físicos el edificio en el cual se encuentra el cuarto de telecomunicaciones acarreado perdidas de información, ya que no se posee un centro de datos alternativo.

Consecuencias:

- Daños en la infraestructura de red y comunicaciones.
- Pérdida de acceso a los servicios principales.
- Daños en las instalaciones físicas.
- Perdida de información.

b) Incendio

Si el fuego es de una magnitud alta y tiene su origen en el edificio de administración en la planta baja conllevaría a grandes perdidas tanto de información como de equipos, ya que en este se encuentra el cuarto de telecomunicaciones el cual esta conformado por los servidores y los equipos de networking, por lo que al ocurrir este siniestro se interrumpiría la operatividad y disponibilidad de la red.

De otra manera si el fuego afectara a otra área de las instalaciones de la institución y este es controlado rápidamente no tendría mayor consecuencia en la paralización de las actividades y disponibilidad de los servicios y red.

Consecuencias:

- Daños en los equipos tecnológicos.
- Daños en la infraestructura de red.
- Daño en las instalaciones físicas.
- Pérdida de información.

c) Corte de Suministro Eléctrico

Según antecedentes, los cortes del suministro eléctrico en la Unidad Educativa Atenas son frecuentes; por tal motivo al producirse este evento se detendrían por completo las actividades en la institución ya que únicamente se cuenta con un UPS de 6KVA en el cuarto de telecomunicaciones el mismo que ayuda a proteger de cortes o variaciones de energía los equipos de networkig y servidores, a pesar de esto la red completa dejaría de funcionar puesto que no se cuenta con un generador para proveer de energía el resto de la institución.

Al contrario si el apagón se debió a alguna mala practica en las instalaciones internas, los daños que esto ocasionaría serian graves.

CONSECUENCIAS

- Daños en las instalaciones de red.
- Daños en el cableado eléctrico.
- Indisponibilidad de servicios.
- Pérdidas de información.

d) Humedad / Fallo de servicios de comunicaciones

Las posibles causas en las fallas de los servicios de comunicación pueden ser, no contar con una adecuada estructura de red la misma que debe cumplir normas y estándares internacionales de instalación del sistema de cableado estructurado (SCE), la Unidad Educativa Atenas posee una red cableada de categoría 5a y 6a la misma que se encuentra debidamente instalada.

Un problema adicional que enfrenta es la falta de administración de los recursos de red, mantenimientos oportunos y actualización de dispositivos lo que conlleva a la interrupción de los servicios afectando de manera parcial o total la disponibilidad de la información.

CONSECUENCIAS

- Interceptación y pérdida de la confidencialidad de la información .
- Alteración y pérdida de la integridad de la información.

e) Desgaste / Daños Físicos

Se puede dar debido al tiempo de uso de los diferentes equipos tanto del cuarto de telecomunicaciones como de los diferentes departamentos y aulas de la institución. Entre las causas tenemos la falta de mantenimiento en los equipos y dispositivos de networking, falta de planificación para colocar los equipos en su área de trabajo, por inexistencia de dispositivos de seguridad como reguladores de voltaje, etc.

CONSECUENCIAS

- Pérdida de la operatividad de los equipos.
- Inaccesibilidad a los servicios.
- Pérdida de información

f) Difusión de software dañino(virus)

Este es un tipo de malware el cual puede infiltrarse en los equipos de la institución, mediante unidades de almacenamiento móviles (USB), por falta de actualización de software, a través de descargas en páginas de internet en lugares no oficiales; pueden afectar el correcto funcionamiento de los ordenadores ya que no es necesario la intervención del usuario para ser ejecutado.

Por lo cual es recomendable contar con antivirus con sus respectivas licencias actualizadas de esta manera reduciremos el riesgo de infección en los diferentes equipos instalados en los predios institucionales.

CONSECUENCIAS

- Pérdida de información y archivos.
- Errores en el sistema operativo.
- Lentitud en el equipo.

PLAN DE CONTINGENCIA INFORMÁTICO

El plan de contingencia informático es un documento planificado adecuadamente el cual contiene procedimientos para responder a la ocurrencia de un evento inesperado de manera oportuna, o a su vez que la institución continúe sus actividades al mínimo de su capacidad.

Para el éxito de este plan, es necesario que todos los involucrados en el incidente colaboren y trabajen de manera conjunta para fortalecer y cumplir con las medidas descritas.

ACTIVIDADES PREVIAS

a) Desastres Naturales / Terremotos

Medidas Humanas

- Identificar rutas de evacuación y áreas seguras para puntos de encuentro de todo el personal de la unidad educativa.
- Realizar simulacros preventivos al menos una vez al año para capacitar al personal.
- Se debe tener un botiquín de primeros auxilios, el cual debe estar colocado en un lugar fácilmente accesible visible.
- Identifique los lugares donde este tipo de desastre representa un gran peligro.
- Mantenga un inventario de materiales, herramientas y equipos necesarios para responder a una emergencia.
- Cuente a la mano una lista de números telefónicos de emergencia.

Medidas Técnicas

- Realizar un etiquetado de todos los equipos más importantes para la institución, para de esta manera priorizarlos en caso de evacuación. Por ejemplo, los Servidores de color rojo, CPUs con información importante de color amarillo y los CPUs con contenido normal en color verde.

- Cree un plan de evacuación de hardware el mismo que permita transportar equipos clave a otro edificio o departamento en el menor tiempo posible, teniendo en cuenta la importancia de cada uno. Evacue los equipos más importantes primero, mientras que los equipos menos importantes pueden esperar.
- Mantenga protegida la información crítica, debe almacenarse en servidores centralizados; la información debe tener un almacenamiento espejo en un centro de datos fuera de la institución.
- Realice copias de seguridad de las configuraciones de los principales servidores, sistemas operativos, programas desarrollados dentro de la institución, software y / o lenguajes de programación.
- Hacer copias de seguridad diariamente para de esta manera siempre tener actualizados y almacenados los datos de la institución.

b) Incendio

Medidas Humanas

- Realice la instalación de sistemas de detección de incendios, para que de esta manera se proporcione alertas al personal de la institución y al departamento de bomberos.
- Realice simulacros con el personal administrativo, docentes y alumnos al menos una vez al año para que estén capacitados en caso de incendio.
- Tenga disponible un equipo de emergencia como extintores ubicados en los departamentos donde hay una mayor probabilidad de incendio.
- Evite almacenar productos inflamables donde exista instalaciones eléctricas.
- Señalizar adecuadamente las de ruta de escape en toda la institución.

Medidas Técnicas

- Las paredes del centro de datos deben estar cubiertas con pintura especializada que retrase la propagación del fuego.
- Realizar un mantenimiento periódico a las instalaciones eléctricas, de por lo menos dos veces al año, que permitan prevenir cortocircuitos y posibles incendios.

- En el cuarto de telecomunicaciones se colocarán sensores de humo conectados a un sistema de alarmas de funcionamiento autónomo.
- En los centros de computo, y lugares donde se encuentre equipos de computación se contará con extintores de incendio tipo C.
- Evite sobrecargar circuitos con múltiples contactos.
- Contrate una póliza de seguros para proteger los activos de la institución.

c) Corte de Suministro Eléctrico

Medidas Técnicas

- La institución debe poseer una fuente de energía eléctrica adicional (generador eléctrico), para que en caso de cortes de energía eléctrica evitar la suspensión de las actividades diarias.
- Todos los equipos en el cuarto de telecomunicaciones deben estar conectados a un UPS para evitar que se apaguen debido a variaciones o cortes de energía.
- Todas las aulas y oficinas de trabajo deben tener un regulador de voltaje para evitar daños a los equipos debido a variaciones de voltaje.
- Verifique el correcto funcionamiento y condición de todos los puntos y conexiones eléctricas.
- Se debe tener la documentación necesaria sobre el cableado de red y eléctrico.

d) Humedad / Fallo de servicios de comunicaciones

Medidas Técnicas

- Evaluar las estaciones de trabajo donde van a ser colocados los equipos, evitando sitios con humedad y poca ventilación ya que esto acarrearía daños en los dispositivos electrónicos.
- Se debe contar con el diseño de la estructura de red físico y lógico, conjuntamente con un listado de todas las direcciones IP de las áreas de trabajo y a quien le pertenece, para de esta manera rastrear el fallo rápidamente y solucionarlo.

- El departamento de sistemas debe contar con un stock de repuestos entre los cuales deben estar: tarjetas de red, cables UTP, conectores Rj45, ponchadoras, etc.
- Evaluar el estado de cada uno de los conectores rj45 y cables de red tanto de las salidas de los servidores del cuarto de telecomunicaciones, las conexiones a los patch cord y switch los cuales permiten la conexión a la estación de trabajo.
- Verifique el estado y funcionamiento de todos los dispositivos intermediarios de comunicación entre el centro de datos y las estaciones de trabajo.
- El proveedor de fibra óptica debe facilitar a la institución dos rutas de acceso a sus servicios, en caso de fallas en la conexión a internet.

e) Desgaste / Daños Físicos

Medidas Técnicas

- Desarrolle un plan que incluya el mantenimiento preventivo y correctivo de todos los equipos informáticos de la institución, al menos cada 6 meses o anualmente.
- Compruebe la vigencia de la garantía técnica tanto de los equipo informático como de comunicación durante 1 a 3 años contra deterioro, daños o desperfectos por parte del fabricante.
- Establecer políticas de seguridad para el uso correcto de los equipos informáticos (hardware).
- Gestionar el posible remplazo de los equipos informáticos una vez que se haya cumplido su vida útil.
- Cuente con un stock de dispositivos de repuesto a remplazar para los equipos de computo, de esta manera se minimizará el tiempo de inoperatividad en las comunicaciones y actividades de la institución.
- Efectuar copias de seguridad tanto del software como de las configuraciones de los servidores, que se consideren críticos en caso de posibles fallas de hardware debido al desgaste físico.

f) Difusión de software dañino (virus)

Medidas Técnicas

- Mantenga actualizada la base de datos del antivirus institucional, con lo cual se logrará proteger de ataques de virus informáticos.
- Cada uno de los computadores de la institución debe contar con software antivirus con su respectiva licencia y actualización.
- En el cuarto de telecomunicaciones los servidores deben estar protegidos mediante antivirus actualizados, firewall y proxy.
- Mantenga actualizados los drivers y parches de seguridad de los sistemas operativos de cada equipo de la institución.
- Se debe evitar acceder a páginas y descargar software en sitios no oficiales.
- Escanee todos los medios extraíbles con el software antivirus antes de abrirlos en los computadores.
- Realice copias de seguridad periódicamente con el fin de salvaguardar la información valiosa.

ACTIVIDADES DURANTE

a) Desastres Naturales / Terremotos

- Si es posible, el personal administrativo y docentes deben salir del sistema guardando los documentos en los que hayan estado trabajando, para evitar pérdida de información.
- Si es posible, desconecte los equipos de la red eléctrica, para evitar que las circunstancias de peligro se maximicen de esta manera eliminara fuentes de incendio. (sin que esto signifique riesgo de exponer su vida).
- El encargado del área de sistemas debe aislar los principales equipos (servidores) que contienen los sistemas de información para limitar el alcance de las fallas y daños.
- Todo el personal de la institución debe evacuar las instalaciones con calma, por la ruta de evacuación y dirigirse a los lugares previamente designados como puntos de encuentro seguros.

b) Incendio

- Si el incendio ocurre durante las horas de trabajo, debe alertar a todo el personal de la oficina, oficinas aledañas y al departamento de bomberos.
- Cada uno de los responsables de su área de trabajo debe desconectar los equipos de las fuentes de alimentación eléctrica. (sin que esto signifique riesgo de exponer su vida).
- Si dispone del tiempo necesario y si la causa del incidente está lejos pero existe la probabilidad de que se extienda hacia el cuarto de telecomunicaciones, deberá retirar los principales equipos de computo (servidores) a un lugar seguro. (sin que esto signifique riesgo de exponer su vida).
- El personal de la institución debe retirarse con calma de sus lugares de trabajo e ir a los lugares designados con anterioridad como seguros.
- El personal de bomberos tratará de sofocar el fuego utilizando el extintor correcto para el incidente, son responsables de salvaguardar la integridad del personal docente y estudiantil, así como de la infraestructura física y tecnológica de la institución.

c) Corte de Suministro Eléctrico

- En caso de poseer una fuente de energía alterna como un generador eléctrico, activarlo para de esta manera restablecer el servicio, garantizando la continuidad de las actividades en toda la institución.
- Póngase en contacto con la agencia EEASA vía telefónica, para obtener información sobre el daño que causo la pérdida del suministro eléctrico y el tiempo aproximado que se tardaran en la reparación.
- En caso de que el corte de suministro eléctrico exceda el tiempo de almacenamiento del UPS del cuarto de telecomunicaciones, proceda al apagado manual de los servidores.
- Si la causa del corte de suministro eléctrico se produjo debido a algún cortocircuito dentro de las instalaciones de la institución, el personal técnico llevara a cabo las evaluaciones apropiadas para determinar el origen del mismo y corregir las conexiones eléctricas.

d) Humedad / Fallo de servicios de comunicaciones

- Si se presenta fallo en la comunicación de las PCs tanto del personal administrativo y docentes con los servidores de la institución, dar aviso del evento al encargado del departamento de sistemas para que realice una evaluación y la respectiva reparación.
- Constatar si no existe problemas de comunicación entre las estaciones de trabajo con los switch y patch cord a la conexión del punto de red en el cuarto de telecomunicaciones mediante la documentación del direccionamiento IP.
- El jefe del departamento de sistemas debe verificar el entorno de red, analizando en que punto pierde la señal y no llega a la estación de trabajo.
- Verificar si los controladores se encuentran actualizados y las tarjetas de red están correctamente instaladas.
- Examinar los componentes internos del equipo, si existe fallo en la tarjeta de red, proceder a realizar el cambio.
- Analizar si no existe dos equipos con la misma dirección IP, ya que esto conllevaría a conflictos en la comunicación.
- Si la institución no tiene acceso a internet comuníquese con el proveedor del servicio, para que lo solucione.

e) Desgaste / Daños Físicos

- Si el daño se encuentra en el equipo informático de los administrativos o docentes, deberán informar de inmediato al encargado del departamento de sistemas, ya que este es responsable de las decisiones a tomar para solucionar daños físicos o por desgaste tanto en los equipos de las estaciones de trabajo como en el cuarto de telecomunicaciones..
- En caso de que la situación lo requiera de inmediato instalar un nuevo equipo, hasta evaluar y determinar la reparación del otro.
- Realizar la configuración del nuevo equipo que fue reemplazado, utilizando las copias de seguridad previas del anterior equipo dejándolo con todo lo necesario para que el usuario continúe con sus actividades, de esta manera garantizando la continuidad de los procesos y actividades en la institución.

- Realizar métodos de recuperación de información en el equipo malogrado, de esta forma evitando la pérdida de información valiosa que este pudo contener.

f) Difusión de software dañino(virus)

Si la infección es a través de la red a los servidores y PCs.

- Una vez que surge el problema, dar aviso al jefe del departamento de sistemas, este evaluará si es necesario declarar el estado de contingencia en caso que este afectando a un proceso crítico, de esta manera evitar que mas estaciones de trabajo se infecten de virus.
- Verifique las alertas enviadas por el software antivirus y determine qué tipo de virus se esta propagando y analice el origen del mismo.
- Proceda a desconectar el equipo infectado de la red institucional, para evitar la propagación del virus hacia los demás equipos que conforman la misma.

Si la infección es a causa de un correo malicioso.

- Si detecta la ralentización de procesos, ventanas del navegador web se demoran en cargar, aparecen anuncios emergentes mas de lo habitual, su equipo se encuentra infectado, de inmediato dar aviso al jefe del departamento de sistemas para que proceda con las acciones correctivas.
- Si la difusión del virus se dio a través de un correo electrónico, ingresar al servidor de correos y deshabilitar el servicio para que de esta manera no siga reenviando los correos.
- Proceda a eliminar el mensaje de correo electrónico malintencionado que se encuentra en cola de reenvío, para evitar mas equipos infectados.

ACTIVIDADES DESPUÉS

a) Desastres Naturales / Terremotos

- Permanecer fuera de las instalaciones de la institución hasta que el personal externo capacitado (COE) o los bomberos hayan declarado el final de la emergencia, de esta manera el personal procederá a regresar a su área de trabajo de forma segura y si las condiciones lo permiten.

- El personal encargado del departamento de sistemas debe verificar si los equipos del cuarto de telecomunicaciones no han sufrido daños significativos, para proceder a levantar los servicios de manera inmediata.
- Verifique que los principales servidores contengan la información íntegra y completa hasta el punto anterior al incidente.
- El jefe de cada departamento investigará las pérdidas físicas y lógicas, se notificará al encargado del departamento de sistemas mismo que verificará la posibilidad de recuperación parcial o total del equipo e información.
- Se procederá a reparar o reemplazar los equipos afectados para restablecer los sistemas críticos, garantizando la continuidad normal en las operaciones de la institución; para ello se debe contar con las configuraciones y copias de seguridad previamente realizadas.
- El encargado del departamento de sistemas debe restaurar los sistemas de mayor prioridad posteriormente notificar al personal institucional que ya tienen acceso a los diferentes sistemas y pueden reanudar sus actividades diarias.

b) Incendio

- La persona a cargo de cada departamento o área afectada solicitará un informe del departamento de bomberos sobre el estado de las instalaciones e informará al jefe del departamento de sistema, para que pueda evaluar el daño a los equipos informáticos.
- Los encargados del departamento de sistemas deberán analizar y determinar el origen y las posibles causas que produjeron el incendio, para poder actualizar las políticas de seguridad y adicionar medidas preventivas.
- Se procederá a realizar una primera estimación de los daños causados por el evento, generando un inventario de los equipos afectados.
- El personal del departamento de sistemas está a cargo de evaluar los daños causados, equipo que dejaron de funcionar y sistemas afectados, luego procederán al cambio y / o reparación de los equipo e instalaciones, reanudando las actividades institucionales.
- El jefe del departamento de sistemas debe comunicarse con el representante de la aseguradora, para hacer uso del servicio contratado, verificando su cobertura contra los daños a los equipos en este incidente.

c) Corte de Suministro Eléctrico

- El responsable de cada estación de trabajo debe inspeccionar y notificar que equipos fueron afectados al encargado del departamento de sistemas, quien sugerirá el remplazo o si existe la posibilidad de recuperación del equipo y la información.
- Haciendo uso de la documentación sobre el cableado de red y eléctrico se detectará los equipos que presenten fallas en las estaciones de trabajo para de esta manera remplazarlos.
- El personal técnico encargado procederá a realizar reparaciones o cambiará las instalaciones en cada uno de los puntos eléctricos afectados.
- Asegúrese de que el fallo no haya dañado el equipo informático, revise las fuentes de alimentación, tarjetas de red, servidores y equipos de networking del cuarto de telecomunicaciones, etc. Así garantizará la continuidad de las actividades diarias de la institución.
- Se procederá con el encendido normal de los equipos tanto del cuarto de telecomunicaciones como de las PCs de las estaciones de trabajo, una vez que los técnicos y encargados del departamento de sistemas hayan realizado las revisiones pertinentes y confirmen que es seguro.
- Los encargados del departamento de sistemas deben notificar la reanudación de las operaciones en cada uno de los sistemas y bases de datos, para que de esta manera los usuarios vuelvan a usarlos y continúen con sus actividades cotidianas.

d) Humedad / Fallo de servicios de comunicaciones

- Evalúe las posibles causas del evento reinstalando el equipo en un lugar donde exista ventilación y este libre de humedad.
- Reparar o cambiar las piezas internas o el equipo afectado por la humedad, para garantizar la continuidad de las actividades de la institución.
- Verificar cada uno de los cables UTP, patch cord, switch que estén funcionando correctamente, caso contrario realizar de inmediato el remplazo del dispositivo de red.
- Cambiar los conectores rj45 defectuosos y evaluar la señal de punto a punto con un tester de conexión de red.

- El proveedor de internet, restablecerá el servicio mediante otra ruta de acceso facilitando la salida a la web.
- Comprobar la integridad y completitud de la información hasta un punto previo al incidente.
- Realice un informe de los daños causados por la interrupción en los servicio de comunicaciones y / o el acceso a la red interna, para poseer un historial de daños y posibles soluciones.

e) Desgaste / Daños Físicos

- Si los daños físicos en los equipos se dieron a causa de defectos de fábrica, el coordinador general debe contactarse con el proveedor y tramitar la garantía que estos ofrecen.
- El encargado del departamento de sistemas debe reemplazar de inmediato los componentes internos de los equipos que sufrieron daños por el desgaste físicos, garantizando la continuidad de los procesos y actividades de la institución.
- El personal responsable haciendo uso de las copias de seguridad debe restablecer en el caso de servidores las bases de datos, servicios, programas e información en los nuevos equipos verificando la integridad de la misma.
- Verificar si las medidas correctivas tomadas fueron exitosas contrarrestando la emergencia, de esta manera notificar al personal institucional que pueden reanudar sus actividades.

f) Difusión de software dañino(virus)

- Ejecutar el antivirus de una manera completa en todos los equipos de la institución para garantizar la seguridad de la información, y así eliminar todo indicio del malware.
- Analizar cada uno de los equipos que conforman la red, en busca de carpetas compartidas infectadas de malware y eliminarlas.
- Si el mensaje de que el virus todavía existe en el sistema persiste, es probable que uno de los equipos en la red haya causado la infección, el encargado del departamento de sistemas debe proceder a retirarla del acceso a la red y realizar una revisión minuciosa.

- Si no se logra una limpieza íntegra del equipo debido a que el malware daña archivos del sistema operativo, el encargado del departamento de sistemas procederá al formateo y reinstalación del S.O, haciendo uso de la copia de seguridad existente.
- Verificar la integridad de la información en los servidores, bases de datos y PCs de las estaciones de trabajo, de esta manera garantizar la confiabilidad de la misma y reanudar los procesos y actividades de la institución.
- El encargado del departamento de sistemas en lo posible debe buscar la forma de regresar a un estado inicial antes de verse afectado por el malware, en los principales sistemas de información.

ACTIVIDADES CORRECTIVAS

Las amenazas más representativas que originarían cada uno de los escenarios propuestos en los flujogramas de recuperación, se representan en el cuadro 3.27

Tabla 3.27: Escenarios de Contingencia

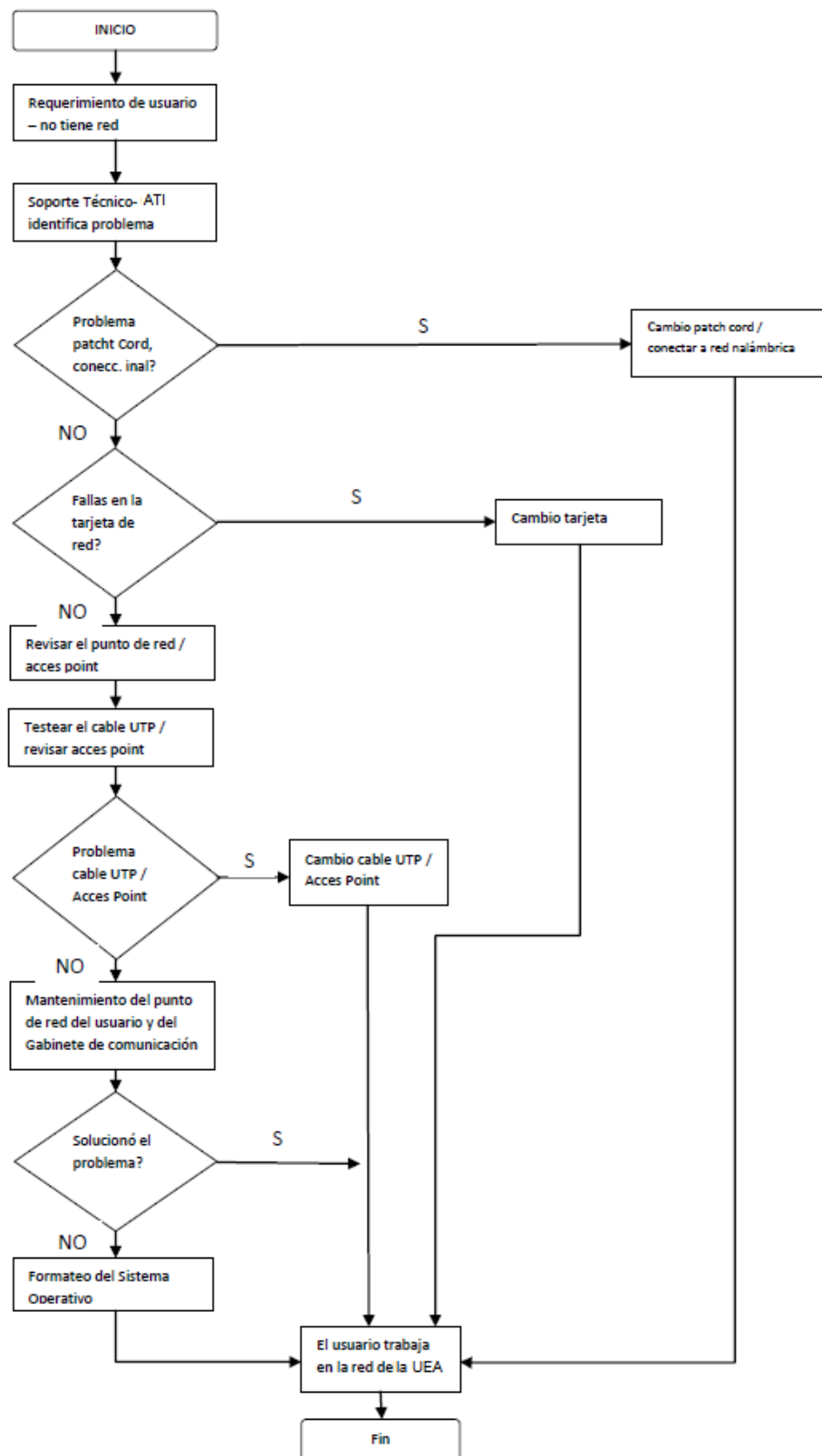
AMENAZAS	ESCENARIOS
<ul style="list-style-type: none"> • Avería de origen físico o lógico. • Desgaste en los componentes de red (cables UTP, tarjetas de red, switch, patch cord). • Códigos maliciosos. • Accesos no autorizados. • Errores de administrador. • Espionaje remoto. 	<p>I. Fallo de servicios de comunicaciones entre cliente – servidor en uno o varios terminales de la UEA.</p>
<ul style="list-style-type: none"> • Daños o errores físicos en los componentes de hardware. • Software dañino (virus). • Agotamiento de recursos (disco). • Suplantación de identidad. • Negación de servicios. • Modificación o alteración de información. • Interceptación de información. • Interrupción de servicios. 	<p>II. Fallo crítico en un servidor del cuarto de telecomunicaciones.</p>
<ul style="list-style-type: none"> • Fallas de energía. • Corte general del suministro eléctrico. 	<p>III. Corte del suministro eléctrico.</p>
<ul style="list-style-type: none"> • Falla en los equipos de comunicación: fibra óptica, antenas, switch. • Comunicación inaccesible hacia los proveedores de internet. • Fallas en el hardware. • Fallas en el software. • Ingeniería social. 	<p>IV. Pérdida de la conectividad a internet.</p>
<ul style="list-style-type: none"> • Terremoto. • Incendio. 	<p>V. Indisponibilidad del centro de telecomunicaciones (Destrucción del cuarto de servidores).</p>
<ul style="list-style-type: none"> • Accidente. • Renuncia Intempestiva. 	<p>VI. Ausencia parcial o total del personal en el área de tecnologías de la información.</p>

Fuente: Elaborado por el Investigador.

Flujogramas de recuperación ante la materialización de amenazas en el Área de Tecnologías de la Información de la Unidad Educativa Atenas.

I. Fallo de servicios de comunicaciones entre cliente – servidor en uno o varios terminales de la UEA.

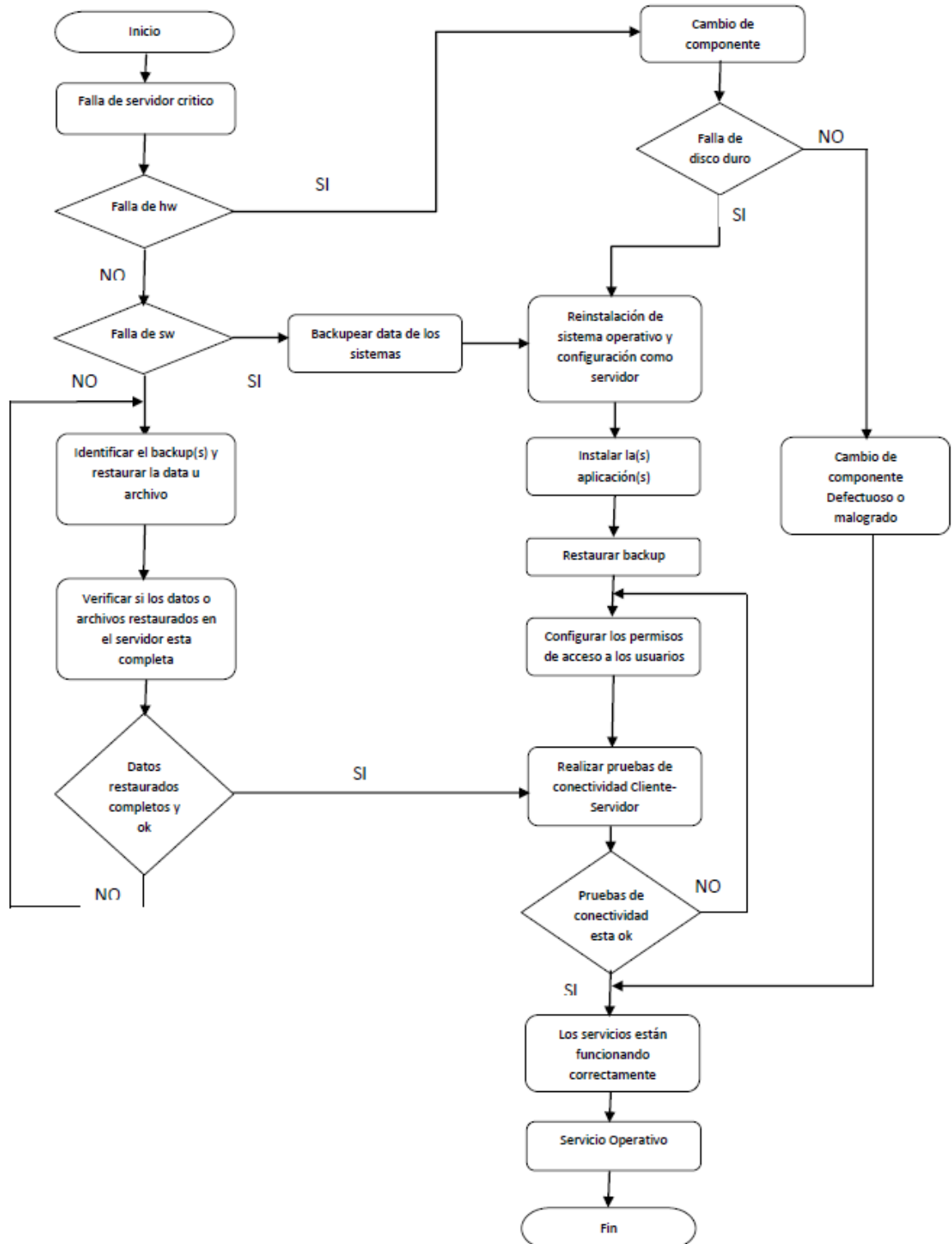
Figura 3.8: Flujoograma ante el fallo en los servicios de comunicaciones entre cliente – servidor de la UEA.



Fuente: Elaborado por el Investigador.

II. Fallo crítico en un servidor del cuarto de telecomunicaciones.

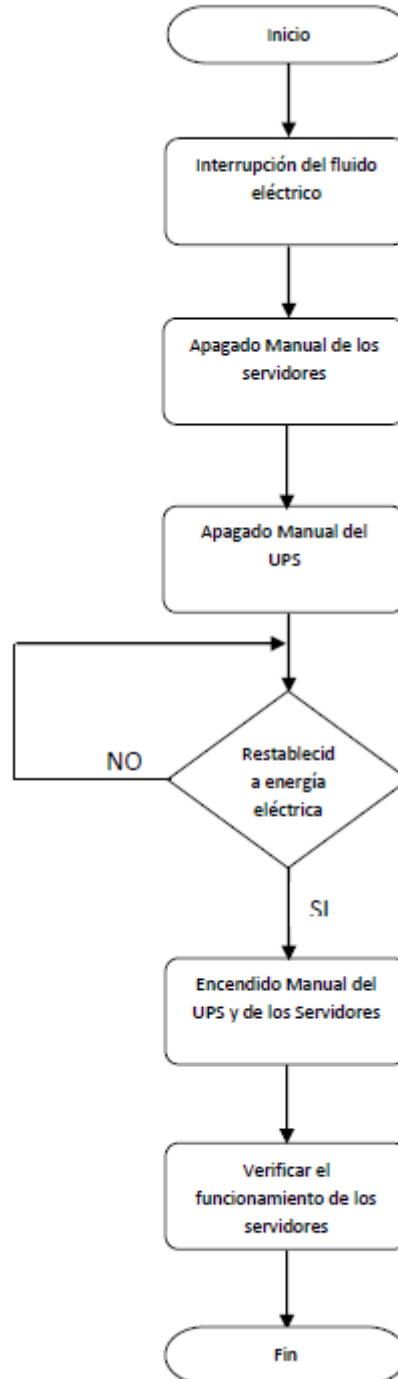
Figura 3.9: Flujograma ante el fallo crítico en un servidor del cuarto de telecomunicaciones.



Fuente: Elaborado por el Investigador.

III. Corte del suministro eléctrico.

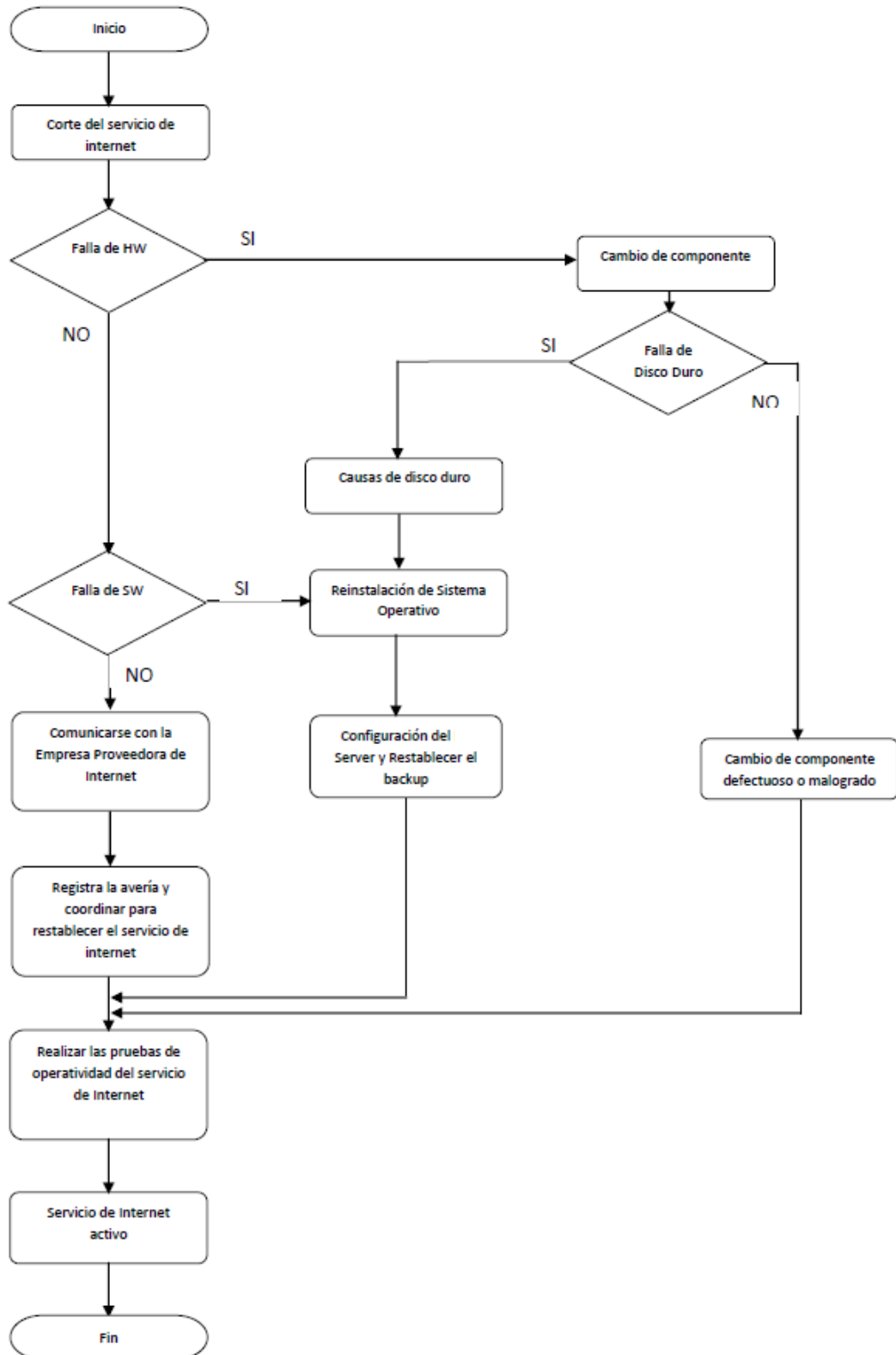
Figura 3.10: Flujograma ante el corte del suministro eléctrico.



Fuente: Elaborado por el Investigador.

IV. Perdida de la conectividad a internet.

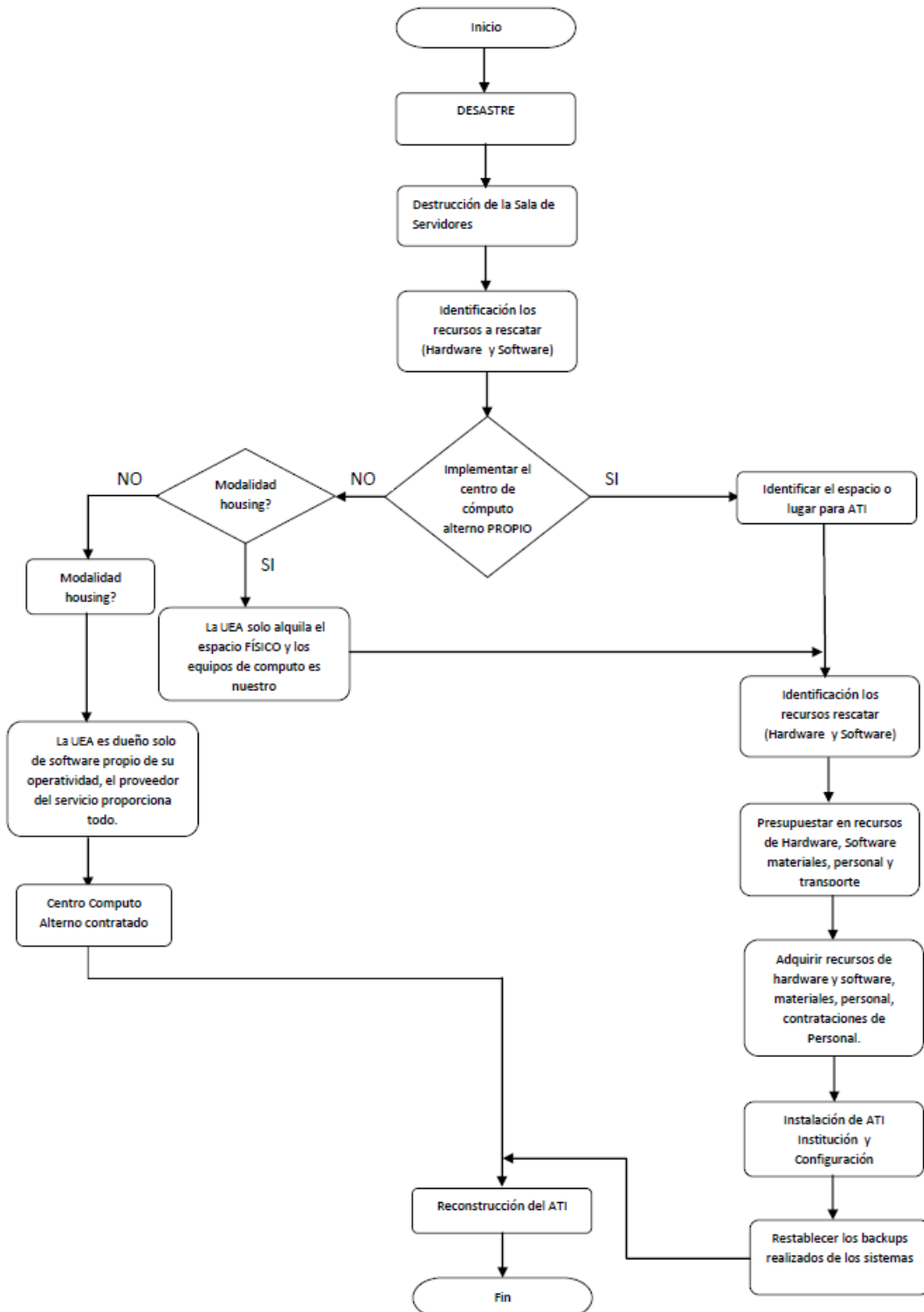
Figura 3.11: Flujograma ante perdida de la conectividad a internet .



Fuente: Elaborado por el Investigador.

V. Indisponibilidad del centro de telecomunicaciones (Destrucción del cuarto de servidores).

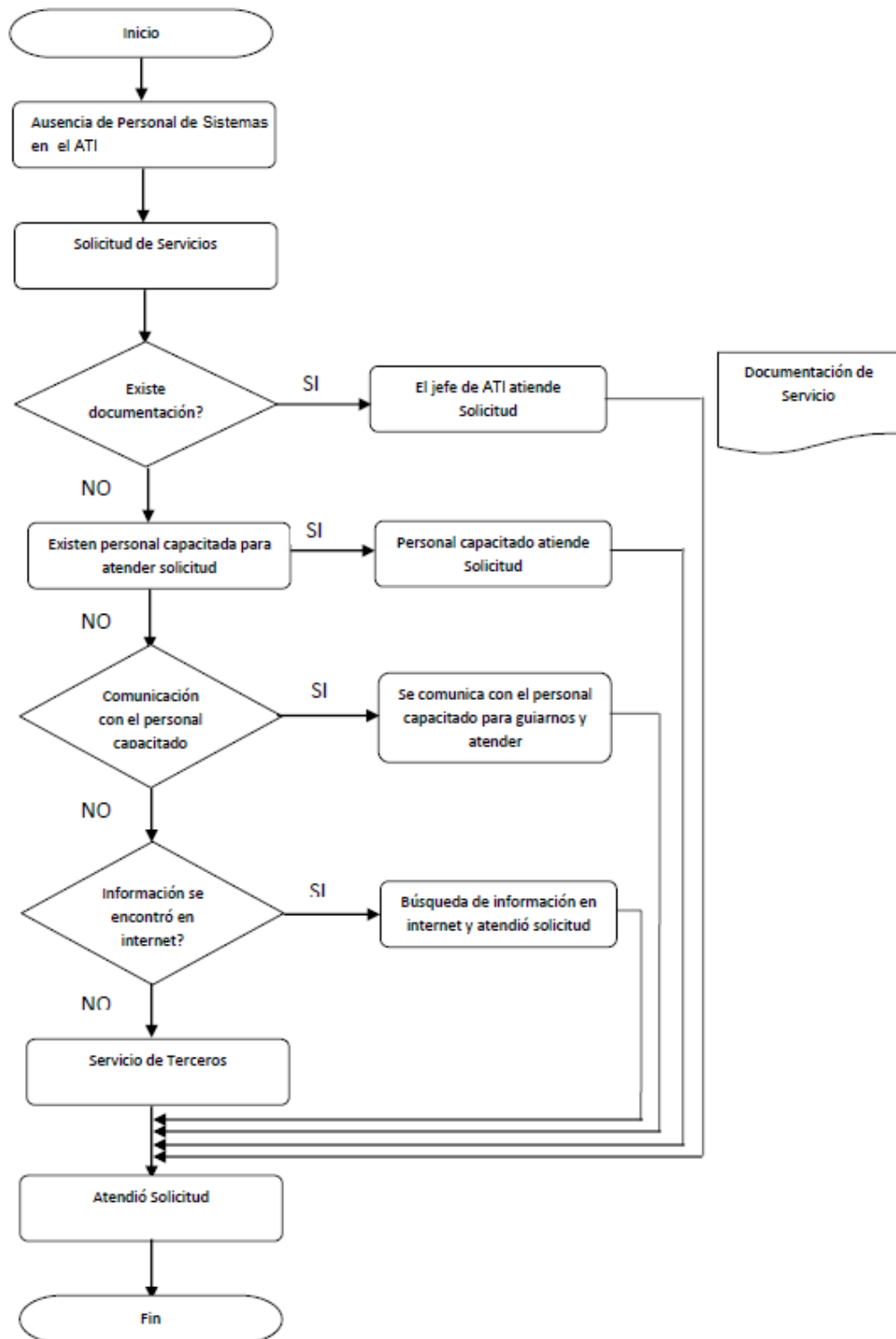
Figura 3.12: Flujograma para la restauración del cuarto de servidores



Fuente: Elaborado por el Investigador.

VI. Ausencia parcial o total del personal en el área de tecnologías de la información.

Figura 3.13: Flujograma ante la ausencia parcial o total del personal en el área de tecnologías de la información.



Fuente: Elaborado por el Investigador.

CAPÍTULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- El diseño del plan de contingencia informático basado en la norma de calidad ISO 27001:2013, permite conocer el nivel de cumplimiento de cada uno de los controles en su Sistema de Gestión de Seguridad de la Información además se analiza cada una de las vulnerabilidades a las que está expuesta la infraestructura tecnológica de la Unidad Educativa Atenas, poniendo las respectivas medidas correctivas a consideración del personal administrativo para minimizar los riesgos.
- Se identificó cada una de las amenazas latentes que pueden generar escenarios de contingencia en los activos y servicios informáticos considerados como críticos para la institución, realizando una evaluación de los riesgos se determinó el nivel de impacto que ocasionarían en caso de que llegaran a materializarse.
- Se define cada una de la acciones a tomar en caso de materializarse una amenaza o escenario de contingencia, esto permite asegurar la operatividad de los procesos y actividades de la institución al mínimo de su capacidad con el fin de minimizar pérdidas económicas y de reputación.
- La creación de grupos y asignación de roles en el departamento de TI en caso de una contingencia, permite una mejor organización al momento de dar solución a un incidente, falla o interrupción de los principales servicios de la institución.
- Toda empresa o institución independientemente de su tamaño debe contar con un plan de contingencia informático bajo la norma ISO 27001:2013, que servirá como guía de recuperación ya que cuenta con medidas oportunas y soluciones eficientes, mismas que ayudarán a estar preparados ante eventos inesperados que conllevarían a una interrupción parcial o total en los servicios informáticos. De esta manera logrando que no se paralicen los procesos y actividades que desarrollan diariamente.

4.2. Recomendaciones

- Los administrativos de la Unidad Educativa Atenas deben analizar la presente propuesta de plan de contingencia informático, y determinar si es factible su implementación ya que el mismo cuenta con medidas humanas, técnicas y flujogramas con el fin de estar preparados y afrontar escenarios de contingencia.
- Lleve a cabo campañas de concientización, dirigidas a todo el personal de la institución para promover la cultura sobre la seguridad de la información y los peligros potenciales a medida que avanza la tecnología.
- Capacitar tanto al personal administrativo y docentes de la institución, para que se encuentren preparados y conozcan cada una de las medidas del plan de contingencia en caso de que se suscite un incidente en el área de TI.
- Mantenga actualizado el plan de contingencias al menos una vez al año, especialmente cuando adquiera equipos nuevos, realice actualizaciones de software, antivirus o dispositivos de red. Para determinar la aparición de nuevos riesgos, el grado de afectación y las respectivas medidas preventivas, de esta manera fortalecer el cumplimiento de los controles de la norma de calidad ISO 27001:2013 y lograr una certificación internacional para la institución.

Bibliografía

- [1] J. Segovia, *Implementación del primer Sistema de Gestión de Seguridad de la Información, en el Ecuador, certificado bajo la norma ISO 27001:2005*. Repositorio ESPOL, 2009.
- [2] K. Méndez, *Plan de contingencia para la unidad de sistemas y tecnología de información del Gobierno Autónomo Descentralizado Antonio Ante en base a la norma ISO/IEC 27001*. Repositorio UTN, 2015.
- [3] H. Ramírez, *Diseño de un Plan de Contingencia del Sistema de Información para la entidad ITRC*. Repositorio UNAD, 2017.
- [4] L. Gina, *Plan de contingencia informático y seguridad de la información*. Pearson Education, 2016.
- [5] *Contingency Planning Guide for Federal Information Systems*. NIST, NIST SP 800-34 rev. 1, 2010.
- [6] *Business Continuity Management Framework*,. Griffith University, 2013.
- [7] D. Chinn, *Objetivo de un plan de contingencia*. Demand Media.
- [8] *Instituto de administración pública*. Junta Andalucía, 2011.
- [9] J. L. C. Laudon, “Sistemas de información gerencial,” pp. 17–18, PEARSON EDUCACION, 2016.
- [10] *Activos dentro de una empresa*. Ministerio de hacienda y administraciones públicas, 2012.
- [11] A. L. S. Villa, “Fundamentos de iso 27001:2013 y su aplicación en las empresas,” in *ISO 27001:2013*, pp. 334–339, Sci.Tech, 2011.
- [12] A. R. E. Stroie, *Security Risk Management - Approaches and Methodology*. No. 1, Citeseer, 2011.
- [13] I. S. Organization, “Directrices para la aplicación de la norma iso 9001:2015,” 2012.

- [14] *Sistema de Gestión de la Seguridad de La Información SGSI*. Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2010.
- [15] *El portal de ISO 27001 en Español, Gestión de Seguridad de la Información*. ISO27000.es, 2012.
- [16] I. S. Organization, *ISO 27001*. ITService, 2013.
- [17] C. Alberts, *OCTAVE-S Implementation Guide Version 1*. 2015.
- [18] A. Siler, “Gestión del riesgo con base en iso27005 adaptando octave-s,” pp. 27–28, 2014.
- [19] J. S. A. Dorofee, *Seguridad de la información en organizaciones en base a OCTAVE catálogo de implementación versión 2*. Software Engineering Institute, 2017.
- [20] J. Landeta, “El método delphi una técnica de previsión del futuro,” 2002.
- [21] J. A. E. García, “Aplicación del método delphi en el diseño de una investigación,” pp. 129–166, EMPIRIA, August 2018.
- [22] D. N. J. Cartaya, *Sinopsis de los modelos SW-CMM y CMMI*. AVANTE, 2007.
- [23] W. Chacón, *SW-CMM y su incidencia en las mejoras de calidad de los sistemas de información*. Repositorio USAC, 2004.
- [24] I. S. Organization, “Tecnología de la información, técnicas de seguridad sistemas de gestión de seguridad de información, ntc-iso/iec 27000:2014,” 2014.
- [25] I. S. Organization, “Tecnología de la información, técnicas de seguridad, gestión del riesgo de seguridad de la información, estándar de seguridad iso/iec 27005,” 2008.
- [26] Z. O. A. Ramírez, “Gestión de riesgos tecnológicos, estándar de seguridad iso/iec 27005:2011,” pp. 56–66, 2011.
- [27] I. S. Organization, “Tecnología de la información, técnicas de seguridad, gestión de incidentes de seguridad de la información, gtc-iso-iec 27035,” 2012.
- [28] I. S. Organization, “Gestión de riesgos de ciberseguridad, estándar internacional iso/iec 27032:2012,” 2012.

- [29] A. R. Z. Ortiz, “Guía para la administración del riesgo,” in *Departamento Administrativo de la Función Pública*, pp. 19–40, DAFP, Colombia, 2011.
- [30] G. P. rural de Izamba, *Plan de Desarrollo y Ordenamiento Territorial de la Parroquia Izamba*. PDyOT cantonales, 2015.

Anexo A

La siguiente encuesta se llevara a cabo en la Unidad Educativa Atenas con el personal Administrativo y los encargados del Departamento de Sistemas, misma que nos permitirá obtener un criterio sobre cuales son los principales activos de información, vulnerabilidades, amenazas a los cuales se encuentran expuestos y determinar si poseen medidas de seguridad para protegerlos.

A.1. Encuesta Técnica



UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS



La presente encuesta esta dirigida a los 2 miembros que actualmente trabajan en el Departamento de Sistemas conjuntamente con los 3 directivos que conforman el personal Administrativo de la Unidad Educativa Atenas (UEA).

1. Posee Ud. conocimientos respecto a la importancia de la seguridad de la información dentro de la institución?.
2. ¿Conoce Ud. Si dentro de la institución, el personal administrativo presta la debida importancia a la seguridad de la información?.
3. ¿Que activos informáticos cree Ud. que son los más importantes para la Unidad Educativa Atenas?.
4. ¿En que escenarios de riesgo cree Ud. que los activos mencionados anteriormente se verían amenazados?.
5. ¿Si los escenarios antes mencionados se materializaran, qué impactos traería para la Unidad Educativa Atenas?.
6. ¿Que requerimientos en cuanto a la seguridad de la información cree Ud. que son los más importantes para cada uno de los activos informáticos?.

7. ¿Para Ud. cual de los requerimientos enlistados en el literal anterior consideraría que es el más importante para cumplir con las actividades diarias de la institución?.

8. ¿La UEA cuenta con políticas, estrategias y procedimientos de seguridad que sean únicos para los activos más importantes con los que cuenta la institución? ¿cuales son?.

9. ¿La institución cuenta con algún plan de contingencia informático que permita trabajar al mínimo de su capacidad, en caso de que ocurra un escenario de riesgo?.

10. ¿Considera Ud. que la UEA necesita un plan de contingencia informático documentado para contrarrestar un escenario de riesgo?.

A.2. Respuestas a encuesta técnica

1. El personal encuestado en su mayoría tienen conocimientos sobre la importancia de la seguridad de la información, pero comentan que no han tomado medidas preventivas como la elaboración de un plan de contingencia informático.

2. Los encuestados en su mayoría comentan, que se da la debida importancia a la seguridad de la información ya que son una institución privada, por lo que poseen políticas de seguridad para garantizar sus activos informáticos.

3. Los encuestados determinaron que los activos más importantes para la UEA son los siguientes:

- Cuarto de Telecomunicaciones.
- Equipos de Networking y Red de Datos.
- Servidores.
- Información.
- Hardware y Software.
- PCs.

4. Entre los encuestados se decidió que los activos informáticos más importantes podrían verse afectados por los siguientes escenarios de riesgo:

- Desastres Naturales / Terremotos.
- Incendio.
- Corte de Suministro Eléctrico.
- Humedad / Fallo de servicios de comunicaciones.
- Desgaste / Daños Físicos.
- Difusión de software dañino (virus).

5. Las consecuencias si los escenarios de riesgo mencionados en el literal anterior llegaran a ocurrir, darían como resultado la pérdida en la disponibilidad de los servicios que proporcionan lo que incide en la paralización parcial o total de las actividades que ejecutan diariamente, además traerían pérdidas económicas para la institución, Todo esto afectaría en la imagen institucional parte de los usuarios.

6. Los encuestados determinaron que existen tres requerimientos que son los más importantes para los activos informáticos de la institución entre los cuales están:

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Otros.

7. Los encuestados mencionaron que el requerimiento de mayor importancia es la disponibilidad ya que la institución cuenta con servicios tanto internos (intranet, telefonía IP, internet, etc) y externos (plataforma virtual de contenidos Iduca, cobros y facturación online de pensiones, etc) y requiere que los datos y servicios se encuentren en óptimas condiciones 24/7.

8. Existe políticas de seguridad específicas para cada uno los activos más relevantes de la institución las mismas que se encuentran documentadas y deben ser cumplidas tanto por el personal administrativo, departamento de sistemas, docentes y alumnos. Entre las políticas de seguridad tenemos:

- Para el uso de la infraestructura física de comunicaciones.

- Respaldo de información.
- Sobre el uso de computadoras en las estaciones de trabajo.
- Sobre el uso de portátiles y celulares.
- Mantenimiento de hardware y software.
- Sobre el uso de correo electrónico.

9. Los encargados del área de Sistemas y personal Administrativo mencionaron que la institución no cuenta con un plan de contingencia informático documentado, que les permita saber que medidas deberían tomar para dar continuidad trabajando al mínimo de su capacidad en los procesos y actividades diarias que realiza la institución en caso de que ocurra un riesgo.

10. Si ya que un plan de contingencia informático sería muy útil y de gran ayuda, ya que permitiría conocer cuales son las medidas que se debería tomar en caso de que se materialice un escenario de riesgo, permitiendo a la institución garantizar la disponibilidad de sus servicios y la continuidad de sus procesos y actividades que realizan diariamente.

CONCLUSIÓN:

- Luego de realizar la encuesta, se evidenció que en su gran mayoría los encuestados conocen la importancia de la seguridad de la información interna en la Unidad Educativa Atenas, mencionaron que cuentan con políticas de seguridad pero adicionalmente necesitan de un plan documentado para mitigar el impacto de los riesgos a los cuales están expuestos (Plan de Contingencia Informático) para de esta manera mejorar y complementar la seguridad ya existente, con el apoyo de todo el personal institucional.
- Mediante la encuesta se logro identificar cuales son los activos más importantes para la Unidad Educativa Atenas, de la misma manera se determinó en que escenarios de riesgo se vería afectada la disponibilidad de los mismos, dando como resultado la interrupción en los procesos y actividades diarias que realiza la institución.