UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

PROYECTO DE INVESTIGACIÓN

"DISEÑO DE UN MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD TÉCNICA DE COTOPAXI".

Proyecto de Titulación presentado previo a la obtención del Título de Ingeniero en Informática y Sistemas Computacionales.

AUTOR:

Tulmo Checa Darío Wladimir

TUTOR:

MSc. Ing. Llano Casa Alex Christian

Latacunga – Ecuador

Julio 2019

Universidad Técnica de Cotopaxi

Ingeniería Informatica Y Sistemas Computacionales

DECLARACIÓN DE AUTORÍA

Yo, **TULMO CHECA DARÍO WLADIMIR** declaro ser autor del presente proyecto de investigación: **"DISEÑO DE UN MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD TÉCNICA DE COTOPAXI"**, siendo el MSc. Ing. Llano Casa Alex Christian tutor del presente trabajo; y eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además, certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

.....

TULMO CHECA DARÍO WLADIMIR

C.I.: 050364202-7

Universidad Técnica de Cotopaxi

Ingeniería Informatica Y Sistemas Computacionales

AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de Tutor del Trabajo de Investigación sobre el título: **"DISEÑO DE UN MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD TÉCNICA DE COTOPAXI"**, de **TULMO CHECA DARIO WLADIMIR**, de la Carrera de Ingeniería en Informática y Sistemas Computacionales, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Consejo Directivo de la Facultad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, Julio, 2019

.....

MSc. Ing. Alex Christian Llano Casa

C.I.: 050258986-4

Universidad Técnica de Cotopaxi

Ingeniería Informatica Y Sistemas Computacionales

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la **FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS**; por cuanto, el postulante: **TULMO CHECA DARÍO WLADIMIR** con el título de Proyecto de titulación: **"DISEÑO DE UN MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD TÉCNICA DE COTOPAXI"** han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, 22 de julio de 2019

Para constancia firman:

Lector 1 (Presidente)
Nombre: Ing. Manuel Villa
CC: 180338695-0

Lector 2
Nombre: Ing. Jorge Rubio
CC: 050323229-2

Lector 3
Nombre: Ing. Félix Murillo
CC: 180299840-9

AGRADECIMIENTO

Agradezco a mis Padres ya que con su esfuerzo y dedicación me ayudaron a culminar mi carrera universitaria y me dieron el apoyo suficiente para seguir adelante.

Asimismo, agradezco infinitamente a mis Hermanos por sus buenos consejos y palabras de aliento que me motivaban a seguir luchando para alcanzar este logro tan anhelado.

De igual forma, agradezco a mi Tutor de Tesis, quien con su experiencia, conocimientos y consejos me oriento en la investigación.

Darío

DEDICATORIA

El presente trabajo de investigación está dedicado a mis Padres, Hermanos, Amigos y Familiares que de alguna u otra manera contribuyeron con un granito de arena para culminar con éxito la meta propuesta.

Darío

ÍNDICE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TÍTULO: "Diseño de un modelo de políticas de seguridad informática para la Universidad Técnica de Cotopaxi"

Autor: Tulmo Checa Darío Wladimir

RESUMEN

Las tecnologías de la información y comunicación (TIC's), han permitido tener un mundo altamente digitalizado y globalizado. Esto hace que individuos y organizaciones se vuelven cada vez más dependientes de la tecnología e Internet por lo tanto los riesgos y amenazas en sus sistemas informáticos crezcan en gran proporción. En la Universidad Técnica de Cotopaxi, existe una amplia infraestructura de TI que brinda acceso a servicios informáticos que deben cumplir lineamientos de buenas prácticas para su disponibilidad. Por tal motivo el presente proyecto de investigación tiene como propósito diseñar un modelo de políticas de seguridad informática para la Universidad, la cual maneja información de vital importancia y necesita contar con mecanismos de seguridad que brinden el suficiente respaldo para proteger la información institucional. El diseñó de un modelo de políticas de seguridad informática permitirá minimizar riesgos y amenazas, que puedan comprometer el correcto funcionamiento de los recursos informáticos como la información, procesos, sistemas y redes. Para fundamentar de mejor manera el trabajo de investigación se utilizó diferentes lineamientos de seguridad informática establecida y sugerida en la Norma ISO/IEC 27001 la cual busca la confidencialidad, integridad y disponibilidad de la información.

Palabras Claves:

Seguridad, Información, Integridad, Confiabilidad, Disponibilidad.

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

Theme: "Design of a computer security policy model for the Technical University of Cotopaxi"

Author: Tulmo Checa Darío Wladimir

ABSTRACT

Information and communication technologies (ICTs) have allowed for a highly digitized and globalized world. This makes individuals and organizations become increasingly dependent on technology and the Internet, therefore the risks and threats in their computer systems grow in large proportion. At the Technical University of Cotopaxi, there is a broad IT infrastructure that provides access to computer services that must comply with good practice guidelines for their availability. For this reason, the present research project aims to design a model of computer security policies for the University, which handles information of vital importance and needs to have security mechanisms that provide sufficient support to protect institutional information. The design of a computer security policy model will minimize risks and threats that could compromise the correct functioning of computing resources such as information, processes, systems and networks. To better support the research work, different computer security guidelines established and suggested in the ISO / IEC 27001 Standard were used, which seeks the confidentiality, integrity and availability of the information.

Keywords:

Security, Information, Integrity, Reliability, Availability.

Universidad Técnica de Cotopaxi

CENTRO DE IDIOMAS

AVAL DE TRADUCCIÓN

En calidad de Docente del Idioma Inglés del Centro de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal **CERTIFICO** que: La traducción del resumen del proyecto de investigación al Idioma Inglés presentado por el señor Egresado de la Carrera de **INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES** de la **FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS TULMO CHECA DARÍO WLADIMIR**, cuyo título versa **"DISEÑO DE UN MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD TÉCNICA DE COTOPAXI"**, lo realizó bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo al peticionario hacer uso del presente certificado de la manera ética que estimare conveniente.

Latacunga, Julio del 2019

Atentamente,

.....

Mg. Patricia Marcela Chacón Porras
DOCENTE CENTRO DE IDIOMAS
C.C. 050221119-6

CENTRO DE IDIOMAS

xiii

1. INFORMACIÓN GENERAL:

1.1. Título del proyecto:

Diseño de un modelo de Políticas de Seguridad Informática para la Universidad Técnica de Cotopaxi.

1.2. Fecha de inicio:

Abril de 2019.

1.3. Fecha de finalización:

Agosto de 2019.

1.4. Lugar de ejecución:

Universidad Técnica de Cotopaxi.

1.5. Facultad que auspicia:

Facultad de Ciencias de la Ingeniería y Aplicadas.

1.6. Carrera que auspicia:

Ingeniería en Sistemas Informáticos y Computacionales.

1.7. Proyecto de investigación vinculación:

Diseño de un modelo de políticas de seguridad informática dirigido a la Universidad Técnica de Cotopaxi para prevenir amenazas y riesgos que puedan comprometer la información.

1.8. Equipo de trabajo:

Datos personales del coordinador de proyecto de investigación:

Nombres: Alex Christian

Apellidos: Llano Casa

C.I.: 050258986-4

Teléfonos: 0999969302

E-mail: alex.llano9864@utc.edu.ec

Estudios: Universidad Técnica de Cotopaxi.

Títulos obtenidos:

Ingeniero en Informática y Sistemas Computacionales.

Master Universitario en Ingeniería de Software y Sistemas Informáticos.

_____

Firma

Datos Personales del Autor:

Nombres: Darío Wladimir

Apellidos: Tulmo Checa

Fecha de nacimiento: 23 de agosto

C.I.: 050364202-7

Teléfono: 0998364396

Correo electrónico: dario.tulmo7@utc.edu.ec

Estudios: Universidad Técnica de Cotopaxi.

_____

Firma

1.9. Área de conocimiento:

Ingeniería en Sistemas Informáticos y Computacionales.

1.10. Línea de investigación:

Tecnologías de la Información y Comunicación (TIC's).

1.10.1. Sub línea de investigación

Seguridad informática.

2. RESUMEN DEL PROYECTO

Las tecnologías de la información y comunicación (TIC's), han permitido tener un mundo altamente digitalizado y globalizado. Esto hace que individuos y organizaciones se vuelven cada vez más dependientes de la tecnología e Internet por lo tanto los riesgos y amenazas en sus sistemas informáticos crezcan en un 12%. En la Universidad Técnica de Cotopaxi, existe una amplia infraestructura de TI que brinda acceso a servicios informáticos que deben cumplir lineamientos de buenas prácticas para su disponibilidad. Por tal motivo el presente proyecto de investigación tiene como propósito diseñar un modelo de políticas de seguridad informática para la Universidad, la cual maneja información de vital importancia y necesita contar con mecanismos de seguridad que brinden el suficiente respaldo para proteger la información institucional. El diseñó de un modelo de políticas de seguridad informática basadas en la Norma ISO/IEC 27001 la cual busca la confidencialidad, integridad y disponibilidad de la información, permitirá minimizar riesgos y amenazas, que puedan comprometer el correcto funcionamiento de los recursos informáticos de la institución como la información, procesos, sistemas y redes.

3. JUSTIFICACIÓN DEL PROYECTO

En la actualidad el mundo se encuentra en constante evolución ya que gracias a las tecnologías de la información y comunicación (TIC's), han permitido tener un mundo altamente digitalizado y globalizado en donde con un par de clics es posible conectarse a cualquier parte del planeta. Esto hace que individuos y organizaciones se vuelven cada vez más dependientes de la tecnología e Internet por lo tanto los riesgos y amenazas en sus sistemas informáticos crezcan exponencialmente.

En la Universidad Técnica de Cotopaxi, se realizó una investigación para conocer si existen riesgos y amenazas que pongan en peligro la protección de la información ya que al ser esta el activo más importante necesita ser resguardado de ataques que puedan poner en peligro los sistemas y equipos de cómputo. Las políticas son esenciales para manejar los asuntos de seguridad y forman parte efectiva de medidas de protección tales como: identificación y control de acceso, resguardo de datos, administración de activos, etc.

Por tal motivo el siguiente proyecto diseñará un modelo de políticas de seguridad informática que sirvan como normativas para garantizar la confidencialidad, integridad y disponibilidad de la información. Estas políticas estarán disponibles para ser aplicadas a la comunidad

Universitaria incluyendo estudiantes, docentes, empleados y cualquier otro ente autorizado por la institución que haga uso de los recursos informáticos.

4. BENEFICIARIOS DEL PROYECTO

4.1. Beneficiarios directos:

Los beneficiarios directos del presente proyecto son la Dirección de TIC's de la Universidad Técnica de Cotopaxi.

4.2. Beneficiarios indirectos:

Grupo de investigación de la Universidad Técnica de Cotopaxi, Departamento de TIC's.

5. EL PROBLEMA DE INVESTIGACIÓN

El mundo del ciber delito no descansa. Según la web Breach Level Index, cada día se roban en el mundo más de seis millones de perfiles con información personal de usuarios y ciudadanos. Eso supone casi 4.250 por minuto y 71 por segundo. En las pasadas Navidades, mientras muchos preparaban suculentas cenas y regalos para la familia, las brechas de seguridad siguieron siendo noticia. La más relevante, no por el número de afectados, pero sí por su significación, se produjo en Alemania. (CABRERA ,2019)

El Ecuador también está incluido en las estadísticas sobre ciber delitos, a partir del año 2010 se presenta un importante crecimiento en el porcentaje de casos reportados por este tipo de delitos, en el presente año 2019, el país a ha registrado más de 40 millones de ciberataques a portales web de instituciones públicas, estos ataques provienen principalmente de Estados Unidos, Brasil, Holanda, Alemania, Rumanía, Francia, Austria, Reino Unido, y también desde aquí, de nuestro territorio. Las principales instituciones afectadas son la cancillería, el banco central, la presidencia, el servicio de rentas internas (SRI) y algunos ministerios y universidades. (EL COMERCIO, 2019)

Constantemente surgen nuevos desafíos y amenazas informáticas que pueden acabar afectando a la institución. Por tal razón se diseñara un modelo de políticas de seguridad informática para prevenir riesgos y amenazas que pongan en peligro la disponibilidad, integridad y confidencialidad de la información. La seguridad informática no es simplemente una opción, sino que cada vez más se va convirtiendo en una obligación de las instituciones que de verdad quieren proteger sus datos y la de sus usuarios. Es importante señalar que las

políticas por sí solas no constituyen una garantía para la seguridad de la institución, ellas deben responder a intereses y necesidades de la institución.

6. OBJETIVOS

6.1. Objetivo general

Diseñar un modelo de Políticas de Seguridad Informática para la Universidad Técnica de Cotopaxi basada en la norma ISO/IEC 27001, la cual busca crear una cultura organizacional de buenas prácticas en el aspecto computacional y fortalezca la protección física y lógica de los activos informáticos de la institución.

6.2. Objetivos específicos

- ✓ Recopilar información de la Dirección de TIC's sobre la seguridad informática de la Universidad Técnica de Cotopaxi, usando herramientas de campo.
- ✓ Analizar la información obtenida para identificar riesgos internos y externos que puedan afectar al correcto funcionamiento de los equipos y sistemas computacionales de la institución.
- ✓ Proveer lineamientos de seguridad informática para garantizar la confidencialidad, disponibilidad e integridad de la información.

7. ACTIVIDADES Y SISTEMAS DE TAREAS EN RELACIÓN A LOS OBJETIVOS

Tabla 1. Sistema de tareas en relación a los objetivos planteados.

Objetivo	Actividad (Tareas)	Resultado de la actividad	Medios de Verificación
Recopilar información de la dirección de TIC's sobre la seguridad informática de la Universidad Técnica de Cotopaxi, mediante visitas de campo y entrevistas.	**Tarea 1:** Realizar entrevistas al director del Departamento de TIC's. **Tarea 2:** Observar la información recopilada para su posterior análisis. **Tarea 3:** Conocer que tan segura es la seguridad informática de la institución.	Fundamentación teórica del proyecto de investigación.	♦ Entrevistas ♦ Investigación Documental ♦ Investigación de campo.
Analizar la información obtenida para identificar posibles riesgos y amenazas que puedan afectar al correcto funcionamiento de los equipos y sistemas computacionales de la institución.	**Tarea 1:**.Observar posibles riesgos existentes en la institución. **Tarea 2:** Conocer cómo se lleva a cabo la seguridad informática en la institución. **Tarea 3:** Mediante la información obtenida establecer lineamientos para el diseño de las políticas.	Proyecto de investigación.	♦ Investigación de campo. ♦ Investigación Documental
Proveer lineamientos de seguridad para garantizar la confidencialidad, disponibilidad e integridad de la información.	**Tarea 1:** Desarrollo del Diseño de las políticas de seguridad informática. **Tarea 2:** Utilizar la norma ISO/IEC 27001 para el diseño de las políticas.	Diseño de las Políticas de Seguridad Informática.	♦ Investigación Documental ♦ Diseño de un Modelo de Políticas de Seguridad Informática.

Fuente: El investigador

8. FUNDAMENTACIÓN CIENTÍFICO TÉCNICA

8.1. Antecedentes

8.1.1. Seguridad de la información

Se define a la seguridad de la información como algo que: dentro de la empresa, la información está protegida contra su divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad). (ISACA, 2012),

Se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad. (Aguilera, 2011)

La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los usuarios, los protocolos que se encuentran implementados, pero siempre la tarea primordial es minimizar los riesgos para obtener mejor y mayor seguridad.

Lo que debe contemplar la seguridad se puede clasificar en tres partes como son los siguientes:

- Los usuarios
- La información, y
- La infraestructura

Los usuarios son imposibles de controlar, un usuario puede en algún momento cometer un error y olvidar algo o tener un accidente y este suceso puede echar a perder el trabajo de mucho tiempo, o en muchos casos el sistema y la información.

La información se considera como el activo más importante de la seguridad informática ya que es lo que se desea proteger y poner a salvo.

Por último, está **la infraestructura** esté puede ser uno de los medios más controlados, pero no por eso deja de estar en riesgo. Se deben de considerar problemas complejos, como los de un

acceso no permitido, robo de identidad, hasta los daños más comunes, por ejemplo, robo de equipos, inundaciones, incendios o cualquier otro desastre natural.

También se afirma que la seguridad informática puede definirse como el conjunto de métodos y de varias herramientas para proteger el principal activo de una organización como lo es la información o los sistemas ante una eventual amenaza que se pueda suscitar. (Aguirre, 2006)

8.1.2. Mecanismos preventivos en seguridad informática

La definición de los mecanismos preventivos, consiste en una serie de revisiones periódicas, algunos cambios o mejoras de diferentes aspectos que pueden ser de hardware, software o de cualquier elemento involucrado en los sistemas y procesos, por eso es que las revisiones dependen de los procesos de la empresa y cada una tiene sus propios procesos. (Romero et al., 2018)

Entre los elementos que se pueden aplicar en los mecanismos preventivos se puede mencionar a:

- ✓ **El respaldo de información:** se refiere al resguardo que se realiza de ciertos datos. El concepto suele emplearse con relación a los datos digitales (que están alojados en el disco duro de una computadora u ordenador.
- ✓ **Horario de respaldo:** Es a qué hora se puede hacer el respaldo, es común seleccionar las horas de menos tráfico.
- ✓ **Control de los medios:** El tener acceso a respaldos es algo de alto riesgo, se puede robar la información, manipular, perder, así que, el respaldo es una solución, pero también es otro problema que se debe resolver.
- ✓ **La comprensión de la información:** No toda la información se puede comprimir, pero existe alguna que, sí lo necesita, así que se deben hacer las valoraciones respectivas

8.1.3. Pilares de la seguridad

Los pilares de la seguridad de la información se fundamentan en la necesidad que se tienen de obtener la información, de su importancia, integridad y disponibilidad de la información para sacarle el máximo rendimiento con el mínimo riesgo. (Romero et al., 2018)

- ✓ **Confidencialidad:** consiste en garantizar que la información solamente va a estar disponible para aquellas personas autorizadas, es decir, que personas ajenas no podrán acceder a la información e interpretación.
- ✓ **Disponibilidad:** consiste en garantizar que tanto el sistema como los datos van a estar disponibles para el usuario en todo momento.
- ✓ **Integridad:** consiste en asegurarse de que la información no se pierde ni se ve comprometida voluntaria e involuntariamente.

8.1.4. Evaluación de riesgos, amenazas y vulnerabilidades

Cuando se plantea mejorar la seguridad de una empresa se debe tener en cuenta varios factores que se muestra a continuación:

- ✓ **Recursos**
- ✓ **Amenazas**
- ✓ **Vulnerabilidades**
- ✓ **Riesgos**

Se entiende a los **recursos** como los bienes tangibles e intangibles con los que se cuenta para realizar las tareas, la información de que se dispone es un bien intangible, ya sean las bases de datos de clientes, proveedores, los manuales de producción, las investigaciones y las patentes. Por otro lado, se tiene a los bienes tangibles, qué son los recursos físicos de que se dispone en la empresa, servidores, equipos de red, computadoras, teléfonos inteligentes, vehículos, bienes inmuebles, etc. (Romero et al., 2018)

El **riesgo** es la probabilidad de que algo negativo suceda dañando los recursos tangibles o intangibles y por tanto impidiendo desarrollar la labor profesional.

Las **amenazas** son esos sucesos que pueden dañar los procedimientos o recursos, las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

Las **vulnerabilidades** son una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

El principal trabajo de un responsable de la seguridad es la evaluación de los riesgos identificando las vulnerabilidades, amenazas y en base a esta información evaluar los riesgos a los que están sujetos las actividades y recursos. (Romero et al., 2018)

8.1.5. Estándares y buenas prácticas

Un estándar es un documento establecido por consenso, aprobado por un cuerpo reconocido y que ofrece reglas, guías y/o características para que pueda usarse repetidamente, los estándares proveen las guías específicas de las mejores prácticas a los directores de proyecto programas y portafolios, así como a sus organizaciones, ahorrando la creación de soluciones constantes para un problema determinado, El organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica, es la Organización Internacional para la Estandarización- International Organization for Standardization (ISO). Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional.

8.1.6. Mecanismos de seguridad

Los mecanismos de seguridad se dividen en tres grupos:

- ✓ **Prevención:** Evitan desviaciones respecto a la política de seguridad.
- ✓ **Detección:** Detectar las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema.
- ✓ **Recuperación:** Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento.

Dentro del grupo de mecanismos de prevención tenemos:

Mecanismos de identificación e autentificación. Permiten identificar de forma única ‘entidades’ del sistema. El proceso siguiente es la autentificación, es decir, comprobar que la entidad es quien dice ser. Pasados estos dos filtros, la entidad puede acceder a un objeto del sistema. En concreto los sistemas de identificación y autentificación de los usuarios son los mecanismos más utilizados. (Pareja, 2014)

Mecanismos de control de acceso. Los objetos del sistema deben estar protegidos mediante mecanismos de control de acceso que establecen los tipos de acceso al objeto por parte de cualquier entidad del sistema. (Pareja, 2014)

Mecanismos de separación. Si el sistema dispone de diferentes niveles de seguridad se deben implementar mecanismos que permitan separar los objetos dentro de cada nivel. Los mecanismos de separación, en función de cómo separan los objetos, se dividen en los grupos siguientes: separación física, temporal, lógica, criptográfica y fragmentación. (Pareja, 2014)

Mecanismos de seguridad en las comunicaciones. La protección de la información (integridad y privacidad) cuando viaja por la red es especialmente importante. (Pareja, 2014)

8.1.7. Normas Orientadas a la Seguridad de Información.

- ✓ **Norma ISO 27000:** Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.
- ✓ **Norma ISO/IEC 27000:** Ofrece información general de las normas que componen la serie ISO 27000 aclarando sus alcances y dando la visión de conjunto de estas normas; cuenta con el vocabulario técnico usado en las normas, igualmente contiene una introducción al Sistema Integrado de Seguridad de la Información (SGSI).
- ✓ **Norma ISO/IEC 27001:** Se considera la norma principal de la serie ISO 27000, donde se plasman los requisitos normativos para establecer el SGSI y su subsecuente operación y mejora; el SGSI girará alrededor de los riesgos y su tratamiento.
- ✓ **Norma ISO/IEC 27002:** Establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa.

8.1.8. Norma ISO/IEC 27001

8.1.8.1. ¿Qué es la ISO 27001?

Sistemas de Gestión de la Seguridad de la Información.

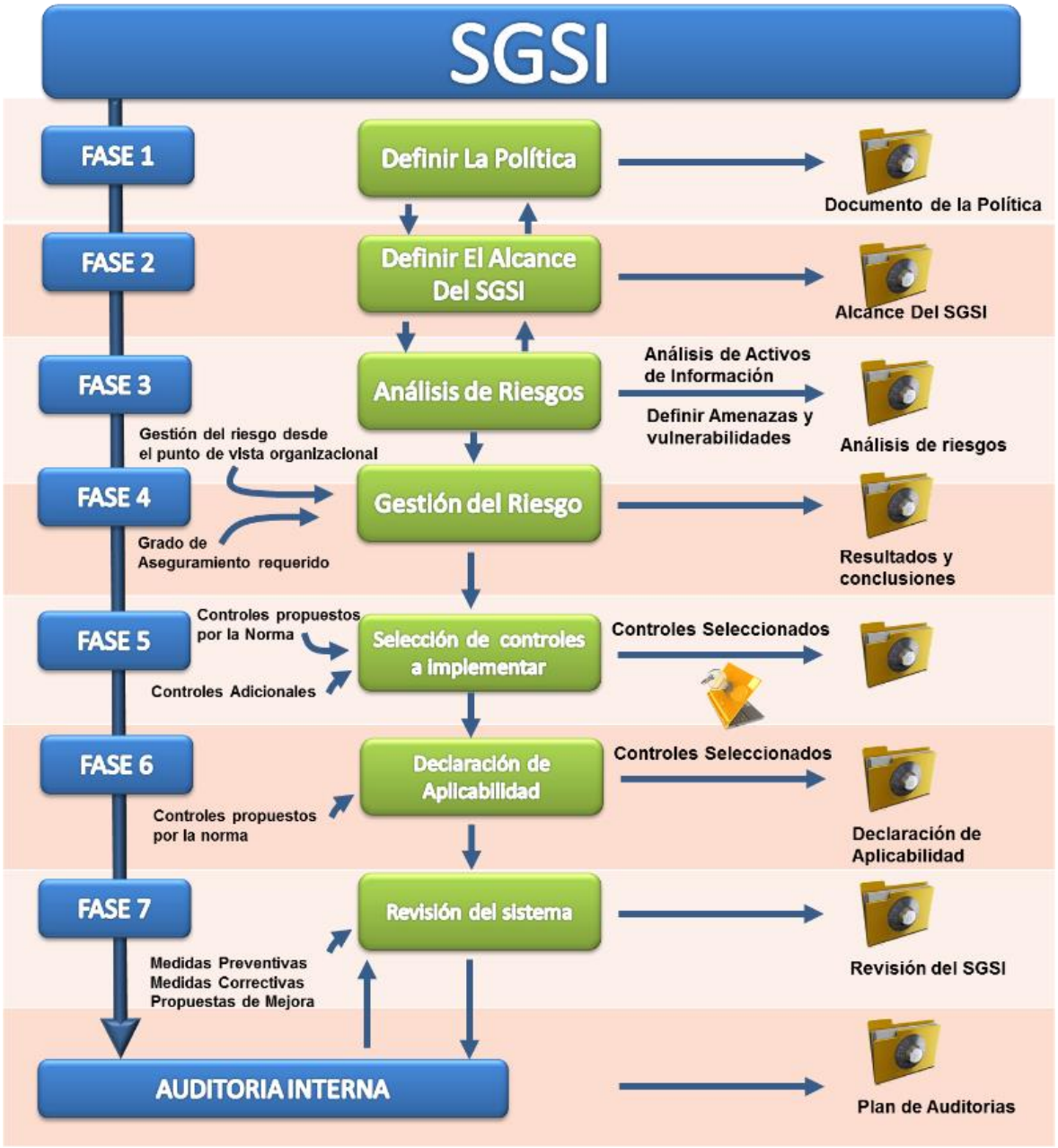
ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El

estándar ISO 27001:2013 para los Sistemas de Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. (ISOTools, 2019)

8.1.8.2. FASES PARA LA IMPLEMENTACIÓN DE UN SGSI

El Sistema de Gestión de la Seguridad de la Información que propone la Norma ISO 27001 se puede resumir en las siguientes fases que se detallan en la figura:

Figura 1. Sistema de Gestión de La Seguridad de la Información.



Fuente: NORMAS ISO

8.1.9. Ciclo de mejora continúa

El ciclo de mejora continua, reconocido como ciclo PDCA (del inglés plan-docheck-act) o PHVA (planificar-hacer-verificar-actuar) o Ciclo de Deming, es un sistema por medio del cual es posible identificar y gestionar los procesos organizacionales y así lograr estandarizar un sistema de mejora continua, el cual está conformado por las siguientes fases:

a. (Planear) - Establecer el qué y cómo hacer para satisfacer la política y objetivos de seguridad de la Información.

b. (Hacer) – Poner en práctica lo planeado.

c. (Verificar) - Verificar si se ha hecho lo planificado y si lo que se ha hecho es eficiente.

d. (Actuar) – Establecer las acciones de cómo y que mejorar.

8.1.10. Políticas, Planes y Procedimientos de Seguridad

Para que un sistema de seguridad informática logre alcanzar y desarrollar todos los objetivos y funcione, es necesario que la organización defina, diseñe e implemente una serie de políticas, planes y procedimiento en materia de seguridad de la información. (Gómez, 2014)

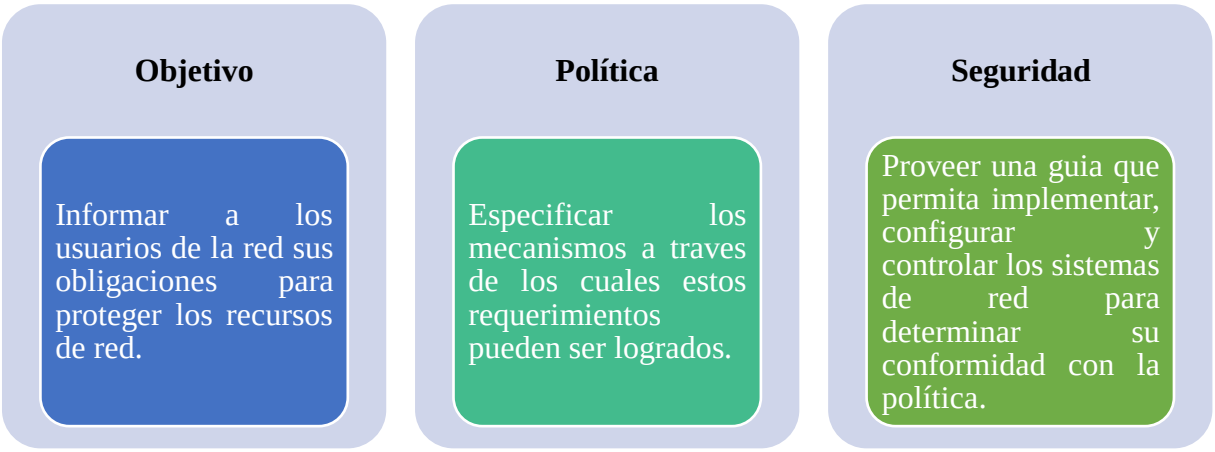
Según (Gómez, 2014), define los siguientes conceptos como:

- ✓ **Política de seguridad:** declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.
- ✓ **Plan de seguridad:** conjunto de decisiones que definen cursos de acción futuros, así como los medios que se van a utilizar para conseguirlos.
- ✓ **Procedimiento de seguridad:** definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los procedimientos de seguridad permiten aplicar e implantar las políticas de seguridad que han sido aprobadas por la organización.

8.1.11. Objetivo principal de las políticas de seguridad

La política de seguridad es un documento formal de reglas destinada a los usuarios que acceden a los recursos de la red de una organización o empresa.

Figura 2. Objetivo principal de las políticas de seguridad.



Fuente: El investigador

8.1.12. Acceso a Recursos Computacionales

8.1.12.1. Usuarios de Red (Active Directory)

El servicio de directorio es uno de los componentes más importantes de un sistema de información, cualquiera que sea su tamaño. Ofrece servicios centrales capaces de unir los múltiples elementos que componen el sistema de información. (Apréa 2010)

Active Directory es una estructura jerárquica de directorios que almacena en una base de datos la información del sistema sobre redes y dominios, se utiliza principalmente para obtener información en línea, está diseñado especialmente para entornos de red distribuidos (topología de red caracterizada por la ausencia de un centro individual o colectivo), utiliza protocolos como LDAP (Lightweight Directory Access Protocol, o Protocolo Ligero Simplificado de Acceso a Directorios), DNS (Domain Name System o sistema de nombres de dominio), DHCP (Dynamic Host Configuration Protocol o protocolo de configuración dinámica de host), manejando un gran número de operaciones de lectura y búsqueda.

El directorio Active Directory debe ofrecer los medios para almacenar toda la información que caracteriza el conjunto de objetos que puedan existir en la red de la empresa así como disponer de los servicios capaces de dar esta información globalmente utilizada por los usuarios, y esto, en función de sus derechos y privilegios. (Apréa, 2010)

Usuario, en informática (user) es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema separado por privilegios y permisos a los que tiene acceso, estos pueden ser personales o grupales, interactuando o ejecutando con el ordenador acciones unipersonales o en una red.

Una Red es un sistema de comunicación inalámbrico flexible, integrada por computadoras o conjunto de equipos informáticos interactuando por un software que los conecta entre sí.

8.1.12.2. Equipos de Cómputo

Un sistema informático está constituido por un conjunto de elementos físicos (hardware, dispositivos, periféricos y conexiones), lógicos (sistemas operativos, aplicaciones, protocolos…). (López, 2011)

Un equipo de cómputo tiene relación intrínseca con la palabra hardware, que en informática se refiere a las partes físicas tangibles de un sistema informático, a sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, cableado, así como los gabinetes o cajas, los periféricos de todo tipo, y cualquier otro elemento físico involucrado, componen el hardware o soporte físico.

8.1.12.3.ERP (ENTERPRISE RESOURCE PLANNING)

Un sistema ERP es una aplicación informática que permite gestionar todos los procesos de negocio de una compañía en forma integrada. Sus siglas provienen del término en inglés ENTERPRISE RESOURCE PLANNING. (Chiesa 2004)

Los Sistemas de Planificación de Recursos Empresariales o ERP son una gran inversión para las empresas, enfrentando los problemas en sistemas de gestión de información que automatizan muchas de las prácticas de un negocio asociadas con los aspectos operativos o productivos de una empresa.

Este tipo de sistemas están compuestos de muchos módulos como:

- ✓ Recursos Humanos
- ✓ Ventas
- ✓ Contabilidad y Finanzas
- ✓ Compras
- ✓ Producción

El ERP provee información integrada de todos los procesos del negocio, y adapta las necesidades específicas de cada organización, como los sistemas de información gerenciales

que manejan los negocios asociados con las operaciones de producción y los aspectos de distribución de una compañía.

8.1.13. Correo electrónico y acceso a internet

8.1.13.1. Correo Electrónico

Una política corporativa de correo electrónico es un documento de gestión que describe formalmente cómo los empleados pueden utilizar herramientas de comunicación electrónica. La política establece directrices para lo que se considera uso aceptable y uso inaceptable.

Una compañía debe tener una política corporativa de correo electrónico instalada para advertir y guiar a los empleados contra amenazas de correo electrónico, tales como ataques de phishing. La política puede poner límites a los tipos de archivos que los empleados son capaces de abrir, descargar o intercambiar con otros. La política debe describir qué hacer si un empleado recibe un correo electrónico ofensivo, para protegerse contra la responsabilidad legal. (Verma, 2018)

8.1.13.2. Acceso a Internet

Internet es una herramienta muy poderosa que contiene una enorme cantidad de información disponible a todo el público. Además de que Internet ha fomentado el desarrollo de una gran variedad de nuevas actividades y servicios que están destinados a facilitar nuevos tipos de interacciones sociales que antes no eran posibles.

8.1.14. Resguardo de la Información

La Seguridad de la Información propende mantener y garantizar la confidencialidad, integridad y disponibilidad de la información, para ello se apoya en políticas, controles y medidas que abarcan lo preventivo y lo reactivo; cabe recalcar que el concepto de información se aplica a nivel global y no se encuentra restringido al tipo de información o medio que lo contenga. (Chaves, 2017)

8.1.15. Bases De Datos

Existen diferentes maneras de ordenar y organizar la información para que este sea accesible para todos. Hay que elegir la estructura que mejor se adapte a nuestras necesidades.

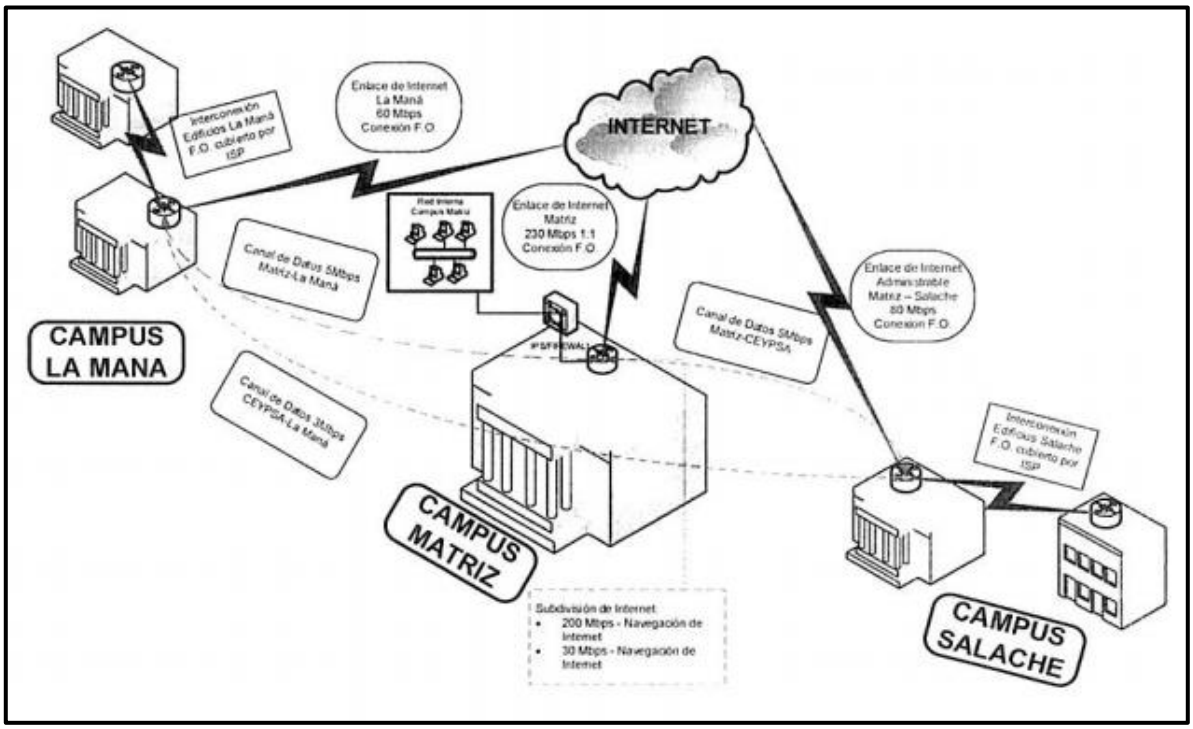
Las bases de datos en red derivan de las jerarquías, pero mejoran la gestión de datos de datos transaccionales están diseñadas para el envío y recepción de datos a grandes velocidades y de forma continua. También se menciona base de datos orientadas a objetos en una estructura lógica. (ANER, 2018)

Sabiendo que la base de datos es la parte principal de la empresa u organización se debe considerar de gran importancia la seguridad, almacenamiento y respaldos de información.

Actualmente la Universidad cuenta con una interconexión de red entre los tres Campus como se muestra en el gráfico siguiente:

Diagrama de interconexión Universidad Técnica de Cotopaxi.

Figura 3. Diagrama de interconexión Universidad Técnica de Cotopaxi.



Fuente: Universidad Técnica de Cotopaxi.

9. HIPÓTESIS

¿El diseño de un modelo de políticas de seguridad informática permitirá a la institución proteger la información de forma segura?

10. METODOLOGÍAS

10.1. Tipos de Investigación

10.1.1. Investigación de Campo

Será utilizada en el proyecto, ya que los datos serán extraídos de forma directa de la realidad y por el propio investigador, a través del uso de instrumentos para recolectar la información. Por otro lado, esta investigación será de apoyó en el empleo de fuentes documentales a partir de las cuales se construirá los fundamentos teóricos que dan sustento al proyecto.

10.1.2. Investigación Bibliográfica

Es aquella que utiliza textos u otro tipo de material intelectual impreso o grabado como fuentes primarias para obtener sus datos. En este sentido, la información que será utilizada derivara de fuentes primarias a través de la aplicación de entrevistas y de fuentes secundarias por medio de la revisión de datos contenidos en libros, trabajos de grado, y todo aquel material bibliográfico que se encuentre relacionado con el objeto de este estudio.

10.2. Técnicas de Investigación

Las técnicas a utilizar son la entrevista y observación, las cuales permitirán recolectar los datos necesarios para su análisis y resultados, permitiendo llegar a una conclusión de la investigación a desarrollar.

10.2.1. Entrevista

Para el presente proyecto se ha tomado la decisión de trabajar con la entrevista estructurada, ya que esta permitirá conocer detalles sobre la seguridad informática que posee la institución, sus amenazas y riesgos.

10.2.2. Observación

La observación ayudara a verificar paso a paso como se lleva a cabo la seguridad de la información de la Universidad Técnica De Cotopaxi y a su vez recolectar los datos necesarios para su posterior análisis y resolución de estos.

10.3. Norma ISO /IEC 27001

Para el desarrollo del diseño de las políticas de seguridad informática se tomó como referencia la norma ISO 27001 la cual se basa en proteger la confidencialidad, integridad y disponibilidad de la información de la institución. Esta norma permite investigar cuáles son los potenciales problemas que podrían afectar la información (evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (mitigación o tratamiento del riesgo).

10.4. DISEÑO DEL MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Una vez realizada la investigación, análisis y levantamiento de información, se procede a diseñar las siguientes Políticas de Seguridad Informática:

- ✓ **PO-1A** Política de control de acceso a recursos computacionales.
- ✓ **PO-1B** Política de Active Directory.
- ✓ **PO-1C** Política de administración de activos de tecnología de información.
- ✓ **PO-1D** Política de resguardo de la información.
- ✓ **PO-1E** Política de seguridad a componentes informáticos.
- ✓ **PO-1F** Política de uso adecuado de internet.
- ✓ **PO-1G** Política de uso adecuado de laboratorios de computación.

Objetivo de las Políticas de Seguridad Informática.

Definir lineamientos de seguridad para garantizar la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información manejada por las áreas o departamentos de la Universidad Técnica de Cotopaxi.

1. Alcance.

Aplica a todos los miembros de la comunidad de la Universidad Técnica de Cotopaxi, incluyendo empleados, contratistas, trabajadores temporales, consultores, socios estratégicos y cualquier otro ente autorizado por la institución para hacer uso de sus recursos informáticos.

2. Documentos de referencia.

RE-01A. Aceptación y cumplimiento de las políticas.

RE-02A. Creación de usuario de red.

RE-03A. Acta de entrega y recepción de equipos.

3. Descripción de la Política.

La forma principal de control y método de seguridad que se utiliza para el acceso a los recursos computacionales son las credenciales de acceso (claves). Para el efecto, ningún usuario recibirá su identificativo de acceso a la red y uso de recursos tecnológicos hasta que acepte y firme el documento correspondiente al RE-01A Aceptación y cumplimiento de políticas.

Los recursos informáticos y la información pueden ser usados solo para propósitos autorizados y en cumplimiento con las metas y objetivos de la institución.

A continuación se consideran las siguientes recomendaciones a ser cumplidas por el usuario:

- Uso consciente, entender que el usuario y la clave que se asigne por parte del área de Tecnología a cualquier miembro de la comunidad de institución, son para uso personal y exclusivo.
- Responsabilidad, entender que cualquier actividad que se registre en los sistemas con la clave asignada, son de total responsabilidad del usuario.
- Seguimiento, entender que la institución puede realizar auditorías periódicas para validar el correcto manejo de la clave y usuario asignado. Adicionalmente la universidad puede

revisar en las Bases de Datos tics correspondientes, cualquier información que se haya generado con esta clave.

- Compromiso, acuerdo comunicar al superior inmediato cualquier comportamiento o situación sospechosa que pueda poner en peligro la información o los activos donde reposa la información.
- Confidencialidad, por ningún motivo el usuario puede divulgar su usuario y clave a ninguna persona; ya que la clave es intransferible.
- Pro actividad, el usuario tiene la obligación y deber de entender, apoyar y cumplir las normas de seguridad dictadas en esta política.
- Buen uso, el usuario y clave asignados al empleado, permiten el ingreso a los sistemas de información con el único y exclusivo propósito de cumplir con las tareas y trabajo asignados.
- Seguridad, el empleado debe mantener y recordar el usuario y clave, evitando escribirla en cualquier medio para que esta, pueda ser encontrada.

Cualquier persona que de incumplimiento a las disposiciones señaladas en esta política, puede ser sujeta a una acción disciplinaria según el Reglamento Interno de la institución.

La universidad por su parte implementará los controles necesarios para mantener un adecuado manejo de los usuarios y claves asignados a los miembros de la comunidad universitaria. Sin embargo, el usuario no deberá intentar descifrar las claves, sistemas, algoritmos de cifrado y cualquier otro elemento de seguridad que la institución implemente.

A continuación se detalla los controles a implementarse, en forma parcial o total, en los accesos a los recursos computacionales y dependiendo de la capacidad tecnológica que dispongamos para cada caso:

Todos los accesos.

- Recursos Humanos notificara a la dirección de servicios informáticos la creación de usuarios para utilizar los sistemas de tecnología de la información.

- Los usuarios creados tendrán como estándar la inicial del primer nombre, guion bajo y el primer apellido (juan_perez).

Equipos de cómputo.

- Todos los usuarios disponen de un usuario y contraseña para acceder a su computador.
- Luego de 5 (cinco) minutos de inactividad en un equipo de computación, este automáticamente se protegerá con clave para evitar que intrusos o personas no autorizadas puedan ingresar al equipo.
- La clave tendrá un mínimo de 6 (seis) caracteres, (sugerido).
- La clave será una mezcla de letras (incluir una mayúscula) y números, no deberá tener caracteres especiales, (sugerido).
- El usuario deberá cambiar su clave en cualquier momento si sospecha que la misma ya no es confidencial.
- La clave tendrá un tiempo estimado de expiración de 3 (tres) meses, el usuario recibirá notificaciones automáticas 15 días antes de su expiración.
- El usuario que no cambie sus credenciales no podrá acceder al equipo ya que este se desactiva.
- Luego de 3 (tres) intentos fallidos tratando de ingresar la clave, esta se deshabilitara y se deberá solicitar al Departamento de Tecnología su activación.

Sistemas Informáticos.

- La clave será una mezcla de letras (incluir una mayúscula) y números, no deberá tener caracteres especiales.
- La clave de acceso a los sistemas expirara obligatoriamente cada 3 (tres) meses, el usuario recibirá notificaciones automáticas 15 días antes de su expiración.
- El usuario que no cambie sus credenciales no podrá acceder al sistema ya que este se desactiva.
- La clave tendrá un mínimo de 6 (seis) caracteres.

- Cuando el sistema solicite cambiar la clave, no se permitirá el ingreso de las últimas 10 (diez) claves ya utilizadas.
- El usuario podrá cambiar su clave en cualquier momento si sospecha que la misma ya no es confidencial.
- Luego de 3 (tres) intentos fallidos tratando de ingresar la clave, esta se deshabilitara y se deberá solicitar al Departamento de Tecnología su activación.
- Luego de 5 (cinco) minutos de inactividad en el sistema, este automáticamente se desactivará para evitar que intrusos o personas no autorizadas puedan ingresar al sistema.

Correo electrónico y acceso internet.

- El Departamento de Tecnología colocara una clave para el acceso al servicio de correo electrónico, de VPN y acceso remoto.
- Las cuentas de correo electrónico tendrán como estándar el primer nombre, punto, primer apellido y los 4 últimos dígitos de la cedula de identidad (juan.perez3247@utc.edu.ec).
- El acceso al internet se establece según el perfil de usuario de red.
- El acceso a internet estará definido por las categorías de usuario establecidas en el Anexo-01F. Categorías de Filtrado Web.

Equipo electrónico y de comunicaciones.

- ✓ El Departamento de Tecnología asignará una clave para su uso o administración.
- ✓ Del mismo modo el área de tecnología administrará las claves de acceso a los diferentes servidores, aplicaciones, equipos electrónicos y demás equipamiento que soporten los servicios mencionados.

4. Registros.

Tabla 2. Documentos de referencia para el Control de Acceso a Recursos Computacionales.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-01A	Aceptación y cumplimiento de Políticas	Departamento de Tecnología	Oficina Sistemas área de Soporte a usuarios	Secuencial alfabético	Cada vez que exista creación de usuarios en la red	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Reciclaje de papel	Uso interno
RE-02A	Creación de usuario de red.	Departamento de Tecnología	Oficina Sistemas área de Soporte a usuarios	Secuencial alfabético	Cada vez que exista creación de usuarios en la red	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Reciclaje de papel	Uso interno
RE-03A	Acta de entrega y recepción de equipos	Departamento de Tecnología	Oficina Sistemas área de Soporte a usuarios	Secuencial alfabético	Cada vez que exista creación de usuarios en la red	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Reciclaje de papel	Uso interno

5. Anexos.

N/A.

(Ciudad y fecha de recibido)

Yo, **(NOMBRE APELLIDO)**, portador (a) de la cédula de identidad **(#)**, manifiesto que he recibido inducción sobres las políticas de seguridad informática de la **Universidad Técnica de Cotopaxi**, en el cual se hace mención de las siguientes políticas:

- ✓ **PO-1A** Política de control de acceso a recursos computacionales.
- ✓ **PO-1B** Política de Active Directory.
- ✓ **PO-1C** Política de administración de activos de tecnología de información.
- ✓ **PO-1D** Política de resguardo de la información.
- ✓ **PO-1E** Política de seguridad a componentes informáticos.
- ✓ **PO-1F** Política de uso adecuado de internet.
- ✓ **PO-1G** Política de uso adecuado de laboratorios de computación.

Por tal motivo hago constar que he revisado y aceptado lo expuesto anteriormente, y cumpliré con sus lineamientos a fin de contribuir al mejoramiento de la seguridad de los recursos que me encomienden.

_____

(Nombre de usuario/colaborador)
(Número de CI)

Tabla 3. Solicitud de Creación de Usuarios de Red y Sistemas.

Fecha: _____/_____/_____/

Equipos de Computo	**Tipo**		**Justificación**	
	Lapto ☐	PC ☐		
Acceso	**Recursos**		**Descripción**	
	Sistema		**Modulo**	
	Mail			
	Interno ☐		Externo ☐	
	Telefonía			
	Interna ☐	Local ☐	Nacional ☐	Internacional ☐
Jefe Inmediato				
Solicitante/Empleado			**Cédula**	
Responsable TI			**Fecha Creación**	
Firmas				
	Responsable TI		**Empleado**	

	ACTA DE ENTREGA Y RECEPCIÓN DE EQUIPOS	Anexo-01A
		Ver. No. 01

En la ciudad de Latacunga, a los ___/ _____/2019, comparecen:

a) [Nombre y cargo del encargado de la entrega de los equipos]; y,

b) [Nombre del personal que recibe el o los equipos].

Quienes, en cumplimiento con el Reglamento interno de la **UNIVERSIDAD TÉCNICA DE COTOPAXI,** suscriben la presente **ACTA DE ENTREGA-RECEPCIÓN** de los siguientes bienes:

Cant.	**Equipo**	**Marca**	**Modelo**	**Nº de inventario y serie**

Se deja constancia que los bienes que se reciben son nuevos y por lo tanto se encuentran en excelente estado de funcionamiento, obligándose al personal receptor de los equipos a su conservación, de acuerdo con su naturaleza y conforme lo dispone el Reglamento interno de la institución.

Para constancia de su aceptación las partes suscriben el presente instrumento en dos ejemplares de igual contenido y efecto, en la ciudad de [nombre del lugar de suscripción y fecha].

_____ _____

(Nombre del encargado de la entrega de equipos)

C.I. (número de cédula)

(Nombre del que recibe el equipo)

C.I. (número de cédula)

Responsable: Analista de Comunicaciones y Arquitectura / Analista de Desarrollo y Base de Datos. Fecha: 19-07-2019	Aprobación: Director DTIC's. Fecha: 19-07-2019

1. Alcance.

Aplica a todos los usuarios enrolados en al Active Directory que utilicen equipos de cómputo de la Universidad.

2. Documentos de referencia.

Anexo-01B Asignación de políticas de AD.

3. Descripción de la Política.

La Universidad, consciente de establecer buenas prácticas para el uso adecuado de las tecnologías y recursos informáticos, establece la implementación de Active Directory para facilitar el control, la administración y consulta de todos los elementos lógicos de una red (como son usuarios, equipos y recursos).

A continuación se detalla los controles a implementarse, en forma parcial o total, dependiendo de la capacidad tecnológica que dispongamos para cada caso:

Del Área de Tecnología.

- Establecer el fondo corporativo de la institución en todos los equipos de cómputo.
- Establecer como protector de pantalla la misión y visión de la Universidad.
- Instalar las impresoras en un servidor de impresión, para facilitar el control de actualización de controladores, configuración de las bandejas, memoria, dúplex, color, etc., sin tener que ir de usuario en usuario configurando los parámetros de cada impresora.
- Definir reglas que controlan el entorno de trabajo, cuentas de usuario y cuentas de equipo, que permita la configuración de sistemas operativos, aplicaciones y de los usuarios en un entorno de AD.
- Asignar políticas de AD según el perfil de usuario establecido en el Anexo-01B Asignación de políticas de AD.
- El área de tecnología tendrá la potestad de habilitar o deshabilitar los siguientes componentes del sistema según crea conveniente:
  - ✓ Bloquear el acceso al Administrador de tareas.
  - ✓ Restringir el acceso a determinadas carpetas.

- ✓ Deshabilitar la descarga de archivos ejecutables.
- ✓ Establecer el título del explorador de Internet.
- ✓ Deshabilitar el uso de REGEDIT.EXE.
- ✓ Establecer qué paquetes MSI se pueden instalar en un equipo.
- ✓ Quitar del Escritorio el icono "Papelera de Reciclaje".
- ✓ Establecer el tiempo de espera del protector de pantalla en 300 segundos (5 minutos).
- ✓ Quitar el icono de Red del menú de Inicio.
- ✓ Prohibir el acceso al Panel de control.
- ✓ Desactivar los gadgets de escritorio.
- ✓ No permitir la ejecución de Windows Messenger.
- ✓ Desactivar la funcionalidad de "Eliminar el historial de exploración" en Internet Explorer.
- ✓ Impedir el acceso al símbolo del sistema.

Responsabilidad de los Usuarios.

- Los usuarios deberán ingresar el comando CTRL+ALT+SUPR para iniciar sesión en los equipos.
- Todos los usuarios disponen de un usuario y contraseña para acceder a su computador.
- Luego de 5 (cinco) minutos de inactividad en un equipo de computación, este automáticamente activara el protector de pantalla evitando que intrusos o personas no autorizadas puedan ingresar al equipo.
- Luego de 5 (cinco) minutos de inactividad de la sesión iniciada, el usuario deberá ingresar nuevamente su contraseña.
- Luego de 3 (tres) intentos fallidos tratando de ingresar la clave, esta se deshabilitara y se deberá solicitar al Departamento de Tecnología su activación.

4. Registros.

N/A.

5. Anexos.

Anexo-01B Asignación de políticas de AD.

A continuación una breve descripción de cada política.

- ✓ **Autenticación.**

  Medida de seguridad que ayuda a proteger la información más importante de usuarios no autorizados.
- ✓ **Tapiz del escritorio.**

  Especifica el fondo de escritorio que se mostrará en los escritorios de los usuarios.
- ✓ **Protector de pantalla.**

  Establece un protector de pantalla con la misión y visión de la institución, pasado 5 (cinco) minutos este bloquea la sesión iniciada y será necesario volver a introducir la contraseña de usuario.
- ✓ **Desactivar cuenta de usuario.**

  Luego de 3 (tres) intentos fallidos tratando de ingresar la clave, esta se deshabilitara y se deberá solicitar al Departamento de Tecnología su activación.
- ✓ **Redirección de carpetas**: Unidad D:/Datos.

  La información almacenada en la Unidad D:/Datos será copiada a la ubicación que se establezca previamente.
- ✓ **Desactivar Reproducción automática**.

  Cuando se conecta una memoria USB o un CD/DVD en el lector del equipo, generalmente se habré una ventana para la "Reproducción automática", pero muchos virus (más que todo en memorias USB) se pueden ejecutar mediante ésta reproducción automática.
- ✓ **Prohibir el acceso al Panel de Control**.

  Por cuestiones de seguridad y de integridad del equipo, se desactiva el panel de control para el usuario final de tal manera que no pueda cambiar configuraciones y dejar que ésta sea una tarea netamente del departamento TI.
- ✓ **Cambiar contraseña**.

  El usuario deberá contar con esta opción para cambiar su clave en cualquier momento si sospecha que la misma ya no es confidencial.

- ✓ **REGEDIT**.

  Es la herramienta que permite editar el registro del sistema operativo Windows.

- ✓ **Accesos directos.**

  Crear un acceso directo en el escritorio de los usuarios.

- ✓ **Establecer contraseñas.**

  La contraseña debe cumplir los requisitos de complejidad.

1. Alcance.

Aplica a todos los usuarios que manipulan activos fijos de la universidad técnica de Cotopaxi, incluyendo empleados, trabajadores temporales y cualquier otro ente autorizado por la institución para hacer uso de estos.

2. Documentos de referencia.

RE-01C Inventario de equipos de cómputo y servidores.

RE-02C Movimiento de equipos de cómputo.

RE-03C Baja de equipos de cómputo.

RE-04C Bitácora de mantenimiento preventivo de PC's.

RE-05C Ficha de mantenimiento preventivo de computadores.

3. Descripción de la Política.

- El departamento de tecnología debe tener la capacidad de asignar equipos a los usuarios previamente creados.
- El departamento de tecnología debe llevar un registro de inventario de equipos de cómputo y servidores.
- El Encargado de los Activos Fijos será responsable del control, ubicación de los bienes muebles e inmuebles propiedad de la institución.
- Los Encargados de las diferentes áreas que conforman la Universidad son los responsables del mobiliario y equipo asignado a su respectiva Unidad o Departamento, como también del buen uso, resguardo y cuido de los mismos.
- Para realizar el mantenimiento del Data Center se realizara un concurso cada dos (2) años con el objetivo de buscar personal apropiado para el manejo de estos equipos, en donde el responsable deberá presentar un informe detallando las actividades realizadas.

Asignación de equipos de cómputo.

- Crear cuentas y asignar equipos de cómputo a los usuarios registrados previamente en la solicitud de creación de usuarios de red y asignación de recursos.
- El usuario al momento de recibir o entregar equipo de cómputo debe firmar el Acta de entrega y recepción de equipos para hacer uso de estos.
- El encargado de activos fijos es responsable de registrar el Movimiento de equipos, sean estos trasladados internamente (dentro de la misma facultad) o externamente (a otra facultad o dependencia).
- El encargado de activos fijos es responsable de dar de Baja a los equipos de cómputo, que se encuentren en mal estado.

Mantenimiento Preventivo de PC's.

- El Departamento de tecnología debe llevar un Cronograma para realizar el mantenimiento de PCs en la institución sin interrumpir las horas de trabajo de cada usuario.
- El mantenimiento preventivo de PC's se debe realizar cada seis (6) meses, una vez finalizado el semestre.
- Se debe llevar una Bitácora de mantenimiento preventivo de PC's para tener registro de las actividades realizadas en cada equipo.

Recomendaciones para mantenimiento preventivo de equipos de cómputo – PC's.

- ✓ Planear de un cronograma de mantenimiento el cual se aplicará de manera anual para los equipos de cómputo de la universidad para asegurar su correcto funcionamiento y durabilidad.
- ✓ Validar según el inventario realizado, la ubicación de los equipos de la universidad y los usuarios (funcionarios y/o contratistas) los cuales hacen uso de estos.
- ✓ Socializar con cada uno de los usuarios la programación definida por la institución para la realización del programa de mantenimiento de los equipos y definir fecha donde se pueden intervenir los equipos sin afectar las labores del diarias de los usuarios.
- ✓ Ejecutar el programa de mantenimiento según las fechas programadas y en compañía del (los) usuario(s) y/o representante(s) técnico(s) del proveedor.

- ✓ Realizar el retiro del equipo del puesto de trabajo y proceder al mantenimiento respectivo; sin causar molestias por el ruido y partículas generadas por la actividad de limpieza.
- ✓ Ejecutar el mantenimiento de cada equipo, esto no deberá superar las dos (2) horas (dependiendo del problema que se presente) minimizando la afectación de las laboras diarias de los usuarios (funcionarios y/o contratistas) de la institución. Cualquier inconveniente presentado deberá ser reportado de manera inmediata para la ejecución de una pronta solución según el caso presentado.
- ✓ Reintegrar nuevamente al puesto de trabajo el equipo, revisando y garantizando su correcta instalación y funcionamiento.

Por otra parte en cada Unidad o Departamento se deberá revisar los siguientes puntos:

- ✓ Limpieza y lubricación de equipos de cómputo.
- ✓ Actualizaciones de Windows automáticas, en caso de Linux ejecutar gpupdate vía consola para realizar actualizaciones.
- ✓ Backup de información
- ✓ Realizar la revisión de instalación por SETUP - Actualización de Firewall - BIOS
- ✓ Desfragmentar el de disco duro, en caso de que sea necesario (PC's)
- ✓ Eliminar los archivos TMP (temporales) en Windows.
- ✓ Para eliminar archivos TMP en Linux ejecutar el comando Systemd vía consola.
- ✓ En Linux es recomendable eliminar los archivos temporales cuando se enciende o apaga el ordenador.
- ✓ Realizar un inventario de software instalado (PC's).
- ✓ Realizar detección de errores.
- ✓ Hacer un vaciado de la papelera de reciclaje.
- ✓ Ejecutar el Antivirus en Windows.
- ✓ Actualización de antivirus en Windows.
- ✓ Limpieza externa.
- ✓ Limpieza del monitor, mouse y teclado (PC's).

Mantenimiento Preventivo de Data Center.

- El Departamento de tecnología debe llevar un Cronograma para realizar el mantenimiento preventivo del Data Center en la institución sin interferir las horas de trabajo de cada usuario.
- El mantenimiento preventivo del Data Center se debe realizar cada seis (6) meses, una vez finalizado el semestre.
- Se debe llevar una Bitácora mantenimiento del Data Center para tener registro de las actividades realizadas.

Equipos de comunicación.

- El departamento de tecnología Asignara claves para su uso y administración de los recursos o equipos computacionales que se encuentran en la universidad.

Todos los usuarios de la institución son responsables por:

- El debido uso, custodia, preservación de los bienes que le sean asignados.
- Demandar con la debida anticipación, los servicios de reparación de los bienes que le sean asignados.

4. Registros:

Tabla 4. Documentos de referencia para la administración de activos de TI.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-01C	Inventario de equipos de cómputo y servidores	Departamento de Tecnología	Oficina Sistemas área de Soporte a usuarios	Secuencial alfabético	Cada vez que exista creación de usuarios en la red	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Reciclaje de papel	Uso interno
RE-02C	Movimiento de equipos	Departamento de Tecnología	Oficina Sistemas área de Soporte a usuarios	Secuencial alfabético	Cada vez que exista creación de usuarios en la red	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Reciclaje de papel	Uso interno
RE-03C	Baja de equipos	Departamento de Tecnología	Oficina Sistemas área de Soporte a usuarios	Secuencial alfabético	Cada vez que exista creación de usuarios en la red	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Reciclaje de papel	Uso interno

RE-04C	Bitácora de mantenimiento preventivo de PCs	Departamento de Tecnología	Oficina Sistemas área de Soporte a usuarios	Secuencial alfabético	Cada vez que exista creación de usuarios en la red	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Reciclaje de papel	Uso interno
RE-05C	Ficha de Mantenimiento Preventivo de Computadores	Departamento de Tecnología	Oficina Sistemas área de Soporte a usuarios	Secuencial alfabético	Cada vez que exista creación de usuarios en la red	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Reciclaje de papel	Uso interno

5. Anexos

Anexo-01C Cronograma de mantenimiento preventivo de PCs.

Anexo-02C Cronograma de mantenimiento preventivo de Data Center.

	INVENTARIO DE EQUIPOS DE COMPUTACIÓN Y SERVIDORES	RE-01C Ver. No. 01

Tabla 5. Inventario de equipos de cómputo y servidores

INVENTARIO DE EQUIPOS DE CÓMPUTO Y SERVIDORES

Nº	Activo Fijo	Nombre de Equipo	Usuario	Profile	Dominio	Departamento / Unidad de negocio	Tipo	Marca	Modelo	Memoria RAM	Disco duro	Procesador	Sistema Operativo	Key Sistema Operativo	Office versión	Key office	Teclado	Mouse	Monitor	Accesorios

Responsable: Analista de Comunicaciones y Arquitectura. Fecha: 19-07-2019	Aprobación: Director DTIC's. Fecha: 19-07-2019

	REGISTRO DE MOVIMIENTO DE EQUIPOS	RE-02C
		Ver. No. 01

Tabla 6. Registro de movimiento de equipos.

Fecha _____ **Consecutivo Nº.** _____

Tipo de movimiento

	Personalización por entrega inicial del activo fijo.
	Traslado interno (dentro de la misma facultad o dependencia).
	Traslado externo (a otra facultad o dependencia).
	Devolución a la Oficina de Activos Fijos por obsolescencia.

Dependencia origen (Entrega)	
Responsable actual	
Documento de identidad No.	
Dependencia	
Código dependencia	

Dependencia destino (Recibe)	
Nuevo responsable	
Documento de identidad No.	
Dependencia	
Código dependencia	

Información básica de los activos fijos			
No.	Descripción del activo	No. inventario	No. serie (en equipos)
1			
2			
3			
4			
5			

Total de activos

Observaciones

Firmas dependencia origen (Entrega)
Firma y sello responsable/dependencia actual
Firma y sello de quien autoriza el traslado

Firma dependencia destino (Recibe)	
Firma y sello nuevo responsable/dependencia	
V.B. Auxiliar activos	**Captura Activos Fijos**

Responsable: Analista de Comunicaciones y Arquitectura. Fecha: 19-07-2019	Aprobación: Director DTIC's. Fecha: 19-07-2019

	REGISTRO DE BAJA DE EQUIPOS	RE-03C Ver. No. 01

Tabla 7. Registro de baja de equipos.

Registro Nº		**Fecha**	_____/_____/_____/ **DD MM AA**

Ubicación del Equipo	

Datos del Usuario

Nombre	
Cargo	
Nombre del Jefe del Área	

Datos del Equipo

Nombre	Tipo	Marca	Modelo	Nº Serie	Nº Inventario	Valor en Libros

Motivo de Baja	**Como se Detecto**

Dictamen: _____

_____

Observaciones: _____

_____

Firmas:

SOLICITANTE	**JEFE DEPARTAMENTO**
_____	_____
Responsable	**Titular o Delegado**

	BITÁCORA DE MANTENIMIENTO PREVENTIVO DE PC’s	RE-04C
		Ver. No. 01

Tabla 8. Bitácora de mantenimiento preventivo de PC's.

Fecha	Activo Fijo	Usuario Responsable	Responsable de TI	Actividades Realizadas	Observación	Firma de Conformidad

Responsable: Analista de Comunicaciones y Arquitectura. Fecha: 19-07-2019	Aprobación: Director DTIC’s. Fecha: 19-07-2019

	FICHA DE MANTENIMIENTO PREVENTIVO DE COMPUTADORES	RE-05C
		Ver. No. 01

Tabla 9. Ficha de mantenimiento preventivo de computadores.

DEPARTANMENTO DE TECNOLOGIA DE INFORMACIÓN							
RESPONSABLE DE TI:			**FECHA:**				
USUARIO/RESPONSABLE:			**DEPARTAMENTO:**				
Información del Hardware		**Inventario del Hardware**					
Tipo de Equipo:		**Componente**	**Cantidad**	**Marca**	**N^{0} Serie**	**Capacidad**	**Tipo de conexión**
Nombre del Equipo:		Procesador:					
Dirección IP:		Memoria Ram:					
Dirección MAC:		Disco Duro:					
Sistema operativo:		Unidad de CD/Rom:					
Versión del Bios:		Teclado:					
Marca de Fabricante:		Mouse:					
Modelo Sistema:		Monitor:					
Tipo de Sistema:		Fuente de Poder:					
Memoria Total de HDD:		**EXTRAS**					
Memoria Total de Ram:							
GPU:							
Generacion Del Procesador:		**Informacion del Procesador**					
Modelo de ManinBoard:							
Cache del Procesador:							
Observación General del Software:		**Observación General del Hardware:**					
DETALLE MANTENIMIENTO:							

Responsable: Analista de Comunicaciones y Arquitectura. Fecha: 19-07-2019	Aprobación: Director DTIC's. Fecha: 19-07-2019

	CRONOGRAMA DE MANTENIMIENTO PREVENTIVO DE PC's	Anexo-01C
		Ver. No. 01

Tabla 10. Cronograma de mantenimiento preventivo de PC's.

UNIDAD O DEPARTAMENTO	MESES											
	ENE.	FEB.	MAR.	ABR.	MAY.	JUN.	JUL.	AGO.	SEP.	OCT.	NOV.	DIC.
Dir. Auditoría Interna												
Dir. Planeamiento y Desarrollo Institucional												
Dir. Evaluación y Aseguramiento de la Calidad												
Dir. Asesoría Jurídica												
Dir. Comunicación Institucional												
Dir. Relaciones Institucionales												
Dir. Investigación												
Dir. Posgrados												
Dir. Educación Continua												
Dir. Vinculación												
Dir. Académica												
Dir. Talento Humano												
Dir. Administrativa												
Dir. Financiera												
Dir. Bienestar Estudiantil												
Dir. Tecnologías e Informáticas												
Centro de Idiomas												
Centro de Cultura Física												
Centro de Experimentación Científica												

Responsable: Analista de Comunicaciones y Arquitectura. Fecha: 19-07-2019	Aprobación: Director DTIC's. Fecha: 19-07-2019

	CRONOGRAMA DE MANTENIMIENTO PREVENTIVO DE DATA CENTER	Anexo-02C
		Ver. No. 01

Tabla 11. Cronograma de mantenimiento preventivo de Data Center

ACTIVIDAD	MESES											
	ENE.	FEB.	MAR.	ABR.	MAY.	JUN.	JUL.	AGO.	SEP.	OCT.	NOV.	DIC.
Verificar Aire Acondicionado												
Sistema de control de incendios												
Verificar Planta eléctrica de Emergencia												
UPS, PDU´s, y Tableros de Emparalelamiento												
Sistema de control de acceso												
Descontaminación y renivelación de pisos falsos												
Mantenimiento arquitectónico a Data Centers (Pinturas retardantes, luminarias, limpieza)												
Servidores												

Responsable: Analista de Comunicaciones y Arquitectura. Fecha: 19-07-2019	Aprobación: Director DTIC's. Fecha: 19-07-2019

1. Alcance.

Aplicar en la infraestructura de las Tics de la Universidad Técnica de Cotopaxi definida en los anexos que apoyan al resguardo de la información.

2. Documentos de referencia.

RE-01B. Bitácora de respaldos de usuarios.
RE-02B. Bitácora de respaldos de bases de datos.

3. Descripción de la Política.

Evitar la pérdida de la información dentro de la institución en caso de que existan eventos fortuitos con el fin de garantizar la integridad y disponibilidad de la misma.

Para asegurar que toda la información esencial pueda recuperarse tras un desastre o fallo, se debe considerar los elementos siguientes:

- ✓ Definir el nivel necesario de información de respaldo.
- ✓ Realizar copias seguras y completas de la información, y establecer los procedimientos de restauración.
- ✓ Probar regularmente los soportes de respaldo para verificar que se encuentran trabajando correctamente.
- ✓ Comprobar habitualmente los procedimientos de restauración para asegurar que son eficaces y que pueden ser utilizados cuando se requieran.
- ✓ Toda información secreta, confidencial o privada debe estar encriptada, ya sea que se encuentre al interior de la institución o externamente, en cualquier medio de almacenamiento.
- ✓ Toda información sensible debe tener un proceso periódico de respaldo, tener asignado un período de retención determinado, la fecha de la última modificación y la fecha en que deja de ser sensible o se degrada. Sin embargo, la información no se debe guardar indefinidamente por lo cual se debe determinar un período máximo de retención para el caso en que no se haya especificado este tiempo.

- ✓ Todos los medios físicos donde la información de valor, sensitiva y crítica sea almacenada por períodos mayores a seis meses (6), no deben estar sujetos a una rápida degradación o deterioro.
- ✓ Los respaldos de información de valor o sensible debe tener un proceso periódico de validación con el fin de garantizar que no ha sufrido ningún deterioro y que se podrá utilizar en el momento en que se necesite.

Responsabilidad de los Usuarios.

- ✓ El usuario debe almacenar su información dentro de la carpeta (UTC_Usuarios), que va estar alojada dentro de la unidad D.
- ✓ El usuario debe almacenar información relevante relacionada con las actividades dentro de la institución.
- ✓ El usuario debe dar acceso de su información cuando el personal de tecnología de información lo requiera.

Departamento de Tecnología.

- ✓ Proporcionar un servidor donde se pueda almacenar los respaldos que se van a realizar.
- ✓ Implementar un software específico que ayude a generar respaldos periódicamente
- ✓ Asignar espacios de almacenamiento específico de acuerdo a la posición que desempeñe el usuario final.
- ✓ Planificar una matriz de ejecución automática de respaldos de usuarios que se ajuste a la herramienta implementada y hacer el control de acuerdo a una bitácora de respaldos de usuarios.
- ✓ Generar un cronograma de respaldo de acuerdo al departamento.
- ✓ Almacenar la información de usuarios respaldada con procedimientos de confidencialidad de acuerdo a la herramienta utilizada.
- ✓ Disponer con una segunda herramienta para respaldos de información.

Bases de datos.

- ✓ El proceso de respaldo de información debe realizarse de dos formas (en la nube y de manera local).
- ✓ El respaldo local de la base de datos se la realizara mediante una librería alojando su información en cintas magnéticas.
- ✓ Planificar una matriz de ejecución automática de respaldos de bases de datos que se ajuste a la herramienta implementada y hacer el control de acuerdo a una bitácora de respaldos de bases de datos.

Área de Recursos Humanos.

- ✓ Realizar la selección adecuada del personal y realizar inducción sobre el uso adecuado de los servicios de tecnología.
- ✓ Proporcionar información de la salida de personal con tiempo suficiente (48 horas) para la planificación de respaldos de información.

4. Registros.

Tabla 12. Documentos de referencia para el resguardo de información.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-01B	Bitácora de Respaldos de Usuarios	Analista de Soporte a usuarios	Oficina Sistemas área de Soporte a usuarios	Secuencial por fecha	Anual	2 años	Reciclaje de papel	Uso interno
RE-02B	Bitácora de respaldos de BDD	Analista de sistemas	Oficina Sistemas área de análisis de sistemas	Secuencial por fecha	Anual	2 años	Reciclaje de papel	Uso interno

5. Anexos.

Anexo-01D Cronograma de respaldos de usuarios finales y de servidores.

Anexo-02D Lista de usuarios existentes en el sistema.

	BITÁCORA DE RESPALDOS DE USUARIOS	RE-01D
		Ver. No. 01

Tabla 13. Bitácora de respaldo de usuarios.

Nº	Nombre de Usuario	Medio utilizado para realizar Backup	Tipo de Backup	Fecha ultimo Backup realizado	Fecha de realización de Backup	Contenido	Ubicación	Responsable

Observación _____

_____

_____ _____

Aprobado **Verificado**

Responsable: Analista de Comunicaciones y Arquitectura. Fecha: 19-07-2019	Aprobación: Director DTIC's. Fecha: 19-07-2019

	BITÁCORA DE RESPALDOS DE BASE DE DATOS	RE-02D
		Ver. No. 01

Tabla 14. Bitácora de respaldo de Base de Datos.

Nº	Nombre del Servidor	Medio utilizado para realizar Backup	Tipo de Backup	Fecha ultimo Backup realizado	Fecha de realización de Backup	Contenido	Ubicación	Responsable

Observación _____

_____

_____ _____

Aprobado **Verificado**

Responsable: Analista de Comunicaciones y Arquitectura. Fecha: 19-07-2019	Aprobación: Director DTIC's. Fecha: 19-07-2019

Tabla 15. Cronograma de respaldos de usuarios finales y servidores.

SERVIDOR	FRECUENCIA DE RESPALDO DE INFORMACIÓN						
	SABADO	DOMINGO	LUNES	MARTES	MIÉRCOLES	JUEVES	VIERNES
ARCHIVOS							
INCREMENTAL							
DOMINIO							
INCREMENTAL							
ANTIVIRUS							
INCREMENTAL							
APLICACIONES							
INCREMENTAL							
CORREO							
INCREMENTAL							
IMPRESIÓN							
INCREMENTAL							
WEB							
INCREMENTAL							

Tabla 16. Usuarios declarados para respaldo de información.

N°	NOMBRE	APELLIDO	PUESTO/CARGO	EQUIPO/IP
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				

1. Alcance.

Aplica a toda la infraestructura de las Tics de la Universidad Técnica de Cotopaxi.

2. Documentos de referencia.

RE-01E Ingreso y salida de equipos.

3. Descripción de la Política.

El Departamento de Tecnología está en la obligación de proteger, planificar y dar seguimiento a los componentes informáticos de la institución, asegurándose que todos los equipos trabajen y sean usados de forma adecuada.

A continuación se detalla los controles a implementarse, en forma parcial o total, dependiendo de la capacidad tecnológica que dispongamos para cada caso:

Protección de equipos.

Antivirus.

- Las computadoras y servidores (tanto físicos como virtuales) pertenecientes a la institución, contarán con un software antivirus, el mismo que será administrado únicamente por el departamento de tecnología.
- Los equipos informáticos serán actualizados de manera periódica con los últimos parches de seguridad del sistema operativo y aplicaciones instaladas en el equipo.
- Por seguridad, los mensajes o archivos adjuntos que contengan virus serán inmediatamente eliminados sin posibilidad de recuperación.
- Analizar con el Antivirus las unidades de disco flexible, discos removibles o memorias USB (flash) antes de usarlas.
- Para prevenir infecciones por virus informático los empleados no deben hacer uso de cualquier clase de software que no haya sido proporcionado y validado por el Departamento de Tecnología.
- El equipo infectado será retirado de la estación de trabajo para su revisión pertinente.

- El Departamento de Tecnologías es responsable de llevar a cabo las acciones para la eliminación de virus y garantizar la pérdida mínima de información, minimizar los daños y el tiempo fuera de servicio del equipo infectado.
- Establecer canales de comunicación para reportar anomalías que sucedan dentro de la red.

Seguridad para las laptops (candado).

- Utilizar un candado físico para anclar la Laptop cuando se ausente temporalmente.
- Guardar todos los detalles del computador, incluyendo fabricante, modelo y número serial para poder llenar formularios en caso de ser necesitados.
- Asegurarse de apagar la Laptop, no dejarla en modo hibernación ni suspenso antes de empacarla.
- No rayar, flexionar, golpear, o presionar la superficie de la pantalla de cristal líquido (LCD) de la Laptop.

Acceso a servidores.

- El departamento de tecnología es el encargado de designar el personal para acceder a las instalaciones de los servidores de la universidad.
- Se debe llevar un registro para controlar las actividades realizadas en equipos de cómputo y servidores.

Ingreso y salida de equipos.

- Los empleados deben contar con la debida autorización del departamento de tecnología para sacar los equipos de la institución y deben responsabilizarse y no dejar abandonados estos equipos en cualquier sitio público ya que están expuestos a robos o cualquier imprevisto que le podrían causar grandes pérdidas económicas a la Universidad.
- Los recursos tecnológicos le la universidad, sean estos computadores, servidores, equipos de red, etc., no podrá moverse ni reubicarse sin la autorización del departamento de tecnología.
- La instalación como la reubicación de los equipos informáticos, se verificara que los equipos cuenten con las condiciones físicas y ambientales aceptables y que exista disponibilidad de energía e infraestructura de conexión de red adecuada, que asegure el correcto funcionamiento de los mismos.

- Los equipos deben ser trasladados en bolsa o equipos especiales en caso de recibir golpes inesperados.
- El registro de salida de equipos estará respaldado por el documento RE-01E Registro de entrada y salida de equipos.

4. Registros.

Tabla 17. Documentos de referencia para la seguridad a componentes informáticos.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-01E	Registro de entrada y salida de equipos.	Departamento de Tecnología	Oficina Sistemas área de Soporte a usuarios	Secuencial alfabético	Cada vez que exista creación de usuarios en la red	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Reciclaje de papel	Uso interno

5. Anexos.

N/A.

	REGISTRO DE ENTRADA Y SALIDA DE EQUIPOS	RE-01E
		Ver. No. 01

Tabla 18. Registro de entrada y salida de equipos.

FECHA : _____ _____ _____
DÍA MES AÑO

DEPENDENCIA DE ORIGEN: _____ **C.I.:** _____

ENTREGA: _____ **FIRMA:** _____

DESCRIPCIÓN DEL BIEN	MARCA	MODELO	SERIE	NO. INVENTARIO	COMENTARIOS ADICIONALES
1.-					
2.-					
3.-					
4.-					
5.-					
6.-					

SERVICIO PRESTADO:

PRESTAMO ( ) **ASIGNACIÓN ( )** **OTRO:** _____

DEPENDENCIA RECEPTORA: _____ **C.I.:** _____

RECIBE: _____ **FIRMA:** _____

OBSERVACIONES: _____

_____

***Nota**: Al firmar esta hoja, el usuario se compromete a entregar el equipo en las mismas condiciones en que lo recibe.

_____
[Nombre y firma de quien autoriza]

Responsable: Analista de Comunicaciones y Arquitectura. Fecha: 19-07-2019	Aprobación: Director DTIC's. Fecha: 19-07-2019

1. Alcance.

Aplica a todos los usuarios de la comunidad Universitaria que tienen acceso al servicio de internet por medio de un equipo de cómputo o dispositivo electrónico.

2. Documentos de referencia.

Anexo-01F. Categorías de Filtrado Web.

3. Descripción de la Política.

La Universidad, consciente de la importancia de internet como una herramienta para el desempeño de las labores diarias, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades.

Departamento de Tecnología.

- ✓ Cuenta con la herramienta Fortinet (FortiGuard) la cual se encarga de restringir el acceso a los sitios web considerados inadecuados, nocivos o molestos.
- ✓ Regular el acceso a internet por medio de un web filter según las categorías mencionadas en el Anexo-01F.
- ✓ Proporciona los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de internet, bajo las restricciones de los perfiles de acceso establecidos.
- ✓ Los privilegios de uso de Internet estarán limitados por la necesidad de acceso que requiera el desarrollo de la función de cada usuario, según las categorías mencionadas en el Anexo-01F.
- ✓ Debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de internet en caso de contingencia interna.
- ✓ Debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de internet y evitar el acceso a sitios catalogados como restringidos.

- ✓ Debe generar registros de la navegación y los accesos de los usuarios a internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de internet.

Responsabilidad de los Usuarios.

- ✓ Hacer uso del servicio de internet que provee la institución para las actividades que guarden relación con su labor dentro de la universidad.
- ✓ Abstenerse de descargar software no autorizado desde internet, así como su instalación en las estaciones de trabajo asignados para el desempeño de sus labores, a menos que sean autorizados por el Departamento de Tecnología.
- ✓ No deben acceder a páginas relacionadas con pornografía, drogas, alcohol, web proxys, hacking y cualquier otra página que vaya en contra de la ética y la moral.
- ✓ No deben utilizar el servicio de internet para el acceso y uso de servicios interactivos o mensajería instantánea como Facebook y otros similares, con el fin de intercambiar información confidencial o de uso interno de la institución o para actividades que no corresponden con el desempeño de las funciones asignadas.
- ✓ No deben descargar, usar, intercambiar o instalar juegos, música, películas, información que de alguna manera atenten contra la propiedad intelectual de sus autores.
- ✓ No deben ejecutar archivos o herramientas que atenten contra la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica de la institución.
- ✓ Deben asegurarse que la información audiovisual (videos e imágenes) descargada y utilizada para las labores diarias no atenten contra la propiedad intelectual de sus autores.
- ✓ No deben intercambiar de ninguna forma, información confidencial para la institución sin la debida autorización.

4. Registros.

N/A.

5. Anexo.

Anexo-01F. Categorías de Filtrado Web.

En esta sección se encuentra información detallada sobre las categorías de filtrado web:

Desnudez: Incluye páginas con contenido explícito de tipo sexual y erótico, inadecuado para personas menores de edad (pornografía), páginas con contenido erótico (erotismo / sexo) y páginas con desnudez total o parcial, sin referencias sexuales (bañadores / ropa interior).

Compras: Esta categoría permite restringir el acceso a tiendas donde se pueda hacer pedidos online (compras online), así como a páginas de subastas y publicitarias (subastas / anuncios).

Sociedad / Educación / Religión: Permite restringir el acceso a páginas relacionadas con organismos oficiales (organizaciones gubernamentales), organizaciones no gubernamentales (ONG), páginas con información sobre ciudades, regiones, países y mapas (ciudades, regiones y países), páginas web de universidades, colegios, diccionarios y enciclopedias (educación y enriquecimiento personal), páginas de partidos políticos (partidos políticos) y páginas de contenido religioso o espiritual (religión y espiritualidad).

Actividades de naturaleza ilegal: Permite bloquear el acceso a páginas con información para construir armas o quitar la vida a otras personas, realizar actividades ilegales, o a páginas de pornografía infantil (actividades ofensivas o delictivas).

- ✓ Por otra parte, también te permite restringir el acceso a páginas con información para manipular dispositivos electrónicos, redes de datos, codificación de contraseñas y a páginas con manuales sobre virus informáticos (crímenes informáticos).
- ✓ Finalmente, dentro de esta categoría también podrás bloquear el acceso a páginas con contenidos discriminatorios o de grupos extremistas (racismo, xenofobia, discriminación), y a páginas ilegales con cracks y números de serie para diversas aplicaciones informáticas (hacking).

Juegos / apuestas: Permite restringir el acceso a páginas de apuestas, vídeo juegos (juegos informáticos), y páginas con información sobre juguetes.

Redes sociales: Portales de redes que conectan a las personas en general o con un determinado grupo de personas por motivos de socialización, interacciones comerciales, etc. Por ejemplo, sitios donde uno puedo crear un perfil de miembro para compartir intereses personales y profesionales. Esto incluye sitios de medios sociales como Twitter.

Entretenimiento / cultura: Permite restringir el acceso a diversos tipos de páginas web de entretenimiento o culturales: cine y televisión, parques de atracciones y parques temáticos, teatros y

museos, música (estaciones de radio online, páginas de grupos musicales, casas discográficas, etc.), literatura en general y páginas de humor.

Información y comunicación: Esta categoría de contenido engloban páginas de información general (noticias, periódicos y revistas), páginas web que permiten enviar y recibir correo electrónico (correo web), charlar en tiempo real con otros usuarios (chat), intercambiar información sobre diferentes temas con otros usuarios (grupos de noticias, VBS, sitios de discusión), enviar mensajes a teléfonos móviles, descargar melodías y fondos de pantalla (SMS, aplicaciones divertidas para teléfonos móviles), enviar postales y felicitaciones digitales (postales digitales) y buscar información en Internet (motores de búsqueda / catálogos web / portales de Internet).

Tecnologías de la información: Esta categoría restringe el acceso a páginas de fabricantes de hardware y software (vendedores y distribuidores de hardware y/o software), páginas de alojamiento de sitios web y proveedores de acceso a Internet (alojamiento web), páginas con información sobre seguridad, privacidad y protección de datos en Internet (seguridad informática), páginas que permiten traducir el contenido completo de un sitio web a otro idioma (sitios de traducción de URLs) y aquellas que permiten a los usuarios visitar páginas web de forma anónima (proxies anónimos).

Drogas: Esta categoría permite restringir el acceso a páginas con información sobre drogas no legalizadas (drogas ilegales), páginas que tratan la ingestión de alcohol como algo placentero (alcohol), así como a páginas relacionadas con el tabaco. Finalmente, en esta categoría también podrás restringir el acceso a páginas de ayuda para luchar contra la adicción a las drogas (ayuda / adicción).

Estilo de vida: Esta categoría permite restringir el acceso a páginas que promocionan las relaciones interpersonales (citas / relaciones), páginas de bares, restaurantes, discotecas y establecimientos de comida rápida (restaurantes / bares), páginas de agencias de viaje, hoteles, complejos turísticos, líneas aéreas y ferroviarias, agencias de alquiler de automóviles (viajes), páginas de agencias de modelos, moda, cosméticos y joyas, páginas sobre competiciones deportivas, equipos, federaciones y eventos deportivos (deportes), páginas sobre mercados inmobiliarios, sitios web de compra-venta de muebles, y casas prefabricadas (construcción / residencia / muebles) y finalmente, páginas protección medio-ambiental, mascotas, etc... (Naturaleza / medio ambiente).

Páginas privadas: Esta categoría de contenido engloba a páginas de carácter personal, así como a los servidores para el alojamiento de este tipo de páginas (páginas privadas).

Búsqueda de empleo: Esta categoría permite restringir el acceso a páginas de ofertas de empleo, agencias laborales, oficinas de empleo, empresas de trabajo temporal, etc. (búsqueda de empleo).

Finanzas / Inversiones: Esta categoría de contenido incluye páginas de información bursátil, (bolsa / seguimiento de mercados financieros), agentes de bolsa (información sobre inversiones y finanzas) y banca en Internet (bancos / banca online).

Armas: Esta categoría permite restringir el acceso a páginas relacionadas con todo tipo de armas de fuego y de fogueo, o armas blancas (armas).

Medicina: Esta categoría permite restringir el acceso a páginas de hospitales, médicos, farmacias, psicología, enfermería, tiendas de comida sana y medicina en general (salud, vida sana y nutrición).

Aborto: Esta categoría permite restringir el acceso a páginas sobre el aborto.

Una vez analizado las categorías de filtrado web se sugiere el acceso a los siguientes contenidos según el perfil de usuario:

Tabla 19. Categorías de filtrado web.

NIVEL	USUARIO	CATEGORÍA
Nivel 1	**Directivos**	Compras, Sociedad/Educación/Religión, Juegos, Redes sociales, Entretenimiento/Cultura, Información y comunicación, Tecnologías de la información, Estilo de vida, Finanzas/Inversiones.
Nivel 2	**Empleados**	Sociedad/Educación/Religión, Cultura, Información y comunicación, Tecnologías de la información.
Nivel 3	**Docentes**	Sociedad/Educación/Religión, Cultura, Información y comunicación, Tecnologías de la información.
Nivel 4	**Estudiantes**	Educación, Cultura, Información, Tecnologías de la información.

1. Alcance.

Aplica a todos los miembros de la comunidad universitaria, incluyendo empleados, docentes, estudiantes, administrativos, contratistas, trabajadores temporales y cualquier otro ente autorizado por la institución para hacer uso de los laboratoritos de cómputo.

2. Documentos de referencia.

RE-01G Registro de docentes por uso de laboratorios.

RE-02G Registro de estudiantes por uso de laboratorios.

3. Descripción de la Política.

La presente política permitirá regular la presentación de los servicios y el funcionamiento de los laboratorios de cómputo de la Universidad Técnica de Cotopaxi, así como facilitar y optimizar el uso de las TIC's, de acuerdo a las necesidades de la comunidad universitaria.

Los laboratorios de cómputo dependen directamente de Departamento de Tecnología y/o de la Unidades Académicas a las que se deban.

Sobre la administración.

- Los administradores de los laboratorios son los encargados del control de los laboratorios de cómputo.
- El administrador de los laboratorios tendrá como funciones:
- Regular el acceso a los laboratorios de cómputo.
- Administrar los recursos que forman parte de los laboratorios de cómputo y accesorios que en ellos se utilicen (equipos, mobiliario, impresoras, útiles de oficina, etc.).
- Garantizar el buen funcionamiento de los equipos en cada laboratorio de cómputo.
- Realizar el mantenimiento preventivo y correctivo periódico de los equipos de cómputo que conforman los laboratorios.
- Controlar el buen uso de los equipos por parte de los usuarios.

- Garantizar un ambiente adecuado para el desarrollo de las actividades académicas y administrativas.
- Garantizar el orden de los laboratorios de cómputo. Antes y después de una sesión de trabajo.
- Determinar los cupos de usuarios en cada laboratorio de cómputo, establecer horarios de servicio y horarios asignados a uso de internet.

Unidades Académicas

- Los horarios académicos serán planificados por las unidades académicas en coordinación con los administradores de los laboratorios de cómputo.
- La unidad académica deberá entregar los horarios académicos de los laboratorios de cómputo al departamento de tecnología 15 días antes de iniciar el ciclo académico.
- Servicios de los laboratorios de cómputo.
- Disponibilidad de equipos para actividades de clase e investigación.
- Disponibilidad de equipos con acceso a internet y/o uso de programas informáticos.
- Préstamo a entidades que requieran los espacios de los laboratorios de cómputo, previa autorización del señor Rector y disponibilidad institucional.
- Para prácticas e investigación de estudiantes, docentes, administrativos y trabajadores según la disponibilidad de los laboratorios de cómputo.

Utilización eventual de los laboratorios de cómputo

- Dirigidas a actividades de capacitación y/o actualización a la comunidad universitaria y público en general, se deberá realizar la solicitud correspondiente al departamento de tecnología con 48 horas de anticipación para su coordinación, previa autorización del señor Rector, Vicerrector, de acuerdo a la disponibilidad institucional.
- Para programar actividades de capacitación y/o actualización en los laboratorios de cómputo en el cual requiera un determinado tipo de software, se deberá realizar la solicitud y correspondiente entrega del mismo, al departamento de tecnología con una semana de anticipación para su coordinación, autorización e instalación.
- Los servicios de uso de software estarán suspendidas en el caso de herramientas que cuenten con autorización legan (llámese licencias de uso).

Préstamo de equipos.

- Solo se prestara los equipos a los responsables de proyectos de investigación o áreas administrativas y estará sujeto a la disponibilidad de los mismos. Para ello, deberá solicitar por escrito al departamento de tecnología, quien asignara al funcionario responsable para que coordine y elabore el acta de entrega-recepción con las correspondientes firmas de resguardo de los bienes por el tiempo requerido.

De los usuarios.

- Para tener derecho al uso de los servicios y de las instalaciones de los laboratorios de cómputo, el usuario deberá presentar la identificación institucional vigente que otorga la Universidad o cédula de identidad.
- Cuando los usuarios requieran equipos para aplicaciones informáticas o internet, la asignación de estos serán de acuerdo a la disponibilidad de los laboratorios.
- El acceso a las horas de clases se realizara de forma ordenada y en compañía del docente, previa reservación al inicio del ciclo académico, en los horarios establecidos. El tiempo de tolerancia para ingresar será de 10 minutos y deberá desocupar los laboratorios de cómputo inmediatamente después de terminar el tiempo de las horas clase, previa revisión del correcto funcionamiento de los equipos.
- El docente será responsable del comportamiento de los alumnos en el área de los laboratorios de cómputo.
- El alumno deberá acudir al área de registro correspondiente, con sus credenciales para solicitar el equipo de cómputo que se le designe para aplicaciones informáticas o internet para un tiempo máximo de dos (2) horas.
- El alumno que se encuentre legal mente matriculado, tendrá derecho a hacer uso de los equipos de los laboratorios en los horarios disponibles.
- El docente que desee realizar evaluaciones o actividades académicas extras fuera de sus horas clase asignadas, deberá realizar una solicitud de reservación por escrito al funcionario responsable del laboratorio, por lo menos con 48 horas de anticipación.
- El software disponible con licencias en los laboratorios es propiedad de la Institución, quedando estrictamente prohibida su reproducción total o parcial.

- Los administradores de los laboratorios no se hacen responsables por el material u objetos personales olvidados en los mismos.
- El uso de los equipos será máximo para dos usuarios por computador.
- Contribuir a mantener en buen estado las instalaciones y los equipos de cómputo.

4. Registros.

Tabla 20. Documentos de referencia para uso adecuado de laboratorios de computación.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-01G	Registro de docentes por uso de laboratorios	Departamento de Tecnología	Oficina Sistemas área de Soporte a usuarios	Secuencial alfabético	Cada vez que exista creación de usuarios en la red	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Reciclaje de papel	Uso interno
RE-02G	Registro de estudiantes por uso de laboratorios	Departamento de Tecnología	Oficina Sistemas área de Soporte a usuarios	Secuencial alfabético	Cada vez que exista creación de usuarios en la red	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Reciclaje de papel	Uso interno

5. Anexos.

N/A.

	REGISTRO DE DOCENTES POR USO DE LABORATORIOS	RE-01G
		Ver. No. 01

Tabla 21. Registro de docentes por uso de laboratorios.

LABORATORIO Y CENTROS DE CÓMPUTO

UNIVERSIDAD TÉCNICA DE COTOPAXI

HOJAS DE CONTROL DE HORAS CLASE/La Matriz ☐ **Bloque Administrativo** ☐ **Bloque "A"** ☐ **Bloque "B"** ☐ **CEYPSA La Maná /Laboratorio Nº.** ☐ **Centro de Cómputo Nº.** ☐

Fecha	Hora Ingreso	Firma Ingreso	Docente Responsable	Cedula de Ciudadania	Ciclo Especialidad	Equipos Usados	Hora Salida	Fima Salida	Tema de Clase	Observaciones

Responsable: Analista de Sistemas. Fecha: 19-07-2019	Aprobación: Director DTIC's. Fecha: 19-07-2019

	REGISTRO DE ESTUDIANTES POR USO DE LABORATORIOS	RE-02G
		Ver. No. 01

Tabla 22. Registro de estudiantes por uso de laboratorios

INGENIERÍA EN SISTEMAS DE INFORMACIÓN
LABORATORIO Y CENTROS DE CÓMPUTO BLOQUE ACADÉMICO [X]

FACULTAD: _____ **CARRERA** _____
DOCENTE: _____ **PERIODO ACADÉMICO [X]**
Ciclo: _____ **Fecha:** _____
Materia: _____ **Hora Entrada:** _____ **Hora Salida:** _____
Tema de Clase: _____ **Software Utilizado:** _____
CENTRO DE COMPUTO Nº [X] **Nº Horas Dictadas:** _____

Nº	APLELLIDOS Y NOMBRES	N° CÉDULA	N° PC	FIRMA
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				

Observaciones: _____

Firmas:

_____ _____
Docente Responsable **Administrador**

Responsable: Analista de Sistemas. Fecha: 19-07-2019	Aprobación: Director DTIC's. Fecha: 19-07-2019

11. ANÁLISIS DE RESULTADOS

El proceso de recolección de información para el desarrollo del proyecto se lo realizo directamente en la Dirección de TIC's, por ser considerada como soporte fundamental para el procesamiento y almacenamiento de datos. Para la recopilación de datos, se utilizó la técnica de la entrevista y la observación.

Mediante la entrevista directa se pudo recopilar información de los administradores de tecnología de información y comunicación de la universidad técnica de Cotopaxi en la cual se ha obtenido resultados relevante. La observación fue un elemento fundamental en todo el proceso investigativo, en ella se apoya el investigador para obtener un mayor número de datos, tomando la información y registrándola para su posterior análisis.

11.1. Análisis de las entrevistas aplicadas

Cabe mencionar que se considera muy importante el criterio de la persona entrevistada, pues es quien posee el nivel de conocimiento de los procesos que se llevan a cabo en la institución.

A continuación se muestran los datos obtenidos al realizar la entrevista al Director del Departamento de TIC's.

Tabla 23. Ficha de entrevista directa

FICHA DE ENTREVISTA DIRECTA	
Entrevistado:	Ing. Xavier Andrade
Lugar:	Universidad Técnica de Cotopaxi, Dirección de TIC's
Objetivo:	Recopilar información de cómo se lleva a cabo el proceso de la seguridad informática de la Universidad Técnica de Cotopaxi.
Entrevistador:	Darío Tulmo

Pregunta	**Interpretación**
1. **¿La universidad cuenta con políticas de seguridad informática?**	"En efecto la universidad cuenta con políticas de seguridad informática."

2. ¿Utilizan algún sistema o software para el almacenamiento de la información?	"Si la institución cuenta con un sistema para respaldar la información, el nombre del sistema es **SI UTC**, el cual fue desarrollado por el mismo personal de la institución y es el que actualmente se encuentra en funcionamiento."
3. ¿Utilizan algún servidor para almacenar la información?	"Por supuesto"
4. ¿Con que frecuencia se realiza el resguardo de información?	"La frecuencia con la que se respalda la información es a diario."
5. ¿Podría mencionar como se lleva a cabo el respaldo de la información?	"El responsable de base de datos en el área de desarrollo es quien se encarga de llevar a cabo los procedimientos para respaldar la información a diario."
6. ¿La Universidad cuenta con herramientas para realizar filtrado web?	"La universidad posee equipos de seguridad a todo nivel, cuenta con equipos de seguridad perimetral, seguridad de los equipos de conectividad, la información tiene q pasar por un sin número de barreras como lo es el firewall, antivirus y las políticas de seguridad que posee cada equipo de cómputo."
7. ¿La Universidad utiliza filtrado web?	"En los equipos existen políticas de seguridad para filtrar la información, por ejemplo páginas con contenido pornográfico se encuentran bloqueadas a los usuarios."
8. ¿Es importante establecer filtros web que restringan el acceso a internet?	"Es necesario restringir el acceso de internet a los estudiantes, ya que la información que se encuentra ahí es muy extensa y de todo nivel, por ende se debe establecer filtros web que controle la información que se busca."

9. ¿La Universidad establece categorías de filtrado web para el acceso a internet?	"No se establecen categorías de filtrado web"
10. ¿Cuenta la institución con un Data Center?	"Si"
11. ¿La Dirección de TIC's se encarga de dar mantenimiento al Data Center?	"En efecto todo lo que corresponde al mantenimiento del Data Center lo realiza el personal de la Dirección de TIC's, excepto la parte eléctrica que eso lo realiza personal especializado. "
"El tipo de mantenimiento que se da al Data Center es preventivo garantizando así buen funcionamiento y fiabilidad. También se realiza mantenimiento correctivo cuando se da el caso de corregir los defectos que se van presentando en los distintos equipos. Además los encargados del mantenimiento llevan una bitácora donde registran la fecha de cada mantenimiento."	
12. ¿Cuenta la institución con un AD (Active Directory)?	"Se encuentra en planificación, pero por falta de recursos no se ha logrado aún su implementación."
13. ¿La institución cuenta con un VPN?	"La universidad no cuenta en si con una VPN, lo que usan son teléfonos por canales de datos los cuales se comunican con la extensión de La Mana y el campus Salache, y se pueden comunicar con una extensión telefónica de telefonía IP."
14. ¿Qué tipo de base de datos utiliza la universidad?	"La base de datos que utiliza la institución es software de paga (con licencia)."

Fuente: El investigador

11.2. Resultado de las entrevistas

Tabla 24. Ficha de entrevista directa (Resultados)

FICHA DE ENTREVISTA DIRECTA	
Entrevistado:	Ing. Xavier Andrade
Lugar:	Universidad Técnica de Cotopaxi, Dirección de TIC's
Objetivo:	Recopilar información de cómo se lleva a cabo el proceso de la seguridad informática de la Universidad Técnica de Cotopaxi.
Entrevistador:	Darío Tulmo
RESULTADOS	
1. ¿La universidad cuenta con políticas de seguridad informática? El resultado de esta pregunta fue que sí, la universidad cuenta con políticas de seguridad informática.	
2. ¿Utilizan algún sistema o software para el almacenamiento de la información? El resultado de la pregunta es que la institución cuenta con un sistema llamado **SI UTC** para respaldar la información.	
3. ¿Utilizan algún servidor para almacenar la información? El resultado de la pregunta es que si poseen servidores para almacenar la información.	
4. ¿Con que frecuencia se realiza el resguardo de información? El resultado de esta pregunta es que la información se respalda a diario.	
5. ¿Podría mencionar como se lleva a cabo el respaldo de la información? Se obtuvo como resultado que el responsable de base de datos se encarga de llevar a cabo los procedimientos para respaldar la información a diario.	
6. ¿La Universidad cuenta con herramientas para realizar filtrado web?	

Se obtuvo como resultado que la universidad si cuenta con herramientas para filtrado web.
7. ¿La Universidad utiliza filtrado web? El resultado fue que la institución si utiliza filtrado web para restringir el acceso a internet.
8. ¿Es importante establecer filtros web que restringan el acceso a internet? El resultado para esta pregunta fue que sí, que es importante establecer controles que regulen el acceso a internet.
9. ¿La Universidad establece categorías de filtrado web para el acceso a internet? El resultado de esta pregunta fue que la institucion no establece categorías de filtrado web.
10. ¿Cuenta la institución con un Data Center? El resultado de esta pregunta es que si poseen un Data Center.
11. ¿La Dirección de TIC's se encarga de dar mantenimiento al Data Center? El resultado aquí fue que la Dirección de TIC's, es responsable del mantenimiento del Data Center, excepto la parte eléctrica que eso lo realiza personal especializado.
12. ¿Cuenta la institución con un AD (Active Directory)? El resultado fue que la institución no cuenta con Active Directory.
13. ¿La institución cuenta con un VPN? El resultado fue que la universidad no cuenta en si con una VPN, solo usan son teléfonos por canales de datos los cuales se comunican por telefonía IP.
14. ¿Qué tipo de base de datos utiliza la universidad? El resultado fue que la base de datos que utiliza la institución es software de paga (con licencia).

Fuente: El investigador

11.3. Observaciones a verificar

Tabla 25. Ficha de observación

FICHA DE OBSERVACIÓN	
Fecha:	**8 de julio de 2019**
Elabora:	**Darío Tulmo Checa**
Lugar:	**Universidad Técnica de Cotopaxi**

Aspectos a Verificar	**Resultados Esperados**
La universidad posee políticas de seguridad informática.	Se verifico de la existencia mediante la entrevista realizada.
Control de Acceso a los equipos y sistemas de cómputo.	Se observó que los equipos de cómputo cuentan con dos tipos de cuenta la de administrador y la de invitado y ambas poseen claves y contraseñas que restringen el acceso de personal no autorizado.
Active Directory	Se comprobó mediante la entrevista que la institución no cuenta con uno.
Sistema para respaldar la información.	Ingresando al sitio web de la universidad en la parte de aplicaciones se comprueba efectivamente que se usa el sistema **SIUTC**.
Frecuencia de respaldo de información	Mediante la entrevista se verifico que el respaldo de información se la hace a diario.
Seguridad a componentes informáticos.	Esto se verifica constantemente al ingresar a la universidad ya que esta cuenta con cámaras de seguridad las cuales registran la entrada y salida de todo el personal, además de que cada estación de trabajo cuenta con normas para proteger la integridad de los equipos.

Filtrado web	Mediante un Smartphone o computador de escritorio se verifico que la institución cuenta con un Web Filter. Ya que se trató de ingresar a paginas no autorizadas.
Categorías de filtrado web	Mediante un Smartphone o Laptop se verifica que no existen categorías de filtrado web ya que la señal inalámbrica de la institución se encuentra disponible para todos los usuarios.
Uso adecuado de laboratorios de computación.	Todos los laboratorios cuentan con reglas de seguridad al momento de ingresar y permanecer en los laboratorios y centros de cómputo de la institución.

Fuente: El investigador

En base al análisis de resultados de las entrevistas dirigidas al encargado de la Dirección de TIC's, se ve la necesidad, de diseñar un modelo de políticas de seguridad informática, la cual abarcará aspectos sobre el control de acceso a los de equipos y sistemas de computacionales, Active Directory, administración de activos, resguardo de información, seguridad a los componentes informáticos, uso adecuado de internet y uso adecuado de laboratorios de computo.

El correcto análisis y diseño de las políticas contribuirá a que la institución permanezca en constante funcionamiento, y que mantenga siempre la integridad, confiabilidad, y disponibilidad de la información. El diseño de las políticas de seguridad será de gran ayuda para contrarrestar posibles riesgos y amenazas que se puedan presentar en la institución.

12. IMPACTOS TÉCNICOS, SOCIALES Y ECONÓMICOS

12.1. Impacto técnico

Se diseñó un modelo de policías de seguridad informática utilizando la norma ISO 27001, las cuales servirán para mitigar los riesgos y amenazas que puedan ocurrir en la Universidad, permitiendo proteger la confidencialidad, integridad y disponibilidad de la información.

12.2. Impacto social

Las políticas de seguridad informática son de gran importancia en las organizaciones ya que permiten proteger los activos de la información frente a cualquier situación que suponga un riesgo o amenaza, permiten controlar el acceso a los equipos y sistemas computacionales, reduciendo las amenazas y riesgos presentes en las instituciones.

12.3. Impacto económico

Por medio del diseño de las políticas de seguridad de la información, se podrán reducir los costos de fuga o pérdida de datos, problemas con los equipos de cómputo y/o dispositivos electrónicos y los costos asociados a solucionar este tipo de problemas contratando personal especializado.

13. PRESUPUESTO PARA EL PROYECTO DE INVESTIGACIÓN

13.1. Gastos Directos

Tabla 26. Gastos Directos.

Descripción:	Cantidad:	Valor Unitario ($):	Valor Total ($):
Hojas de papel Bond	2 Resmas	4	8,00
Impresiones	300	0,08	24,00
Copias	150	0,02	3,00
Esferos	2	0,45	0,90
Anillados	3	5,00	15,00
Conexión Internet	5 Meses	18,00	90,00
Empastados del proyecto	3	10,00	30,00
Computador	1 Laptop HP	Uso diario	0,00
Sub Total			170,90
IVA 12%			20,51
Total Gastos Directos:		$ 37,55	**$ 191,41**

Fuente: El investigador

13.2. Gastos Indirectos

Tabla 27. Gatos Indirectos.

Descripción:	Valor:
Movilidad	$ 30,00
Alimentación	$ 40,00
Total:	**$ 70,00**

Fuente: El investigador

13.3.Gastos Totales del Proyecto

Tabla 28. Presupuesto Total del Proyecto.

Gastos:	Total:
Gastos Directos	$ 191,41
Gastos Indirectos	$ 70,00
10% de Imprevistos	$ 30,00
Total Presupuesto:	**$ 291,41**

Fuente: El investigador

14. CONCLUSIONES Y RECOMENDACIONES

14.1. Conclusiones

- ✓ Poseer conocimientos sobre metodologías y mecanismos de seguridad informática es de suma importancia ya que las tecnologías de la información y comunicación avanzan a pasos agigantados y es sustancial para la institución contar con elementos que ayuden a resguardar la información de forma adecuada, confiable y segura.
- ✓ La Universidad Técnica de Cotopaxi al contar con el diseño de políticas de seguridad informática, podrá contar con una guía para contrarrestar los riesgos a los cuales se encuentra expuesta y además sirven como pauta para la utilización correcta de los recursos informáticos con los que cuentan la institución.
- ✓ El diseño de las políticas de seguridad informática tuvo como base la utilización de la norma ISO/IEC 27001:2013, la cual tiene como propósito el aseguramiento, la confidencialidad e integridad de la información y de los sistemas que la procesan.

14.2. Recomendaciones

- ✓ La Universidad Técnica de Cotopaxi cada cierto tiempo deberá realizar un análisis de riesgo, para reconocer potenciales amenazas. Este periodo de tiempo deberá establecerse según el impacto de riesgo en el que se encuentre la institución, pues la seguridad que se requiere proporcionar es permanente para lo cual es necesario de un proceso continuo.
- ✓ Realizar auditorías a la seguridad informática de la institución para conocer sus vulnerabilidades y que procedimientos seguir para minimizar los riesgos.
- ✓ Concientizar a todo el personal (Empleados, Docentes, Estudiantes, etc.) de la institución sobre las políticas de seguridad informática, para contribuir al cumplimento de las mismas, mitigar los riesgos a los cuales se encuentran expuestos y reducir los costos que se deriven por algún suceso informático.

15. BIBLIOGRAFÍA

Aguilera, P. (2011). Redes seguras (Seguridad informática). Madrid, España: Editex.

Aguirre, J. R. (2006). Libro electrónico de seguridad Informática y Criptografía. Madrid, España: Universidad Politécnica de Madrid.

Apréa, J. F. (2010). Windows Server 2008: arquitectura y gestión de los servicios de dominio Active Directory (AD DS). Ediciones ENI.

Cabrera, J.I. (14 de 01 de 2019). 12 ataques informáticos que nos pusieron en jaque en el último año. Obtenido de nobbot: https://www.nobbot.com/redes/ataques-informaticos/

Chaves, A. (2017). RESGUARDAR LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL DOCUNET EN LA EMPRESA CONTACTAR - PASTO. BOGOTA. Obtenido de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12691/3/98400266.pdf

Chiesa, F. (2004). Metodología para selección de sistemas ERP. Reportes técnicos en ingeniería del software, 6(1), 17-37.

EL COMERCIO, (2019). Ecuador denuncia 40 millones de ciberataques tras retiro de asilo a Assange. Obtenido de EL COMERCIO: https://www.elcomercio.com/actualidad/ecuador-denuncia-millones-ciberataques-assange.html

Gómez, A. (2014). Enciclopedia de la Seguridad Informática. Segunda edición, Madrid, España.

ISOTools. (2019). Software ISO Riesgos y Seguridad. Recuperado el 05 de Mayo de 2019, de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

López, P. A. (2011). Seguridad del hardware (Seguridad informática). Editex.

NORMAS ISO, (2014). ISO 27001 SEGURIDAD DE LA INFORMACIÓN. Obtenido de https://www.normas-iso.com/iso-27001/

Pareja, D. (2014). Políticas de seguridad informática en las empresas. Obtenido de https://www.grafitto.es/politicas-de-seguridad-informatica-en-las-empresas/

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., Murillo, A., Castillo, M., (2018). Introducción A La Seguridad Informática Y El Análisis De Vulnerabilidades. Primera edición. Manabí, Ecuador.

Rouse, M. (2018). GOOGLE ACADEMICO. Obtenido de GOOGLE ACADEMICO: http://www.uleam.edu.ec/wp-content/uploads/2016/10/Politica-de-Uso-de-Internet.pdf

Segovia, A. (2014). ¿Qué es norma ISO 27001? Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001/

Universidad Técnica de Cotopaxi, (2017). CONTRATACIÓN ANUAL DEL SERVICIO DE INTERNET EN INTERCONEXIÓN DE DATOS PARA LOS TRES CAMPUS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI. Obtenido de la Universidad Técnica de Cotopaxi: http://www.utc.edu.ec/Portals/0/BELEN/PDF/Contrato%202017%20Internet.pdf?ver=2017-05-23-120052-573

ANEXOS

Universidad Técnica de Cotopaxi

Ingeniería Informatica Y Sistemas Computacionales

Latacunga, 22 de julio de 2019

Estimado

Ing. Javier Andrade

DIRECTOR DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

Presente.

De mi consideración.

Por medio de la presente hago entrega del Proyecto de Investigación titulado **"DISEÑO DE UN MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD TÉCNICA DE COTOPAXI",** realizado en el presente semestre por el estudiante **TULMO CHECA DARÍO WLADIMIR**, portador de la cédula de identidad **050364202-7**, en el cual se hace mención las siguientes políticas:

- ✓ **PO-1A:** Política Control de acceso a recursos computacionales.
- ✓ **PO-1B:** Política Active directory.
- ✓ **PO-1C:** Política Administración de activos de tecnología de información.
- ✓ **PO-1D:** Política Resguardo de la información.
- ✓ **PO-1E:** Política Seguridad a componentes informáticos.
- ✓ **PO-1F:** Política Uso adecuado de internet.
- ✓ **PO-1G:** Política Uso adecuado de laboratorios de computación.

Firma

Anexo 1: Glosario de términos.

Tabla 29. Glosario de términos.

TERMINO	DEFINICIÓN
Acceso remoto	Es poder acceder desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar, a través de una red local o externa (como Internet).
Active Directory (AD)	Es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.
Activo Fijo	Corresponde a la propiedad, planta y equipo tangible que posea una entidad para su uso en producción o suministro de servicios, para arrendarlos a terceros o para propósitos administrativos; y, que se espere usar durante más de un ejercicio económico.
Autenticación	Es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadores.
Backup completo	Se realiza una copia integral de los datos, copiando todos los contenidos de los sistemas a mantener.
Backup diferencial	Partiendo de una copia de backup completa, se realiza una copia de todos los datos modificados desde que se hizo ese backup completo.
Backup incremental	Partiendo de una copia de backup completa, se realiza una copia sólo de los datos modificados desde el último backup (sea completo o incremental).
Confidencialidad	Es asegurar que la información es accedida sólo por las personas autorizadas para ello.

Directivas de Grupo (GPO: Group Policy Object)	Permiten implementar configuraciones específicas para uno o varios usuarios y/o equipos. Controla lo que los usuarios pueden y no pueden hacer en un sistema informático.
Disponibilidad	Es asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando éstos sean requeridos.
Dominio	Un dominio tiene un nombre único y permite el acceso a las cuentas de usuario mantenidas por el "Administrador" del dominio; cada dominio tiene sus propias directivas de seguridad y relaciones de seguridad con otros dominios, y representa el límite de seguridad en una red; los dominios suelen representar la estructura lógica de la organización.
Enajenar	Vender, donar o ceder el derecho o el dominio que se tiene sobre un bien o una propiedad.
ERP	Es una aplicación informática que permite gestionar todos los procesos de negocio de una compañía en forma integrada. Sus siglas provienen del término en inglés Enterprise Resource Planning, o bien, Planeamiento de Recursos Empresariales.
Filtro web	Comúnmente conocido como "software de control del contenido", es un software diseñado para restringir los sitios web que un usuario puede visitar en su equipo.
Fortinet	"Fortinet Inc." ofrece variedad de productos de seguridad y un servicio de filtros web, que permite restringir el acceso a los sitios web considerados inadecuados.
Inconsistencia	Se refiere a que la información que se respalde, permitirá su restauración posterior sin contener errores lógicos o físicos.
Integridad	Es la protección de la exactitud y estado completo de los activos.

Inventario	Conteo, identificación física de los activos.
LCD	Pantalla de cristal líquido o LCD (sigla del inglés Liquid Crystal Display) es una pantalla delgada y plana formada por un número de píxeles en color o monocromos colocados delante de una fuente de luz o reflectora.
Meraki	El sofisticado filtrado de contenido de Cisco Meraki permite a los usuarios de su red disfrutar de los beneficios de Internet mientras se mantienen protegidos de contenido inapropiado o dañino, manteniendo la productividad y el cumplimiento de los requisitos comerciales y normativos aplicables.
Paquetes MSI (Microsoft Installer)	Se definen como instaladores de Microsoft, es decir, aquellos paquetes de software que contienen la información necesaria para automatizar su instalación sin necesidad de intervención manual del usuario en dicho proceso, pues toda esa información ya va contenida en el propio fichero **"msi"**.
Parches	Un parche consta de cambios que se aplican a un programa, para corregir errores, agregarle funcionalidad, actualizarlo, etc.
Regedit.exe	Es el editor del registro de Windows de 16 bits, que se usa para modificar la base de datos de registro de Windows. La base de datos se encuentra en el directorio de Windows y se denomina REG.DAT.
Respaldo	Es la copia de información a un medio del cual se puede recuperar y restaurar la información.
Systemd	Systemd dispone del servicio systemd-tmpfiles para crear, borrar y limpiar archivos y directorios temporales.
TIC's	Son todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información, mediante diversos soportes tecnológicos.

Unidades Organizativas (UO)	Es un objeto contenedor de Active Directory que se utiliza en los dominios; las unidades organizativas son contenedores en los que pueden ubicarse usuarios, grupos, equipos y otras Unidades Organizativas, pudiendo contener únicamente objetos de su dominio principal; una unidad organizativa es el ámbito más pequeño al que se puede aplicar una directiva de grupo.
Usuario final	Persona para la que se diseña un software o un dispositivo de hardware, aquella persona que utiliza el computador para manipular toda la información de una compañía o entidad.
VPN (Virtual Private Network)	Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar estas redes para que sus empleados, desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían.
WAP o AP (Wireless Access Point)	Es un punto de acceso inalámbrico, en una red de computadoras, es un dispositivo de red que interconecta equipos de comunicación inalámbricos, para formar una red inalámbrica que interconecta dispositivos móviles o tarjetas de red inalámbricas.

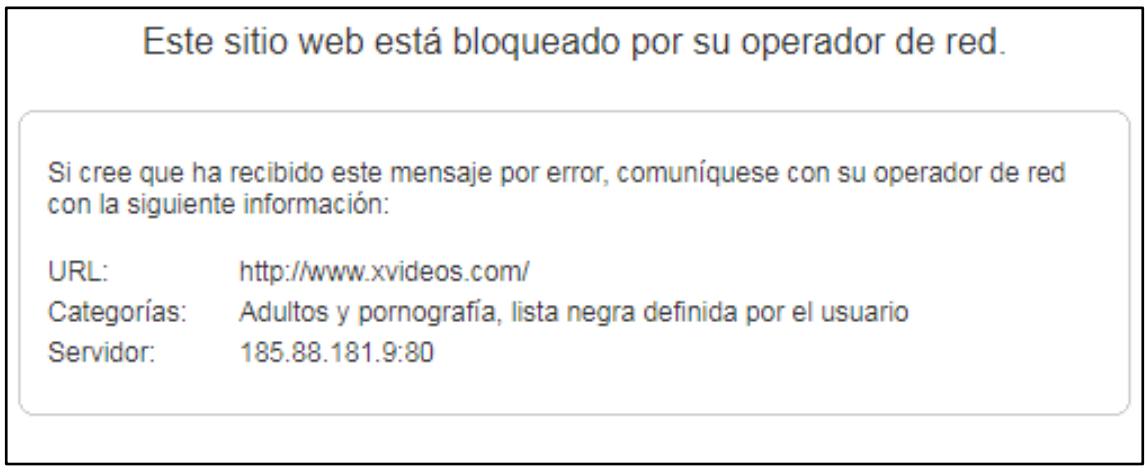
Anexo 2: Filtrado Web

Al ingresar a una página no apropiada dentro de la universidad, el filtrado web mostrara el siguiente mensaje:

Teléfonos móviles.

Fuente: El investigador

Computadoras de la institución.



Fuente: El investigador

Anexo 3: Entrevista.

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

Entrevista dirigida para el personal encargado del Departamento de Servicios Informáticos de la UTC.

Fecha: _____/_____/_____

Nombre del Entrevistado: _____

Objetivo: Recopilar información de cómo se lleva a cabo el proceso de la seguridad informática de la Universidad Técnica de Cotopaxi.

1. **¿La universidad cuenta con políticas de seguridad informática?**
2. **¿Utilizan algún sistema o software para el almacenamiento de la información?**
3. **¿Podría mencionar el nombre del sistema que utilizan?**
4. **¿Utilizan algún servidor para almacenar la información?**
5. **¿Con que frecuencia se realiza el resguardo de información?**
6. **¿Podría mencionar como se lleva a cabo el respaldo de la información?**
7. **¿La Universidad cuenta con herramientas para realizar filtrado web?**
8. **¿La Universidad utiliza filtrado web?**
9. **¿Es importante establecer filtros web que restringan el acceso a internet?**
10. **¿La Universidad establece categorías de filtrado web para el acceso a internet?**
11. **¿Cuenta la institución con un Data Center?**
12. **¿La Dirección de TIC's se encarga de dar mantenimiento al Data Center?**
13. **¿Cuenta la institución con un AD (Active Directory)?**
14. **¿La institución cuenta con un VPN?**
15. **¿Qué tipo de base de datos utiliza la universidad?**