UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

PROPUESTA TECNOLÓGICA

TEMA:

DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, BASADO EN LA NORMA ISO 27000

Propuesta Tecnológica presentada previo a la obtención del Título de Ingenieros en Informática y Sistemas Computacionales

AUTORES:

Álvarez Marcalla Williams Manuel

Llulluna Chasipanta Johnny Danilo

DIRECTOR DE TESIS:

Ing. Mg. Jorge Bladimir Rubio Peñaherrera

LATACUNGA – ECUADOR

2021

DECLARACIÓN DE AUTORÍA

Nosotros, **Álvarez Marcalla Williams Manuel** con C.I.: 175156349-3 **y Llulluna Chasipanta Johnny Danilo** con C.I.: 172303055-5, declaramos ser autores del presente proyecto de investigación: **"DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, BASADO EN LA NORMA ISO 27000.",** siendo el Ing. Msc. Rubio Peñaherrera Jorge Bladimir tutor del presente trabajo, 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 investigativos, son de mi exclusiva responsabilidad.

……. **…….**

Álvarez Marcalla Williams Manuel **Llulluna Chasipanta Johnny Danilo**

C.I. 175156349-3 **C.I. 172303055-5**

AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de tutor del trabajo de investigación sobre la titulación:

"DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, BASADO EN LA NORMA ISO 27000", de los estudiantes: Álvarez Marcalla Williams Manuel y Llulluna Chasipanta Johnny Danilo, de la carrera de Ingeniería en Informática y Sistemas Computacionales, considero que dicho informe investigativo cumple con los requerimientos metodológico y aportes científicos – técnicos suficientes para ser sometidos a la evaluación del tribunal de validación de Proyecto que el Honorable Consejo Académico de la Facultad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe , para su correspondiente estudio y calificación.

Latacunga, 04 de agosto del 2021

…….

Ing. Msc. Rubio Peñaherrera Jorge Bladimir

C.C.: 050222229-2

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, los postulantes Álvarez Marcalla Williams Manuel y Llulluna Chasipanta Johnny Danilo con el título de proyecto de Investigación: "**DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, BASADO EN LA NORMA ISO 27000"**, han considerado las recomendaciones emitidas oportunamente y reúnen los méritos suficientes para ser sometidos al acto de Sustentación de Proyecto.

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

Latacunga, 04 de agosto del 2021

……..	……
Ing. Mg Llano Casa Alex	Ing. Mg. Villa Quishpe Manuel
C.C.:	C.C.:

……..

Ing. Mg. Medina Matute Victor

C.C.:

AGRADECIMIENTO

A la universidad que me abrió sus puertas para continuar mis estudios, las oportunidades que me ha concedido son demasiadas y antes de todo eso pensé que iba a ser demasiado difícil el poder llegar hasta aquí

Agradezco a mis maestros que han sido el pilar de mi educación, transmitiéndome todos sus conocimientos, a mis compañeros que con ellos he pasado demasiadas experiencias en mi vida universitaria y se me hubiese hecho difícil llegar hasta aquí sin la ayuda mutua.

WILLIAMS ÁLVAREZ

En primer lugar, agradezco a Dios por ser uno de los pilares fundamentales en mi vida, a mis formadores, personas de gran sabiduría quienes se han esforzado por ayudarme a llegar al punto donde me encuentro, en especial a mi tutor Ing. Msc. Jorge Bladimir Rubio Peñaherrera que con sus sabios conocimientos hizo posible la elaboración y culminación de esta tesis, a mi madre Luz Chasipanta por bridarme su apoyo incondicional y no permitir que me rinda ante ninguna dificultad, a mi padre Williams Llulluna (+) por ser quien en su momento me brindo sus consejos y su apoyo, a mis hermanos por ser parte fundamental en mi vida y mi ejemplo de lucha y perseverancia. A mis abuelitos Edelina Morales y Alejandro Chasipanta (+) mis segundos padres quienes me enseñaron que con esfuerzo, trabajo y constancia todo se consigue. A mi compañero de tesis Williams quien con su apoyo y colaboración se hizo posible la culminación de esta tesis.

JOHNNY LLULLUNA

DEDICATORIA

Dentro de todo mi recorrido universitario he aprendido demasiadas cosas, he desarrollado varias destrezas y habilidades que nunca habría pensado, por eso dedico esta tesis a todos mis compañeros y profesores ya que ellos han sido de gran importancia para obtener los conocimientos necesarios para desarrollarla.

A mis padres porque gracias a su sacrificio me he esforzado tanto desde un comienzo, apoyándome a la distancia con todo lo que necesite, económica y emocionalmente.

A mi tía Carmita Álvarez, que me apoyó en todo lo que necesite y me recibía en su vivienda como si fuese su propio hijo.

WILLIAMS ÁLVAREZ

Dedico este trabajo a Dios por darme la fortaleza y tenacidad para terminar este proyecto, a mi madre Luz Chasipanta y Williams Llulluna (+), mis hermanos Maricela, Paola, Bryan que con sus consejos han formado la persona que soy, a mi sobrina Alejandra que llego a mi vida para ser una mejor, a mis segundos padres Alejandro y Edelina que me inculcaron valores para ser un excelente ser humano.

JOHNNY LLULLUNA

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TITULO: "DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, BASADO EN LA NORMA ISO 27000"

Autores:

Álvarez Marcalla Williams Manuel

Llulluna Chasipanta Johnny Danilo

RESUMEN

La evolución de los sistemas de información hace necesaria el surgimiento de profesionales en el área informática responsable de evaluar su correcto funcionamiento, detectar aquellos puntos débiles que requieran de medidas preventivas y correctivas para evitar pérdidas de información que podrían causar costes importantes a las organizaciones. En la actualidad, las instituciones están expuestas no solo a robo de material o asaltos en sus instalaciones, sino a delitos de seguridad informática que pueden afectar los datos e información relevante de la organización. El presente proyecto de investigación tiene como propósito diseñar una política de seguridad de la información para la Universidad, la cual necesita contar con seguridad y que brinden el suficiente respaldo para proteger la información de la institución. El diseño de políticas de seguridad informática permitirá minimizar riesgos y amenazas, que puedan comprometer el correcto uso de los recursos informáticos como la información, procesos, sistemas y redes. Para esto se utilizó la Norma ISO/IEC 27000 la cual busca la confidencialidad, integridad y disponibilidad de la Información.

Palabras Claves: Normas ISO, Seguridad, Información, Riesgo, Política

TUTOR DE TITULACIÓN
Ing.MSc. Jorge Bladimir Rubio Peñaherrera
CC: 050222229-2

TECHNICAL UNIVERSITY OF COTOPAXI

FACULTY OF ENGINEERING SCIENCES

AND APPLIED

THEME: "DESIGN OF AN INFORMATION SECURITY POLICY FOR INFORMATION AND TECHNOLOGIES DEPARTMENT OF TECHNICAL UNIVERSITY OF COTOPAXI, BASED ON ISO 27000"

Authors:

Álvarez Marcalla Williams Manuel

Llulluna Chasipanta Johnny Danilo

ABSTRACT

The information systems evolution requires the emergence of professionals in IT area responsible to evaluate their correct operation, detecting those weak points that require preventive and corrective measures to avoid loss of information that could cause significant costs to organizations. At present, institutions are exposed not only to material theft or assaults on their facilities, but also to computer security crimes that can affect the organization of data and relevant information. The purpose of this research project is to design an information security policy for the University, which needs to have security and provide sufficient support to protect the information of the institution. The design of computer security policies will allow to minimize risks and threats that may compromise the correct use of computer resources such as information, processes, systems and networks. For this, ISO / IEC 27000 Standard was used, which seeks information, confidentiality, integrity and availability.

Keywords: ISO Standards, Security, Information, Risk, Policy.

AVAL DE TRADUCCIÓN

ÍNDICE GENERAL

PORTADA PROYECTO DE INVESTIGACIÓN i
DECLARACIÓN DE AUTORÍA..... ii
AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN iii
APROBACIÓN DEL TRIBUNAL DE TITULACIÓN iv
AGRADECIMIENTO v
DEDICATORIA..... vi
RESUMEN..... vii
ABSTRACT..... viii
AVAL DE TRADUCCIÓN..... ix
ÍNDICE DE TABLAS xiv
ÍNDICE DE FIGURAS.....xv
ÍNDICE DE ANEXOS..... xvii
1. INFORMACIÓN GENERAL.....18
2. INTRODUCCIÓN 20
2.1. EL PROBLEMA.....20
2.1.1. Situación Problema.....20
2.1.2. Formulación del problema.....21
2.2. OBJETO Y CAMPO DE ACCIÓN.....22
2.3. BENEFICIARIOS.....22
2.4. JUSTIFICACION 22
2.5. HIPÓTESIS.....23
2.6. OBJETIVOS 23
2.6.1. Objetivo General 23
2.6.2. Objetivos Específicos.....23
2.7. SISTEMA DE TAREAS.....24
3. FUNDAMENTACIÓN TEORICA.....25
3.1. SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN ..25
3.1.1. Seguridad de la información 25
3.1.2. Líder u oficial de Sistema de gestión de seguridad de la información - SGSI ...26
3.1.3. Plan de Gestión de Seguridad 28
3.1.4. Mecanismos preventivos en seguridad informática 30
3.1.5. Análisis de Riesgos de la Información.....30

3.1.6 Fases del análisis de riesgo....31
3.1.7. Políticas de seguridad....31
3.1.8. Resguardo de la información....32
3.1.9. Bases de Datos....33
3.2.1. Gestión de Acceso de Usuario....35
3.2.2. Responsabilidades del Usuario....35
3.2.3. Control de Acceso en red....35
3.2.4. Control de Acceso al sistema Operativo....35
3.3. Evaluación de riesgos, amenazas y vulnerabilidad....36
3.4. Normas ISO....36
3.4.1. Certificación ISO....37
3.4.2. Normas ISO 27000....37
3.4.3. Familia ISO 27000....38
3.4.4. Beneficios de las Normas ISO 27000....40
3.5. Software....40
3.5.1. Wireshark....40
3.5.2. The dude....40
4. MATERIALES Y MÉTODOS....41
4.1 TIPOS DE INVESTIGACIÓN....41
4.1.1. Investigación de Campo....41
4.1.2. Investigación Bibliográfica....41
4.2 MÉTODOS DE INVESTIGACIÓN....41
4.2.1. Método Inductivo – deductivo....41
4.2.2. Método Analítico y Sintético....41
4.3 TÉCNICAS DE INVESTIGACIÓN....41
4.3.1. Entrevista....41
4.3.2. Observación....41
4.3.3. Normas ISO 27000....42
4.4 INSTRUMENTOS DE INVESTIGACIÓN....42
4.5 POBLACIÓN Y MUESTRA....42
4.6 DISEÑO DEL MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA 42
5. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS....96
5.1. Análisis de Entrevista Aplicada....96
5.2. Resultados de la entrevista....98

5.3. Análisis de la Observación....100
5.4. Análisis de riesgos de la Universidad Técnica de Cotopaxi....101
5.4.1. Metodología para el análisis de riesgo....101
5.5. Matriz de factores Internos y Externos....104
5.6. Matriz para el análisis de riesgo....106
5.7. Análisis de riesgo promedio....109
5.8. Análisis de trafico de red mediante Wireshark....109
5.9. Plan de mitigación de riesgos....110
6. IMPACTOS TÉCNICOS, SOCIALES Y ECONÓMICOS....112
6.1 Impactos técnicos....112
6.2 Impactos sociales....112
6.3 Impactos económicos....112
7. CONCLUSIONES Y RECOMENDACIONES....113
7.1 CONCLUSIONES....113
7.2 RECOMENDACIONES....113
8. MANUAL DE IMPLEMENTACIÓN DE UN ACTIVE DIRECTORY CON WINDOWS SERVER 2012, SIMULACIÓN....114
8.1. ALCANCE....114
8.2. DESCRIPCIÓN DEL MANUAL....114
8.2.1. Recursos necesarios:....114
8.2.2. Pasos a seguir:....114
9. PLAN DE CONTINGENCIA UTC – POLITICAS DE SEGURIDAD....140
9.1. INTRODUCCION....140
9.2. OBJETIVO....140
9.3. PLAN DE RIESGOS....140
9.3.1. Anàlisis de Riesgo....141
9.3.2. Anàlisis de fallas en la seguridad....142
9.4. POLÌTICAS DE SEGURIDAD....142
9.5. ANÀLISIS Y EVALUACIÓN DE RIESGOS....143
9.5.1. Eventos Considerados para el plan de contingencia....143
9.6. PLAN DE RECUPERACION Y RESPALDO DE LA INFORMACION....148
9.7. PLAN DE RECUPERACION DE DESASTRES....149
9.7.1. Actividades previas al desastre....149
9.7.2. Actividades Durante el desastre....149

9.7.3. Actividades despues del desastre 150
10. BIBLIOGRAFÍA.....151
11. ANEXOS.....153

ÍNDICE DE TABLAS

Tabla 1. *Planificación de las actividades* 24
Tabla 2. Documentos de referencia 48
Tabla 3. Solicitud de creación de usuarios. 51
Tabla 4. Documento de referencia activos. 62
Tabla 5. Inventario de equipos de cómputo y servidores 64
Tabla 6. Inventario de software 66
Tabla 7. Registro de movimiento de equipos. 67
Tabla 8. Registro de baja de equipos. 68
Tabla 9. Bitácora de mantenimiento preventivo de PC's. 69
Tabla 10. Ficha de mantenimiento preventivo de computadores. 70
Tabla 11.Cronograma de mantenimiento preventivo de PC's. 71
Tabla 12. Cronograma de mantenimiento preventivo de Data Center 72
Tabla 13. Documento de referencia para el resguardo de la información. 76
Tabla 14. Bitácora de respaldo de usuarios. 77
Tabla 15. Bitácora de respaldo de Base de Datos. 78
Tabla 16. Cronograma de respaldos de usuarios finales y servidores. 79
Tabla 17. Usuarios declarados para respaldo de información. 80
Tabla 18. Documentos de referencia para la seguridad a componentes informáticos. 83
Tabla 19. Registro de entrada y salida de equipos. 84
Tabla 20. Bitácora de antivirus. 85
Tabla 21. Categorías de filtrado web. 89
Tabla 22. Documentos de referencia para uso adecuado de laboratorios de computación. 93
Tabla 23. Registro de uso de laboratorio Docentes 94
Tabla 24. Registro de uso de laboratorio estudiantes 95
Tabla 25. Ficha de entrevista directa - Aplicada 96
Tabla 26. Ficha de entrevista directa - Resultados 98
Tabla 27. Ficha de Observación 100
Tabla 28. Cuestionario de Factores Internos y Externos 102
Tabla 29. Tabla de rango de calificación de factores internos y externos 104
Tabla 30. Factores Internos 104
Tabla 31. Factores externos 105
Tabla 32. Valoración de Probabilidad de Amenaza 107
Tabla 33. Plan de mitigación de riesgos 110
Tabla 34. Eventos considerados para el plan de contingencia 143

ÍNDICE DE FIGURAS

Figura 1. Orgánico estructural actual- Departamento de TIC - UTC 27
Figura 2. Sistema de gestión de la seguridad de la información 29
Figura 3. Objetivo principal de las políticas de seguridad 32
Figura 4. Diagrama de interconexión Universidad Técnica de Cotopaxi 34
Figura 5. Niveles de riesgo 106
Figura 6. Salvapantalla de programa Wireshark 110
Figura 7. Programa Active Directory. 115
Figura 8. Confirmación de Instalación 115
Figura 9. Promover este servidor a controlador de dominio 116
Figura 10. Agregar un nuevo bosque 116
Figura 11. Controlador de dominio 117
Figura 12. Mensaje de advertencia 117
Figura 13. Dominio de NetBIOS (UTC) 118
Figura 14. Ruta de la ubicación de los archivos 118
Figura 15. Revisar opciones 119
Figura 16. Comprobación de requisitos 119
Figura 17. Reiniciación automática 120
Figura 18. Inicio de sesión 120
Figura 19. Administrador del servidor 121
Figura 20. Usuarios y equipos de Active Directory 121
Figura 21. Nueva Carpeta 122
Figura 22. Nombre de la nueva Unidad 122
Figura 23. Crear Subunidades 123
Figura 24. Crear nuevo objeto 123
Figura 25. Crear Contraseña 124
Figura 26. Crear equipos 124
Figura 27. Unir un cliente-equipo 125
Figura 28. Ingresar las credenciales del primer usuario 125
Figura 29. Unión de dominio 126
Figura 30. Reinicio del equipo 126
Figura 31. Dominio 127
Figura 32. Reiniciar el equipo con Windows 10 127
Figura 33. Información en el sistema 128
Figura 34. Máquina virtual con Windows 8.1 128
Figura 35. Reiniciar la máquina virtual 129
Figura 36. Unidad organizativa 129
Figura 37. Nueva política 130
Figura 38. Ediciones de las políticas 130
Figura 39. Papel tapiz 131
Figura 40. Opción de habilitación 131
Figura 41. Protector de pantalla 132

Figura 42. Impedir instalación 132
Figura 43. Impedir el uso del Símbolo del sistema y PowerShell 133
Figura 44. Centro de Movilidad 133
Figura 45. Restringir el acceso a “Red”. 134
Figura 46. Panel de control. 135
Figura 47. Desactivar eliminación del historial 135
Figura 48. Administrador de tareas 136
Figura 49. Opción Habilitar 136
Figura 50. Reproducción automática de dispositivos extraíbles 137
Figura 51. Windows Installer 137
Figura 52. Configuración para las cuentas de usuario 138
Figura 53. Configuración del bloqueo de cuentas de usuario 139

ÍNDICE DE ANEXOS

Anexo 1: Hoja de vida del tutor.....153
Anexo 2: Hoja de vida de investigadores.....162
Anexo 3: Filtrado Web.....167
Anexo 4. Formulario de Encuesta.....168
Anexo 5: Formulario de Entrevista.....170

1. INFORMACIÓN GENERAL

Titulo:

DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, BASADO EN LA NORMA ISO 27000.

Fecha de Inicio:

Abril 2021

Fecha de Finalización:

Agosto 2021

Lugar de ejecución:

Universidad Técnica d Cotopaxi, Departamento de TIC`S

Unidad Académica que Auspicia:

Facultad de Ciencias de la Ingeniería y Aplicadas

Carrera que Auspicia:

Ingeniería en Informática y Sistemas Computacionales

Proyecto de Investigación Vinculado:

Diseño de una política de seguridad de la información para la dirección de tecnologías de la información de la Universidad Técnica de Cotopaxi, basado en la norma ISO 27000. Para prevenir alguna amenaza que pudiere afectar la información.

Equipo de trabajo:

COORDINADOR:

Nombre: Jorge Bladimir Rubio Peñaherrera.

Nacionalidad: ecuatoriano

Fecha de Nacimiento: Pujilí, 16 de mayo de 1976

Estado Civil: Casado.

Residencia: Pujilí, Calle Gabriel Álvarez 1-13 y Juan José Merizalde.

E-mail: jorge.rubio@utc.edu.ec

Teléfono: 0995220308

Títulos Obtenidos:

PREGRADO: Ingeniero en Informática y Sistemas Computacionales. Universidad Técnica de Cotopaxi.

POSGRADO: Magister en Gerencia Informática, mención Desarrollo de Software y Redes. Pontificia Universidad Católica del Ecuador.

ESTUDIANTES:

1.-Nombre: Álvarez Marcalla Williams Manuel

Nacionalidad: ecuatoriano

Fecha de Nacimiento: 26 de Julio de 1996

Estado Civil: Soltero

Residencia: TENA, MARPINDO Y PITON

Correo: williams.alvarez9128@utc.edu.ec

Teléfono: 0995746464

2.- Nombre: Llulluna Chasipanta Johnny Danilo

Nacionalidad: ecuatoriano

Fecha de Nacimiento: 6/03/1996

Estado Civil: Soltero

Residencia: Pintag - Quito

Correo: johnny_9603@hotmail.com

Celular: 0988210756

ÁREA DEL CONOCIMIENTO:

06 /061 Información y comunicación (TIC) / 0611 El uso del ordenador

LÍNEA DE INVESTIGACIÓN:

Tecnología de la información y comunicación (TIC's)

SUB LÍNEA DE INVESTIGACIÓN DE LA CARRERA:

Diseño implementación y configuración de redes y seguridad computacional aplicando normas y estándares internacionales.

2. INTRODUCCIÓN

2.1. EL PROBLEMA

2.1.1. Situación Problema

En la sociedad actual, donde la información se divulga utilizando las computadoras y las redes, el internet se ha convertido en el principal medio del avance económico, político y social. La vida cotidiana de las personas se ha adaptado a las nuevas tecnologías de la información: así como también dio pasó al campo del ataque cibernético en especial al ciber delito que pone en riesgo la información almacenada.

El ciber delito ha aumentado significativamente a nivel mundial en estas últimas décadas.

Raudales (2017) indicó que los ataques cibernéticos no sólo suceden en países desarrollados o con tecnologías de primer nivel. Indicó que América Latina ha sido víctima en numerosas ocasiones de delitos cibernéticos. En América Latina y el Caribe, el costo de ciberataques asciende a un promedio de US$90.000 millones al año debido a la falta de una política orientada a la respuesta oportuna a incidentes. Citado por Izaguirre & León. [1]

A nivel mundial la información se ha visto afectado por grupos de delincuentes informáticos llamados Hackers, que, debido a la globalización digital, no se ven limitados a ningún ataque, por lo que cualquier país se ve susceptible a recibir ciberataques actualmente con la modalidad del teletrabajo, por la pandemia, trajo consigo un mayor número de ataques. “En Ecuador, el informe ‘ESET Security Report 2020 de Latinoamérica’ indica que el 70% de las empresas en el país reportó incidentes de seguridad.” [2]

Ecuador presenta falencias muy considerables para identificar los riesgos de los ciberataques por ello no se libra de estos programas maliciosos. Según la empresa de seguridad Kaspersky, nuestro país se ha mantenido en la posición 49 dentro de las estadísticas de países con mayores incidencias de software malicioso o malware [2]. Estos datos muestran que nuestro pais tiene una cultura escaza en cuanto a seguridad de la informaciòn.

En la Universidad Técnica de Cotopaxi, existe una amplia infraestructura de TIC’s que permiten el acceso a servicios informáticos que deben cumplir lineamientos para su disponibilidad, por tal motivo surge la necesidad de diseñar un modelo de política de seguridad de la información para el departamento de las TIC’s, ya que la Universidad no está libre de amenazas informáticas esto permitirá proteger la información confidencial, este proceso se realizará utilizando la norma ISO 27000.

La seguridad informática cada vez se convierte en una obligación o política de las instituciones que quieran proteger los datos del usuario.

2.1.2. Formulación del problema

Existen políticas de seguridad en Departamento de las TIC’s de la Universidad Técnica de Cotopaxi, que permitan mantener la información segura, libre de ataques o robos cibernéticos.

2.2. OBJETO Y CAMPO DE ACCIÓN

Objeto:

Política de seguridad de la información basado en la norma ISO27000.

Campo de Acción:

Diseño de una política de seguridad de la información para la dirección de tecnologías de la información de la Universidad Técnica de Cotopaxi, basado en la norma ISO 27000.

2.3. BENEFICIARIOS

Los beneficiarios directos del presente proyecto son el Departamento de la Unidad de TIC`s de la Universidad Técnica de Cotopaxi.

2.4. JUSTIFICACION

En los últimos años, las tecnologías de la Información han penetrado en los distintos sectores; han permitido el desarrollo de un mundo ampliamente digitalizado donde con solo tener un aparato tecnológico conectado a internet que es posible ingresar u obtener información desde cualquier parte del mundo. Esto hace que la humanidad sea cada vez más dependiente a la tecnología por lo que esto hace que existan riesgos y amenazas en los sistemas informáticos.

El proyecto de investigación tiene como finalidad el diseño de políticas de seguridad aplicando normas ISO 27000, para la protección de datos e información de la Universidad Técnica de Cotopaxi, identificando si existen riesgos o amenazas que pongan en peligro la información almacenada de los estudiantes, docentes etc., es así que esta información debe ser resguardada de los ataque o virus que ponen en peligro los sistemas y equipos de la institución. Las políticas son esenciales para el buen manejo de los asuntos de seguridad y forman parte efectiva de medidas de protección tales como: identificación y control de acceso, resguardo de datos, administración de archivos, etc.

Por tal motivo el siguiente proyecto diseñara políticas de seguridad de la información basada en la norma ISO 27000 que sirva como normativas para garantizar la confidencialidad, integridad y disponibilidad de la información. Estas políticas estarán disponibles para ser aplicadas a la comunidad Universitaria o cualquier otro ente autorizado por la institución que haga uso de los recursos informáticos.

2.5. HIPÓTESIS

¿Cuál es el beneficio de diseñar un modelo de políticas de seguridad Informática en el Departamento de TIC’s de la Universidad Técnica de Cotopaxi?

2.6. OBJETIVOS

2.6.1. Objetivo General

Diseñar políticas de seguridad de la información para la gestión de la información y las herramientas informáticas en la dirección de tecnologías de la información de la Universidad Técnica de Cotopaxi, basado en la norma ISO 27000.

2.6.2. Objetivos Específicos

- Recopilar información de la dirección de TIC’s sobre la seguridad informática de la Universidad Técnica de Cotopaxi.
- Analizar la información obtenida para identificar riesgos que afecten al correcto funcionamiento de los equipos y sistemas computacionales.
- Plantear los controles para asegurar el correcto uso de recursos y sistemas por parte del personal encargado del departamento de las TIC’s

2.7. SISTEMA DE TAREAS

Tabla 1. *Planificación de las actividades*

OBJETIVO	ACTIVIDADES	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.	**1.-** Realizar una entrevista al encargado del departamento de la TIC`s **2.-** Analizar la información obtenida.	Fundamentación teórica	Entrevista Observación
Analizar la información obtenida para identificar riesgos que afecten al correcto funcionamiento de los equipos y sistemas computacionales.	**1.-** Analizar los riegos que podría sufrir la información de la institución. **2.-** Conocer como es la seguridad informática de la institución.	Proyecto de Investigación	Investigación Documental Investigación de Campo
Plantear los controles para asegurar el correcto uso de recursos y sistemas por parte del personal encargado del departamento de las TIC's	1.- Desarrollo del diseño de las políticas de seguridad informática. 2.- Utilizar la norma ISO27000.	Diseño de las políticas de seguridad informática	Investigación Documental

Elaborado por: Álvarez Williams y Llulluna Johnny

3. FUNDAMENTACIÓN TEORICA

3.1. SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

La gestión e la información en los actuales momentos requiere de la planificación y asignación de estrategias que involucren actividades encaminadas a la gestión de la información que son sustentadas en normas de calidad con el fin de garantizar la continuidad de las actividades tecnológicas.

"Se espera que la implementación de un SGSI sea proporcional de acuerdo con las necesidades de la organización; por ejemplo, una situación simple requiere una solución de un SGSI sencillo". [3, p. 73]

3.1.1. Seguridad de la información

Actualmente la población puede conectarse a las redes sin ningún inconveniente, es así que las aplicaciones y los softwares son cada vez más accesibles, por lo que la información se vuelve más vulnerable. Cuando hablamos de seguridad de la información tiene una relevancia en un contexto determinado y por tanto hay que proteger, por lo que consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

La seguridad informática se encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa sólo por el medio informático, se preocupa por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático. Romero, et al., [4, pp. 13 - 14]

La seguridad siempre busca la forma de evitar o prevenir cualquier tipo de acciones peligrosas o robo de información, por esto la seguridad debe disponer de medios que permitan reducir los peligros que pueda tener la información. Los hackers y crackers están vigilando a diario las redes con el fin de encontrar las debilidades del sistema de información y así apoderarse de la información llegando a manipular de forma maliciosa toda la información.

Según Aguilera (2011) citado en Romero, et al., [4] "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."

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.

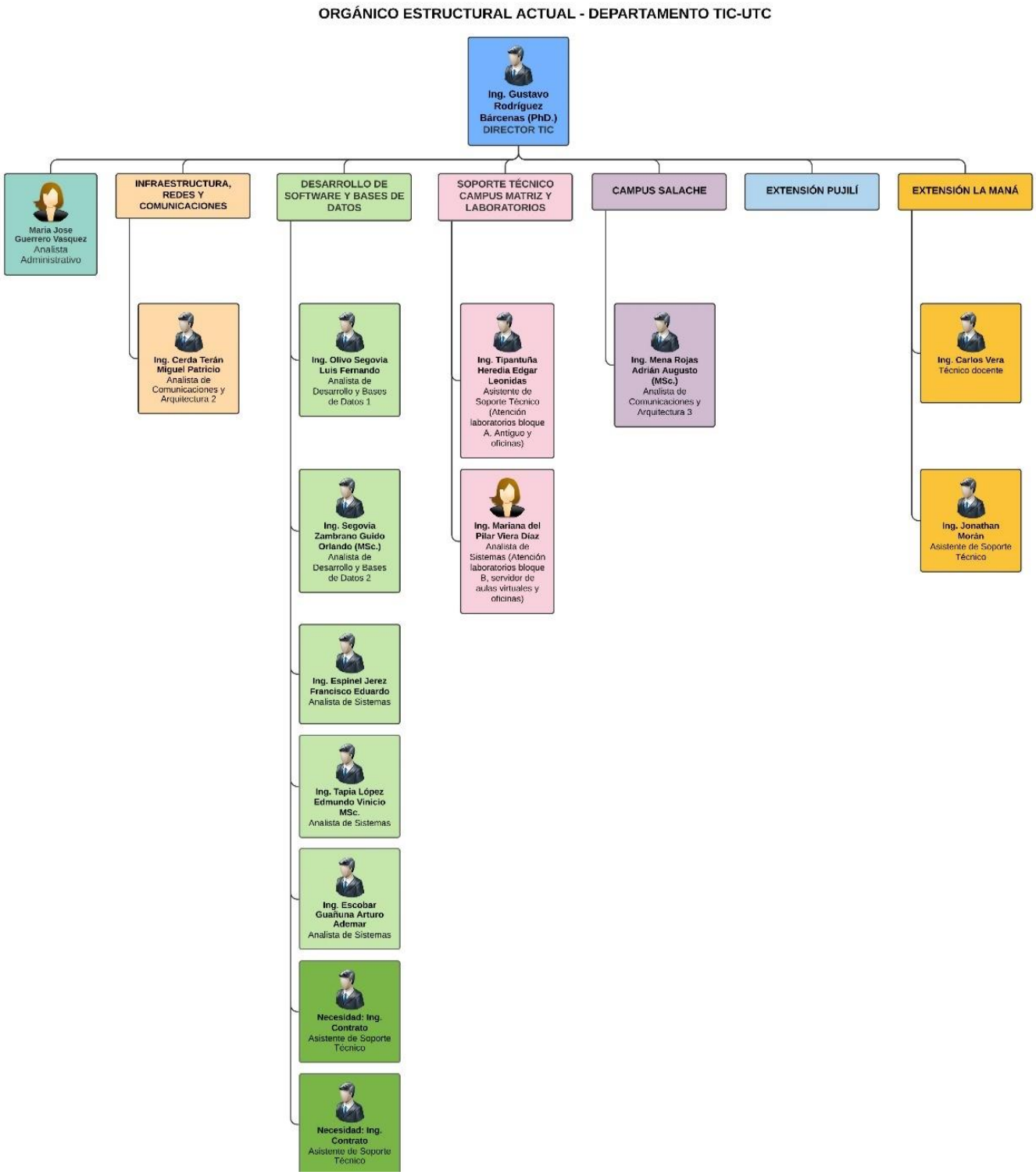
Lo que se debe contemplar la seguridad se puede clasificar en tres partes:

- Los usuarios
- La información
- La infraestructura

3.1.2. Líder u oficial de Sistema de gestión de seguridad de la información - SGSI

El jefe de la oficina de tecnologías de información asignara la responsabilidad correspondiente al rol, el líder u oficial de seguridad de la información a un tercero para efectos de garantizar y liderar la implementación, mantenimiento y mejora del SGSI.

Figura 1. Orgánico estructural actual- Departamento de TIC - UTC



Fuente: Departamento TIC's - UTC

3.1.3. Plan de Gestión de Seguridad

Un plan de gestión es un sistema general establecido por una organización que puede incluir una estructura organizativa de tal manera que los procesos que hay en ella, son verificados y evaluados para determinar la planificación de las actividades del beneficiario que labora en el departamento, además permitirá detallar con un medio físico que dará soluciones ante un caso de emergencia guiara las acciones que se deben tomar para que una organización no se va afectada o por lo menos que el daño sea el más mínimo posible.

La gestión de seguridad ordena los procedimientos, los procesos y recursos con los que tiene una organización para mantener y llevar un mejor control de dichos procesos y de esta manera mantener una política de prevención y calidad de los servicios.

Figura 2. Sistema de gestión de la seguridad de la información

Fuente: Normas ISO

3.1.4. Mecanismos preventivos en seguridad informática

Los mecanismos preventivos son los que nos permite prevenir la ocurrencia de un ataque informático básicamente se concentran en el monitoreo de la información.

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. Los mecanismos preventivos en realidad son a largo plazo y por esta razón son considerados por la mayoría como una pérdida de tiempo y dinero. Romero, et al., [4, p. 18]

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

- **El respaldo de información:** se refiere al resguardo que se realiza de ciertos datos.
- **Horario de respaldo:** Hace referencia a la hora que se puede hacer el respaldo.
- **Control de medios:** El tener acceso a respaldos es algo de alto riesgo, se puede robar información.
- **La comprensión de la información:** No toda la información se puede comprimir.

3.1.5. Análisis de Riesgos de la Información

El análisis de riesgos informáticos es la evaluación de los distintos peligros que afectan a nivel informático y que pueden producir situaciones de amenaza como robos o intrusiones que comprometan los datos o ataques externos que impidan el funcionamiento de los sistemas propiciando periodos de inactividad empresarial.

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos. MAGERIT [5, p. 10]

3.1.6 Fases del análisis de riesgo

El proceso de análisis de riesgos según lo expresa Martínez, citado en [6] debe cumplir con tres etapas:

Fase 1: construir perfiles de amenazas basados en activos: activos críticos, requerimientos de seguridad para los activos críticos, amenazas a los activos críticos, prácticas de seguridad actuales, vulnerabilidades actuales de la organización.

Fase 2: identificar vulnerabilidades de infraestructura: componentes clave, vulnerabilidades actuales de la tecnología.

Fase 3: desarrollar planes y estrategias de seguridad: riesgos de los activos críticos, medidas de riesgo, estrategias de protección, planes de mitigación de riesgos. p.p. 36

3.1.7. Políticas de seguridad

Las políticas de seguridad se desarrollan con el fin de preservar la información y los sistemas garantizando la integridad, confidencialidad y disponibilidad de la información, En [7] describe que "La política de seguridad se implementa mediante una serie de mecanismos de seguridad que constituyen las herramientas para la protección del sistema. Estos mecanismos normalmente se apoyan en normativas que cubren áreas más específicas."

Las políticas de seguridad se desarrollan con el fin de preservar la información y los sistemas de una Empresa, y garantizando la integridad, confidencialidad y disponibilidad de la información. Los documentos relativos a las políticas de seguridad deben contemplar los procedimientos para hacer cumplir las reglas, las responsabilidades en todos los niveles. Todos ellos deben tener el apoyo gerencial de la organización. [8]

Por lo general las políticas de seguridad de la información tiene como objetivo garantizar la protección de los activos de información involucrados en la ejecución de los procesos. Las políticas deben contener claramente las prácticas que serán adoptadas por la compañía. Y estas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente.

Las políticas deben:

- Definir qué es seguridad de la información, cuáles son sus objetivos principales y su importancia dentro de la organización.
- Mostrar el compromiso de sus altos cargos con la misma.
- Definir la filosofía respecto al acceso a los datos.
- Establecer responsabilidades inherentes al tema.
- Establecer la base para poder diseñar normas y procedimientos referidos a Organización de la seguridad.
- Clasificación y control de los datos.
- Seguridad de las personas.
- Seguridad física y ambiental.
- Plan de contingencia.
- Prevención y detección de virus.
- Administración de los computadores.

A partir de las políticas se podrá comenzar a desarrollar, primero las normas, y luego los procedimientos de seguridad que serán la guía para la realización de las actividades.

Figura 3. Objetivo principal de las políticas de seguridad

Fuente: Los investigadores

3.1.8. 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 medida que abarcan lo

preventivo y lo reactivo; cabe recalcar que el concepto de información se aplica a nivel global y no se encuentra restringirlo al tipo de información o medio que lo contenga.

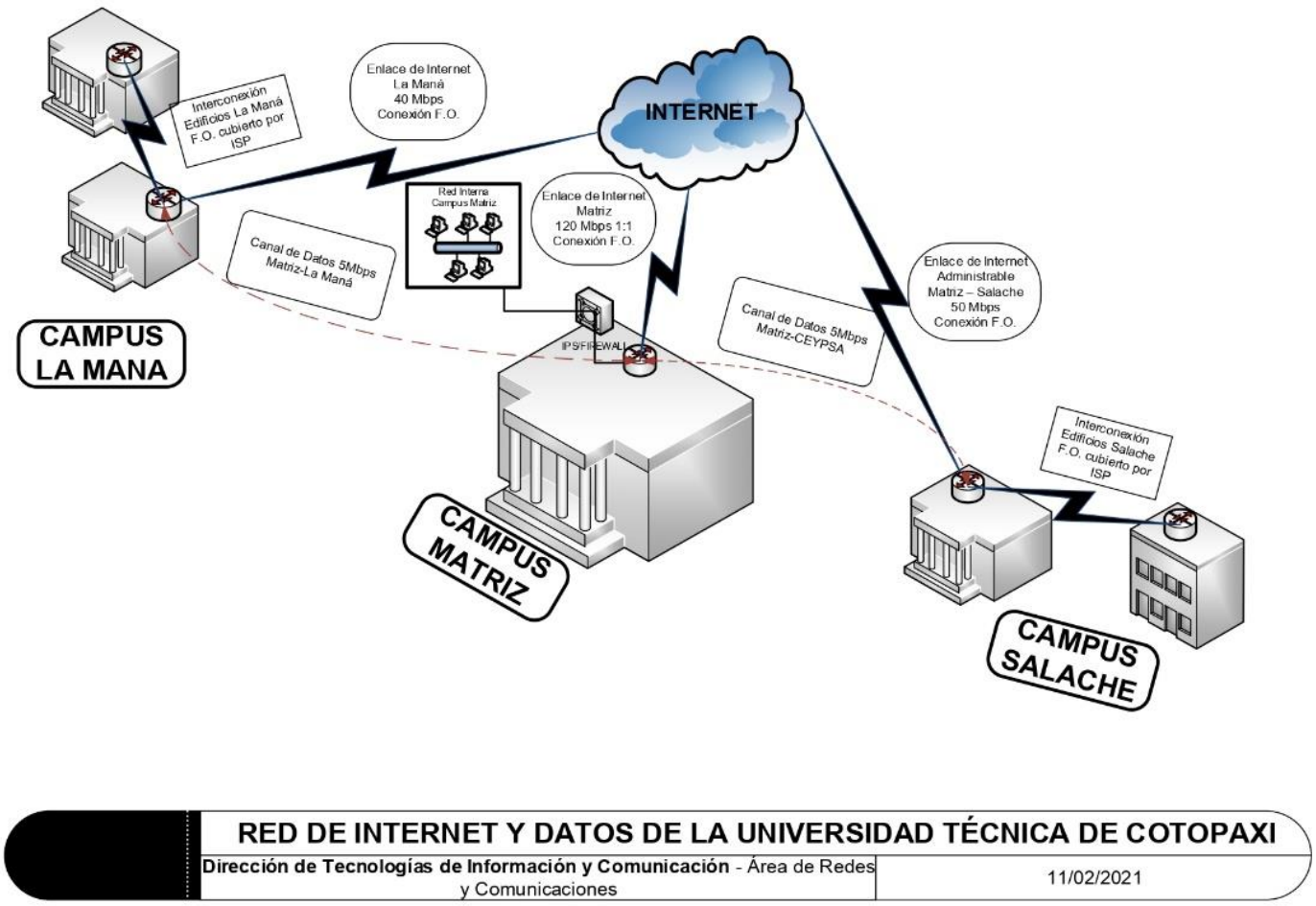
3.1.9. Bases de Datos

La sociedad actualmente se encuentra en una época donde se manifiesta gran cantidad de datos estructurados y no estructurados ya sea en tiempo real o diferido. En [9] explica como “La sociedad crea datos y más datos, cada vez existen más dispositivos eficientes para almacenarlos. Los datos son vistos como una infraestructura o un capital en sí mismos para la organización ya sea pública o privada que disponga de ellos.”

Las bases de datos en red derivan de las jerarquías, pero mejoran la gestión de datos transaccionales están diseñadas para el envío y recepción de datos a grandes velocidades y de forma continua. Sabiendo que la base de datos es la parte fundamental de las instituciones se debe considerar de gran importancia la seguridad almacenamiento y respaldo de la información.

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

Figura 4. Diagrama de interconexión Universidad Técnica de Cotopaxi



Fuente: Universidad Técnica de Cotopaxi

3.2. Control de Accesos

El principal objetivo de este dominio es dar a conocer la importancia del control de acceso a la red y a los recursos del sistema como medida de prevención de abusos tanto internos como externos. De igual manera trata de impedir el acceso no autorizado a los diferentes sistemas de información y servicios, implementar técnicas de autenticidad y autorización

3.2.1. Gestión de Acceso de Usuario

En [10] explica a "la gestión de acceso trata de asegurar que los usuarios autorizados tengan un acceso adecuado al sistema y evitar el acceso no autorizado al sistema." Siendo importante crear un procedimiento qué contenga todas las fases del acceso de los usuarios, desde donde inicia el registro hasta la fase final de su ingreso.

3.2.2. Responsabilidades del Usuario

El principal Objetivo es evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.

Se debe concientiza a los usuarios sobre sus responsabilidades para el mantenimiento de controles de acceso eficaces, en particular con relación al uso de contraseñas y a la seguridad del equipo.

3.2.3. Control de Acceso en red

Evita el acceso no autorizado a los servicios en red, mediante control de acceso de usuarios a los servicios. El acceso de los usuarios a redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que existen interfaces apropiadas entre la red y las redes pertenecientes a otras organizaciones y las redes públicas.

3.2.4. Control de Acceso al sistema Operativo

Evita el acceso no autorizado a los sistemas operativos. Se deben utilizar medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos. Tales medios deberían tener la capacidad para:

- Autenticar usuarios autorizados, de acuerdo a una política definida de control de acceso.
- Registrar intentos exitosos y fallidos.
- Suministrar medios adecuados para la autenticación: cuando sea apropiado restringir el tiempo de conexión de los usuarios.

3.3. Evaluación de riesgos, amenazas y vulnerabilidad

Cuando se plantea mejor la seguridad de una empresa se debe tener en cuenta varios factores como:

- Recursos
- Amenazas
- Vulnerabilidad
- 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. [4, p. 28]

Los riesgos son muy probables a surgir algo negativo dañando así a los recursos tangibles o intangibles por lo que impide desarrollar la labor.

Las amenazas son esos sucesos que pueden dañar los procedimientos o recursos, mientras que las vulnerabilidades son los fallos de los sistemas de seguridad o en los propios que el usuario utiliza para desarrollar las actividades que permitirían que una amenaza tuviese éxito a la hora de generar un problema. [4, p. 28]

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.

3.4. Normas ISO

En [11] Las normas ISO son considerados estándares con un alto grado de complejidad lo que dificulta su entendimiento debido en su mayor parte a que se encuentran desagregadas en varios documentos que tienden a confundir a los interesados en su implementación y esto implica un aumento en los esfuerzos y costos para preparar la documentación e implantación de los sistemas. Las normas ISO están encargadas a ordenar la gestión de una empresa en sus distintos ámbitos, las normas son establecidas por el Organismo Internacional de Estandarización ISO que están compuestas por estándares y guías relacionados con sistemas y herramientas.

3.4.1. Certificación ISO

Las entidades de certificación son organismos de evaluación de la conformidad, encargados de realizar una declaración objetiva de que el SGSI opera de acuerdo con la finalidad y objetivos definidos, con la norma ISO 27000 así como con los procedimientos internos y cumple con la legislación aplicable y otras normativas. Estas entidades han de ser neutrales y cumplir con los requisitos de independencia, imparcialidad, competencia e integridad. [12]

La certificacion ISO es un documento wur se entrega a instituciones que cumplean a cabalidad con las normas y estandares dictados por la organización ISO, lo que dictamina que son instituciones que predominan la calidad de sus servicios y productos, este certificado trae varios beneficios para quien lo obtenga.

3.4.2. Normas ISO 27000

La norma ISO 27000 se refiere a los Sistemas de Gestión de la Seguridad de la Información, y como todas las ISO, es una norma internacional que per-mite el aseguramiento, la confidencialidad y la integridad de los datos y de la información, así como de los sistemas que la procesan, por medio de la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. Por su parte, la norma ISO 27001 sugiere ante todo el conocimiento de la organización y su contexto, la comprensión de las necesidades y de las expectativas de las partes interesadas y la determinación del alcance del SGSI, antes de adoptar dicha norma. [13]

De acuerdo con Baca [13] La norma enfatiza la importancia de la determinación de riesgos y oportunidades cuando se planifica un Sistema de Gestión de Seguridad de la Información, así como el establecimiento de objetivos de seguridad de la información y el modo de lograrlos. Dicho logro depende en gran parte de que la organización cuente con los recursos, las competencias, la conciencia, la comunicación y la información documentada pertinente en cada caso. p.p. 264-265.

La norma indica que para cumplir con los requisitos de seguridad de la información se debe planificar, implementar y controlar los procesos de la organización, así como hacer una valoración de los riesgos de la seguridad de la información y un tratamiento de éstos. Asimismo, también establece la necesidad y la forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información, a fin de asegurar que funciona según lo planeado

La norma ISO/IEC 27000 son un conjunto de estándares que fueron y están siendo desarrolladas por la International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC), con el fin de proporcionar un marco de trabajo y administración de la seguridad de la información, para que esta pueda ser utilizada por cualquier organización sea esta pública, privada micro, mediana o grande. [14]

3.4.3. Familia ISO 27000

La serie ISO 27000 contempla un conjunto de estándares desarrolladas por ISO e IEC que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización. Las más conocidas son:

De acuerdo con lo que cita Aguirre, [15] en su tesis las normas ISO/IEC 27000. Es una norma internacional que busca dar información general sobre los sistemas de gestión de seguridad de información, así como definir algunos términos que son usados por todos los estándares de la familia 27000.

A diferencia de las otras normas de esta familia, esta es de libre distribución y se caracteriza por brindar un listado de las normas mencionadas junto con una pequeña descripción [ISO/IEC 27000, 2012]:

ISO/IEC 27001: El estándar principal de la familia, brinda los requerimientos para el desarrollo y operación de SGSI incluyendo una lista de controles para el manejo y mitigación de los riesgos asociados a los activos de información. Se puede confirmar la eficacia de la implementación del SGSI mediante una auditoria o certificación

ISO/IEC 27002: Este estándar brinda la guía de implementación de la lista de las mejores prácticas y los más aceptados objetivos de control presentados como anexo en la ISO/IEC 27001, con el objetivo de facilitar la elección de controles para asegurar la seguridad de los activos de información.

ISO/IEC 27003: Este estándar brinda información y una guía práctica para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI según lo establecido por la ISO/IEC 27001.

ISO/IEC 27004: Este estándar provee guías prácticas para el uso de métricas que evalúen la efectividad, objetivos de control y controles usados en un SGSI.

ISO/IEC 27005: Este estándar provee una guía para la gestión de los riesgos de seguridad de información según los requerimientos establecidos por la ISO/IEC 27001.

ISO/IEC 27006: Este estándar se complementa con el ISO/IEC 17021 y brinda los requerimientos necesarios para la acreditación de la certificación de una organización que certifique los SGSI según la ISO/IEC 27001.

ISO/IEC 27007: Provee una guía para conducir una auditoria de un SGSI, así como las competencias necesarias de los auditores de sistemas de gestión de seguridad complementando la ISO/IEC 19011

ISO/IEC TR 27008: Es un reporte técnico que brinda una guía para la revisión de la implementación de los controles del SGSI.

ISO/IEC 27010: Provee una guía para gestionar la seguridad de la información en caso la organización intercambie o comparta información importante, ya sea que pertenezca al sector público o privado, que lo haga nacional o internacionalmente, o en el mismo sector u otros sectores del mercado en el que opera.

ISO/IEC 27011: Provee una guía para apoyar la implementación de un SGSI en una empresa de telecomunicaciones.

ISO/IEC 27013: Brinda una guía para la implementación integrada del ISO/IEC 27001 y el ISO/IEC 20000 (gestión de servicios de TI), ya sea implementándolos al mismo tiempo o uno después de otro.

ISO/IEC 27014: Brinda una guía para conocer los principios y procesos del gobierno de la seguridad de la información, que busca que las organizaciones puedan evaluar, dirigir y monitorear la gestión de la seguridad de la información.

ISO/IEC TR 27015: Sirve como complemento a las normas de la familia ISO/IEC 27000 para la implementación, mantenimiento y mejora del SGSI en empresas que provean servicios financieros.

ISO/IEC TR 27016: Es un reporte técnico que brinda una metodología que permite a las organizaciones saber cómo valorar adecuadamente los activos de información identificados, los riesgos potenciales a los activos, apreciar el valor de los controles que protegen a estos activos y determinar el nivel óptimo de recursos que deben ser usados para asegurarlos.

ISO/IEC 27799:2008: Brinda una guía para apoyar la implementación de un SGSI en las empresas de salud con la adaptación del ISO/IEC 27002 según los requerimientos de este sector. [15, pp. 30 - 31]

3.4.4. Beneficios de las Normas ISO 27000

Las normas ISO se crearon con la finalidad de ofrecer orientación, coordinación, simplificación y unificación de criterios a las organizaciones con el objeto de reducir costes y aumentar la efectividad.

Las Normas ISO 27000 nos permiten tener una garantía en los controles y procesos internos para garantizar la continuidad de la productividad, permite la identificación y gestión de riesgos. Esta familia de la norma ISO es totalmente certificable para cualquier institución pública o privada puede oscilar entre 8 y 12 meses en relación de los niveles de seguridad de la información.

3.5. Software

Este compuesto de aplicaciones, servicios, ejecutables, páginas web y otros servicios. Para reducir esta superficie de ataque, hay que reducir al mínimo el software instalado en las computadoras y servidores, mantener actualizado el software y aplicar todos los parches de seguridad publicados por los desarrolladores. Romero, et al., [4]

3.5.1. Wireshark

Es un analizador de protocolos deseñado por Gerald Combs y que actualmente está disponible para plataformas Windows y Unix.

Wireshark es un analizador de protocolos de red, con interfaz gráfico, que nos permitirá capturar las tramas que entran y salen de nuestro ordenador para luego "diseccionarlas" y estudiar el contenido de los mismas.

3.5.2. The dude

Es una herramienta para el monitoreo de la red orientados a equipos mikoritk, pero también puede adaptarse a otras redes que no sean enteramente con equipos mikoritk como disco juniper, etc es una solución para monitoreo de una red compatible con todo dispositivo que este activo el servicio.

4. MATERIALES Y MÉTODOS

4.1 TIPOS DE INVESTIGACIÓN

4.1.1. Investigación de Campo

La investigación de campo nos ayudó en el proyecto, ya que los datos que obtuvimos fueron extraídos de forma directa de la realidad, a través del uso de un instrumento para recolectar la información.

4.1.2. Investigación Bibliográfica

Se empleó la investigación Bibliográfica, ya que nos permitió adentrarnos en el tema con mayor profundidad, esta investigación nos permitirá obtener información de diferentes fuentes de información como los libros, revistas e investigaciones previas al tema que servirán de guía para el desarrollo.

4.2 MÉTODOS DE INVESTIGACIÓN

4.2.1. Método Inductivo – deductivo

Este método se utilizó para la recolección de información de manera independiente de varias fuentes las mismas que son libros, páginas web, revistas, artículos científicos entre otros relacionados con el tema para luego realizar la relación de lo particular a lo general.

4.2.2. Método Analítico y Sintético

Este método se utilizó para ilustrar la base teórica, porque la información recolectada de las principales fuentes ha sido analizada e integrada en el marco teórico del proyecto.

4.3 TÉCNICAS DE INVESTIGACIÓN

4.3.1. Entrevista

Se utilizó la entrevista con la finalidad de conocer cada uno de los detalles sobre la seguridad informática que posee la institución, como las amenazas y riesgos que se puede presentar en la información guardada.

4.3.2. Observación

Observación ayudo a verificar como se lleva a cabo la seguridad de la información que posee la Universidad Técnica de Cotopaxi y a su vez recolectar los datos que sean necesarios para su posterior análisis y resolución.

4.3.3. Normas ISO 27000

Para el desarrollo del diseño de las políticas de seguridad informática se tomó como referencia la norma ISO 27000 la cual se basa en proteger la confidencialidad, integridad y disponibilidad de la información de la institución. Esta norma permite investigar cuales son los potenciales problemas que podrían afectar la información y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan.

4.4 INSTRUMENTOS DE INVESTIGACIÓN

4.4.1. Entrevista Estructurada

La entrevista estructurada permitirá recolectar información directa del encargado del departamento de las TIC's de la Universidad Técnica de Cotopaxi.

4.4.2. Ficha de registro de observación

Nos permitirá recopilar datos e información directa del departamento de las TIC's.

4.5 POBLACIÓN Y MUESTRA

La población de estudio está constituida por el encargado del departamento de las TIC's de la Universidad Técnica de Cotopaxi.

4.6 DISEÑO DEL MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Al realizar la investigación y analizar todos los datos obtenidos, se procede a diseñar las siguientes políticas de seguridad informática:

- ✓ **PO-1A** Política de control de acceso.
- ✓ **PO-1B** Política de Active Directory.
- ✓ **PO-1C** Política de Gestión de Activos.
- ✓ **PO-1D** Política de resguardo y protección de la información.
- ✓ **PO-1E** Política de seguridad a componentes informáticos.
- ✓ **PO-1F** Política de control de acceso a la red de internet.
- ✓ **PO-1G** Política de uso adecuado de laboratorios de computación.

Objetivo de las Políticas de Seguridad Informática.

Establecer reglamentos de seguridad para garantizar la privacidad, control, integridad y autenticidad de la información que maneja el departamento de las TIC’s de la Universidad Técnica de Cotopaxi.

1. Objetivo

Controlar los accesos a la información que se procesa dentro del departamento de la TIC's de la Universidad.

2. Alcance

Controlar el acceso a la información y los medios de la misma, aplicando políticas para su divulgación y autorización.

3. Documentos de referencia.

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

RE-02A. Creación de usuario de red.

RE-03A. Creación de usuarios para el aula virtual.

RE-04A. Acta de entrega y recepción de equipos.

4. Descripción de la Política.

Se debe establecer y documentar quien será el responsable de control los accesos a las plataformas, aplicaciones y recursos que contengan información, que en todo caso será el departamento de las TIC's de la universidad, como parte de esta política el personal de la organización deberá cumplir con las siguientes medidas:

Todo acceso a la red de la universidad será autorizado por el departamento de las TIC's, quien definira los permisos adecuados según el tipo de usuario, principal método de control que se utiliza para la seguridad y el acceso a los recursos computacionales, son las credenciales de acceso (claves), las cuales no podrá recibirlas sin antes haber aceptado y formado el documento correspondiente al RE-01A "Aceptación y cumplimiento de las políticas".

Todo usuario interno o externo que requiera acceso a la red de la Universidad deberá estar autenticado y sus conexiones deberán utilizar cifrado de datos, ya sea que el acceso sea por internet, teléfono o por otro medio.

Los recursos informáticos serán entregados solamente después de hacer la solicitud del documento RE-02A "Creación de usuarios" y haber Firmado el documento RE-04A "Acta de entrega y recepción de equipos", y la información concedida por parte de la universidad, solo pueden ser usados para propósitos previamente autorizados, cumpliendo los objetivos que la institución establezca.

Gestión de acceso del usuario

Los procedimientos que se determinan en esta etapa, son un detalle cronológico que comprende desde el registro inicial de los usuarios hasta el personal que requiera acceso a los sistemas y servicios de información, para este cumplimiento se deberá:

- Realizar el registro de los usuarios que serán creados con el siguiente estándar: se usarán las credenciales de su cédula de identidad o pasaporte (1500727473) único que permitirá vincular y responsabilizar las acciones realizadas con cada perfil, dicha autorización la realizara el departamento de las TIC's quienes serán los únicos responsables de la creación, modificación y eliminación de cada usuario y contraseña

Responsabilidad del Usuario

- Todos los usuarios dispondrán de un usuario y contraseña único que le permita acceder a su equipo de cómputo asignado.
- La clave designada tendrá un mínimo de 8 caracteres.
- La clave estará compuesta por letras (incluyendo mayúsculas), números y caracteres especiales.
- El usuario tiene permitido cambiar la clave de acceso designada solo en el caso que presienta que ya no es confidencial.
- Pasados los 6 meses, el equipo de cómputo pasará por un mantenimiento preventivo restaurando la antigua clave.

Control de acceso al sistema operativo

Para proteger el sistema operativo es importante evitar que personas no autorizadas ingresen o lo manipulen a su conveniencia, para evitar este tipo de riesgo se debe:

- Realizar un registro seguro que muestre una advertencia a la computadora que controla los demás equipos em línea, los intentos no autorizados de acceder al sistema.
- Establecer una clave de usuario para identificar las actividades hasta la persona responsable.
- Las claves de acceso proporcionadas para los usuarios serán una mezcla de letras (incluir una mayúscula), números y caracteres especiales.
- La clave de acceso a los sistemas expirará de forma obligatoria cada 3 meses, y el usuario recibirá notificaciones automáticas 15 días antes de su expiración.
- El usuario tiene permitido el cambiar su clave de acceso solo en el momento que está ya no sea confidencial.
- Después de 3 intentos fallidos de ingreso de la clave, su cuenta se deshabilitará y deberá realizar la solicitud de la habilitación de su cuenta al Departamento de Tecnologías de la Información
- Pasados los 30 minutos de inactividad después de iniciar sesión, se cerrará la sesión, protegiendo la cuenta de personas no autorizadas.

Correo electrónico y acceso internet.

- El Departamento de Tecnologías de la Información creará una contraseña para el acceso al servicio de correo electrónico, VPN y acceso remoto a la información de la Universidad.
- Las cuentas de correo electrónico estarán estandarizadas de la siguiente forma: el primer nombre, punto, primer apellido y los 4 últimos dígitos de la cedula de identidad (luis.lopez3358@utc.edu.ec).

Usuarios para el aula virtual.

Están completamente prohibidas las siguientes actividades:

- Utilizar el Correo Electrónico para cualquier propósito comercial, fines de lucro, o actividades ajenas a las funciones institucionales.
- Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para nuestra Institución
- Toda información o contenido que sea transmitido por las cuentas de correo de este sitio, son responsabilidad únicamente del dueño de la cuenta, por lo que dichos contenidos no reflejan las preferencias o ideas de la institución.
- El usuario de aula virtual será creado una vez hecha la solicitud llenando el documento RE-03A "Creación de usuarios para el aula virtual" definiendo el tipo de usuario a crearse.
- Los usuarios serán creados con el siguiente estándar: (primer nombre). (primer apellido) (cuatro últimos dígitos de la cédula) @utc.edu.ec.
- La contraseña que se establece como valor inicial es su número de cédula, se recomienda cambiar la primera vez que ingrese y sustituirla por una contraseña segura (compuesta de letras mayúsculas, minúsculas, números y caracteres especiales), no menor de ocho caracteres.
- Si el usuario no ingresa a el aula virtual en un periodo de 2 meses, el sistema lo deshabilitará y para volver a habilitarlo tendrá que realizar una solicitud al área de Tecnologías de la Información.
- Si el usuario no ingresa al aula virtual por más de 2 años, el sistema eliminará el usuario de forma permanente.

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

4. Registros.

Tabla 2. Documentos de referencia.

Código	**Nombre**	**Responsable**	**Ubicación**	**Actualización**	**Retención**	**Acceso**
RE-01A	Aceptación y cumplimiento de Políticas	TIC's	Departamento de la TIC's	Una vez que se cree un nuevo usuario	Una vez que el usuario finalice el periodo académico o hasta la fecha que permanece dentro de la universidad durante el periodo académico.	Uso interno
RE-02A	Creación de usuario de red.	TIC's	Departamento de la TIC's	Una vez que se cree un nuevo usuario	Una vez que el usuario finalice el periodo académico o hasta la fecha que permanece dentro de la universidad durante el periodo académico.	Uso interno
RE-03A	Creación de usuarios para el aula virtual	TIC's	Departamento de la TIC's	Una vez que se cree un nuevo usuario	Una vez que el usuario finalice el periodo académico o hasta la fecha que permanece dentro de la	Uso interno

					universidad durante el periodo académico.	
RE-04A	Acta de entrega y recepción de equipos	TIC's	Departamento de la TIC's	Una vez que se cree un nuevo usuario.	Una vez que el usuario finalice el periodo académico o hasta la fecha que permanece dentro de la universidad durante el periodo académico.	Uso interno

5. Anexos.

N/A.

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	**ACTA DE ACEPTACIÓN Y CUMPLIMIENTO DE LAS POLÍTICAS.**	RE-01A
		Ver. No. 01

(Ciudad y fecha de recibido)

Yo, **(NOMBRE APELLIDO)**, portador (a) de la cédula de identidad **(#)**, afirmo que he recibido indicaciones 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.
- ✓ **PO-1B** Política de Active Directory.
- ✓ **PO-1C** Política de Gestión de Activos.
- ✓ **PO-1D** Política de resguardo y protección de la información.
- ✓ **PO-1E** Política de seguridad a componentes informáticos.
- ✓ **PO-1F** Política de control de acceso a la red de internet.
- ✓ **PO-1G** Política de uso adecuado de laboratorios de computación.

Por tal motivo certifico que he revisado y aceptado las normas anteriormente expuestas, cumpliendo cada uno de sus lineamientos con el fin de contribuir al mejoramiento de la seguridad de los recursos que me encomienden.

_____

(Nombre de usuario/colaborador)

(Número de CI)

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	**SOLICITUD DE CREACIÓN DE USUARIOS DE RED Y SISTEMA – ERP**	RE-02A
		Ver. No. 01

Tabla 3. Solicitud de creación de usuarios.

Fecha:

_____/_____/_____/

Equipos de Computo	**Tipo**			**Justificación**
	Laptop ☐	PC☐	Teléfono☐	
Acceso	**Recursos**			**Descripción**
	Sistema			**Modulo**
	Correo institucional			
	Teléfono			
Jefe Inmediato				
Solicitante/Empleado			**Cédula**	
Responsable TI			**Fecha Creación**	
Firmas				
	Responsable TI		**Empleado**	

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	**SOLICITUD DE CREACIÓN DE USUARIO PARA EL AULA VIRTUAL**	RE-03A
		Ver. No. 01

Tabla 4. Solicitud de creación de usuarios para el Aula virtual

Fecha:

_____/_____/_____/

Usuario	**Tipo**		**Justificación**	
	Profesor ☐	Estudiante ☐		
Acceso	**Sistema**		**Descripción**	
	Correo institucional			
Jefe Inmediato				
Solicitante/Empleado			**Cédula**	
Responsable TI			**Fecha Creación**	
Firmas				
	Responsable TI		**Solicitante**	

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	**ACTA DE ENTREGA Y RECEPCIÓN DE EQUIPOS**	Anexo-04A
		Ver. No. 01

En la ciudad de Latacunga, a la fecha ___/ _____/2021, en la Unidad de Control de Bienes de la Universidad Técnica de Cotopaxi, se constituye por una parte el *(nombre y cargo del solicitante),* y por otra parte a *(nombre y cargo del encargado de entrega de equipos);* se procede a la entrega-recepción de lo siguiente que a continuación se detalla:

CÓDIGO	**DESCRIPCIÓN**	**SERIE**	**ESTADO**

Por la demostración que antecede a la entrega de bienes a *(nombre y cargo del solicitante);* quien recibe conforme y queda bajo su responsabilidad y custodia.

Para constancia de lo actuado en fe y conformidad, suscriben el presente documento en tres ejemplares del mismo tenor y efector, quienes interviene en la presente diligencia

(Nombre del encargado de la entrega de bienes)

CC…….

(Nombre del solicitante)

CC…….

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC’s Fecha:

1. Objetivo

Almacenar datos y hacer que estos datos estén disponibles para los usuarios y administradores de la red.

2. Alcance.

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

3. Documentos de referencia.

Anexo-01B Asignación de políticas de AD.

4. Descripción de la Política.

La Universidad, consciente de ejecutar buenas prácticas para el uso adecuado de sus recursos informáticos, establece la implementación de Active Directory para facilitar la administración de todos los elementos lógicos (usuarios, equipos y recursos informáticos).
De esta forma, a continuación, se detallará todos los controles que se implementarán de forma parcial o total, dependiendo de la capacidad tecnológica que dispongamos para cada caso:

Del Área de Tecnología.

- Establecer de imagen de fondo el logo corporativo de la institución en todos los equipos de cómputo de la institución.
- Fijar como protector de pantalla la misión y visión de la Universidad Técnica de Cotopaxi.
- Instalar las impresoras en un servidor de impresión, facilitando la actualización de controladores, configuración de las bandejas, memoria, color, etc., sin la necesidad de tener que ir de usuario en usuario configurando los parámetros de cada impresora.
- Delimitar reglamentos que controlen el entorno de trabajo, cuentas de usuario y cuentas de equipo, que permita la configuración de sistemas operativos y usuarios en un entorno de AD.

- Asignar políticas de AD según el perfil de usuario anteriormente establecido en el Anexo-01B Asignación de políticas de AD.
- La Dirección de Tecnologías de la Información tendrá la autoridad de habilitar o deshabilitar los siguientes componentes del sistema según crea conveniente:
- Restringir y negar el acceso a determinadas carpetas.
- Desactivar cualquier tipo de gadgets del escritorio.
- Deshabilitar la funcionalidad de "Eliminar el historial de exploración" en el navegador de internet predefinido.
- Quitar el icono de Red del menú de Inicio.
- Negar el acceso al Panel de control.
- Negar el acceso al símbolo del sistema.
- Deshabilitar la descarga de archivos ejecutables.
- Establecer qué paquetes MSI se pueden instalar en un equipo.
- Bloquear el acceso al Administrador de tareas.

Responsabilidad de los Usuarios.

- Todo usuario dispone de una cuenta con usuario y contraseña para acceder al equipo de cómputo designado.
- Después de 5 minutos de inactividad en un equipo de cómputo, se cerrará la sesión de forma automática y se activará el protector de pantalla, evitando que personas no autorizadas ingresen al equipo.
- Después de 3 intentos fallidos de ingresar la clave, se deshabilitará de forma automática y el usuario tendrá que solicitar al Departamento de Tecnologías de la Información su reactivación.

4. Registros.

N/A.

5. Anexos.

Anexo-01B Asignación de políticas de AD.

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

A continuación, se describirá de forma breve cada política.

- ✓ **Autenticación.**

Medida de seguridad para proteger la información de usuarios no autorizados.

- ✓ **Tapiz del escritorio.**

Fondo de escritorio que se utilizará en todos los equipos de cómputo designados a los usuarios.

- ✓ **Protector de pantalla.**

Designar como protector de pantalla la misión y visión de la institución que, pasado los 5 minutos, se bloqueará de forma automática siendo necesario volver a iniciar sesión con el usuario y contraseña designado.

- ✓ **Desactivar cuenta de usuario.**

Después de 3 intentos fallidos de ingresar la clave, se deshabilitará de forma automática y el usuario tendrá que solicitar al Departamento de Tecnologías de la Información su reactivación.

- ✓ **Desactivar Reproducción automática**.

En el momento de conectar una memoria USB o un CD/DVD en el lector del equipo, se abre una ventana para la "Reproducción automática", esta será deshabilitada para la protección de los archivos del computador minimizando la ejecución de algún tipo de virus.

- ✓ **Prohibir el acceso al Panel de Control**.

Se desactivará el uso del panel de control para el usuario final, negándole el acceso a cambios de configuración del computador.

- ✓ **Cambiar contraseña**.

El usuario contará con la opción de cambiar su contraseña en el momento que está ya no sea confidencial.

- ✓ **Establecer contraseñas.**

La contraseña establecidas o editadas deberán cumplir con todos los requisitos de complejidad.

UNIVERSIDAD TÉCNICA DE COTOPAXI	POLÍTICA GESTIÓN DE ACTIVOS	PO-1C
		Ver. No. 01

1. Objetivo.

Proteger apropiadamente los activos del Departamento de las TIC's de la Universidad Técnica de Cotopaxi

2. Alcance.

La Universidad debe identificar e inventariar sus activos y designar responsables del mantenimiento y cumplimiento de los controles aplicables a los mismos,

3. Documentos de referencia.

RE-01C Inventario de equipos informáticos y servidores.

RE-02C Inventario de software.

RE-03C Movimiento de equipos informáticos.

RE-04C Baja de equipos informáticos.

RE-05C Bitácora de mantenimiento preventivo de PC's.

RE-06C Ficha de mantenimiento preventivo de computadores.

4. Descripción de la Política.

- La Dirección de Tecnologías de la Información debe tener el aforo de designar equipos informáticos a los usuarios previamente creados.
- La Dirección de Tecnologías de la Información llevará un registro del inventario de equipos informáticos utilizando el documento de referencia RE-01C "Inventario de equipos informáticos y servidores".
- De igual manera para el control del software de cada uno de sus componentes informáticos, la Dirección de tecnologías de la información utilizará el documento RE-02C "Inventario de software".

- El personal encargado de los Activos Fijos se hará responsable del control de estos y de la ubicación de los bienes muebles e inmuebles propiedad de la institución.
- Si es necesaria la movilidad de equipo informático, el solicitante tendrá que llenar el documento RE-03C “Movimiento de equipos informáticos” para solicitarlo.
- Para solicitar la baja de un equipo informático es necesario el uso del documento RE-04 “Baja de equipos informáticos”.
- El personal encargado de las diferentes áreas que conforman la Universidad se hará responsables de todo el mobiliario y equipos designados en su respectivo departamento, al igual que el buen uso y cuidado de estos.
- Para ejecutar el mantenimiento del Data Center, se buscará el personal apropiado para el manejo de estos equipos, por lo cual el responsable designado deberá presentar un informe ostentando y detallado todas las actividades que realizó.

Responsabilidad de los activos

Inventario de los activos:

Cada área y sus colaboradores deben garantizar el uso y protección adecuada de los activos, además de realizar periódicamente un inventario que permitirá llevar un registro actualizado y evitar riesgos en las operaciones de la Universidad.

Clasificación de la información

Lineamientos de clasificación

La información se deberá clasificar en función de su valor, requisitos legales, sensibilidad y criticidad para la Universidad.

Las actividades a realizar para llevar a cabo una adecuada clasificación son las siguientes:

- Definir la clasificación de un activo
- Revisión periódica
- Actualización de la información.

Etiquetado y manejo de la información.

- Desarrollar procedimientos para el procesamiento, resguardo, transferencia, clasificación y destrucción de la información.
- El etiquetado se realizará a todos los activos que contengan información en formato físico y electrónico.
- Los sistemas que contengan información clasificada como sensible o critica, deberá llevar una etiqueta de clasificación apropiada que permita identificar su clasificación.

Responsabilidades de la dirección de tecnologías de la información

La dirección de Tecnologías de la Información se hace responsable de la adquisición, instalación, mantenimiento y buen funcionamiento de los equipos informáticos cumpliendo los siguientes lineamientos:

- Vigilar y acarrear un inventario detallado de la infraestructura de Hardware que posee la Institución, de acuerdo con las necesidades existentes de la misma.

- La Dirección de Tecnologías de la Información será la única responsable de crear los requerimientos de los activos informáticos que se hayan solicitado según las necesidades que se presente en cada área de trabajo.

- La dirección de Tecnologías de la Información determinará la vida útil de los equipos informáticos con la finalidad de optimizar el uso de estos.

- La Dirección de Tecnologías de la Información tendrá participación activa en los contratos de adquisición de bienes y servicios en los cuales incluye equipos informáticos como parte integrante o complementaria de otros.

- La Dirección de Tecnologías de la Información se encargará de la confirmación que los equipos informáticos cumplan con las especificaciones indicadas en las solicitudes de compra, encargándose de la devolución de estos si no los cumplen.

- Realizará el mantenimiento técnico preventivo de todos los equipos informáticos con los que la institución cuenta utilizando el documento RE-05C “Mantenimiento preventivo de PC’s”.

- Con el documento “RE-06 “Ficha de mantenimiento preventivo de computadores”, el personal de mantenimiento detallará las características del equipo al cual realizará dicho mantenimiento.

- El personal encargado de realizar el mantenimiento, usará el Anexo-01C para llevar un registro del mantenimiento realizado a todos los departamentos existentes.

- Se responsabilizará de la instalación de los equipos y los programas informáticos utilizados por la institución.

- Se responsabilizará en la evaluación del área en el cual se instalará un nuevo equipo informático, confirmando que dicha área sea óptima para la instalación de los mismos.

- Se encargará con la verificación de los equipos informáticos, teniendo en cuenta la disponibilidad de energía, cableado estructurado adecuado y condiciones físicas apropiadas.

- La Dirección de Tecnologías de la Información velará por el adecuado uso de las instalaciones eléctricas requeridas para el funcionamiento de los equipos tecnológicos.

- Se encargará en la verificación del inventario de los programas y equipos informáticos que sean instalados, llevando el control de los mismos.

- Realizará la instalación de las aplicaciones de los equipos y programas manejados por la institución.

- Instruirá a los usuarios sobre el manejo adecuado de los equipos informáticos y aplicaciones instaladas.

Mantenimiento Preventivo de Data Center.

- El Departamento de Tecnologías de la Información deberá llevar un Registro para llevar el cronograma de mantenimiento preventivo a realizar en el Data Center de la institución utilizando el documento Anexo-02C "Cronograma de mantenimiento preventivo de Data Center", evitando la interferencia de las horas de trabajo de los usuarios.
- El mantenimiento preventivo del Data Center será realizado cada 6 meses.
- El registro será llevado mediante una Bitácora de mantenimiento del Data Center en el cual se detallará las actividades realizadas.

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

4. Registros:

Tabla 4. Documento de referencia activos.

Código	**Nombre**	**Responsable**	**Ubicación**	**Actualización**	**Retención**	**Acceso**
RE-01C	Inventario de equipos informáticos y servidores	Departamento de la TIC’s	Oficinas Departamento de la TIC’s	Cada vez que se ingrese o se dé de baja un equipo informático.	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Uso interno
RE-02C	Inventario de software	Departamento de la TIC’s	Oficinas Departamento de la TIC’s	Cada vez que se ingrese o se dé de baja un equipo informático.	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Uso interno
RE-03C	Movimiento de equipos informáticos	Departamento de la TIC’s	Oficinas Departamento de la TIC’s	Cada vez que haya registro de movimiento de equipos.	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Uso interno

RE-04C	Baja de equipos informáticos	Departamento de la TIC’s	Oficinas Departamento de la TIC’s	Cada vez que se dé de baja un equipo informático.	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Uso interno
RE-05C	Bitácora de mantenimiento preventivo de PCs	Departamento de la TIC’s	Oficinas Departamento de la TIC’s	Cada vez que se realice un mantenimiento.	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Uso interno
RE-06C	Ficha de Mantenimiento Preventivo de Computadores	Departamento de Tecnologías de la Información	Oficinas Departamento de la TIC’s	Cada vez que se realice un mantenimiento.	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Uso interno

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC’s Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	**INVENTARIO DE EQUIPOS INFORMÁTICOS Y SERVIDORES**	RE-01C
		Ver. No. 01

Fecha

Tabla 5. Inventario de equipos de cómputo y servidores

UNIVERSIDAD TÉCNICA DE COTOPAXI — FICHA TÉCNICA INVENTARIO DE EQUIPOS — DIRECCIÓN DE TECNOLOGÍA DE LA — Ver. No. 1

Nombre Equipo	Equipo Nº	Fecha Apertura	Cod. Institucional	Tipo	Campus	Nombre Usuario	Cargo Usuario	Area de Trabajo	Marca	Modelo	Presentación	Serie CPU	Tiempo Gar. Años	Proveedor	Marca RAM	Tipo	Capacidad RAM	Marca Procesador	Modelo PC	Velocidad Procesador	Marca Disco Duro	Modelo Disco	Serie Disco	Capacidad Disco	Tipo	Marca Tarjeta Madre	Marca Monitor	Modelo	Serie	Descripción	Marca teclado	Modelo	Serie	Descripción	Marca Mouse	Modelo	Serie	Descripción	Grupo de Trabajo	Dirección IP	Mascara de Sured	Dirección MAC	Puerta de Enlace

Matriz en donde los datos a llenar son los siguientes:

- Nombre de Equipo
- Equipo N°
- Fecha Apertura
- Cod. Institucional
- Tipo
- Campus
- Nombre usuario
- Cargo usuario
- Área de trabajo
- Marca
- Modelo
- Presentación
- Serie CPU
- Tiempo Gar. Años
- Proveedor
- Marca Ram
- Tipo
- Capacidad Ram
- Marca Procesador
- Modelo Pc
- Velocidad Procesador
- Marca Disco Duro
- Modelo Disco
- Serie Disco
- Capacidad Disco
- Tipo
- Marca Tarjeta Madre
- Marca Monitor
- Modelo
- Serie
- Descripción
- Marca Teclado
- Modelo
- Serie
- Descripción
- Marca Mouse
- Modelo

- Serie
- Descripción
- Grupo de Trabajo
- Dirección IP
- Máscara de Sub Red
- Dirección MAC
- Puerta de Enlace

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC’s Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	INVENTARIO DE SOFTWARE	RE-02C
		Ver. No. 01

Fecha

Tabla 6. Inventario de software

UNIVERSIDAD TÉCNICA DE COTOPAXI	FICHA TÉCNICA DE INVENTARIO DE SOFTWARE DE EQUIPOS DE CÓMPUTO						Versión:	01
	DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN						Vigencia:	
NOMBRE EQUIPO	CODIGO INSTITUCIONAL	DEPENDENCIA	DESCRIPCION	LIBRE PROPIETARIO	VERSION	SERIE	LICENCIA SI /NO	FECHA CADUCIDAD

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC’s Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	**REGISTRO DE MOVIMIENTO DE EQUIPOS**	RE-03C
		Ver. No. 01

Tabla 7. Registro de movimiento de equipos.

Fecha _____ **Consecutivo N.º.** _____

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	
Responsable actual	
Documento de identidad Nº.	
Dependencia	
Código de dependencia	

Dependencia destino	
Nuevo responsable	
Documento de identidad Nº.	
Dependencia	
Código de dependencia	

Información básica de los activos fijos			
Nº.	Descripción	Nº. inventario	Código institucional
1			
2			
3			
4			
5			

Total de activos

Observaciones

Firmas dependencia de origen
Firma y sello responsable
Firma y sello quien autoriza el traslado

Firmas dependencia de origen
Firma y sello responsable
Firma y sello quien autoriza el traslado

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	REGISTRO DE BAJA DE EQUIPOS	RE-04C
		Ver. No. 01

Tabla 8. Registro de baja de equipos.

Registro Nº		**Fecha**	_____/_____/_____

Ubicación del Equipo	

Datos del Usuario

Nombre	
Cargo	
Nombre del jefe del Área	

Datos del Equipo

Nombre	**Tipo**	**Marca**	**Modelo**	**Código institucional**	**Nº Inventario**	**Valor en Libros**

Motivo de Baja	Cómo se Detectó

Dictamen:

Observaciones:

Firmas:

SOLICITANTE **Responsable**		**JEFE DEPARTAMENTO** **Titular o delegado**

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	**BITÁCORA DE MANTENIMIENTO PREVENTIVO DE PC's**	RE-05C Ver. No. 01

Fecha

Tabla 9. Bitácora de mantenimiento preventivo de PC's.

Fecha	**Activo**	**Usuario Responsable**	**Responsable de TI**	**Actividades Desarrolladas**	**Observaciones**	**Firma de Conformidad**

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	**FICHA DE MANTENIMIENTO PREVENTIVO DE COMPUTADORES**	RE-06C
		Ver. No. 01

Tabla 10. Ficha de mantenimiento preventivo de computadores.

DEPARTANMENTO DE TECNOLOGIAS DE LA INFORMACIÓN						
RESPONSABLE DE TI:		**FECHA:**				
USUARIO/RESPONSABLE:		**DEPARTAMENTO/lab:**				
Información del Equipo		**Especificaciones Técnicas**				
Tipo de Equipo:		**Componente**	**Cantidad**	**Marca**	**N^0 Serie**	**Capacidad**
Nombre del Equipo:		Procesador:				
Dirección IP:		Memoria Ram modelo:				
Dirección MAC:		Disco Duro:				
Sistema operativo:		Unidad de CD/Rom:				
Marca de Fabricante:		Teclado:				
Modelo Sistema:		Mouse:				
Tipo de Sistema:		Monitor:				
Memoria Total de HDD:		Fuente de Poder:				
Memoria Total de Ram:		**EXTRAS**				
GPU:						
Generacion Del Procesador:						
Modelo de ManinBoard:						
Observación General del Software:		**Observación General del Hardware:**				
DETALLE DEL MANTENIMIENTO:						

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC’s Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	**CRONOGRAMA DE MANTENIMIENTO PREVENTIVO DE PC's**	Anexo-01C
		Ver. No. 01

Tabla 11.Cronograma de mantenimiento preventivo de PC's. **Fecha:**

DEPARTAMENTO	**MESES**											
	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
Centro de Cultura Física												
Centro de Experimentación Científica												
Centro de Idiomas Dir. Asesoría Jurídica												
Dir. Académica												
Dir. Administrativa												
Dir. Asesoría Jurídica												
Dir. Auditoría Interna												
Dir. Bienestar Estudiantil												
Dir. Comunicación Institucional												
Dir. Educación Continua												
Dir. Evaluación y Aseguramiento de Calidad												
Dir. Financiera												
Dir. Investigación												
Dir. Posgrados												
Dir. Relaciones Institucionales												
Dir. Talento Humano												
Dir. Tecnologías de la Información												
Dir. Vinculación												

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	**CRONOGRAMA DE MANTENIMIENTO PREVENTIVO DE DATA CENTER**	Anexo-02C Ver. No. 01

Fecha

Tabla 12. Cronograma de mantenimiento preventivo de Data Center

ACTIVIDAD	**MESES**											
	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
Descontaminación y renivelación de pisos falsos												
Mantenimiento arquitectónico a Data Centers (pinturas retardantes, luminarias, limpieza)												
Servidores												
Sistema de control de acceso												
Sistema de control de incendios												
UPS, PDU´s, y Tableros de Emparalelamiento												
Verificación Aire Acondicionado												
Verificación Planta eléctrica de Emergencia												

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC’s Fecha:

1. Objetivo.

Proteger y mantener segura la información que posee la Universidad

2. Alcance.

Aplicar en toda la infraestructura del área de TIC's de la Universidad Técnica de Cotopaxi.

3. Documentos de referencia.

RE-01B. Bitácora de respaldos de usuarios.

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

4. Descripción de la Política.

Se debe impedir de cualquier modo la pérdida o filtración de la información dentro de la Universidad en caso de que exista algún evento fuera del alcance se debe garantizar la recuperación de la información, por lo que se debe tener en cuenta lo siguiente:

- ✓ Ejecutar copias de seguridad completas de la información y establecer los procesos de restauración.
- ✓ Analizar que los soportes de se encuentran trabajando correctamente para así verificar su efectividad.
- ✓ Comprobar regularmente los procesos de restauración, asegurando su eficacia para ser utilizados en el momento requerido.
- ✓ Toda información confidencial se debe encontrar encriptada, ya sea interna o externa de la Institución.
- ✓ Toda información confidencial o sensible debe tener un proceso periódico de respaldo, asignando un período de retención determinado, la fecha de su última modificación y la fecha en la que deja de ser confidencial.
- ✓ Todo medio físico en donde se encuentre información de valor, será almacenado por períodos no mayores a seis meses.

- ✓ Toda información de valor respaldada debe someterse a un proceso periódico de validación garantizando que no haya sufrido algún tipo de deterioro, permitiendo su uso en otro momento.

Responsabilidad de los Usuarios.

- ✓ El usuario deberá almacenar la información que procese dentro de la carpeta (UTC_Usuarios), que estará alojada dentro de la unidad D.
- ✓ El usuario deberá almacenar solo la información que sea importante para la institución y se encuentre relacionada con las actividades dentro de esta.
- ✓ El usuario deberá dar acceso de su información cada que el personal de Tecnologías de la Información lo solicite.

Departamento de Tecnologías de la Información.

- ✓ Proporcionar un servidor en el cual permita almacenar todos los respaldos necesarios que se realizarán.
- ✓ Implementar un software específico y de fácil uso que contribuya en la generación de respaldos periódicos a realizar.
- ✓ Establecer los espacios de almacenamiento conforme a la posición que desempeñe cada usuario creado.
- ✓ Crear y planificar una matriz de ejecución automatizada de todos los respaldos de usuarios para así llevar un control adecuado mediante una bitácora de respaldos de usuarios.
- ✓ Suscitar un cronograma de respaldo de archivos de la información de acuerdo a cada área o departamento existente en la Institución utilizando el documento RE.01B “Bitácora de respaldos de usuarios”.
- ✓ Almacenar con privacidad la información de usuarios respaldada teniendo en cuenta el documento Anexo-02D “Usuarios declarados para respaldo de Información” para tener un registro detallado de cuáles son los usuarios a los que se tiene que realzar un respaldo, utilizando herramientas específicas para dicho proceso.
- ✓ Disponer de una herramienta secundaria para respaldos de información.

Bases de datos.

- ✓ Utilizando el documento RE-02B “Bitácora de respaldos de bases de datos” junto al documento Anexo-01D “Cronograma de respaldo de usuarios finales y servidores”, se realizará el registro del respaldo de la base de datos.
- ✓ El proceso de respaldo de información se realizará de dos formas (de manera local y en la nube).
- ✓
- ✓ El respaldo local de la base de datos será realizado en un servidor NAS.
- ✓ Programar una matriz de ejecución automática de respaldos de bases de datos que será planificada mediante el ajuste de la herramienta implementada para así, tener un control adecuado mediante la 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.

5. Registros.

Tabla 13. Documento de referencia para el resguardo de la información.

Código	**Nombre**	**Responsable**	**Ubicación**	**Archivo**	**Acceso**
RE-01D	Bitácora de Respaldos de Usuarios	Encargado de la TIC’s	Departamento de la TIC’s	Periódicamente por fecha	Uso interno
RE-02D	Bitácora de respaldos de BDD	Encargado de la TIC’s	Departamento de la TIC’s	Periódicamente por fecha	Uso interno

6. Anexos.

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

Anexo-02D Usuarios declarados para respaldo de Información.

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC’s Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	BITÁCORA DE RESPALDOS DE USUARIOS	RE-01D
		Ver. No. 01

Fecha

Tabla 14. Bitácora de respaldo de usuarios.

UNIVERSIDAD TÉCNICA DE COTOPAXI	BITÁCORA DE RESPALDO DE USUARIOS			**Versión:**	01
	DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN			**Vigencia:**	
N°.	**Nombre de Usuario**	**Medio utilizado para realizar Backup**	**Tipo de Backup**	**Fecha última Backup realizado**	**Fecha de realización de Backup**	**Contenido**

Observaciones:

Aprobado **Verificado**

Responsable: Grupo de investigación	Aprobación: Director de TIC’s
Fecha:	Fecha:

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

Fecha

Tabla 15. Bitácora de respaldo de Base de Datos.

UNIVERSIDAD TÉCNICA DE COTOPAXI	BITÁCORA DE RESPALDO DE BASES DE DATOS	**Versión:**	01
	DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN	**Vigencia:**	

N°.	Nombre del Servidor	Medio utilizado para realizar el Backup	Tipo de Backup	Fecha último Backup realizado	Fecha de realización de Backup	Contenido	Responsable

Observaciones:

Aprobado

Responsable: Grupo de investigación	Aprobación: Director de TIC’s
Fecha:	Fecha:

Verificado

UNIVERSIDAD TÉCNICA DE COTOPAXI	CRONOGRAMA DE RESPALDOS DE USUARIOS FINALES Y DE SERVIDORES	Anexo-01D
		Ver. No. 01

Fecha

Tabla 16. Cronograma de respaldos de usuarios finales y servidores.

UNIVERSIDAD TÉCNICA DE COTOPAXI	**CRONOGRAMA DE RESPALDOS DE USUARIOS FINALES Y DE SERVIDORES**	**Versión:**	01
	DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN	**Vigencia:**	

SERVIDOR	**FRECUENCIA DE RESPALDO DE INFORMACIÓN**						
	LUNES	**MARTES**	**MIERCOLES**	**JUEVES**	**VIERNES**	**SÁBADO**	**DOMINGO**
ARCHIVOS							
INCREMENTAL							
DOMINIO							
INCREMENTAL							
ANTIVIRUS							
INCREMENTAL							
APLICACIONES							
INCREMENTAL							
CORREO							
INCREMENTAL							
IMPRESIÓN							
INCREMENTAL							
WEB							
INCREMENTAL							

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC’s Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	USUARIOS DECLARADOS PARA RESPALDO DE INFORMACIÓN	Anexo-02D
		Ver. No. 01

Fecha

Tabla 17. Usuarios declarados para respaldo de información.

UNIVERSIDAD TÉCNICA DE COTOPAXI	USUARIOS DECLARADOS PARA RESPALDO DE INFORMACIÓN DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN			
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				

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC’s Fecha:

1. Objetivo

Proteger, planificar y dar seguimiento a los componentes informáticos de la institución, asegurándose que todos los equipos trabajen y sean usados de forma adecuada.

2. Alcance

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

3. Documentos de referencia.

RE-01E Ingreso y salida de equipos.

RE -02E Bitácora de control de antivirus

4. Descripción de la Política.

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.
- El seguimiento y control de estos antivirus serán gestionados por la Dirección de Tecnologías de la Información por medio del documento RE-02 “Control de antivirus”.
- 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.

Ingreso y salida de equipos.

- Los empleados deben contar con la debida autorización del departamento de tecnología, utilizando el documento RE-01E “Ingreso y salida de equipos” como referencia 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.

4. Registros.

Tabla 18. Documentos de referencia para la seguridad a componentes informáticos.

Código	Nombre	Responsable	Ubicación	Actualización	Retención	Acceso
RE-01E	Registro de ingreso y salida de equipos.	Departamento de Tecnologías de la Información	Oficina Sistemas área de Soporte a usuarios	Cada vez que se registre la entrada o salida de equipos informáticos.	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Uso interno
RE-02E	Bitácora de control de antivirus	Departamento de Tecnologías de la Información	Oficina Sistemas área de Soporte a usuarios	Cada vez que se registre la entrada o salida de equipos informáticos.	Hasta que el usuario salga de la Institución lo que se actualizará al final del año.	Uso interno

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC’s Fecha:

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

Tabla 19. Registro de entrada y salida de equipos.

UNIVERSIDAD TÉCNICA DE COTOPAXI	**REGISTRO DE ENTRADA Y SALIDA DE EQUIPOS** **DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN** Ver. No. 01				
DEPENDENCIA DE ORIGEN:				**FECHA:**	DD/MM/AA
ENTREGA					
DESCRIPCIÓN EQUIPO	**MARCA**	**MODELO**	**SERIE**	**Código institucional**	**COMENTARIOS ADICIONALES**

SERVICIO DE

PRÉSTAMO ( ) ASIGNACIÓN ( ) OTRO ( )

DEPENDENCIA RECEPTORA: C.I.:

OBSERVACIONES: FIRMA _____

RECIBE:	

(Nombre y firma de quién autoriza)

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	BITÁCORA DE ANTIVIRUS	RE-02E
		Ver. No. 01

Tabla 20. Bitácora de antivirus.

Fecha

N° Inventario PC	Ubicación	Nombre Antivirus	Tipo	Versión	Fecha última actualización	Estado	Responsable

Responsable: Grupo de investigación Fecha:	Aprobación: director de TIC's Fecha:

1. Objetivo

Establecer las normas que regulen el uso adecuado del servicio.

2. Alcance

Abarca a todos los usuarios de la comunidad Universitaria poseedores de un equipo de cómputo o dispositivo electrónico con el cual poseen acceso al servicio de internet.

3. Documentos de referencia.

Anexo-01F. Categorías de Filtrado Web.

4. Descripción de la Política.

El servicio institucional de internet se constituye en una herramienta tecnológica que facilita el cumplimiento de las funciones y responsables de los servidores de la Universidad. El área de redes e infraestructura es responsable de implementar las herramientas informáticas que permitan la administración del servicio institucional del internet, u minimizar los riesgos que afecte a la continuidad del servicio.

Departamento de Tecnologías de la Información.

- ✓ Posee la herramienta Fortinet (FortiGuard) la cual se encarga de negar por completo el acceso a los sitios web considerados inadecuados, nocivos o molestos para las funciones institucionales a realizar por los usuarios.
- ✓ Regular el acceso a internet por medio de un web filter según las categorías mencionadas en el Anexo-01F.
- ✓ Suministra todos los recursos necesarios para la administración y mantenimiento requerido para un seguro manejo del servicio de internet con las restricciones establecidas para cada perfil de acceso de usuario.
- ✓ Cada privilegio de uso de Internet estará delimitado por el nivel de acceso que requiera el desarrollo del cargo de cada usuario, por las categorías previamente 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.

✓ Llevará registro de la navegación y los accesos a internet de cada usuario conectado a internet, monitoreándolos en tiempo real para el correcto uso del servicio de internet.

Responsabilidad de los Usuarios.

✓ Solo tienen permitido hacer uso del servicio de internet para realizar actividades relacionadas con sus labores diarias en la institución.

✓ Tiene negado las descargas de cualquier tipo de software no autorizado, al igual que la instalación de estos por el motivo que este trabajo forma parte de las labores del Departamento de Tecnologías de la Información.

✓ Tiene prohibido el acceso a páginas pornográficas, al igual que páginas relacionadas con drogas, web proxys, hacking, redes sociales o cualquier otra que esté en contra de la ética y moral de la institución.

✓ Tiene determinantemente prohibido realizar la instalación o descarga de juegos videos, música o cualquier tipo de aplicaciones de páginas de internet que no cuenten con algún tipo de relación con la Universidad Técnica de Cotopaxi.

4. Registros.

N/A.

5. Anexo.

Anexo-01F. Categorías de Filtrado Web.

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	CATEGORÍAS DE FILTRADO WEB	Anexo-01F
		Ver. No. 01

En esta sección se detallará la información de las categorías de filtrado web:

Pornografía: Incluye toda página que tenga contenido sexual o erótico y sea inadecuado para menores de edad.

Compras: Categoría que restringe el acceso a todo tipo de tiendas en las cuales se pueda hacer compras online.

Sociedad / Educación / Religión: Categoría que restringe el acceso a páginas relacionadas con organismos gubernamentales y no gubernamentales, mapas, diccionarios, partidos políticos, contenido religioso y páginas web universitarias no relacionadas con la institución.

Juegos / apuestas: Categoría que restringe el acceso a páginas de apuestas, y juegos informáticos.

Redes sociales: Categoría que restringe el acceso a todo tipo de páginas web relacionadas con redes sociales y conecten personas de forma general con el objetivo de socializar, comerciar, etc.

Entretenimiento / cultura: Categoría que permite la restricción de acceso a páginas netamente de entretenimiento o cultura como: cine, televisión, música, etc.

Información y comunicación: Esta categoría restringe el acceso a páginas de noticias, periodismo y revistas.

Tecnologías de la información: Categoría que restringe el acceso a páginas de fabricantes de hardware y software, así como el alojamiento de sitios web de protección de datos como traducción de estos a otro idioma, incluyendo páginas que permiten visitar otros sitios web de forma anónima.

Drogas: Categoría que restringe el acceso a páginas con información de drogas no legales, incluyendo páginas que traten de drogas legales como el alcohol l tabaquismo, permitiendo al usuario concentrarse en su trabajo sin ningún tipo de distracciones.

Páginas privadas: Categoría que restringe el acceso a páginas de carácter personal y servicios de alojamiento.

Búsqueda de empleo: Categoría que restringe el acceso a todo tipo de páginas de oferta de empleo y agencias laborales incluyendo a la búsqueda de trabajos temporales.

Finanzas / Inversiones: Categoría de contenido a la información del mercado financiero, incluyendo la bolsa de valores y agentes de bolsa, además de bancas online que permitan realizar pagos excluyentes a los procesos financieros de la institución.

Armas: Categoría que permite restricción de acceso a páginas con contenido de todo tipo de armas de fuego y armas blancas.

Medicina: Categoría la cual restringe el acceso a páginas médicas, así como hospitales, farmacia, psicología y tiendas de medicina en general.
Aborto: Categoría que permite la restricción de acceso a páginas relacionadas con el aborto.

Una vez establecidas las categorías de filtrado web, el usuario tendrá acceso dependiendo de su nivel, permitiéndole ingresar a las diferentes categorías de filtrado web:

Tabla 21. 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, 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. Objetivo

Mantener el orden y la organización dentro de las instalaciones.

2. Alcance

Aplica a todos las personas que integran la comunidad universitaria, incluyendo contratistas, trabajadores temporales y cualquier ente externo autorizado por la institución para hacer uso de los laboratoritos de cómputo.

3. Documentos de referencia.

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

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

4. Descripción de la Política.

La presente política regulará la prestación de los servicios informáticos y el funcionamiento de todos los laboratorios de cómputo que la Universidad Técnica de Cotopaxi posee, facilitando su uso y la optimización de estos mediante el Departamento de Tecnologías de la Información de acuerdo a las solicitudes y necesidades de la comunidad universitaria.

Todo laboratorio de cómputo dependerá directamente del Departamento de Tecnologías de la Información y de las Unidades Académicas a las que correspondan.

Sobre la administración.

El administrador de cada laboratorio poseerá las siguientes funciones:

- Utilizar el documento RE-01G “Registro de docentes por uso de laboratorios” destinada a los docentes, con el cual llevará un registro de los docentes y sus horas de clase, y el documento RE.02 “Registro de estudiantes por uso de laboratorios” para el control de los estudiantes al utilizar los laboratorios.
- Regular el acceso de del personal a los laboratorios de cómputo.

- Administrar todos los recursos y accesorios que formen parte de los laboratorios de cómputo.
- Responder por el correcto de cada uno de los equipos informáticos.
- Efectuar un mantenimiento preventivo y correctivo de forma periódica, asegurando que los equipos informáticos que conforman los laboratorios se encuentren en perfecto estado.
- Gestionar y controlar el uso adecuado de los equipos informáticos asignados a cada uno de los usuarios.
- Garantizar un ambiente apropiado para el desarrollo de las actividades a realizar.
- Responsabilizarse por el orden de los laboratorios, antes y después de laborar una sesión de trabajo en ellos.
- Establecer que cada usuario cuente con un equipo de cómputo, garantizando su aprendizaje.

Unidades Académicas

- Todos los horarios académicos serán planeados con anticipación por todas las unidades académicas en coordinación con los administradores de cada uno de los laboratorios de cómputo.
- Toda unidad académica deberá realizar la entrega de los horarios académicos establecidos de los laboratorios de cómputo al departamento de Tecnologías de la Información 15 días antes de iniciar el ciclo académico.
- Disponibilidad de equipos con acceso a internet y/o uso de programas informáticos.
- Las unidades académicas realizarán el préstamo a entidades externas que requieran los espacios de los laboratorios de cómputo, previa a una autorización realizada al Rector.

Utilización eventual de los laboratorios de cómputo

- Están dirigidas a todo tipo de actividades de preparación y/o actualización a la comunidad universitaria y público en general, se realizará una solicitud dirigida al departamento de Tecnologías de la Información con 48 horas de anticipación para su debida coordinación previa a una autorización del rector o vicerrector.
- Se realizará una solicitud al departamento de Tecnologías de la Información para organizar una capacitación o actualización de los laboratorios en caso que se requiera un software específico, de tal manera se coordinará su instalación mediante esta autorización.
- Los servicios de determinadas aplicaciones de software serán suspendidos si no cuentan con las debidas licencias de uso.

Préstamo de equipos.

- Los equipos informáticos estarán disponibles solo para los responsables de los proyectos de investigación o áreas administrativas, solicitando de manera escrita al departamento de Tecnologías de la Información, el cual quien establecerá al funcionario responsable para que elabore el acta de entrega-recepción con las firmas correspondientes de resguardo de los bienes por el tiempo requerido.

De los usuarios.

- Para tener derecho al acceso de los servicios y recursos informáticos como los laboratorios de cómputo, los usuarios deberán presentar su identificación institucional otorgada por la Universidad Técnica de Cotopaxi o su cédula de identidad.
- El acceso a los laboratorios en las horas de clases se hará previa la reservación realizada al inicio del ciclo académico y serán realizadas de forma metódica y ordenada y solo en compañía del docente a cargo, en los horarios anteriormente establecidos. El tiempo de tolerancia para el ingreso al laboratorio será de un máximo de 10 minutos y los laboratorios deberán ser desocupados de forma inmediata después de la revisión del correcto funcionamiento de cada uno de los equipos informáticos posteriormente a las horas de clase.
- El docente asignado a dicha hora de clase se hará responsable del comportamiento de todos los alumnos que ingresen a los laboratorios de cómputo en sus horas de clase.
- Todo alumno que se encuentre matriculado de forma legal en la institución, tiene el derecho de usar los equipos de laboratorios en los horarios establecidos.
- Para realizar evaluaciones o actividades académicas extras y fuera de su horario de clases designados, el docente deberá realizar una solicitud escrita al responsable del laboratorio de cómputo con una anticipación de 48 horas.
- Todo software que se encuentre disponible en los laboratorios de cómputo con licencia, son de propiedad de la institución, prohibiendo su reproducción o copia.

4. Registros.

Tabla 22. Documentos de referencia para uso adecuado de laboratorios de computación.

Código	**Nombre**	**Responsable**	**Ubicación**	**Actualización**	**Acceso**
RE-01G	Registro de docentes por uso de laboratorios	Departamento TIC's	Oficina Sistemas área de Soporte a usuarios	Cada vez que un docente solicite el uso de los laboratorios	Uso interno
RE-02G	Registro de estudiantes por uso de laboratorios	Departamento TIC's	Oficina Sistemas área de Soporte a usuarios	Cada vez que un estudiante solicite el uso de los laboratorios	Uso interno

5. Anexos.

N/A.

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	**REGISTRO DE DOCENTES POR USO DE LABORATORIOS**	RE-01G
		Ver. No. 01

Tabla 23. Registro de uso de laboratorio Docentes

	Capus:			Ubicación:			Facultad:			
Fecha	**Responsable**	**Software utilizado**	**Ciclo**	**Carrera**	**Hora Uso**		**Número de Equipos**	**LAB. N°.**	**Observaciones**	**Firma**
					Entrada	**Salida**				

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC’s Fecha:

UNIVERSIDAD TÉCNICA DE COTOPAXI	**REGISTRO DE ESTUDIANTES POR USO DE LABORATORIOS**	RE-02G
		Ver. No. 01

Tabla 24. Registro de uso de laboratorio estudiantes

LABORATORIOS Y CENTROS DE COMPUTO BLOQUE ACADÉMICO "__"					
LABORATORIO N° ___					
	Carrera:		Periodo:		
DOCENTE:			HORA ENTRADA		HORA SALIDA:
MATERIA:					
CICLO:					
FECHA:					
SOFTWARE UTILIZADO:			TEMA DE CLASE:		
N.-	APELLIDOS Y NOMBRES	N.- CEDULA	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					
31					
32					
33					
34					
35					
36					
37					
38					
39					
40					
Observaciones:					
Firmas:					
	DOCENTE RESPONSABLE			**ADMINISTRADOR**	

Responsable: Grupo de investigación Fecha:	Aprobación: Director de TIC's Fecha:

5. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

El proceso de recolección de información para el desarrollo del proyecto se lo realizo directamente al encargado del departamento de las TIC's. Para la recopilación de datos se utilizó la técnica de la entrevista y la observación.

Una vez realizada la entrevista al Ing., Gustavo Rodríguez encargado del Departamento de las TIC's de la Universidad Técnica de Cotopaxi, se obtuvo información que más adelante se realizara su respectivo análisis. Mientras que en la observación fue el apoyo para obtener un mayor número de datos, tomando la información y registrándola para su posterior análisis

5.1. Análisis de Entrevista Aplicada

A continuación, se muestra los datos obtenidos de la entrevista realizada al encargado del departamento de TIC's.

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TEMA: DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, BASADO EN LA NORMA ISO 27000.

Tabla 25. Ficha de entrevista directa - Aplicada

Nombre del entrevistado: **Ingeniero Gustavo Rodríguez**	Fecha:
Esta entrevista será realizada para garantizar la efectividad del proyecto, dirigida al encargado del Departamento de tecnologías de la información.	
1. La Universidad cuenta con políticas de seguridad informática.	Sí, pero no están evidenciadas en documentos que regulen como hacerlo.
2. En la universidad se utiliza algún sistema o software para el almacenamiento de la información.	Si,

3. Qué sistema de almacenamiento de la información utilizan en la universidad.	Microsoft SQL Server
4. Utilizan algún servidor para almacenar la información	Si
5. Con que frecuencia se realiza el resguardo de información.	Se realizan frecuentemente cada 10 o 15 días, no hay un plan que regule esta acción.
6. La universidad cuenta con herramientas para realizar filtrado web.	Si
7. La universidad cuenta con filtrado web.	Si
8. Es importante establecer filtros web que registran el acceso a internet.	si
9. La universidad establece categorías de filtrado web para el acceso a internet.	Los mismos equipos Fortinet y Cico tienen sistemas de gestión, que tienen implícito categorías.
10. Cuenta la universidad con un Data Center.	si
11. Conoce que son las normas ISO 27000 relacionadas a la seguridad de la información.	si
12. La Universidad cuenta con un AD (Active Directory)	no
13. La Universidad cuenta con un VPN	si
14. Qué tipo de bases de datos utiliza la universidad	Microsoft SQL Server
15. Han realizado un análisis de riesgo dentro de la universidad.	no
16. Existen políticas de respeto a la seguridad de la información.	Sí, pero no están documentadas

17. Cree usted que la información que se maneja en la Universidad es segura.	Sí, pero puede mejorarse
18. Considera usted que la información es vulnerable a los hackers o personas mal intencionadas que podrían alterarlas.	No

Fuente: Encargado de Departamento de la TIC's

5.2. Resultados de la entrevista

A continuación, se presenta la interpretación a los resultados obtenidos de la entrevista realizada al Departamento de las TIC's de la Universidad Técnica de Cotopaxi.

Tabla 26. Ficha de entrevista directa - Resultados

FICHA DE ENTREVISTA
Esta entrevista será realizada para garantizar la efectividad del proyecto, dirigida al encargado del Departamento de tecnologías de la información.
1. La Universidad cuenta con políticas de seguridad informática. La universidad si cuenta con políticas de seguridad, pero no son políticas que no están evidenciadas en documentos.
2. En la universidad se utiliza algún sistema o software para el almacenamiento de la información. Si y el único sistema de gestión de datos que poseen es Microsoft SQL Server
3. Qué sistema de almacenamiento de la información utilizan en la universidad. Microsoft SQL Server que les permite almacenar y recuperar datos.
4. Utilizan algún servidor para almacenar la información Si
5. Con que frecuencia se realiza el resguardo de información. El departamento de TIC's de la Universidad realiza cada 10 o 15 días, el resguardo de la informacion.
6. La universidad cuenta con herramientas para realizar filtrado web.

Si, existen equipamientos de interconexión como son IPS firewall fortigate 1000 d, FortiSwitch 800 d capa 3 e IPS firewall Cisco MX400 y switch capa 3, que en su sistema de gestión permite el filtrado web.
7. La universidad cuenta con filtrado web. Si, cuenta con filtrado web.
8. Es importante establecer filtros web que registran el acceso a internet. Si, es muy importante establecer controles que regulen el acceso a internet.
9. La universidad establece categorías de filtrado web para el acceso a internet. Si son los mismos equipos Fortinet y Cico tienen sistemas de gestión.
10. Cuenta la universidad con un Data Center. Si, poseen un Data center
11. Conoce que son las normas ISO 27000 relacionadas a la seguridad de la información. Si, las conocen, pero no las han utilizado frecuentemente
12. La Universidad cuenta con un AD (Active Directory) No, cuentan con un Active Directory
13. La Universidad cuenta con un VPN Si, lo que permite estar conectados a los estudiantes a sitios web.
14. Qué tipo de bases de datos utiliza la universidad Únicamente utilizan Microsoft SQL Server
15. Han realizado un análisis de riesgo dentro de la universidad. No, en los últimos meses no lo han hecho
16. Existen políticas de respeto a la seguridad de la información. Sí, pero no están documentadas
17. Cree usted que la información que se maneja en la Universidad es segura. Sí, pero aun así existe el riesgo de amenaza a la información.
18. Considera usted que la información es vulnerable a los hackers o personas mal intencionadas que podrían alterarlas. No, la principal vulnerabilidad es confiar en la espontaneidad, no existen documentaciones de estos procedimientos y esa constituye la principal vulnerabilidad.

Fuente: Encargado de Departamento de la TIC's

5.3. Análisis de la Observación

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TEMA: DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, BASADO EN LA NORMA ISO 27000.

Tabla 27. Ficha de Observación

FICHA DE OBSERVACIÓN	
Fecha:	
Lugar:	**Universidad Técnica de Cotopaxi**
Encargado del departamento de tecnologías.	**Ingeniero Gustavo Rodríguez**
ASPECTO A VERIFICAR	***RESULTADOS***
1) La universidad posee políticas de seguridad informática.	No posee un registro de cómo llevar las políticas de seguridad.
2) Existe un control de acceso a los equipos y sistemas de cómputo.	No, pero para el acceso al área de la dirección de tecnologías de la información primero tienen que pasar por gerencia (la secretaria) la cual guía al solicitante a qué área de tecnologías de la información tiene que dirigirse.
3) Posee la universidad el Active Directory	No posee active directory.
4) Posee un sistema para respaldar la información	No cuenta con un sistema o algún tipo de registro para el respaldo de archivos.
5) Frecuencia de respaldo de información	Cada 7 o 15 días de manera espontánea sin realizar algún tipo de registro físico.
6) Seguridad a componentes informáticos.	No cuentan con algo establecido, algunas computadoras poseen seguridad para no ser extraídas como candados, pero no todas.

	Tampoco poseen algún registro que permita identificar el hardware que posee la Universidad. Para el acceso área de la data center posee una puerta de seguridad blindada, el data center trabaja con vmware ya que la mayoría de servidores se encuentran virtualizados.
7) Filtrado web	Utilizan la tecnología Fortinet para realizar el filtrado web.
8) Categorías de filtrado web	Solo usan el filtrado predeterminado que cuenta Fortinet, no han agregado algún tipo de filtrado extra.

Fuente: Departamento de la TIC's

Una vez obtenido los resultados de la entrevista y conociendo la necesidad que tiene el departamento de las TIC's, se procede a diseñar una política de seguridad informática, la estará basada en la norma ISO2700.

El correcto diseño y uso de las políticas permitirá a la Universidad específicamente al departamento de las TIC's, mantener segura la información y contrarrestará los riesgos y amenazas se suelen presentarse a nivel institucional.

5.4. Análisis de riesgos de la Universidad Técnica de Cotopaxi

5.4.1. Metodología para el análisis de riesgo

Para la elaboración del FODA se realiza un banco de preguntas que va dirigido al encargado de las TIC's lo cual nos va a permitir identificar las fortalezas, oportunidades, debilidades y amenazas que tiene el departamento de las TIC's.

Tabla 28. Cuestionario de Factores Internos y Externos

UNIVERSIDAD TÉCNICA DE COTOPAXI				
Entrevistado: Ing. Gustavo Rodríguez				
Cargo: Encargado del departamento de las TIC's.				
PREGUNTAS	**RESPUESTA**			**OBSERVACIONES**
FORTALEZAS				
	Siempre	A veces	Nunca	
1. Se realizan respaldos de las bases de datos	X			El procedimiento se realiza dentro de un servidor NAS de forma automática 4 veces al día y una vez a la semana de forma manual (no existe respaldo en la nube) No existe seguimiento para hacerlo
2. Cuentan con un antivirus	X			Los laboratorios cuentan con congeladores y en los distintos departamentos se utiliza software libre.
3. Infraestructura adecuada y equipamiento	X			
4. Cuentan con una red física estructurada	X			
DEBILIDADES				
	Siempre	A veces	Nunca	
1. Cuentan con plan de mantenimiento preventivo		X		El mantenimiento preventivo se realiza 1 vez al año y otro cada vez que se finaliza el ciclo académico.

				En laboratorios se realiza el mantenimiento cada semestre (hardware y software).
2. Se realizan respaldos de los equipos		X		El respaldo se realiza cada semestre o cada vez que se lo solicite.
3. Cuentan con listas de acceso para la navegación en internet			X	
4. Usan el dominio de email corporativo	X			
OPORTUNIDADES				
	Siempre	A veces	Nunca	
1. Existe presupuesto destinado a TIC's	X			
2. La página de la Universidad es un sitio seguro	X			
AMENAZAS				
	Siempre	A veces	Nunca	
1. Cuentan con políticas de seguridad informáticas		X		No posee políticas escritas
2. Cuentan con un acuerdo de confidencialidad de la información con los estudiantes			X	No se lo realiza de forma escrita pero sí de manera espontánea.
3. Cuentan con control de acceso a los equipos de computo		X		No todos los equipos informáticos cuentan con credenciales de acceso ni seguridad física suficiente.

4. Cuenta con un plan de contingencia por desastres naturales	X			

Fuente diseñado por: Cruz & Gaibor [16]

Rediseñado por: Los investigadores

Fuente: Departamento de la TIC's

5.5.Matriz de factores Internos y Externos

Para realizar la matriz de factores López, (2015) explica la asignación del campo valor que corresponde al impacto que ese factor tiene, se acerca a 1 si es muy importante y 0 es de poca importancia. Así mismo el campo de calificación que corresponde al tipo de respuesta está en capacidad de dar, va de 1 a 4 siendo 4 el nivel más alto.

Tabla 29. Tabla de rango de calificación de factores internos y externos

		CLASIFICACIÓN
Factores Internos	Fortalezas	Entre 3-4
	Debilidades	Ente 1-2
Factores externos	Oportunidades	Entre 3-4
	Amenazas	Entre 1-2

Fuente: (López, 2015) [17]

El resultado del total del valor ponderado de acuerdo con [17] menciona que se suma los valores, estos valores deben estar entre 1 y 4. Donde 1 es el valor mas bajo, 4 el valor mas alto y 2,5 es el valor promedio ponderado. Si el valor ponderado esta por debajo de la media, significaque la marca es debil internamente, mientras si el valor ponderado esta por encima.

Tabla 30. Factores Internos

FACTORES INTERNOS			
FORTALEZAS	**VALOR**	**CLASIFICACIÓN**	**VALOR PONDERADO**
Base de datos respaldados	0,17	4	0,68
Antivirus	0,15	3	0,45
Plan de contingencia	0,17	4	
Estructura de la red	0,17	4	0,68
DEBILIDADES			

Carencia de plan de mantenimiento	0,08	1	0,08
Respaldos a los equipos	0,18	2	0,18
Redes sociales y otras paginas	0,08	1	0,08
Total	1		2,15

Fuente diseñado por: Cruz & Gaibor [16]

Rediseñado por: Los investigadores

Fuente: Departamento de la TIC's

El valor ponderado de factores internos es de 2,15 lo que significa que el valor de factores internos está por debajo del valor promedio ponderado. Por lo que quiere decir que el valor puede encontrarse débil internamente

Tabla 31. Factores externos

FACTORES EXTERNOS			
OPORTUNIDADES	**VALOR**	**CLASIFICACIÓN**	**VALOR PONDERADO**
Presupuesto destinado a las TIC's	0,17	3	0,51
Plan de contingencia	0,18	4	0,72
Control de acceso a páginas seguras	0,17	3	0,51
AMENAZAS			
Carencias políticas de seguridad	0,16	1	0,16
Acuerdos de confidencialidad de la información	0,16	1	0,16
Escaso nivel de seguridad	0,16	1	0,16
Total	1		2,22

Fuente diseñado por: Cruz & Gaibor [16]

Rediseñado por: Los investigadores

Fuente: Departamento de la TIC's

El valor ponderado de factores internos es de 2,22 lo que significa que el valor de factores internos está por debajo del valor promedio ponderado. Por lo que quiere decir que el valor puede encontrarse débil internamente.

5.6. Matriz para el análisis de riesgo

Para [19] la matriz de riesgo, Se utiliza la matriz de riesgo como herramienta de análisis y determinación del nivel de los mismos, en términos alto, medio o bajo, para gestionar las acciones a tomar y en consecuencia darles respuesta e incluso diseñar controles internos que permitan cubrirlos, minimizarlos y/ o eliminarlos.

La matriz de riesgo permitirá evaluar el riesgo por lo que se realizará un diagnóstico de la situación de la institución, se calculará utilizando la formula Riesgo = Impacto x probabilidad.

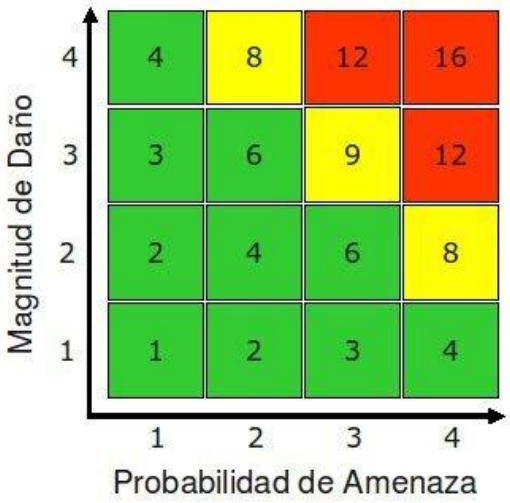
En virtud de esto se debe realizar la identificación de las actividades principales además de los riesgos a la que puede estar expuesta. Seguidamente desde su concepción metodológica las matrices se componen de dos vectores. Estos vectores tienen valores que están en un rango:

Bajo riesgo: menor o igual que 2 (Verde)

Medio riesgo: mayor 2 y menor o igual que 4 (amarrillo)

Alto riesgo: Mayor o igual que 4 (rojo)

Figura 5. Niveles de riesgo



Fuente: [20]

De acuerdo a los antecedentes investigados acerca de la matriz de riesgo se procede a llenar la matriz tomando en consideración la información que se obtuvo del departamento de las TIC’s, de la Universidad Técnica de Cotopaxi.

Tabla 32. Valoración de Probabilidad de Amenaza

	AMENAZAS	IMPACTO	PROBABILIDAD	TOTAL	
Recursos humanos	Divulgación de información	2	4	8	11,14
	Perdidas de datos	3	4	12	
	Saturación de información	3	4	12	
	Procesamiento de datos ilegales	4	4	16	
	Robos de equipo	3	4	12	
	Destrucción de los equipos o medios	2	3	6	
	Códigos maliciosos	3	4	12	
Sucesos derivados de la negligencia de los usuarios y decisiones institucionales	Falta de mantenimiento físico	3	1	3	11.6
	Modificación de la información	3	4	12	
	Datos de fuentes no confiables	4	4	16	
	Cambio Hardware	3	4	12	
	Cambio Software	3	4	12	
	Falla de equipo	3	4	12	

	Falta de disponibilidad de los recursos humanos	3	4	12	
	Monitoreo del tráfico de la red	3	4	12	
	Uso de contraseñas débiles	4	4	16	
	Acceso a los archivos de contraseñas	3	3	9	
Estructuras físicas / Daños naturales	Sobre carga eléctrica	3	2	6	8.28
	Interrupción de fuentes de energía	3	3	9	
	Fenómeno climático	3	4	12	
	Fenómeno volcánico	3	3	9	
	Fenómeno sísmico	3	3	9	
	Fuego	1	4	4	
	Errores en los sistemas operativos	**3**	**3**	**9**	

Fuente diseñado por: Cruz & Gaibor [16]

Rediseñado por: Los investigadores

Fuente: Departamento de la TIC’s

5.7. Análisis de riesgo promedio

La valoración de la probabilidad de amenazas según sus resultados:

- **Baja**: Muy lejana la posibilidad de un ataque.
- **Mediana:** Sostienen que existen condiciones que hacen poco probable un ataque en corto plazo, pero no son suficientes para evitarlo en largo plazo.
- **Alta:** El ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque.

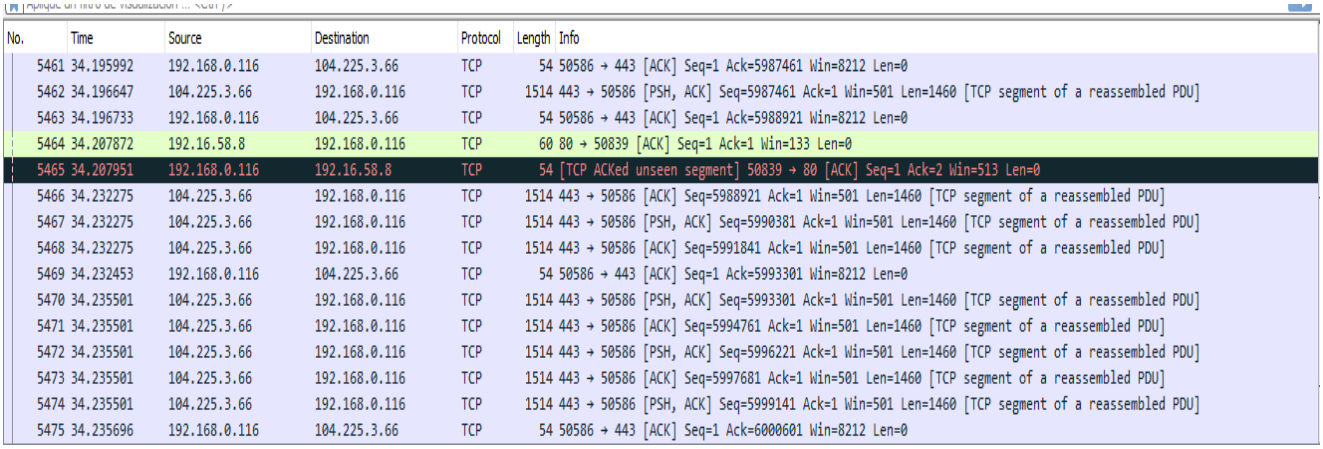
Para continuar con el análisis de riesgos depende de la información obtenida en las fases de identificación anteriormente descritas, de esta forma se procede a hacer la calificación del riesgo, en el cual se realiza una estimación, del cual podría ser la probabilidad de ocurrencia del riesgo y el impacto que traería este.

De manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final de la matriz, así es como la los recursos humanos y Sucesos derivados de la negligencia de los usuarios y decisiones institucionales sostiene un nivel de riesgo alto, mientras que la zona de riesgo de Estructuras físicas / Daños naturales, se encuentra dentro del estándar de riesgo mediano. Por lo que con la creación de las políticas de seguridad permitirá una mejor protección de la información de la Universidad.

5.8.Análisis de trafico de red mediante Wireshark.

Con la ayuda del Software Wireshark, programa que permite analizar y solucionar el tráfico de red de comunicaciones en tiempo real. Con esta herramienta ayudo a detectar los datos y los protocolos que se realiza en la Universidad Técnica de Cotopaxi.

Figura 6. Salvapantalla de programa Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
5461	34.195992	192.168.0.116	104.225.3.66	TCP	54	50586 → 443 [ACK] Seq=1 Ack=5987461 Win=8212 Len=0
5462	34.196647	104.225.3.66	192.168.0.116	TCP	1514	443 → 50586 [PSH, ACK] Seq=5987461 Ack=1 Win=501 Len=1460 [TCP segment of a reassembled PDU]
5463	34.196733	192.168.0.116	104.225.3.66	TCP	54	50586 → 443 [ACK] Seq=1 Ack=5988921 Win=8212 Len=0
5464	34.207872	192.16.58.8	192.168.0.116	TCP	60	80 → 50839 [ACK] Seq=1 Ack=1 Win=133 Len=0
5465	34.207951	192.168.0.116	192.16.58.8	TCP	54	[TCP ACKed unseen segment] 50839 → 80 [ACK] Seq=1 Ack=2 Win=513 Len=0
5466	34.232275	104.225.3.66	192.168.0.116	TCP	1514	443 → 50586 [ACK] Seq=5988921 Ack=1 Win=501 Len=1460 [TCP segment of a reassembled PDU]
5467	34.232275	104.225.3.66	192.168.0.116	TCP	1514	443 → 50586 [PSH, ACK] Seq=5990381 Ack=1 Win=501 Len=1460 [TCP segment of a reassembled PDU]
5468	34.232275	104.225.3.66	192.168.0.116	TCP	1514	443 → 50586 [ACK] Seq=5991841 Ack=1 Win=501 Len=1460 [TCP segment of a reassembled PDU]
5469	34.232453	192.168.0.116	104.225.3.66	TCP	54	50586 → 443 [ACK] Seq=1 Ack=5993301 Win=8212 Len=0
5470	34.235501	104.225.3.66	192.168.0.116	TCP	1514	443 → 50586 [PSH, ACK] Seq=5993301 Ack=1 Win=501 Len=1460 [TCP segment of a reassembled PDU]
5471	34.235501	104.225.3.66	192.168.0.116	TCP	1514	443 → 50586 [ACK] Seq=5994761 Ack=1 Win=501 Len=1460 [TCP segment of a reassembled PDU]
5472	34.235501	104.225.3.66	192.168.0.116	TCP	1514	443 → 50586 [PSH, ACK] Seq=5996221 Ack=1 Win=501 Len=1460 [TCP segment of a reassembled PDU]
5473	34.235501	104.225.3.66	192.168.0.116	TCP	1514	443 → 50586 [ACK] Seq=5997681 Ack=1 Win=501 Len=1460 [TCP segment of a reassembled PDU]
5474	34.235501	104.225.3.66	192.168.0.116	TCP	1514	443 → 50586 [PSH, ACK] Seq=5999141 Ack=1 Win=501 Len=1460 [TCP segment of a reassembled PDU]
5475	34.235696	192.168.0.116	104.225.3.66	TCP	54	50586 → 443 [ACK] Seq=1 Ack=6000601 Win=8212 Len=0

Fuente: Programa Wireshark

5.9.Plan de mitigación de riesgos

Tabla 33. Plan de mitigación de riesgos

Objetivo	**Riesgo**	**Actividad de Control**	**Responsable**
Incrementar la seguridad de la información en los equipos.	F. interno: Respaldo equipos	Gestionar una política que contenga un cronograma para respaldos	Encargado del departamento de las TIC's
	F. Externo plan de contingencia	Recomendar utilizar el plan de contingencia	Encargado del departamento de las TIC's
Controlar los equipos que ingresen a la institución además	F. interno. Acceso a redes sociales	Proponer una política sobre el uso adecuado del internet	Encargado del departamento de las TIC's

de reducir la saturación de la red por mal uso del internet.	F. Externo Nivel de seguridad bajo, en el control de acceso a equipos	Política sobre el control de acceso	Encargado del departamento de las TIC's
Diseñar políticas de seguridad informática para proteger la información.	F. interno Carecer un plan de mantenimiento preventivo	Uso de las políticas de seguridad.	Encargado del departamento de las TIC's
	F. externo Carencia de políticas de seguridad informática.	Implementar las políticas a diseñar	Encargado del departamento de las TIC's

Elaborado por: los investigadores

6. IMPACTOS TÉCNICOS, SOCIALES Y ECONÓMICOS

6.1 Impactos técnicos

Desarrollo de políticas de seguridad informática utilizando la norma ISO 27000, ayudaran a disminuir los riesgos y amenazas que se puedan suscitar dentro de la Universidad, a su vez nos permitirá cuidar y proteger la confidencialidad, integridad y disponibilidad de la información.

6.2 Impactos sociales

En las últimas décadas las políticas de seguridad informática se han convertido en un eje muy importante dentro de las distintas organizaciones e instituciones ya que proteger cualquier tipo de información de situaciones de riesgo o amenaza, permiten controlar el acceso a los equipos y sistemas computacionales de la institución.

6.3 Impactos económicos

Una vez obtenido el diseño de las políticas de seguridad e implementado en el departamento de las TIC’s de la Universidad se reducirán las pérdidas de datos, se evitarán tráfico de datos entre otras cosas, lo cual mas adelante los costos asociados a solucionar dichos problemas serán un ahorro para los gastos de la universidad.

7. CONCLUSIONES Y RECOMENDACIONES

7.1 CONCLUSIONES

- Se recopiló la información de manera adecuada para identificar los riesgos de seguridad informática que puede afectar a la información del Departamento de Tecnologías de la Información.
- Después de identificar los riesgos a los que está expuestos la información en la Dirección de Tecnologías de la Información, se procedió al diseño de políticas de seguridad informática en el cual tuvo base el uso de la norma ISO/IEC 27000, la cual tiene como propósito el aseguramiento, la confidencialidad e integridad de la información y de los sistemas que van procesar.
- Al contar con el diseño de políticas de seguridad informática, la Universidad Técnica de Cotopaxi podrá poseer una guía para neutralizar los riesgos a los cuales se encuentran expuestas, además de que servirá como pauta para el correcto uso de los recursos informáticos con los que cuenta la institución.

7.2 RECOMENDACIONES

- El encargado del departamento de las TIC’s debe realizar el mantenimiento análisis de riesgo, cada 6 meses para conocer potenciales amenazas, pues la seguridad que se requiere es permanente para lo cual es necesario de un proceso continuo.
- Concientizar al o los encargados del departamento de las TIC’s de la universidad sobre las políticas de seguridad informática para contribuir al cumplimiento de las mismas, y así mitigar los riesgos a los cuales se encuentran expuestos y reducir los costos que se deriven por algún suceso informático.
- Establecer programas de mejora continua para mantener en constante actualización al personal del departamento de las TIC’s como también a docentes y estudiantes de la Universidad, sobre los diferentes métodos para la seguridad de la información que a diario van cambiando, proponiendo mejores resultados.

8. MANUAL DE IMPLEMENTACIÓN DE UN ACTIVE DIRECTORY CON WINDOWS SERVER 2012, SIMULACIÓN.

8.1. ALCANCE.

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

8.2. DESCRIPCIÓN DEL MANUAL.

La Universidad, consciente de ejecutar buenas prácticas para el uso adecuado de sus recursos informáticos, establece la implementación de un Active Directory que facilitará la administración de todos los elementos lógicos (usuarios, equipos y recursos informáticos).

De tal forma que en este manual se describirá los pasos necesarios para la implementación de un Active Directory.

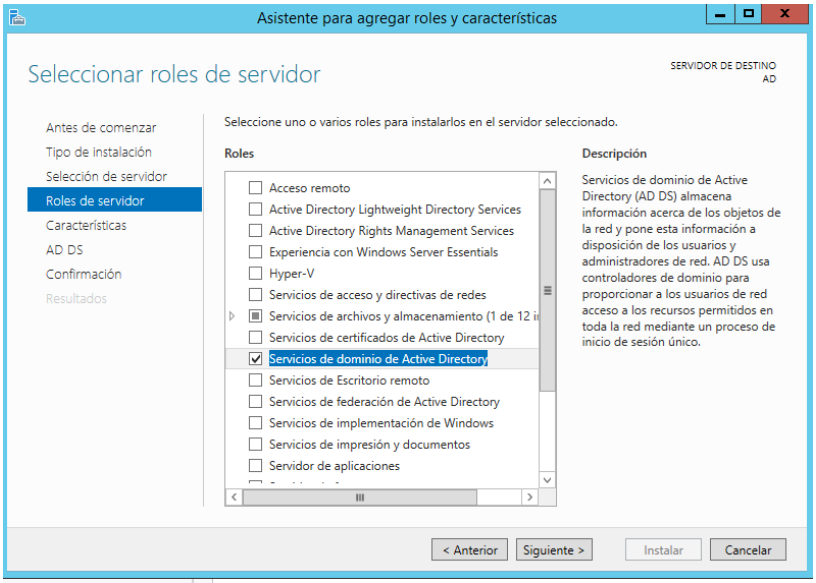
8.2.1. Recursos necesarios:

- Máquina virtual con Windows Server 2012 (Usuario: Administrador Contraseña: Server2012@).
- Máquina virtual con Windows 10 (Usuario: Administrador Contraseña:).
- Máquina virtual con Windows 8.1 (Usuario: Administrador Contraseña:).

8.2.2. Pasos a seguir:

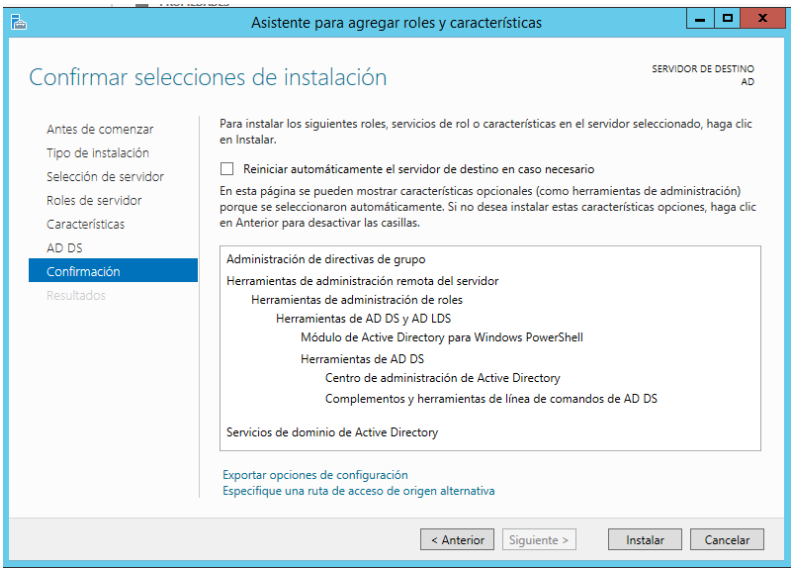
- Iniciamos el Asistente para agregar roles y características y seleccionamos “Servicio de dominio de Active Directory”.

Figura 7. Programa Active Directory.



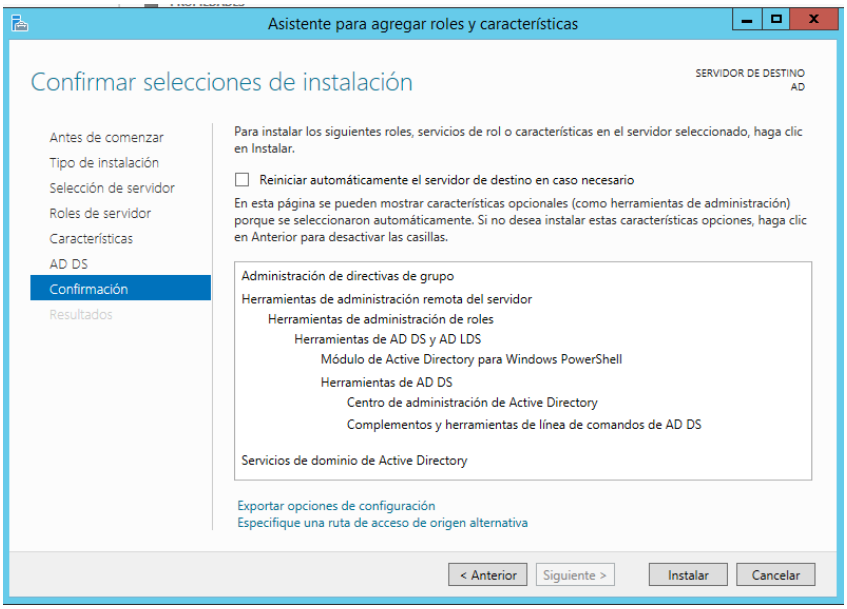
- Seleccionamos “Siguiente” y confirmamos la instalación.

Figura 8. Confirmación de Instalación



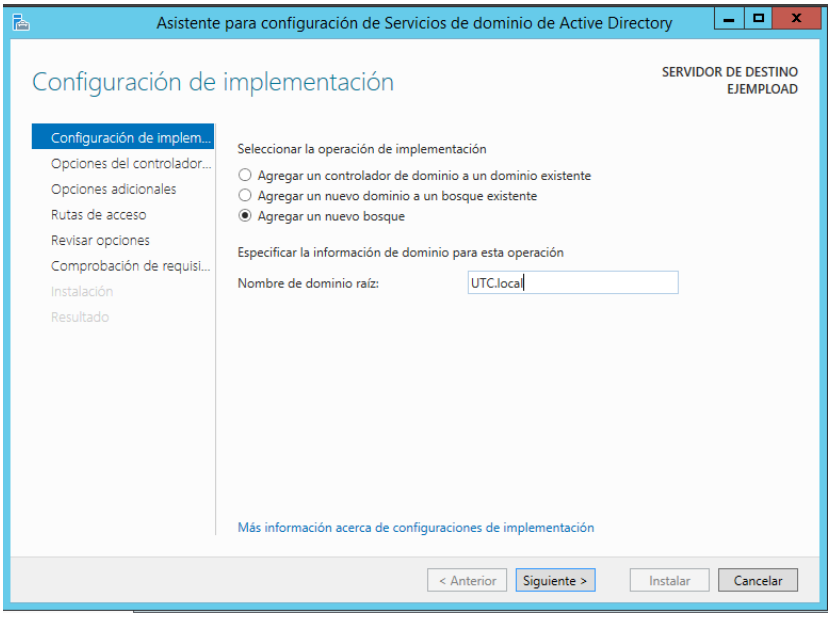
- Al finalizar la instalación seleccionamos “Promover este servidor a controlador de dominio”.

Figura 9. Promover este servidor a controlador de dominio



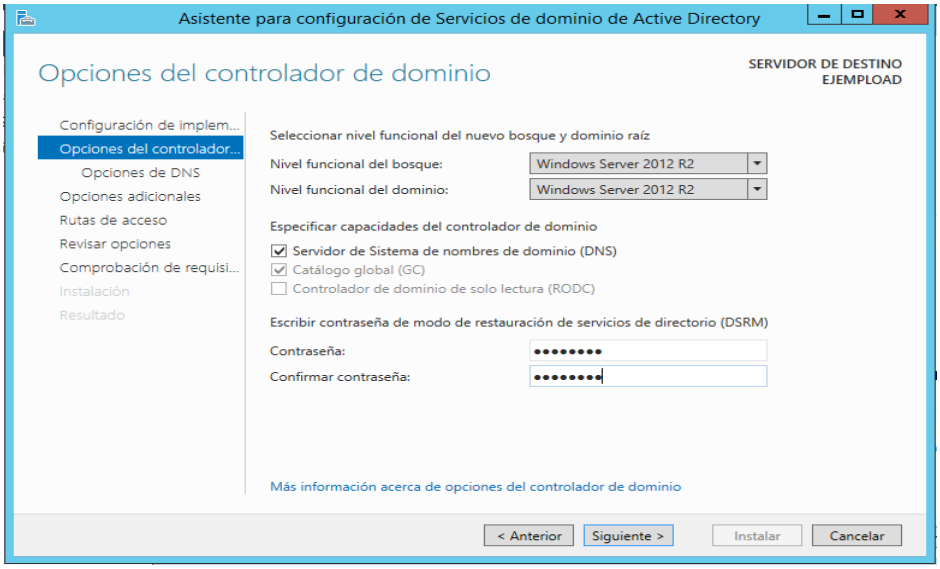
- Seleccionar la opción "Agregar un nuevo bosque" y escogemos el nombre del dominio raíz (UTC. local).

Figura 10. Agregar un nuevo bosque



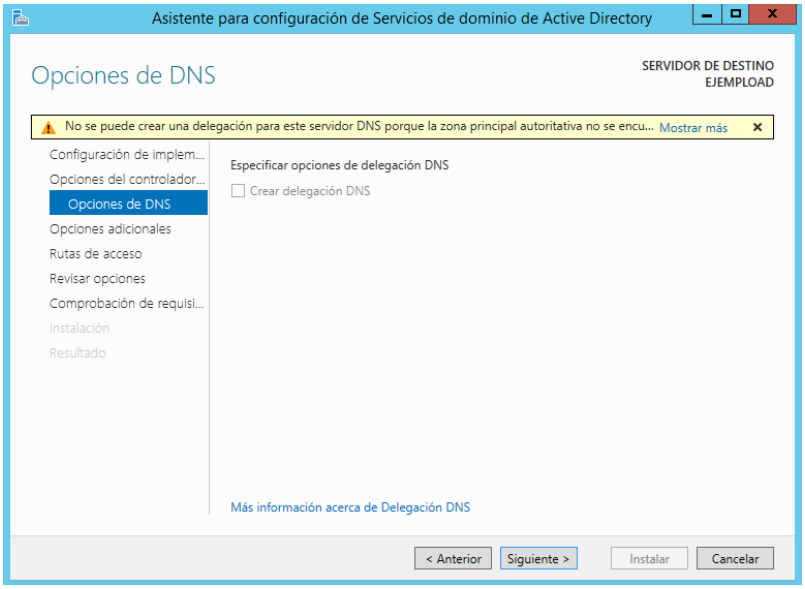
- Ingresamos una contraseña con todos los requisitos de complejidad por si falla o existe algún problema con el controlador de dominio (12345678@Q).

Figura 11. Controlador de dominio



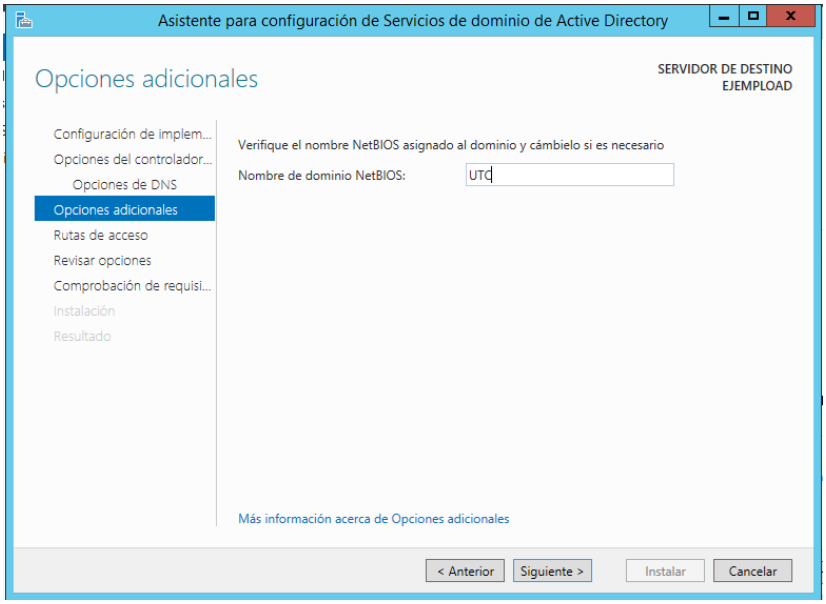
- Seleccionar siguiente después del mensaje de advertencia que aparecerá por ser el primer servidor de dominio.

Figura 12. Mensaje de advertencia



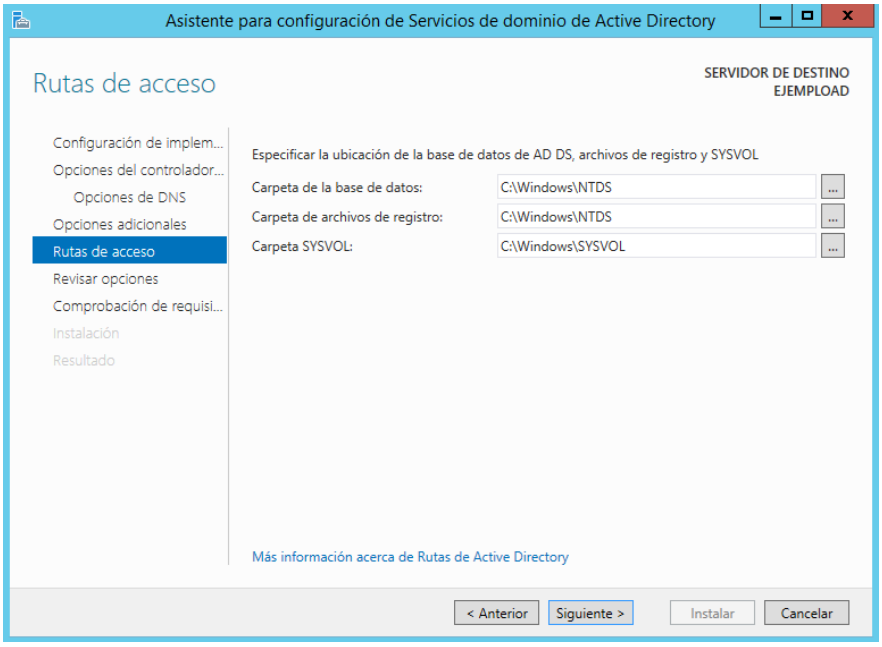
- Ingresar el nombre de dominio de NetBIOS (UTC) y después siguiente.

Figura 13. Dominio de NetBIOS (UTC)



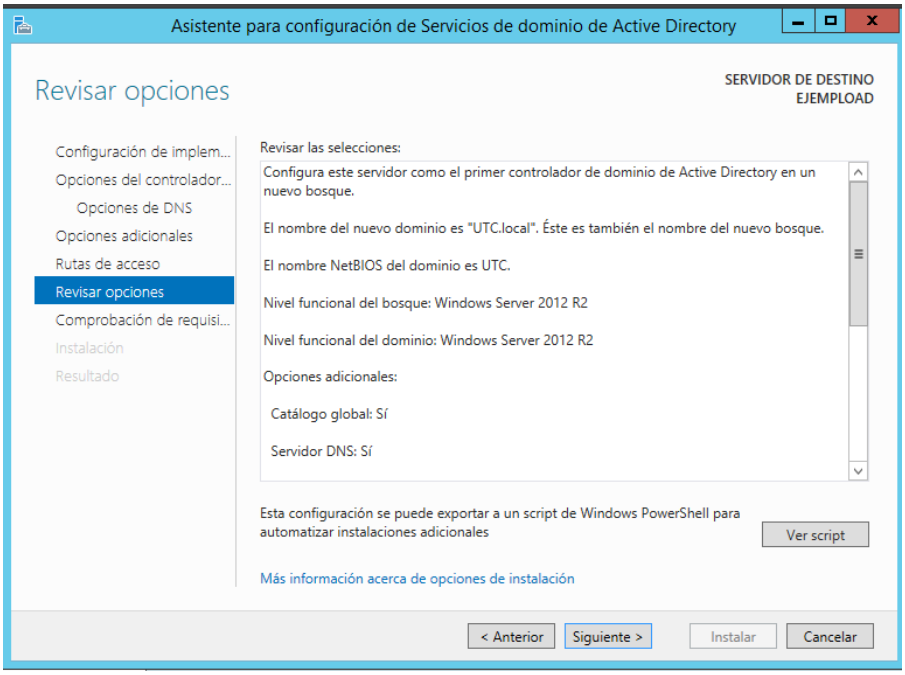
- Confirmar la ruta de la ubicación de los archivos (es recomendable que la carpeta de la base de datos se encuentre en otro disco duro).

Figura 14. Ruta de la ubicación de los archivos



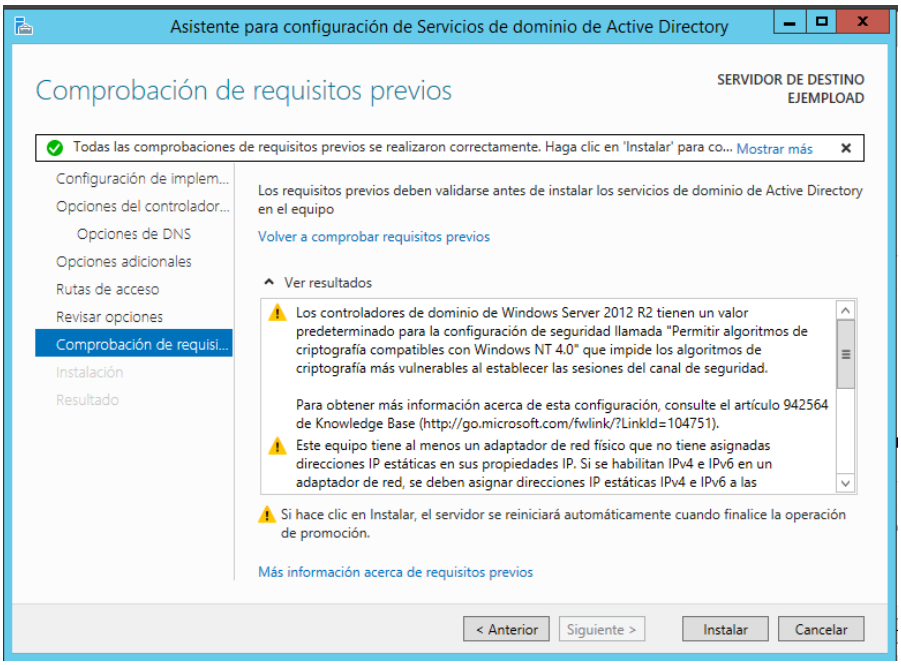
- Click en siguiente después de visualizar el resumen de opciones.

Figura 15. Revisar opciones



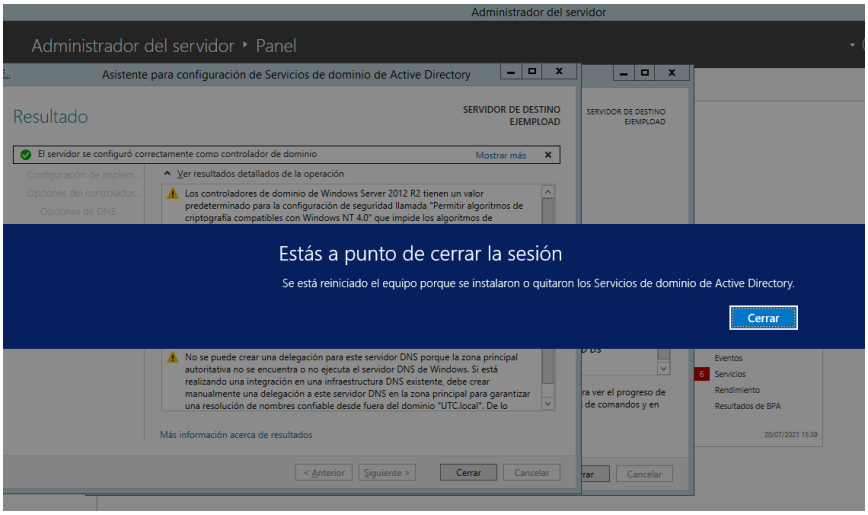
- En comprobación de requisitos se confirma que los requisitos previos se realizaron correctamente, seleccionar “Instalar”.

Figura 16. Comprobación de requisitos



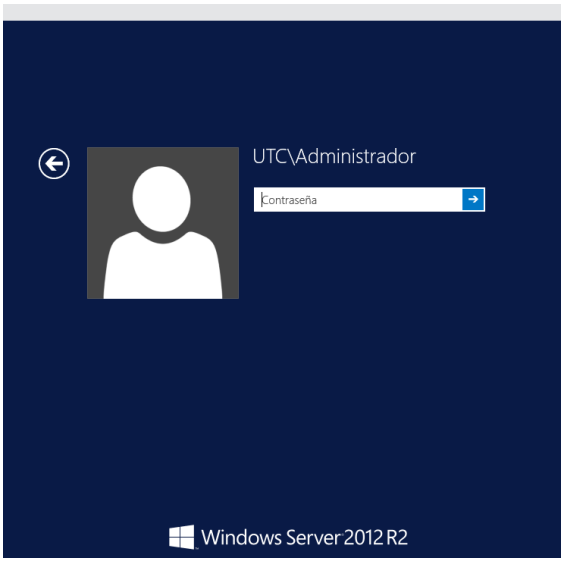
- Al finalizar la instalación se reiniciará el servidor automáticamente.

Figura 17. Reiniciación automática



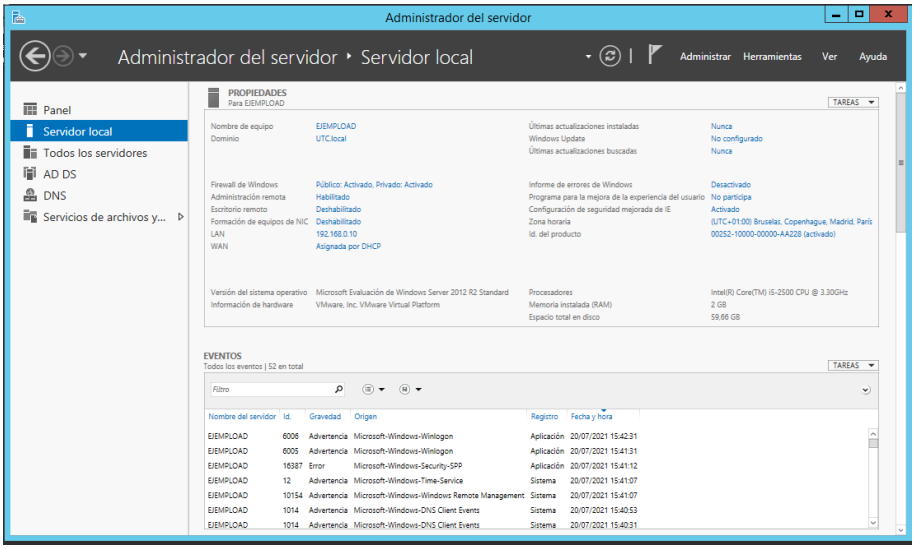
- Al reiniciarse el servidor, en el inicio de sesión ya se antepondrá el dominio después del usuario.

Figura 18. Inicio de sesión



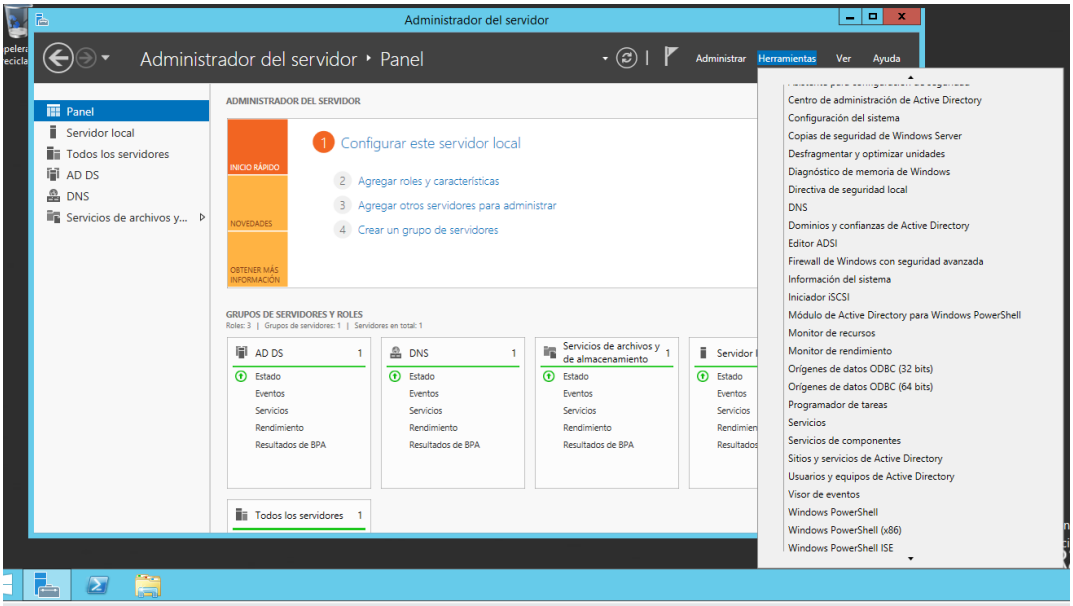
- En el Administrador del servidor – Servidor local se observará el nombre del dominio anteriormente seleccionado.

Figura 19. Administrador del servidor



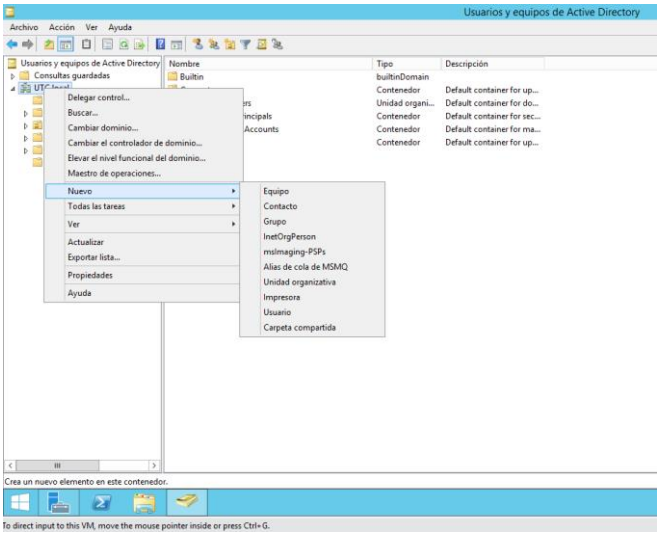
- Dirigirse a Herramientas – “Usuarios y equipos de Active Directory”.

Figura 20. Usuarios y equipos de Active Directory



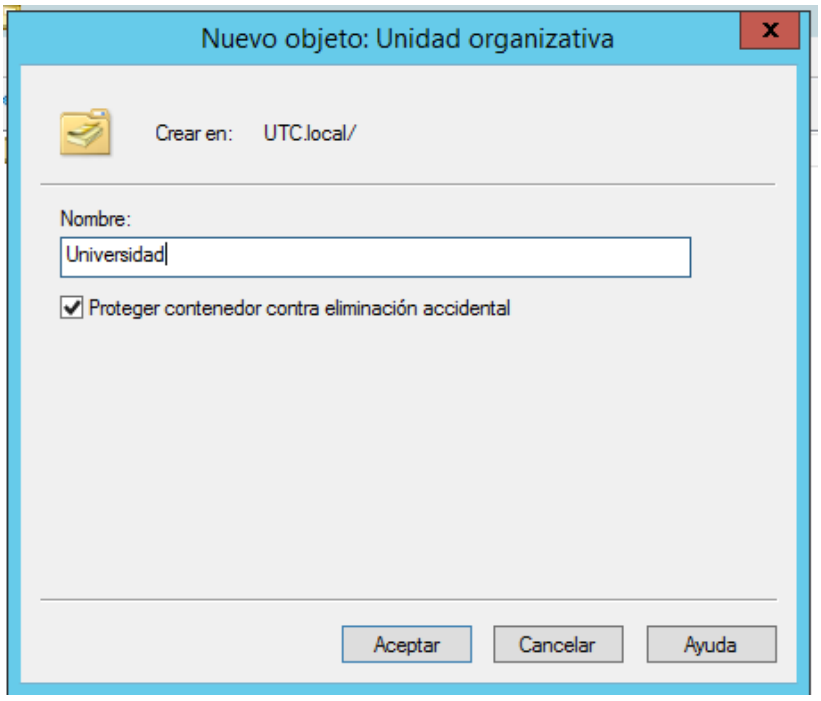
- En el nombre del dominio (UTC.local) crear una nueva unidad organizativa.

Figura 21. Nueva Carpeta



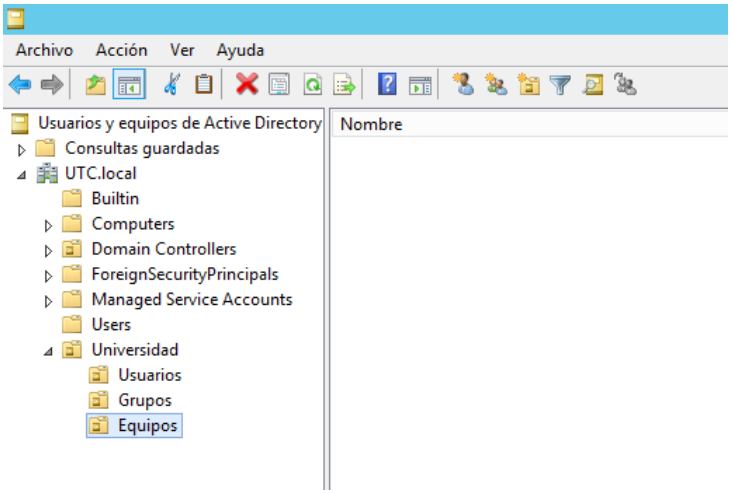
- Ingresar el nombre de la nueva Unidad organizativa (Universidad).

Figura 22. Nombre de la nueva Unidad



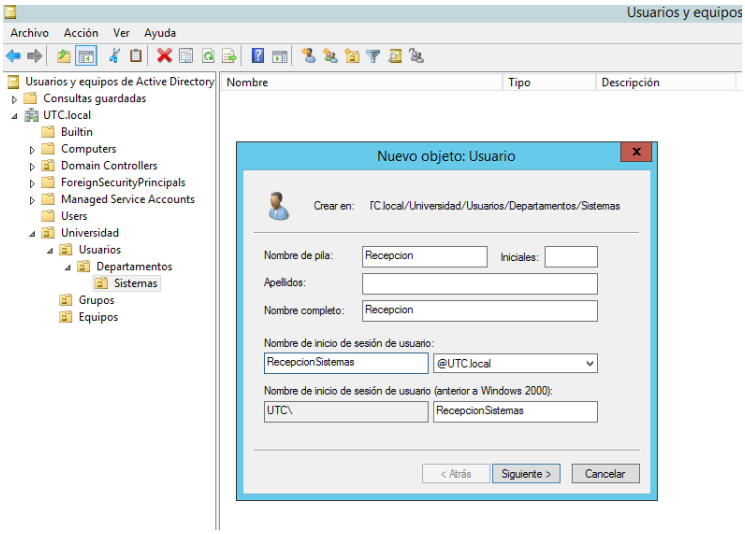
- Crear Subunidades organizativas para mayor organización (Usuarios, Grupos y Equipos).

Figura 23. Crear Subunidades



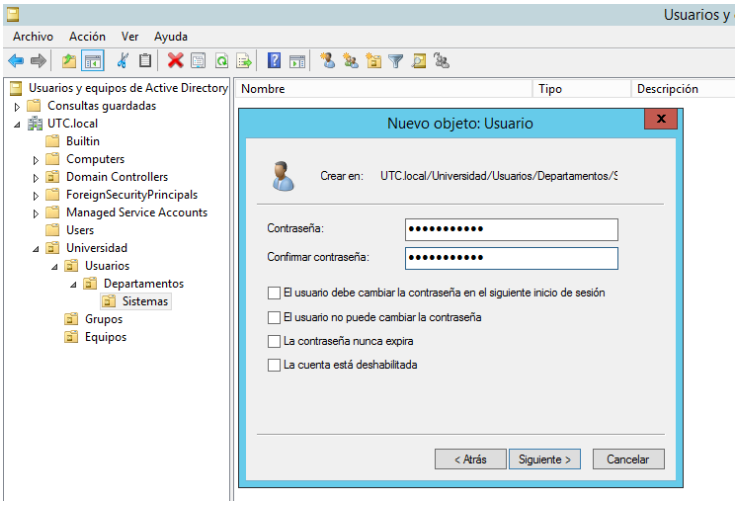
- En usuarios, crear nuevo objeto: usuario.

Figura 24. Crear nuevo objeto



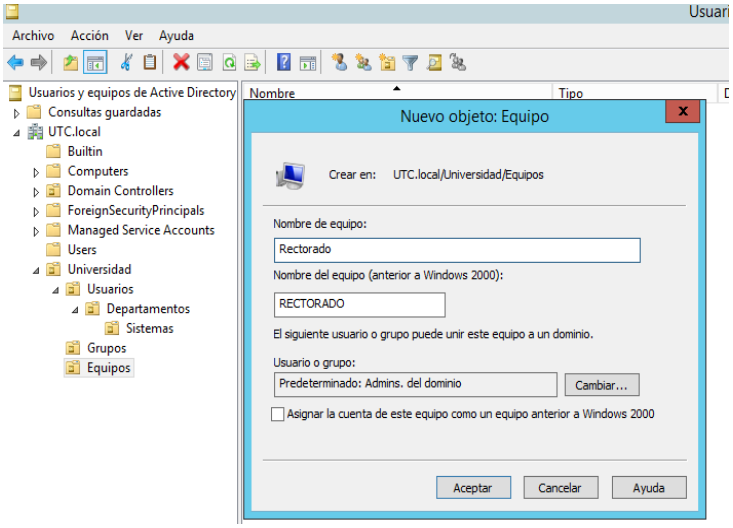
- Ingresar la contraseña con la complejidad necesaria de mayúsculas, minúsculas, caracteres especiales y números (SistemasR#2021).

Figura 25. Crear Contraseña



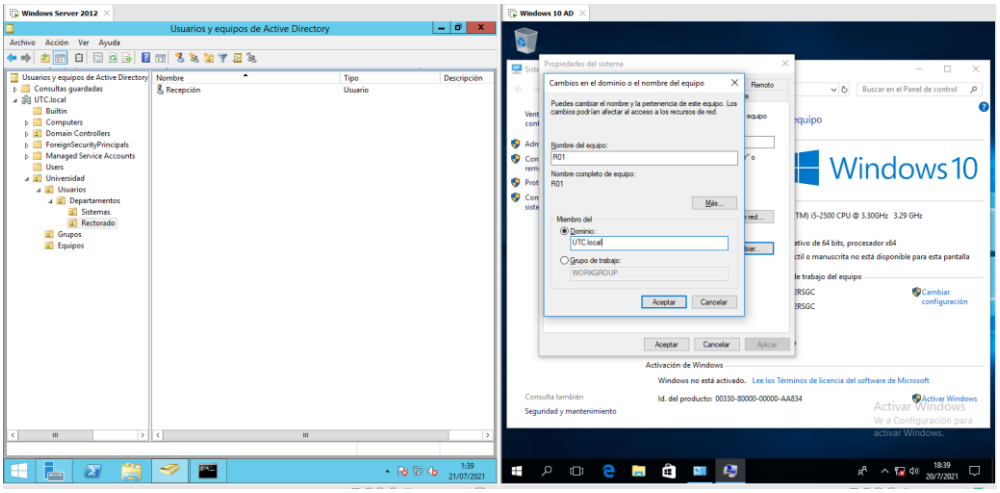
- De igual manera se puede crear equipos de forma manual.

Figura 26. Crear equipos



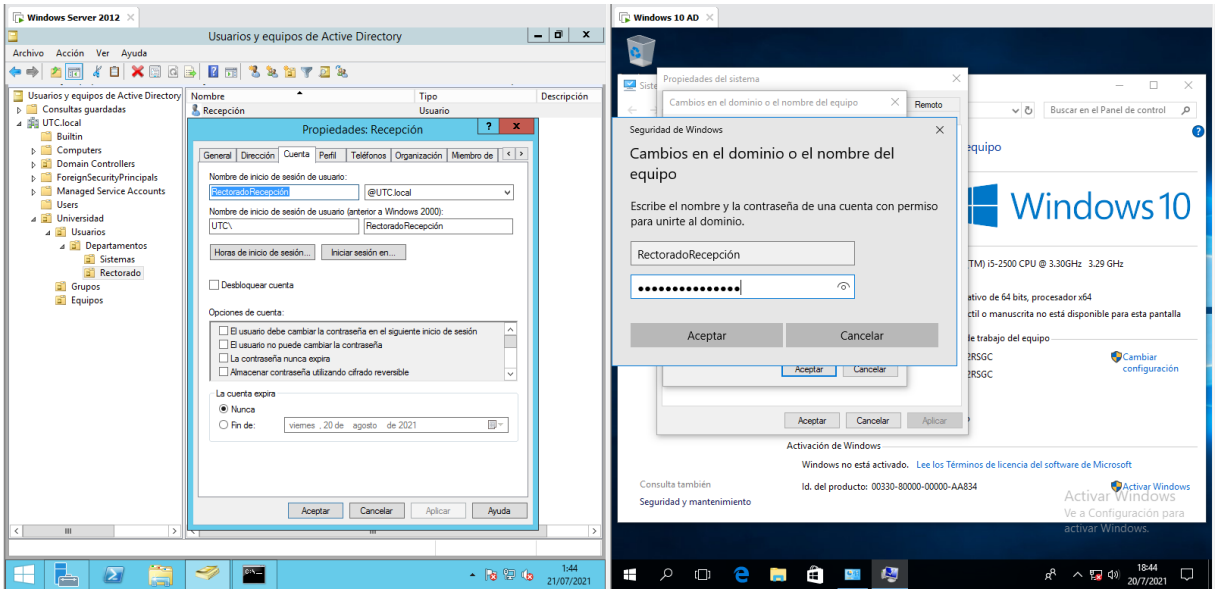
- Para unir un cliente-equipo con un servidor, en la máquina virtual con Windows 10, dirigirse a Información del sistema – Cambiar configuración.
- Renombrar el equipo y escribir el dominio anteriormente creado (UTC.lcoal).

Figura 27. Unir un cliente-equipo



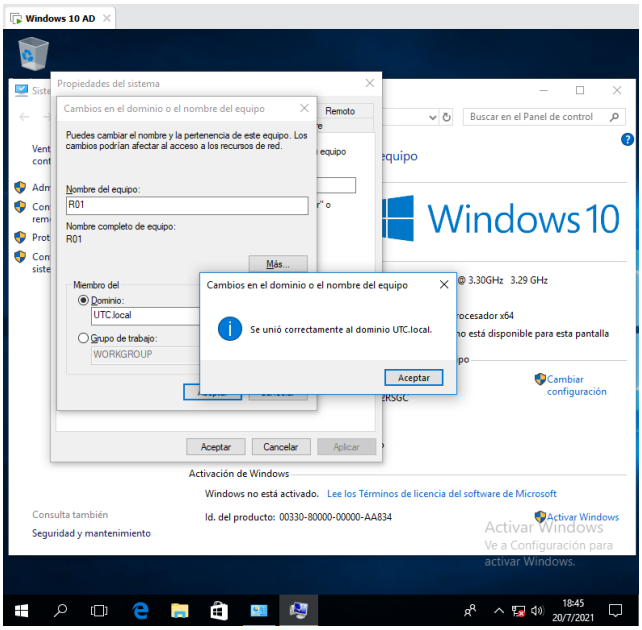
- Ingresar las credenciales del primer usuario (Rectorado Recepción C: RecepciónR#2021).

Figura 28. Ingresar las credenciales del primer usuario



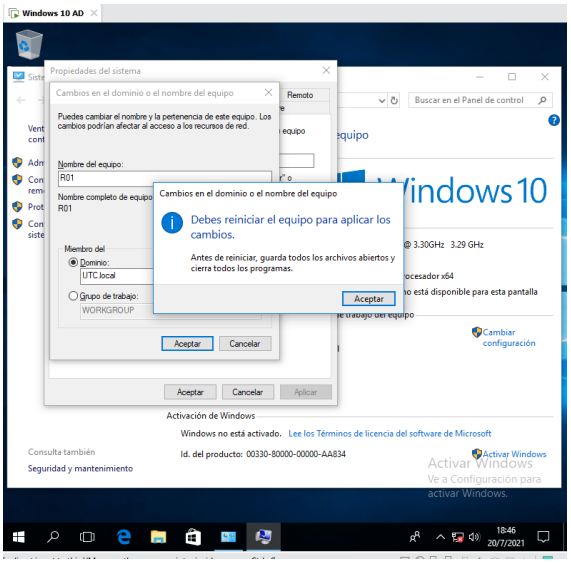
- Aparecerá el mensaje informando que se unió correctamente al dominio UTC.local

Figura 29. Unión de dominio



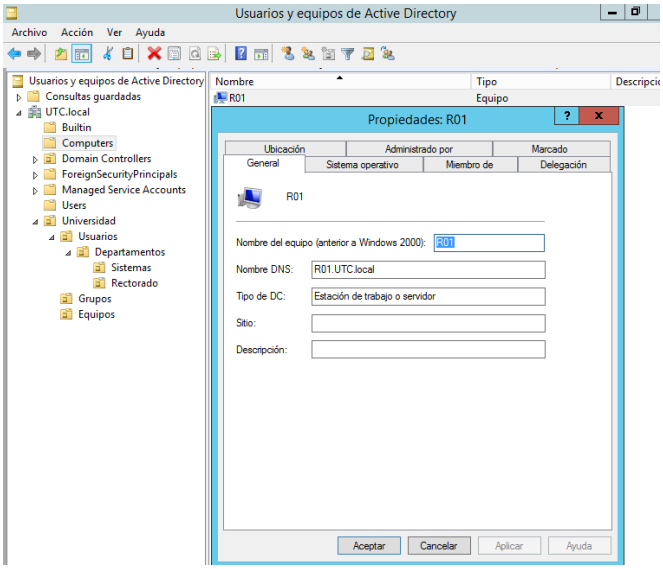
- Es necesario reiniciar el equipo para poder iniciar sesión con las nuevas credenciales.

Figura 30. Reinicio del equipo



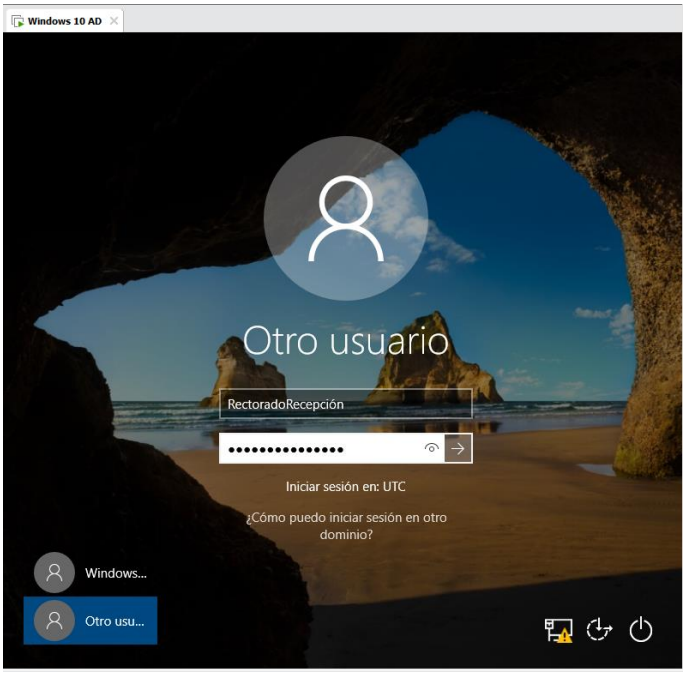
- En la máquina virtual con Windows Server 2012, en “Computers” se visualiza el equipo recién agregado al dominio.

Figura 31. Dominio



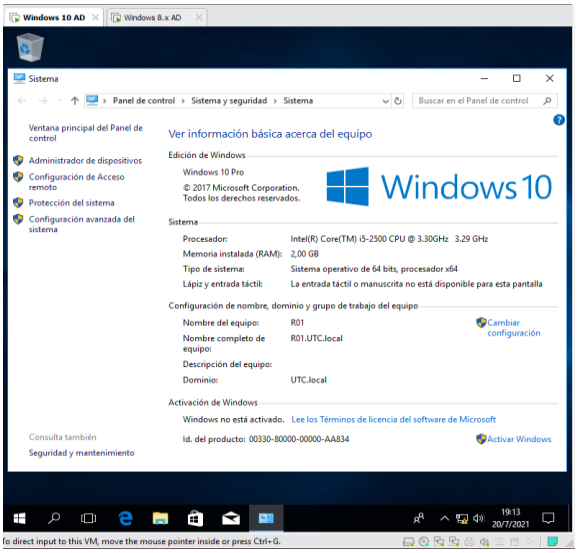
- Al reiniciar el equipo con Windows 10 seleccionamos otro usuario e ingresamos las credenciales correctas (U: Rectorado Recepción C: RecepciónR#2021).

Figura 32. Reiniciar el equipo con Windows 10



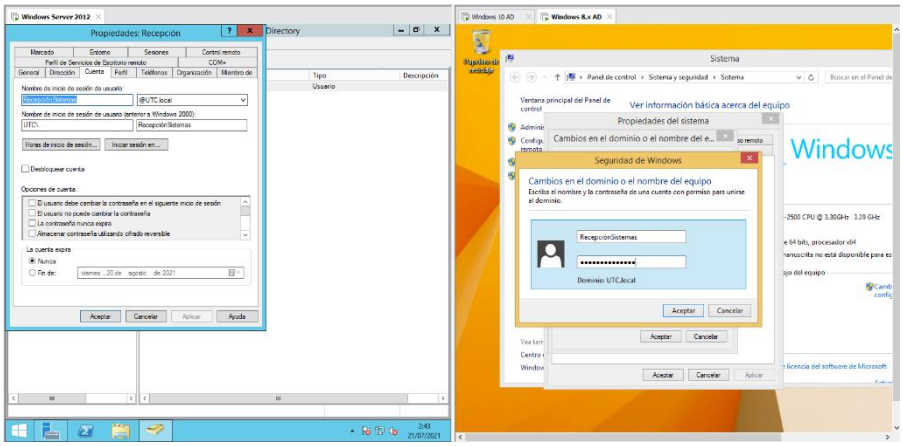
- Ingresar a la información del sistema para confirmar que el equipo se encuentra en el dominio.

Figura 33. Información en el sistema



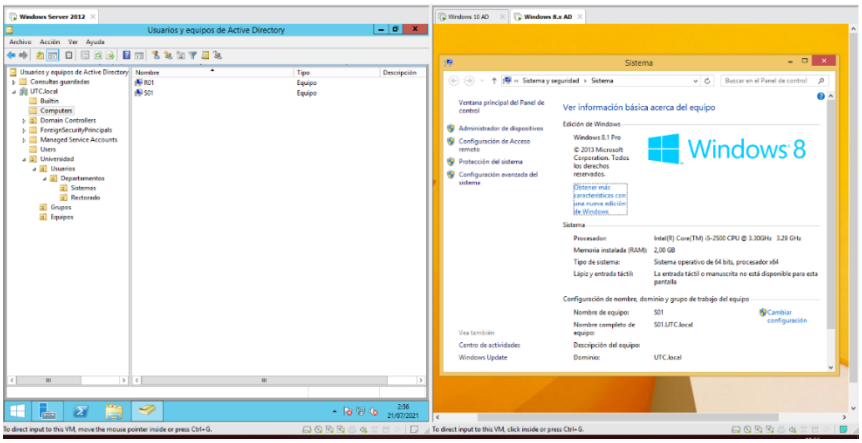
- Realizamos los mismos pasos en la máquina virtual con Windows 8.1 (U: Recepción Sistemas C: SistemasR#2021)

Figura 34. Máquina virtual con Windows 8.1



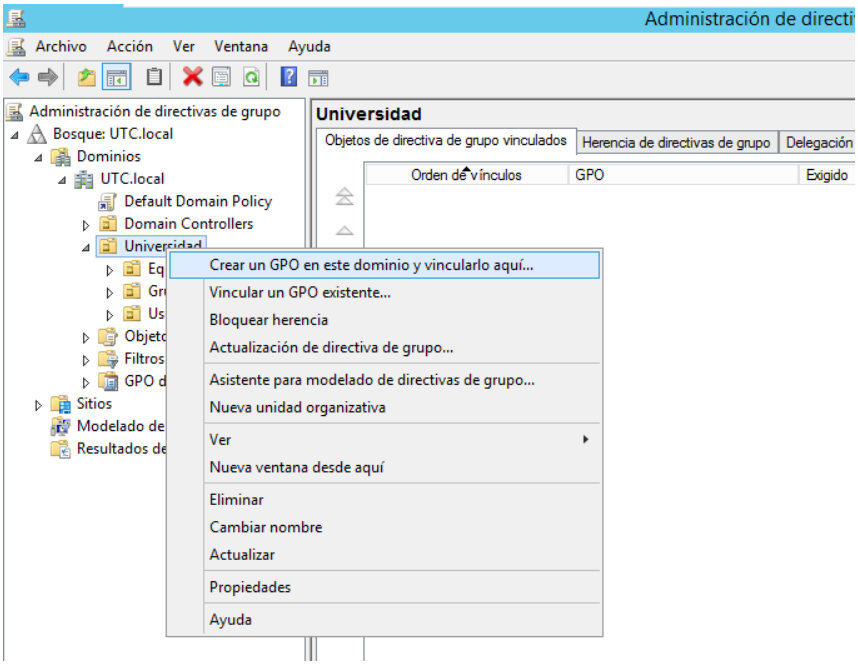
- Al reiniciar la máquina virtual se puede observar que se ya se encuentra en el dominio y que Windows Server ya agregó el nuevo equipo.

Figura 35. Reiniciar la máquina virtual



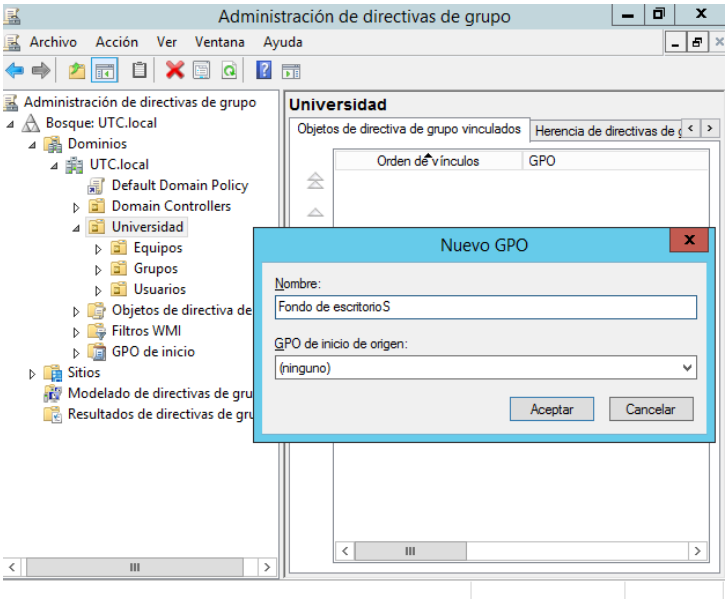
- Una vez agregada las máquinas virtuales al dominio creado, en la administración de directivas de grupo de Windows Server 2012, seleccionar la unidad organizativa anteriormente creada (Universidad) y “Crear un GPO en este dominio y vincularlo aquí”, de esta forma se crearán las nuevas directivas para los usuarios y equipos pertenecientes a esta unidad organizativa.

Figura 36. Unidad organizativa



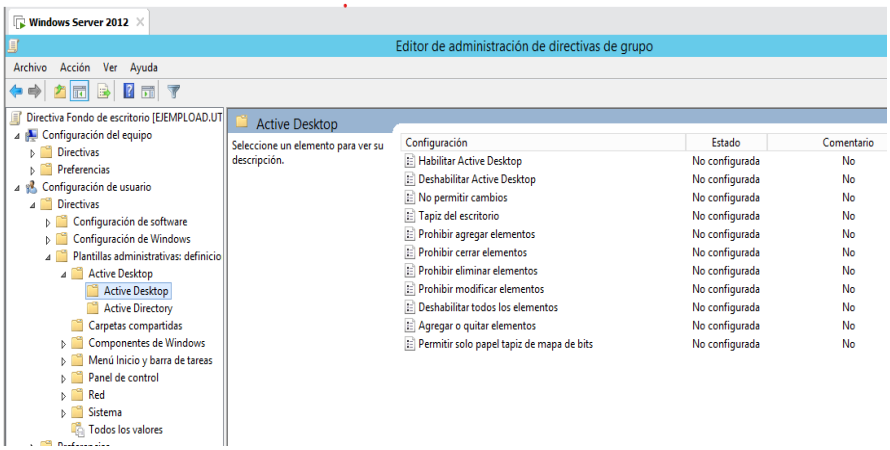
- Ingresamos el Nombre de la nueva Política de grupo.

Figura 37. Nueva política



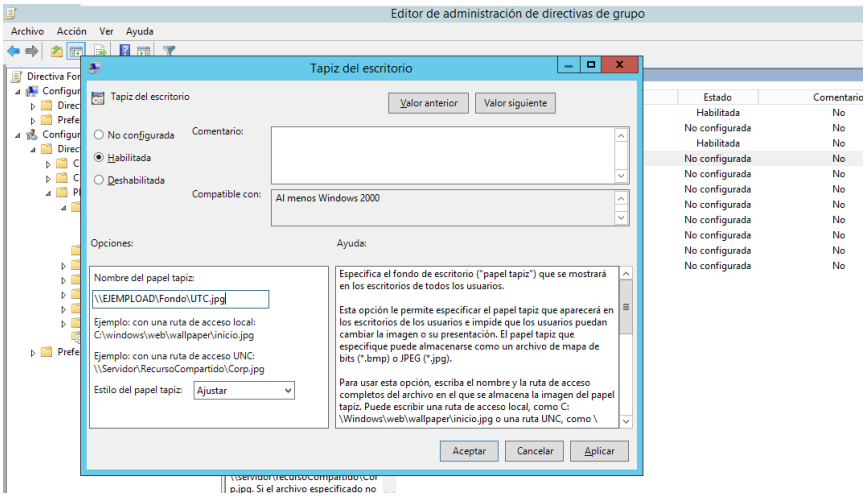
- Click derecho en editar a la política de grupo recién creada y modificar los siguientes parámetros.

Figura 38. Ediciones de las políticas



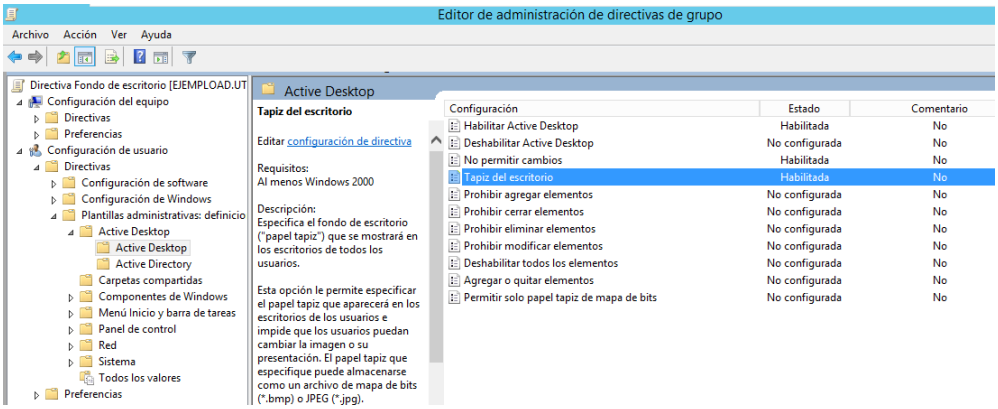
- Papel tapiz (fondo de escritorio)
    - Dirigirse a configuración de usuario.
    - Plantillas administrativas.
    - Active Desktop.
    - Habilitar “Tapiz de escritorio” e ingresar la ruta de la imagen que se desea usar.

Figura 39. Papel tapiz



- Habilitar “No permitir cambios”.
- Habilitar “Active Desktop”.

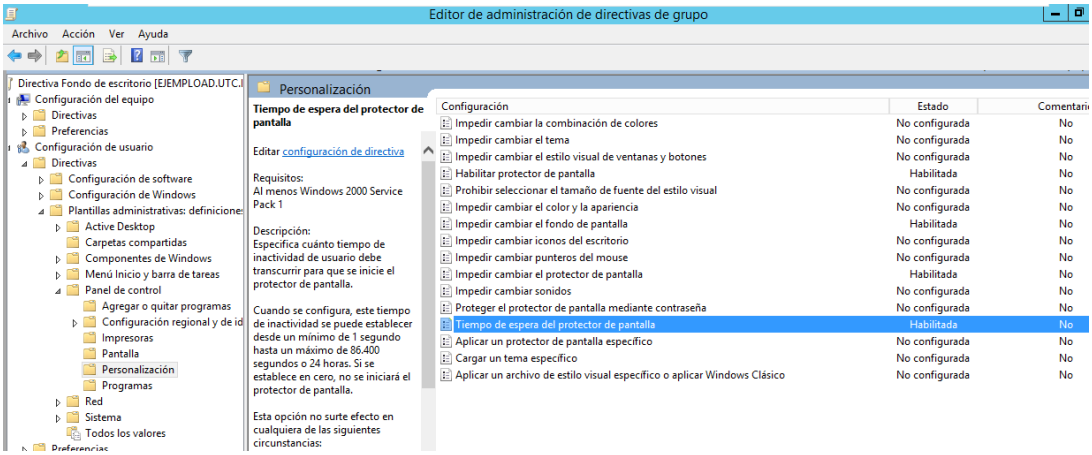
Figura 40. Opción de habilitación



- Protector de pantalla por inactividad:
  - Dirigirse a Configuración de usuario.
  - Directivas.
  - Plantillas administrativas.
  - Panel de control.
  - Personalización.
  - Habilitar protector de pantalla.
  - Habilitar “Impedir cambiar el protector de pantalla”.
  - Habilitar “Impedir cambiar el fondo de pantalla”.

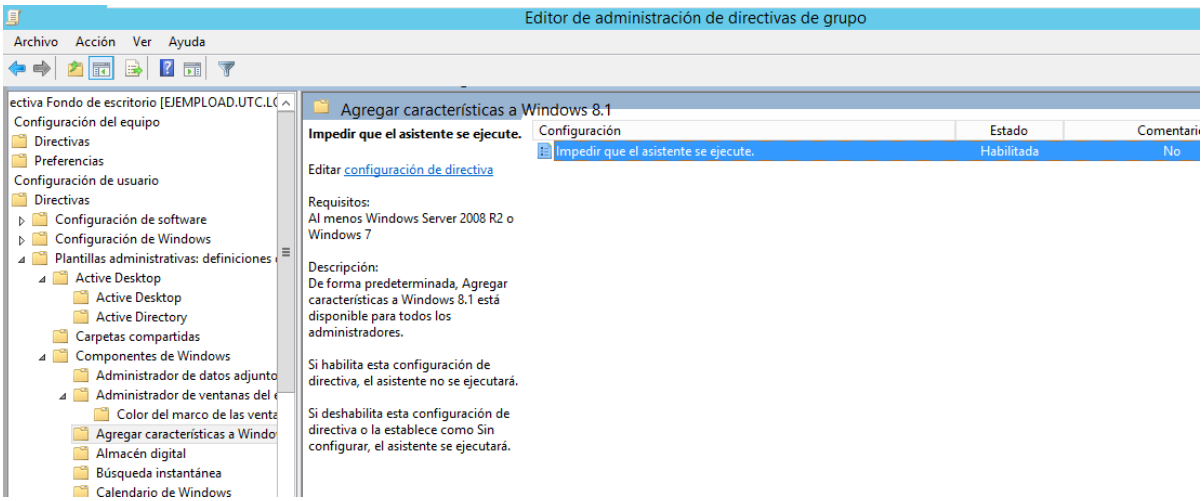
- Habilitar “Tiempo de espera del protector de pantalla (5 minutos).
- Habilitar “Aplicar un protector de pantalla específico” e ingresar la ruta del protector de pantalla que se desea usar.

Figura 41. Protector de pantalla



- Impedir instalación de características y uso de gadgets.
  - Ingresar en Configuración de usuario – Componentes de Windows.
  - Agregar características a Windows.
  - Habilitar “Impedir que el asistente se ejecute”.

Figura 42. Impedir instalación

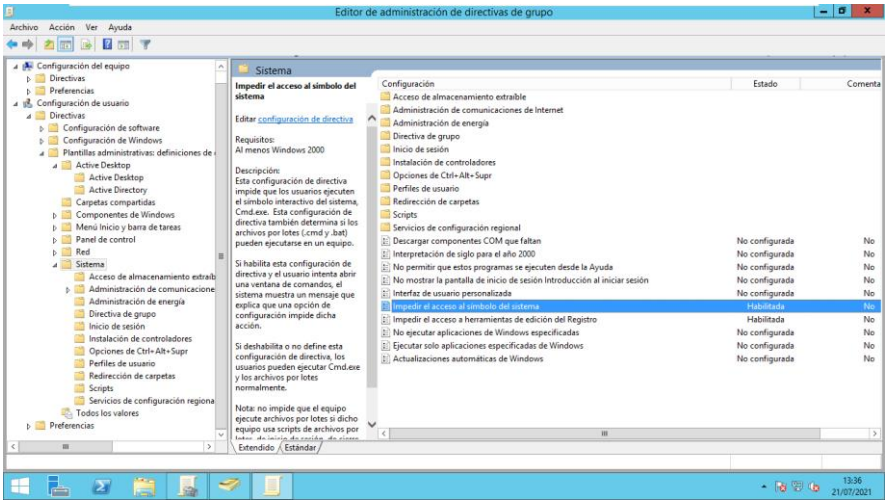


  - En Componentes de Windows – Gadgets de escritorio.

- Habilitar “Desactivar los gadgets de escritorio”.

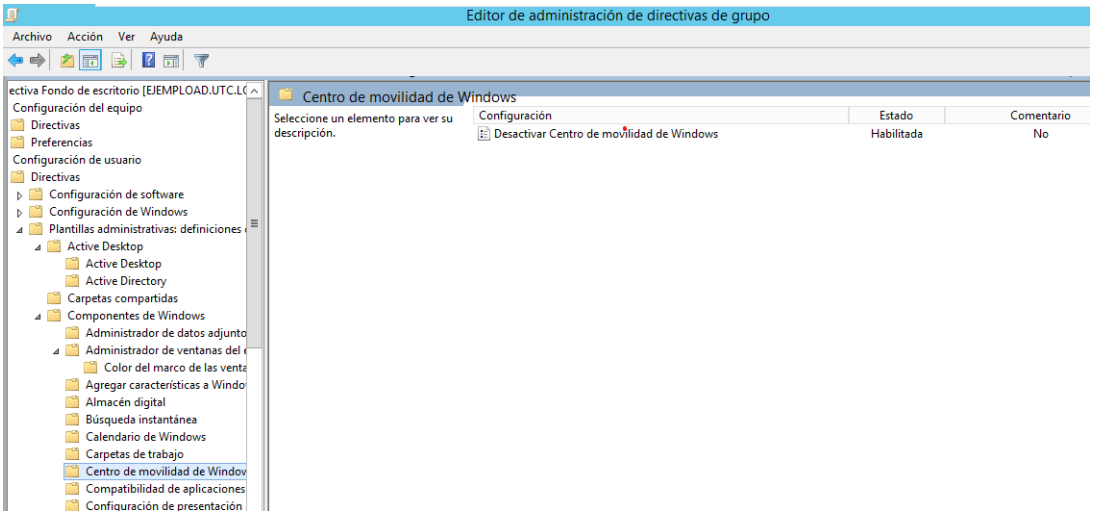
- Impedir el uso del Símbolo del sistema y PowerShell:
  - En plantillas administrativas – Sistema.
  - Habilitar “Impedir el acceso al símbolo del sistema”.

Figura 43. Impedir el uso del Símbolo del sistema y PowerShell



  - En componentes de Windows – Centro de movilidad de Windows.
  - Habilitar “Desactivar Centro de modalidad de Windows”.

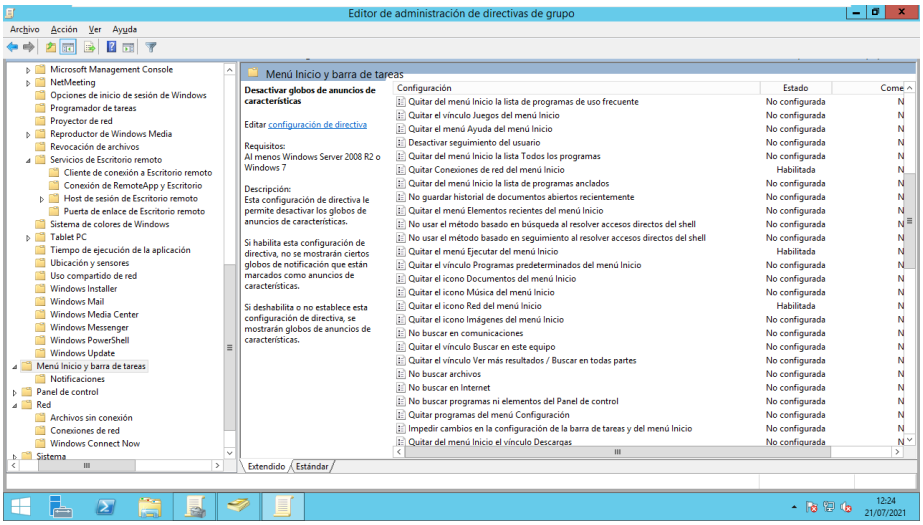
Figura 44. Centro de Movilidad



  - En Windows PowerShell Deshabilitar “Activar registro de módulos”.

- Restringir el acceso a “Red”.
    - Dirigirse a “Menú Inicio y barra de tareas”
    - Habilitar “Quitar conexiones de red del menú inicio”.
    - Habilitar “Quitar el menú ejecutar del menú inicio”.
    - Habilitar “Quitar el ícono Red del menú inicio”.

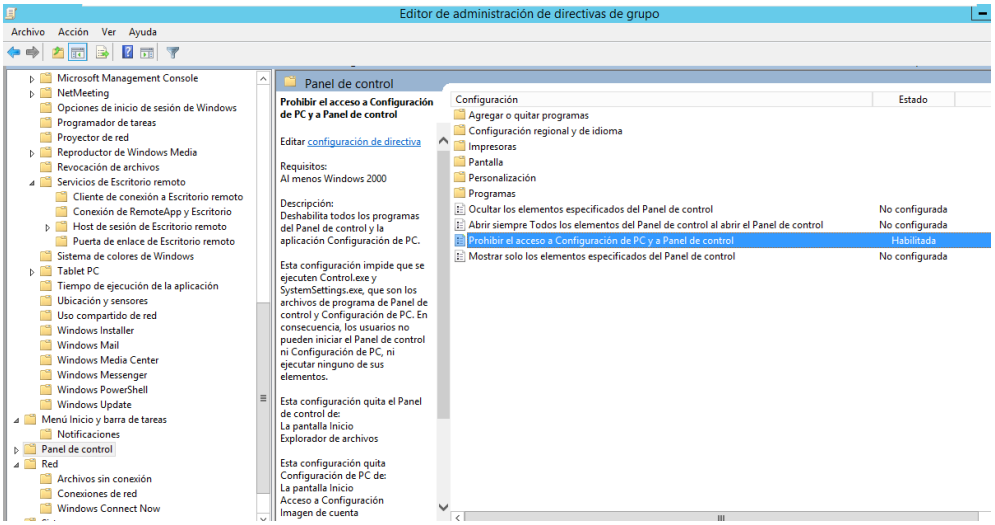
Figura 45. Restringir el acceso a “Red”.



    - En Red – Conexiones de red.
    - Habilitar “Prohibir la habilitación o des habilitación de componentes de una conexión LAN.

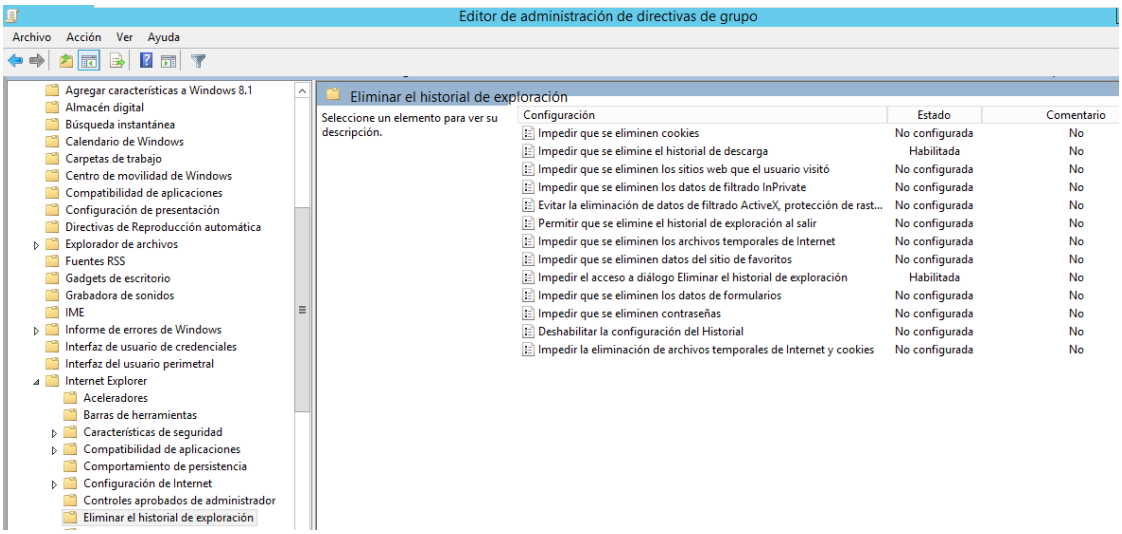
- Prohibir el acceso al Panel de control.
    - Dirigirse a Configuración de usuario – Panel de control.
    - Habilitar “Prohibir el acceso a Configuración de PC y a Panel de control”.

Figura 46. Panel de control.



- Desactivar eliminación del historial del navegador web predeterminado.
    - Ingresar a Configuración de usuario – componentes de Windows.
    - Internet Explorer.
    - Eliminar historial de exploración.
    - Habilitar "Impedir que se elimine el historial de descargar".
    - Habilitar Impedir el acceso al diálogo Eliminar historial de exploración".

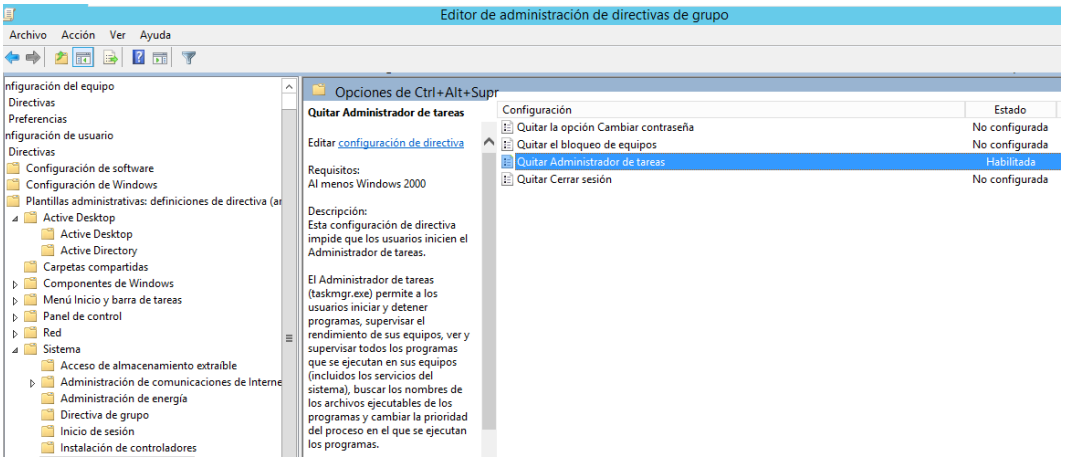
Figura 47. Desactivar eliminación del historial



- Prohibir el acceso al Administrador de tareas.

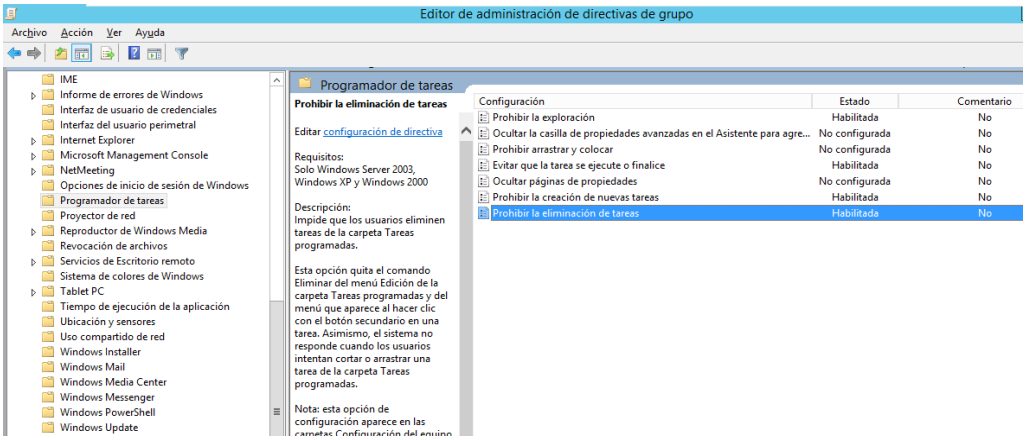
- Ingresar en Configuración de usuario – Sistema.
- Opciones de Ctrl + Alt + Supr.
- Habilitar “Quitar Administrador de tareas”.

Figura 48. Administrador de tareas



- En Configuraciones de usuario – Programador de tareas.
- Habilitar “Prohibir la creación de nuevas tareas”.
- Habilitar “Prohibir la eliminación de tareas”.
- Habilitar “Prohibir la exploración”.

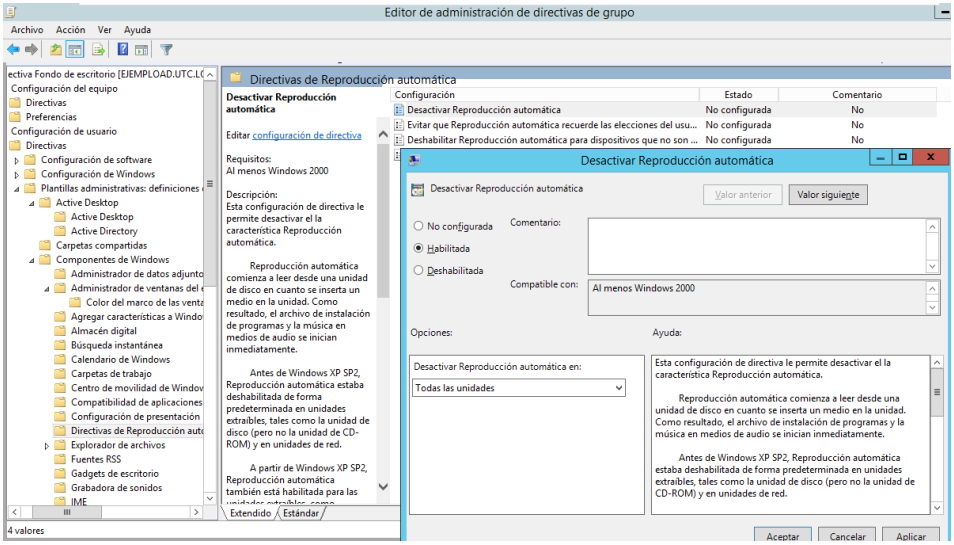
Figura 49. Opción Habilitar



- Desactivar reproducción automática de dispositivos extraíbles.
  - Ingresar en Configuración de usuario – Componentes de Windows.
  - Directivas de Reproducción automática.

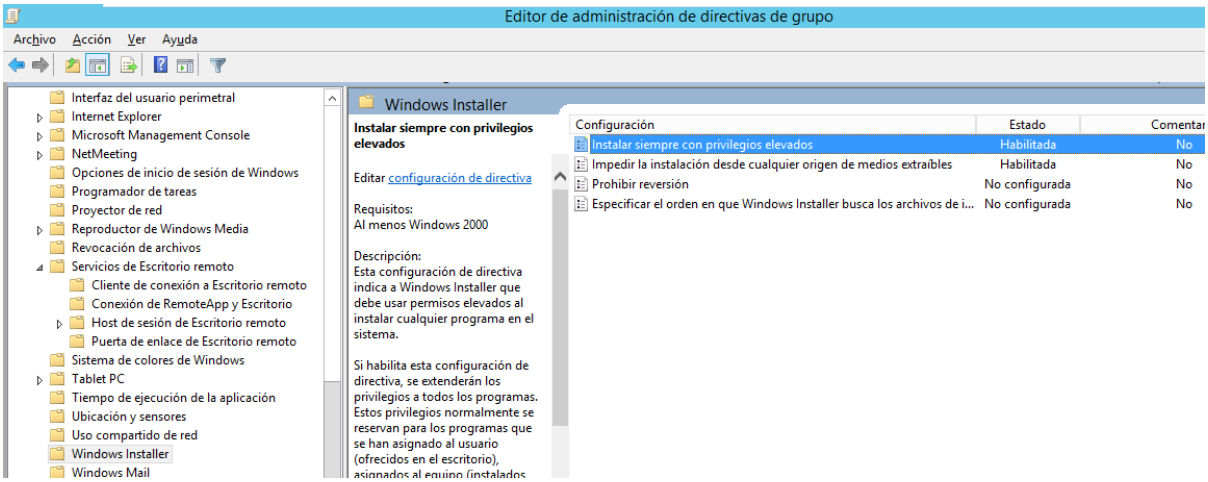
- Habilitar “Desactivar Reproducción automática”.

Figura 50. Reproducción automática de dispositivos extraíbles



- En Windows Installer.
- Habilitar “Instalar siempre con privilegios elevados”.
- Habilitar “Impedir la instalación desde cualquier origen de medios extraíbles.

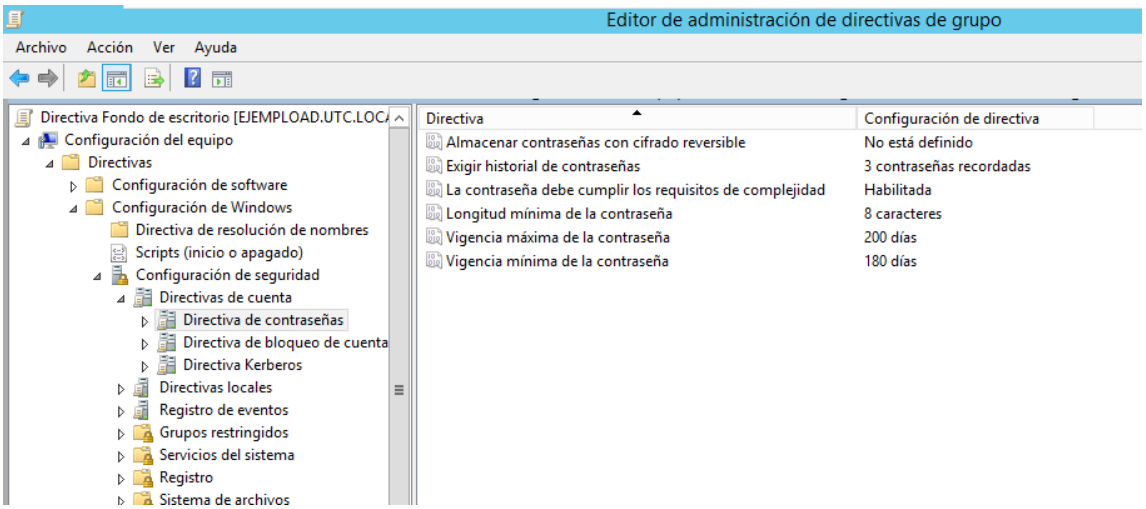
Figura 51. Windows Installer



- Configuración para las cuentas de usuario.
  - Ingresar en Configuración del equipo – Directivas.
  - Configuración de Windows.
  - Configuración de seguridad.

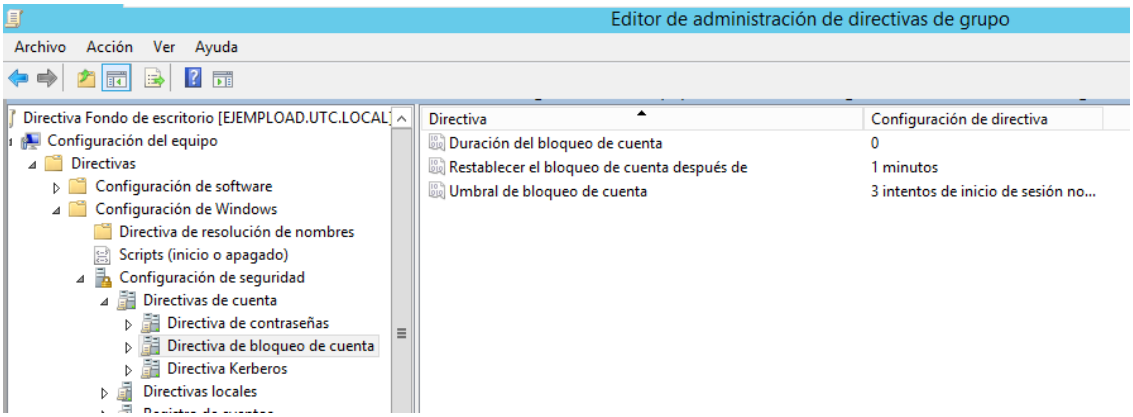
- Directivas de cuenta.
- Directiva de contraseñas.
- Habilitar “Elegir historial de contraseñas” en 3.
- Habilitar “La contraseña debe cumplir los requisitos de complejidad.
- Habilitar “Longitud mínima de la contraseña” en 8 caracteres.
- Habilitar “Vigencia máxima de la contraseña” en 200 días.
- Habilitar “Vigencia mínima de la contraseña” en 180 días.

Figura 52. Configuración para las cuentas de usuario



- Configuración del bloqueo de cuentas de usuario.
  - Ingresar en Configuración del equipo – Directivas.
  - Configuración de Windows.
  - Configuración de seguridad.
  - Directiva de bloqueo de cuenta.
  - Habilitar “Duración del bloqueo de cuenta” en 0 para que solo el administrador del Active Directory pueda desbloquearla.
  - Habilitar “Restablecer el bloqueo de cuenta después de” en 1 minuto.
  - Habilitar “Umbral de bloqueo de cuenta” en un máximo de 3 intentos.

Figura 53. Configuración del bloqueo de cuentas de usuario



9. PLAN DE CONTINGENCIA UTC – POLITICAS DE SEGURIDAD

9.1. INTRODUCCION

El presente documento Plan de Contingencia políticas de seguridad de la UTC basado en normas ISO en especial la 27000 implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los sistemas de información y datos contenidos en los diversos medios de almacenamiento. Con esto se pretende reducir la posibilidad que ocurra cualquier riesgo y se realiza los procedimientos a seguir en caso de que se presente algún problema.

9.2. OBJETIVO

Minimizar los riesgos que atentan contra la seguridad de la información. Incluye, además, las políticas de seguridad, el análisis de sensibilidad de la información manejada.

Alcanzar un nivel de riesgo menor que el soportando por la institución, para preservar la confidencialidad, integridad y disponibilidad de la información.

9.3. PLAN DE RIESGOS

Se consideran todas las políticas que puedan darse, para ello se elabora una lista de todos los riesgos conocidos, en caso de suceder algún imprevisto, se pueda actuar en forma inmediata y dar solución al problema presentado, de manera que no se paralicen las actividades del Departamento de las TIC's.

En si la Universidad esta propensa a diversos riesgos entre ellos el principal riesgo es el Volcán Cotopaxi, pone en peligro la integridad de las personas y es el punto mas vulnerable, seguido de los datos de información que pueda perderse, otro riesgo es la falta de seguridad que se encuentra en los

cables de electricidad y datos; entonces es en esta área donde se realizan una lista detallada de los riesgos a lo que está expuesta el departamento de las TIC's de la Universidad:

- Corto circuito
- Mala conexión
- Falta de protección al equipo
- Fallas tarjeta de red
- Falla IP asignado
- Fallas de componentes de hardware del servidor
- Virus
- Falta de equipos actualizados para mantenimiento
- Ingreso de personal no autorizado
- Terremotos, temblores
- Inundaciones
- Erupción volcán Cotopaxi
- Desbordes de ríos
- Humedad
- Falta de ventilación
- Falta de protección diferentes cables.

9.3.1. Anàlisis de Riesgo

Consiste en identificar y cuantificar los riesgos presentados. La identificación depende, en gran medida de la información disponible que tenga el plan de riesgos. Hay que tener en cuenta que, al realizar el análisis de riesgo es importante identificar todos los recursos cuya seguridad esta en riesgo de quebrantarse.

Los recursos a considerar al estimar las amenazas de seguridad son:

- Hardware
- Software
- Datos
- Usuarios
- Infraestructura: se refiere al edificio en sí, a los mobiliarios que se encuentran instalados, sin pasar por alto la documentación.

9.3.2. Anàlisis de fallas en la seguridad

Contempla tanto en el aspecto físico como lógico que es donde las fallas de seguridad son muy notorias y comunes; de ahí la importancia de realizar una bitácora donde se vaya almacenando y enriqueciendo con los problemas actuales y los futuros con sus respectivas soluciones que permitan eliminar o minimizar estas fallas de seguridad.

Esto conlleva al desarrollo de políticas bien establecida que permitan brindar información completa y detallada de la seguridad de equipos y de sistemas de información.

9.4. POLÌTICAS DE SEGURIDAD

Las politicas de seguridad establecen el canal de forma de actuacion del perdonal, en relaciòn con los recursos y servicios informàticos, importantes de la instituciòn.

Cada politica de seguridad es consciente y vigilante del personal por el uso y limitaciones los recursos, servicios informaticos criticos de la institucion.

En este caso el encargado del Departamento de las TIC’s de la Universidad es el principal involucrado para establecer medidas, es conveniente que dichas politicas, sean planteadas ante un grupo de personal capacitados involucrador que al establecer dichas politicas, sean planteadas ante un grupo de personalcapacitados involucrados en el area para que sean discutidas y dar a conocer la necesidad de implementar este tipo de medidas. Las politicas de seguridad a considerarse constan de los siguientes elementos:

Alcance de las politicas, incluyendo facilidades, sistemas y personal sobre la cual se aplica. Es una invitacion de la organizcioncomo uno de sus principales activos, asi como un motor de intercambio y desarrollo.

Objetivos de la politica y descripcionclara de los elementos involcrados en su definición

Responsabilidad por cada uno de los servicios y recursos informaticos a todos los niveles de la organización.

Requerimientos mínimos para la configuración de la seguridad de los sistemas que cobija el alcance de la política.

Responsabilidad de los usuarios con respecto a la informacion que tienen acceso.

Las politicas de seguridad deben ofrecer explicaciones comprensibles acerca del por que deben tomarse ciertas decisiones, transmitir porque son importantesestos u otros recursos o servicios, esindispensable mantener el recurso existente de la institucion operativo salvo cualquier amenaza o riesgo que puede ocurir en la institución. Se considera que las políticas de seguridad son procesos dinamicos, de tal manera que este actuando permanentemente, evitando la desactualización que cuando se descubran debilidades se pueda subsanar.

9.5. ANÀLISIS Y EVALUACIÓN DE RIESGOS

9.5.1. Eventos Considerados para el plan de contingencia

Cuando se efectua un riesgo, este puede producir un evento, pot tanto, a continuación, se describen los eventos a considerar dentro del plan de contingencia.

Tabla 34. Eventos considerados para el plan de contingencia

RIESGO	**EVENTO**
• Fallas corte de cable UTP • Fallas tarjeta de Red • Fallas IP asignado • Fallas punto de Switch • Fallas punto Pacht Panel • Fallas Punto de red	NO EXISTE COMUNICACIÓN ENTRE CLIENTE Y SERVIDOR
• Fallas de Componentes de Hardware del servidor • Fallas del UPS(falta de suministro electronico) • Virus • Sobrepasar el limite del almacenamiento del disco • Computador de escritorio funciona como Servidor	FALLAS EN EL EQUIPO SERVIDOR

• Incapacidad • Accidente • Renuncia Intempestiva	AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE TECNOLOGIA DE LA INFORMACIÒN
• Corte general del fluido electrico	INTERRUPCION DEL FLUIDO ELECTRONICO DURANTE LA EJECUCION DE LOS PROCESOS.
• Fallas de equipo de comunicacionSwitch, Antenas, Fibra optica • Fallas en el software de Acceso a Internet • Perdida de comunicación con proveedores de internet	PERDIDA DE SERVICIO DE INTERNET
• Incendio • Sabotaje • Corto Circuito • Terremoto • Tsunami	INDISPONIBILIDAD DEL CENTRO DE COMPUTO (DESTRUCCIÒN DE LA SAL DE SERVIDORES)

9.5.1.1. No hay comunicación entre Cliente – Servidor

- Requerimiento del usuario procedera a identificar el problema
- El técnico de sistemas procedera a identificar el problema
- Si se constata el problemacon el Pachr Panel, realizar cambio del mismo.
- Si no se resuelve el problema proceder a constartar si existe en la tarjeta de red, en caso de afirmativo realizar cambio o arreglo de la misma.
- Testear el cable UTP. Si existe daño, realizar el cambio del cable.
- Realizar mantenimiento del punto de red del usuario y del gabinete de comunicaciones
- Recuperacion del sistema de red para el usuario.

Recursos de Contingencia

Componente de remplazo, tarjeta de red; Conector RJ – 45, JACK RJ – 45. Diagrama logico de la red

9.5.1.2. Fallas en el equipo servidor

Puede producir perdida de Hardware y software, perdida del proceso automatico de Backup y restore e Interrupción de las operaciones. A continuación, se describen algunas causas de fallo en un servidor.

9.5.1.2.1. Causas de fallas del servidor

Error Fisico del Disco de un Servidor

Dado el caso critico deqe el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

- Ubicar el diSco malogrado.
- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y telefono a jefes de area.
- Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
- Bajar el sistema y apagar el equipo.
- Retirar el disco malo y reponerlo con otro del mismo tipo formatearlo y darle particion.
- Restaurar el ultimo Backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
- Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
- Habilitar las entradas al sistema para los usuarios.

Error de la memoria RAM

En este caso se dan los siguientes sintomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimales.

Error de trajet(s) controladara(s) de disco

Para los errores de cambio de Memoria RAM o Tarjeta Controladora de disco se debe tomar las siguientes acciones:

- Avisar a los usuarios que deben salir del sistema utilizar mensajes por red y telefono a jefes de area.
- El servidor debe estar apagado, dando un corrcto apagado del sistema.
- Ubicar la posicion de la pieza a cambiar.
- Retirar la pieza con sospecha de deterioro y tener a la mano otra igual o similar.
- Retirar la conexión de red del servidor, ello evitara que, al encender el sistema, los usuarios ingresen.
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizaran las pruebas.
- Al final de las pruebas, luego de los resultados de una buena lectura de informacion, habilitar las entradas al sistema para los usuarios.

Error lógico de datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

- Caida del servidor de archivos por falla de software de red.
- Falla en el suministro de energia electrica por mal funcionamiento del UPS.
- Bajar Incorrectamente el servidor de archivos.
- Fallas causadas usualmente por un error de chequeo de inconsistencia fisica.

Recursos de contingencia

Componente de remplazo (memoria, disco duro, etc)

Backup diario de informacion del servidor.

9.5.1.3.Ausencia parcial o permanente del personal de técnologia de la información

- Directriz del controlador (escrita o email) para que el administrador alterno se encargue del centro de computo del negocio especificando el periodo de asignacion.
- Obtener la relacion de los sistemas de informacion con los que cuenta la universidad, detallando usuarios en que equipos se encuntran instalados y su utilidad.
- Conocer la ubicación de los Backus de informacion.
- Contar con el dagrama logico de red actualizado.

Recursos de Contigencia

Manual de funciones actualizado del técnico de sistemas.

Relacion de los sistemas de informacion.

Diagrama logico de la red actualizado.

9.5.1.4. Interrupción del fluido electronico durante la ejecución de los procesos

- Si fuera corto circuito, el UPS mantendra activo los servidores, mientras se repare la averia electrica.
- Para el caso de apagon se mantendra la autonomia de corriente que la UPS nos brinda (corriente de emergencia), hasta que los usuarioncomplenten sus operacionees para que no corten bruscamente el proceso que tienen en el momento del apagon.
- Cuando el flluido electronico de la calle se ha restablecido se tomaran los mimso cuidados para el paso de UPS a corriente normal (corriente brindada por la empresa electrica).

Recursos de contigencia

Asegurar que el estado de las baterias del UPS se encuentren siempre cargadas.

9.5.1.5.Perdida de servicio de Internet

- Realizar pruebas para identificar posible problema dentro la universidad.
- Si se envidencia problema de hardware, se procedera a cambiar el componente.
- Si se evidencia problemas con el software, se debe reinstalar el sistema operativo del servidor.
- Si no se evidencia falla en los equipos de la entidad, se procedera a comunicarse con la empresa prestadora del servicio, para asistencia tecnica.
- Es necesario registrar la averia para llevar un historial que servira de guia para futuros daños.
- Realizar pruebas de operatividad del servicio.
- Servicio de internet activo.

Recursos de Contingencia

- Hardware
- Router
- Software
- Herramientas de internet

9.5.1.6. Indisponibilidad del centro de computo

- Contar con el inventario total del sistema actualizado.
- Identificar recursos de hardware y software que se pueden rescatar.
- Salvaguardar los Backus de informacion realizados.
- Identificar un nuevo espacio para restaurar el centro de computo.
- Presupuestar la adquisicion de software, hardware, materiales personales y transporte.
- Adquisicion de recursos de software, hardware, materiales y contralacion de personal.
- Reestablecer los Backus realizandos a los sistemas.

Recursos de Contingencia

Router (proveido por el proveedor de internet)

Servidores y equipos de comunicación

Gabinete de comunicaciones y servidores.

Materiales y herramientas para cableado estructurado.

9.6. PLAN DE RECUPERACION Y RESPALDO DE LA INFORMACION

El costo de la recuperacion en caso de deastres severos, como los de un terremoto que destruya completamente el interior de edificios e instalaciones, estara directamente relacionado con el valor de los equipos de computo e informacion que no fueron informados oportunamente y actualizados en la relacion de equipos informaticos asegurados que obre en poder de la compañía de seguros. El costo de recuperacion en caso de desastres de proporciones menos severeros, como los de un terremoto de grado inferior a 7 o un incendio controlable, estara dado por el valor no asegurado de equipos informaticos e informacion mas el costo de oportunidad que significa, el costo del menor tiempo de recuperacionestrategica, si se cuenta con parte de los equipos e informacion recuperados.

Este plan de restablecimiento estrategico del sistema de red, software y equipos informaticos sera abordado en la parte de actividades posteriores al desastre.

El paso inicial en el desarrollo del plan contra desastres, es la identificacion de las personas que seran las rsponsables de la ejecucion del plan de contingencia. Por tanto, se definen los siguientes responsables:

Tecnico / ingeniero de sistemas: sera responsable de llevar a cabo las acciones correctivas definidas anteriormente a fin de minimizar los riesgos establecidos.

9.7. PLAN DE RECUPERACION DE DESASTRES

Una vez conocidos los riesgos y sus características que pueden envolver al departamento del TIC's de la Universidad, es importante y necesario definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre para poder actuar en forma inmediata, oportuna y suplir este inconveniente.

Además, cuando se presente un desastre, es fundamental el detalle del motivo que origino y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido, para una próxima falla, afectara menos y se sabrá a que enfrentar y la contingencia será inmediata.

Los procedimientos que se desarrollen para actuar frente a cualquier eventualidad deben ser planeados y aprobado debidamente. Además, se requiere verificar para establecer el cumplimiento de dichos procedimientos, que debe ser común para todo el personal que labora en el departamento de las TIC's de la Universidad.

9.7.1. Actividades previas al desastre

Debe existir una planificación de actividades previas al desastre de manera que permitan actuar frente a dichas eventualidades y permitir recuperarse en el medio tiempo y a un costo mínimo.

Algunos desastres son impredecibles como la erupción del volcán, terremotos, etc, para mitigar estos riesgos es necesario realizar simulacros con las personas involucradas.

Pero antes de tener las actividades previas a un desastre es mejor fomentar una cultura preventiva y de mantenimiento de todos los procesos que normalmente se realizan para que solo en casos extremos aplicar actividades para evitar riesgos.

9.7.2. Actividades Durante el desastre

Esta etapa es muy importante porque es el momento mismo de ocurrencia de una contingencia o siniestro, es donde debe primar la calma y la inteligencia de saber cómo actuar frente a estas adversidades debido a que es la fase donde la toma de decisiones es fundamental para aplicar en forma eficiente el plan de emergencias. Cabe recalcar que es esencial que este una segunda persona informada del plan de contingencia, si fuera el caso de faltar el encargado, está preparado el segundo para tomar las acciones pertinentes.

9.7.3. Actividades despues del desastre

Las actividades después del desastre son acciones que se realizan luego de lo ocurrido del desastre y comprende de evaluaciones de daños, resultados, ejecución de actividades, y retroalimentación

10.BIBLIOGRAFÍA

[1] J. Izaguirre y F. Leòn , «Análisis de los Ciberataques Realizados en América Latina,» *INNOVA Research Journal,* vol. 3, nº 9, p. 183, 2018.

[2] El Comercio, «Ecuador, una de las naciones más atacadas por los 'hackers',» El Comercio, 12 01 2021. [En línea]. Available: https://www.elcomercio.com/tendencias/ecuador-naciones-atacadas-hackers-tecnologia.html. [Último acceso: 2021].

[3] F. Silva , L. Segadas y E. Kowask, Gestión de la seguridad de la información, Bogotá: RENATA, 2014.

[4] M. Romero , G. Figueroa, D. Vera, J. Álava, G. Parrales, C. Álava, Á. Murillo y M. Castillo, INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES, ECUADOR : CIENCIAS Editorial Área de Innovación y Desarrollo,S.L., 2018.

[5] MAGERIT, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información., Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[6] M. Mujica y Y. Alvarez, «El Analisis de Riesgo en la seguridad de la informacion,» *Publicaciones en Ciencias y Tecnologıa,* vol. 4, nº 2, pp. 33-37, 2010.

[7] L. Calderón , «Seguridad informática y seguridad de la información,» *Universidad Piloto de Colombia,* pp. 1-7, s.f.

[8] W. Vega , «POLITICAS Y SEGURIDAD DE LA INFORMACION,» *Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia,* vol. 2, nº 2, pp. 63-69, 2008.

[9] A. Monleón, «El impacto del Big-data en la Sociedad de la Información. Significado y utilidad,» *Historia y Comunicación Social,* vol. 20, nº 2, pp. 427 - 445, 2015.

[10] M. Martín, «Implementación de un sistema de control de acceso para mejorar la seguridad de la información de la empresa SNX S.A.C.,» 2016. [En línea]. Available: https://core.ac.uk/download/pdf/323348923.pdf. [Último acceso: 10 07 2021].

[11] . Y. Benitez y S. Martínez, «Requisitos de Seguridad para aplicaciones web.,» *Revista Cubana de Ciencias Informáticas,* vol. 12, pp. 205-221, 2018.

[12] Grupo de Nuevas Actividades Profesionales del COIT, «Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001,» 07 2009. [En línea]. Available: https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de

_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf. [Último acceso: 1 06 2021].

[13] G. Baca, Introduccion a la seguridad Informàtica, Mèxico: GRUPO EDITORIAL PATRIA, 2016.

[14] G. Baena , R. Mendoza y E. Joel, «“Importancia de la norma ISO/EIC 27000 en la implementación de un sistema de gestiónde la seguridad de la información”,» *Revista contribuciones a la Economía*, 2019.

[15] D. Aguirre , «DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA SERVICIOS POSTALES DEL PERÚ S.A.,» 10 2014. [En línea]. Available: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/5677/AGUIRRE_DAVID_SISTEMA_GESTION_SEGURIDAD_INFORMACION_SERVICIOS_POSTALES.pdf?sequence=1&isAllowed=y.

[16] C. Cruz y M. Gaibor , "PoliticasSeguridadInformatica" Tesis de pregrado, Universidad Tecnica de Cotopaxi, Latacunga, 2020.

[17] Yi Min Shum, «Matriz de evaluación de factores internos (Matriz EFI – MEFI),» 2018. [En línea]. Available: https://yiminshum.com/matriz-evaluacion-factores-internos-mefi/.

[18] A. Morón , M. Reyes y . Á. Urbina , «Gestión de riesgos en la empresa R.C. Agelvis, C.A,» *Multiciencias,* pp. 417 - 427, 2015.

[19] E. Markus , «Gestión de Riesgo en la Seguridad Informática,» s.f. [En línea]. Available: https://protejete.wordpress.com/.

[20] K. López, «DISEÑO DE UN PLAN DE MITIGACIÓN DE RIESGOS EMPRESARIALES IDENTIFICANDO LOS RIESGOS INTERNOS Y EXTERNOS DE COMERCIAL NOVEDADES LEYDI EN EL CANTÓN LA TRONCAL DEL AÑO 2014,» 2015. [En línea]. Available: http://186.5.103.99/bitstream/reducacue/7293/3/TESIS_KARLA%20LOPEZ.pdf.

[21] MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información., España, 2012.

11. ANEXOS

Anexo 1: Hoja de vida del tutor

CURRÍCULUM VITAE

1. DATOS PERSONALES

NOMBRE COMPLETO: Jorge Bladimir Rubio Peñaherrera.

CEDULA DE IDENTIDAD: 050222229-2

FECHA DE NACIMIENTO: Pujilí, 16 de mayo de 1976. EDAD: 45 años.

ESTADO CIVIL: Casado.

DIRECCIÓN: Pujilí, Calle Gabriel Álvarez 1-13 y Juan José Merizalde.

NÚM. CELULAR: (593)0995220308

E-MAIL: jorge.rubio@utc.edu.ec jbladimirrp@hotmail.com

COLEGIO PROFESIONAL: # 15 - 05029 Conferida por la Sociedad de Ingenieros del Ecuador

2. ESTUDIOS REALIZADOS

CUARTO NIVEL: Pontificia Universidad Católica del Ecuador.

TERCER NIVEL: Universidad Técnica de Cotopaxi.

NIVEL SECUNDARIO: Instituto Tecnológico "Vicente León".

NIVEL PRIMARIO: Escuela "Antonio Aristarco Jácome" (Pujilí).

POSTGRADO: Magister en Gerencia Informática, mención Desarrollo de Software y Redes.

Año de obtención: 2010. NÚMero de Registro: **1027 - 10 – 712825**

3. TÍTULOS

POSTGRADO: Diplomado Superior en Gerencia Informática

Año de obtención: 2007

NÚMero de Registro: **1027 – 07 - 669360**

PREGRADO: Ingeniero en Informática y Sistemas Computacionales

Año de obtención: 2003

NÚMero de Registro: **1020 – 03 –459773**

4. EXPERIENCIA LABORAL

Universidad Técnica de Cotopaxi

Docente Titular Auxiliar 2 (Nombramiento).

Pontificia Universidad Católica del Ecuador sede Ambato

Docente de Postgrados (2011 - Actualidad).

Pontificia Universidad Católica del Ecuador sede Ibarra

Docente de Postgrados (2010 - Actualidad).

Universidad Tecnológica Indoamérica, Quito

Docente de Pregrado Modalidad Semipresencial (2008 - 2013).

Universidad Politécnica Salesiana

Docente (2003 -2005).

Universidad Técnica Particular de Loja. Centro asociado Latacunga

Docente (2004 -2008).

Instituto Tecnológico Superior Aeronáutico. ITSA

Docente (2009 -2010).

Instituto Tecnológico Victoria Vásconez Cuvi

Docente – Coordinador de Carrera (2001 - 2007).

Cooperativa de Ahorro y Crédito "Andina" Ltda.

Jefe de Sistemas(2010).

Babel Software

Programador – Desarrollador (2008 - 2009).

5. CARGOS DESEMPEÑADOS

COORDINADOR DE LA CARRERA DE INGENIERIA EN INFORMATICA Y SISTEMAS COMPUTACIONALES– UA-CIYA.

Universidad Técnica de Cotopaxi, Septiembre 2015 hasta 30 de septiembre del 2016.

COORDINADOR DE TRABAJO DE GRADO DE LA UNIDAD ACADEMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS – CIYA.

Universidad Técnica de Cotopaxi, Septiembre 2011 hasta 30 DE Septiembre del 2015.

COORDINADOR DE INVESTIGACIÓN DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES – CIYA.

Universidad Técnica de Cotopaxi, Marzo 2011 hasta Septiembre 2011.

6. CERTIFICACIONES

CERTIFICACIÓN CISCO DevNet:

Cisco ESPOL – en proceso

CERTIFICACIÓN CISCO CCNAv7: Bridging (Instructor)_ Actualización

Cisco ESPOL – Mayo del 2020.

CERTIFICACIÓN CISCO CCNAv6_Mod_4 (Instructor)

Cisco ESPOL – Enero del 2020.

CERTIFICACIÓN CISCO CCNA v6_Mod_3 (Instructor)

Cisco ESPOL – Noviembre del 2019.

CERTIFICACIÓN CISCO CCNA v6_Mod_2 (Instructor)

Cisco ESPOL – Octubre del 2019.

CERTIFICACIÓN CISCO CCNA v6_Mod_1 (Instructor)

Cisco ESPOL – Agosto del 2019.

CERTIFICACIÓN EN SEGURIDAD INFORMÁTICA Y ETICAL HACKING

Colombia – Agosto del 2015

CERTIPORT MICROSOFT

IBEC del Ecuador – Agosto del 2012.

IC3 INTERNET AND COMPUTING CORE CERTIFICATION

IBEC del Ecuador – Agosto del 2012.

7. CAPACITACIONES EN EL EXTERIOR

METODOLOGÍA DE LOS PROCESOS DE IMPLEMENTACIÓN DEL SOFTWARE

“EXACTUS ERP”.

País: Costa Rica.

Localidad: Heredia.

Empresa: SOFTLAND.

Fecha: Del 06 al 10 de julio del 2009.

8. PARTICIPACIÓN EN PROYECTOS DE INVESTIGACIÓN

RED DE ESTUDIOS CIENCIOMÉTRICOS (REDEC).

Universidad Técnica de Cotopaxi – Departamento de Investigación (**en desarrollo**, duración 24 meses).

IDENTIFICACIÓN DE SISTEMAS DE INFORMACIÓN QUE CONTRIBUYAN CON LA ORGANIZACIÓN Y GOBIERNO ELECTRÓNICO).

Facultad de Ciencias de la Ingeniería y Aplicadas, Carrera de Ingeniería en Informática y Sistemas Computacionales.

Investigación Formativa (en desarrollo, duración 24 meses).

“TIC´S EN LA EDUCACIÓN SUPERIOR E INNOVACIÓN DEL DOCENTE DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI”

Universidad Técnica de Cotopaxi – Departamento de Investigación 2012.

DESARROLLO E IMPLEMENTACIÓN DE UN SOFTWARE DE AYUDA EN EL APRENDIZAJE DE CÓDIGO BRAILLE, APLICANDO LA TECNOLOGÍA VISUAL 6.0, MEDIANTE UN CIRCUITO ELECTRÓNICO CONECTADO AL PUERTO PARALELO DEL COMPUTADOR, DIRIGIDO AL INSTITUTO DE EDUCACIÓN ESPECIAL DE NO VIDENTES DE LA PROVINCIA DE COTOPAXI.

Universidad Técnica de Cotopaxi – Departamento de Investigación 2011 - 2012.

9. LIBROS PUBLICADOS

"SISTEMAS DE COMUNICACIÓN Y REDES INFORMÁTICAS"

ISBN 978-9978-395-41-7

Editorial UTC Autor

http://investigacion.utc.edu.ec/libros/index.php/libros/catalog/view/11/13/45-1

"TIC + Información + Conocimiento=Inteligencia Organizacional: Una Excelente Fórmula para la Toma de Decisiones acertadas"

ISBN 978-9978-395-41-7

Editorial UTC Co-Autor

http://investigacion.utc.edu.ec/libros/index.php/libros/catalog/view/15/17/61-1

"LAS TRES CAPAS DE LOS SISTEMAS DE INFORMACIÓN WEB CON (una) JAVA"

ISBN 978-9978-395-41-7

Editorial UTC Co-Autor

http://investigacion.utc.edu.ec/libros/index.php/libros/catalog/view/8/10/33-1

CAPÍTULO DE LIBROS

"INSTRUCCIÓN HÍBRIDA: LA EDUCACIÓN CON MIRAS AL FUTURO TECNOLÓGICO "

ISBN 978-958-56608-7-8

Editorial Corporación CIMTED La Ceja, Antioquia – Colombia Páginas: 260 - 273

http://memoriascimted.com/wp-content/uploads/2018/11/libro-coincom-congreso- 2018.pdf

10. ARTÍCULOS PUBLICADOS (Publicaciones Científicas)

METAHEURISTIC ALGORITHMS HELPING TO TAKE DECISIONS IN INVESTMENT PORTFOLIOS.

ISSN: 2309-0685 - Vol. 4 No. 2016

INTERNATIONAL JOURNAL OF ECONOMICS AND STATISTICS.

Bases de Datos Indexada

German National Library of Economics e Index Copernicus

Link de la publicación http://www.naun.org/main/NAUN/economics/2016/a082015-063.pdf

LEVELS OF SIMILARITY IN USER PROFILES BASED CLUSTER TECHNIQUES AND MULTIDIMENSIONAL SCALING

ISSN: 2074-1308 - Volumen 10, 2016

INTERNATIONAL JOURNAL OF SYSTEMS APPLICATIONS, ENGINEERING & DEVELOPMENT

Bases de Datos Indexada

Inspec - The IET, Index Copernicus.

Link de la publicación http://www.naun.org/main/UPress/saed/2016/a202014-058.pdf

LAS AUDITORÍAS DEL CONOCIMIENTO COMO HERRAMIENTAS DE APOYO A LA ORGANIZACIÓN Y GESTIÓN DEL CONOCIMIENTO: UN ESTUDIO DE CASO

ISSN 2346-9161 - Vol. 7 No. 1

IBEROAMERICAN JOURNAL OF PROJECT MANAGEMENT.

Bases de Datos Indexada Latindex e Index Copernicus.

Link de la publicación http://www.ijopm.org/index.php/IJOPM/article/view/254/333

PLATAFORMA CON INFORMACIÓN GEOGRÁFICA, DE APOYO AL PLAN DE EVACUACIÓN LATACUNGA, EN CASO DE ERUPCIÓN DEL VOLCÁN COTOPAXI.
ISSN: 1390 1117- Vol. 1 No. 1

Revista Ciencias ESPE. (Escuela Politécnica del Ejercito)

Bases de Datos Indexada Latindex.

Link de la publicación https://ia601508.us.archive.org/30/items/Articulo8_201705/Arti%CC%81culo

%208.pdf

GENXMLDC: SOFTWARE PARA MOSTRAR EL USO DE TECNOLOGÍAS DE LA WEB SEMÁNTICA.

ISSN: 2602-8255 - Vol. 1 No. 1

Revista CIYA – UTC - indexada en DRJI

Link de la publicación http://investigacion.utc.edu.ec/revistasutc/index.php/ciya/article/view/72

/70

TECNOLOGÍA MÓVIL COMO ASISTENTE VIRTUAL EN EL MUSEO DE LA ESCUELA ISIDRO AYORA.

ISBN: 978-9942-948-14-4 - Página – 567

Publicación en el LIBRO del Congreso de la "Primera Convención Internacional de la Universidad Técnica de Manabí".

Link de la publicación

https://issuu.com/edicionesutm/docs/cciutm_2017_____libro_d_eresumenes_1r

a/30/items/Articulo8_201705/Arti%CC%81culo%208.pdf

TECNOLOGÍAS SEMÁNTICAS PARA LA GESTIÓN DE REDES INFORMÁTICAS.

ISSN: 2602-8255 - Vol. 1 No. 1

Revista CIYA – UTC - indexada en DRJI

Link de la publicación http://investigacion.utc.edu.ec/revistasutc/index.php/ciya

OTRAS PUBLICACIONES EN REVISTAS REGIONALES O LOCALES

SEMILLERO DE ROBÓTICA

RevistaAlmaMater,N°10,UniversidadTécnicadeCotopaxi,2013,Pág.343. ISBN: 978-9978-395-08-0

DESARROLLO DE UNA APLICACIÓN SOFTWARE Y HARDWARE PARA LA ENSEÑANZA DEL CÓDIGO BRAILLE PARA PERSONAS CON DEFICIENCIA VISUAL.

RevistaAlmaMater,N°10,UniversidadTécnicadeCotopaxi,2013,Pág.343. ISBN: 978-9978-395-08-0

RECURSOS EDUCATIVOS WEB 2.0 PARA MEJORAR EL PROCESO DE ENSEÑANZA APRENDIZAJE.

RevistaAlmaMater,N°10,Universidad TécnicadeCotopaxi,2013,Pág.343.

ISBN: 978-9978-395-08-0

IPV6, LA NUEVA VERSIÓN DEL INTERNET.

Revista Desafíos, N° 2, enero del 2013, Pág. 18 - 19.

ESTUDIO COMPARATIVO ENTRE J2EE Y .NET PARA EL DESARROLLO DE APLICACIONES WEB.

Revista de Investigación Científica Nº1 UTCiencia Universidad Técnica de Cotopaxi - 2011

ISSN: 1390 - 6909

11. PONENCIAS EN CONGRESOS INTERNACIONALES

LEVELS OF SIMILARITY IN USER PROFILES BASED CLUSTER TECHNIQUES AND MULTIDIMENSIONAL SCALING

Autores: Alex Cevallos, Jorge Rubio, Gustavo Rodríguez.

Congreso Internacional de INASE, en Enero 17 del 2016, **Viena Austria**

GUÍA VIRTUAL INTERACTIVA EN ANDROID A TRAVÉS DE CÓDIGOS QR EN EL MUSEO DE LA ESCUELA ISIDRO AYORA DEL ECUADOR

Autores: Jorge Rubio, Fausto Vizcaíno, Gustavo Rodríguez.

Congreso Internacional de Información INFO´2016, **La Habana - Cuba** – 2 de noviembre del2016.

A WEB PLATAFORM WITH GEOGRAPHIC INFORMATION, TO SUPPORT EVACUATION CONTINGENCY PLAN OF LATACUNGA, IN THE CASE OF COTOPAXI VOLCANO ERUPTION

Autores: Alex Cevallos, Jorge Rubio, Gustavo Rodríguez.

Congreso Internacional de Innovación y Transferencia del Conocimiento CIITC 2016, Quito - Ecuador del 25 al 27 de octubre del 2016.

TECNOLOGÍA MÓVIL COMO ASISTENTE VIRTUAL EN EL MUSEO DE LA ESCUELA ISIDRO AYORA.

Autores: Jorge Rubio, Fausto Viscaino, Fredy Baño.

3rd International Conference on Technology Trends CITT 2017. Universidad Técnica deBabahoyo.

Anexo 2: Hoja de vida de investigadores

II. FORMACIÓN ACADÉMICA

NOMBRES Y APELLIDOS: WILLIAMS MANUEL ALVAREZ MARCALLA

DOCUMENTO DE IDENTIDAD: 175156349-3

FECHA DE NACIMIENTO: 26 DE JULIO DE 1996

ESTADO CIVIL: SOLTERO

DIRECCIÓN: TENA, MARPINDO Y PITON

CELULAR: 0995746464

E-MAIL: williams.alvarez9128@utc.edu.ec

NACIONALIDAD: ECUATORIANO

ESTUDIOS SECUNDARIOS	
INSTITUCION EDUCATIVA	UNIDAD EDUCATIVA SAN JOSÉ.
TITULO	BACHILLERATO GENERAL UNIFICADO
ESTUDIOS UNIVERSITARIOS	
UNIVERSIDAD	UNIVERSIDAD TÉCNICA DE COTOPAXI
CARRERA	INGENIERÍA EN INFORMATÍCA Y SISTEMAS COMPUTACIONALES (CURSANDO ACTUALMENTE 9NO SEMESTRE)
CURSOS REALIZADOS	
ESTABLECIMIENTO	**TEMATICA**
SEMINARIOS	
LUGAR	**TEMATICA**

EDUCACIONIT	**SEMINARIO DE ANDROID**
	SEMINARIO DE IOT
Certificaciones	
ACADEMIA CISCO	**Introducción a IoT**
	Introducción a la Seguridad Cibernética
	NDG Linux Unhatched
	Get Connected

I. DATOS DE IDENTIFICACION PERSONAL

NOMBRES: Johnny Danilo

APELLIDOS: Llulluna Chasipanta

FECHA DE NACIMIENTO: 6 de Marzo de 1996

EDAD: 25 años

ESTADO CIVIL: Soltero

CEDULA DE CIUDADANIA: 172303055-5

DOMICILIO: Sector Pacaypamba - Pintag

TELÉFONO: 2149-104 0988210756

CORREO: Johnny_9603@hotmail.com

II. ESTUDIOS REALIZADOS:

SUPERIOR: Universidad Técnica de Cotopaxi

Facultad de Ciencias e Ingeniería

Ingeniería en Informática y Sistemas Computacionales.

SECUNDARIA: Colegio Nacional “Juan de Salinas” Sangolquí

Bachiller Químico - Biológicas.

III. CURSOS Y SEMINARIOS:

- CONCURSO DE BOOTS – ESPOCH

  Diseño de prototipos programables seguidores de líneas

  Duración: 48 horas.

  Fecha: Mayo 2017.

- CONCURSO INTERNACIONAL DE BOOTS - UTA

Diseño de prototipos programables seguidores de líneas

Duración: 48 horas.

Fecha: Noviembre 2016.

- SINDICATO DE CHOFERES PROFESIONALES "LURA ALMEIDA"

  Licencia Profesional tipo "C"

  Duración: 6 meses.

  Fecha: 22 de Julio del 2016.

IV. EXPERIENCIA LABORAL:

- **RESTAURANTE RINCON CONTINENTAL**

Cajero a tiempo parcial

Tiempo: Agosto 2015 - Mayo 2016

- **CONSTRUCCCIONES METALICAS**

  Mantenimiento industrial

  Armadura y soldadura.

  Duración: 1 año

- **LIBRERÍA ATLAS**

  Mantenimiento preventivo y correctivo de PC´S

  Conexión de redes inalámbricas.

  Duración: 3 meses.

- **CHOFER INDEPENDIENTE DEL DOCTOR HENRY RIVERA**

Chofer a tiempo parcial.

Duración: 6 meses.

V. REFERENCIAS PERSONALES:

Ing. Wilmer Ushiña

Ingeniero Civil Independiente

wilmer1720@hotmail.com

Celular: 0987553519

Dr. Henry Rivera

Medico Ocupacional de la Empresa Crilamit S.A

Consultoriomedico.crilamyt@gmail.com

Celular: 0984003485

Sra. Esperanza Oscullo

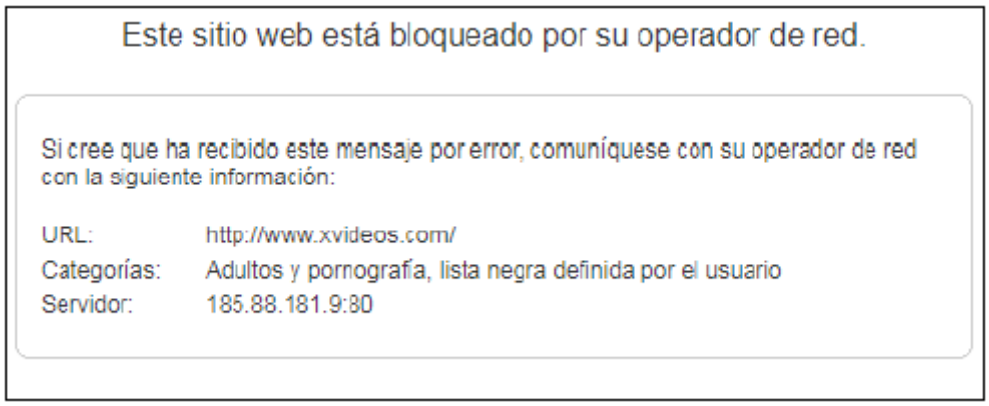
Propietaria del Restaurante Rincón Continental

Teléfono: 2334779

Celular: 0979231417

Anexo 3: Filtrado Web

Al momento de ingresar a una pagina no autorizada dentro de la universidad, el filtrado web mostrara un mensaje:



Fuente: Computadora de las TIC’s

Anexo 4. Formulario de Encuesta

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TEMA: DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, BASADO EN LA NORMA ISO 27000.

Nombre del entrevistado:	Fecha:
Esta entrevista será realizada para garantizar la efectividad del proyecto, dirigida al personal del Departamento de tecnologías de la información.	
1) La Universidad cuenta con políticas de seguridad informática.	
2) En la universidad se utiliza algún sistema o software para el almacenamiento de la información.	
3) Qué sistema de almacenamiento de la información utilizan en la universidad.	
4) Utilizan algún servidor para almacenar la información	
5) Con que frecuencia se realiza el resguardo de información.	
6) La universidad d cuenta con herramientas para realizar filtrado web.	
7) La universidad cuenta con filtrado web.	
8) Es importante establecer filtros web que registran el acceso a internet.	
9) La universidad establece categorías de filtrado web para el acceso a internet.	
10) Cuenta la universidad con un Data Center.	

11) Conoce que son las normas ISO 27000 relacionadas a la seguridad de la información.	
12) La Universidad cuenta con un AD (Active Directory)	
13) La Universidad cuenta con un VPN	
14) Qué tipo de bases de datos utiliza la universidad	
15) Han realizado un análisis de riesgo dentro de la universidad.	
16) Existen políticas de respeto a la seguridad de la información.	
17) Cree usted que la información que se maneja en la Universidad es segura.	
18) Considera usted que la información es vulnerable a los hackers o personas mal intencionadas que podrían alterarlas.	

Anexo 5: Formulario de Entrevista

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

FICHA DE OBSERVACIÓN	
Fecha:	
Lugar:	
Encargado del departamento de tecnologías.	
ASPECTO A VERIFICAR	***RESULTADOS***
1. La universidad posee políticas de seguridad informática.	
2. Existe un control de acceso a los equipos y sistemas de cómputo.	
3. Posee la universidad el Active Directory	
4. Posee un sistema para respaldar la información	
5. Frecuencia de respaldo de información	
6. Seguridad a componentes informáticos.	
7. Filtrado web	
8. Categorías de filtrado web	