UNIVERSIDAD TÉCNICA DE COTOPAXI

TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNIVERSIDAD TECNICA DE COTOPAXI
FECHA 28/11/2022
HORA 11h20
FIRMA

Latacunga noviembre 28,2022
D.T.I.C.-432-2022

Ingeniero. Mgs.
Patricio Bastidas Pacheco
VICERRECTOR ADMINISTRATIVO DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.
Presente. –

De mi consideración:

Reciba un atento y cordial saludo, por este medio hago llegar el Plan de Seguridad Informática de la Dirección de Tecnologías de Información, para su análisis y aprobación.
Particular que comunico para los fines pertinentes.

Atentamente,

"POR LA VINCULACIÓN DE LA UNIVERSIDAD CON EL PUEBLO"

PhD. Gustavo Rodríguez Bárcenas
DIRECTOR DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
GR
soledad g

Anexo: (Lo indicado)

PLAN DE SEGURIDAD DE LA INFORMACIÓN

UNIVERSIDAD TÉCNICA DE COTOPAXI

2022

Tabla de contenido

1. Alcance del Plan de Seguridad Informática

Cómo antecedentes importantes considerados se plantean los siguientes aspectos:

Inciso segundo del artículo 314 de la Constitución de la República, dispone que el "Estado garantizará que los servicios públicos, prestados bajo su control y regulación, respondan a principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad;"

Numeral 2 del artículo 16 de la Constitución de la República del Ecuador establece como derecho de las personas, en forma individual o colectiva, el acceso universal a las tecnologías de información y comunicación;

Numeral 21 del artículo 66 de la Constitución de la República del Ecuador reconoce y garantiza a las personas el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; derecho que protege cualquier otro tipo o forma de comunicación;

El artículo 140 de la Ley Orgánica de Telecomunicaciones, dispone: "Rectoría del sector. El Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información. A dicho órgano le corresponde el establecimiento de políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información, de conformidad con lo dispuesto en la presente Ley, su Reglamento General y los planes de desarrollo que se establezcan a nivel nacional. Los planes y políticas que dicte dicho Ministerio deberán enmarcarse dentro de los objetivos del Plan Nacional de Desarrollo y serán de cumplimiento obligatorio tanto para el sector público como privado";

Acuerdo Ministerial nº 011-2018, del 08 de agosto de 2018, se expide el Plan Nacional de Gobierno Electrónico 2018-2021; este instrumento muestra la situación actual del país en materia de gobierno electrónico, las acciones que serán ejecutadas en tres programas; Gobierno Abierto, Gobierno Cercano y Gobierno Eficaz y Eficiente. En el Capítulo 1. Fundamentos Generales, literal 5. Diagnóstico; se enfatiza que: "Dentro de las iniciativas relevantes que ha implementado el gobierno entorno a la ciberseguridad se encuentra la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI)…"

ACUERDO MINISTERIAL nº 025-2019, de 20 de septiembre de 2019, del MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN.- que se enfoca en implementar el Esquema Gubernamental de Seguridad de la Información (EGSI). El EGSI preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la Información y la selección de controles para el tratamiento de los riesgos identificados".

El código 410 de la Norma de Control Interno de la Contraloría General del Estado sobre Tecnologías de Información y Comunicación.

El presente Plan de Seguridad Informática es aplicable en su totalidad en las áreas de la Universidad Técnica de Cotopaxi sito en Av. Simón Rodríguez s/n Barrio El Ejido Sector San Felipe, Latacunga - Ecuador.

Este será de dominio y conocimiento pleno de todas las personas que participen en el uso, aplicación, explotación y mantenimiento de las tecnologías donde se procesa la información.
Las políticas expresadas en este plan son de obligatorio cumplimiento para todo el personal de la Institución.

2. Caracterización del Sistema Informático

Como soporte tecnológico se tienen como infraestructura un servidor HP BLADE adquirido por el 2012, con 9 años de longevidad, estos tienen las siguientes especificaciones:

Tabla1. Infraestructura servidor HP BLADE.

MARCA	CARACTERÍSTICA	MODELO	PROCESADOR
HP	HP BLc7000 1PH 6PS 10Fan 16 IC Plat Encl - HP BLc7000 Platinum Enclosure with 1 Phase 6 Power Supplies 10 Fans ROHS 16 Insight Control Licenses. Gabinete monofásico, con 16 licencias de Insight Control Suite *, 6 fuentes de poder AC, 10 ventiladores Active Cool 200 Fans, Rail Kit, 1 módulo Onboard Administrator con KVM port. El gabinete posee cuatro zonas. Cada zona puede contener hasta 2 servidores de altura completa o hasta 4 servidores de altura media.	BLC700	

	HP 2400W Gold Ht Plg Pwr Supply Kit.		
	HP 40A HV Core Only Corded PDU.		
	HP 6125G Blade Switch Opt Kit	6125G Blade Switch	
	HP 6125G Blade Switch Opt Kit	6125G Blade Switch	
	HP TFT7600 KVM Console US Kit		
	HP BL460c Gen8 E5-2670 2P 64GB Svr / (2) Intel® Xeon® E5-2670 (2.60GHz/8-core/20MB/115W) / 20MB (1x20MB) Level 3 cache / 64GB (8x 8GB) PC3-12800R (DDR3-1600) / HP FlexFabric 10Gb 2-port 554FLB / HP Smart Array P220i Controller with 512MB FBWC RAID 0,1 / HP iLO Management Engine / Garantía 3-3-3.	BL460c Gen8	2 PROCESADORES Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz
	BL460c Gen8 E5-2650 1P 32GB Svr / (1) Intel® Xeon® E5-2650 (2.0GHz/8-core/20MB/95W) / 20MB (1x20MB) Level 3 cache / 32GB (4x 8GB) PC3-12800R (DDR3-1600 Registered DIMMs at 1.5V) / HP FlexFabric 10Gb 2-port 554FLB FlexibleLOM / HP Smart Array P220i Controller with 512MB FBWC RAID 0,1 / 2 standard - Slot 1 supports Type A mezzanine Cards. Slot 2 supports Type A and Type B mezzanine cards / HP iLO Management Engine / Garantía 3-3-3.	BL460c Gen8	Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
	BL460c Gen8 E5-2650 1P 32GB Svr / (1) Intel® Xeon® E5-2650 (2.0GHz/8-core/20MB/95W) / 20MB (1x20MB) Level 3 cache / 32GB (4x 8GB) PC3-12800R (DDR3-1600 Registered DIMMs at 1.5V) / HP FlexFabric 10Gb 2-port 554FLB FlexibleLOM / HP Smart Array P220i Controller with 512MB FBWC RAID 0,1 / 2 standard - Slot 1 supports Type A mezzanine Cards. Slot 2 supports Type A and Type B mezzanine cards / HP iLO Management Engine / Garantía 3-3-3.	BL460c Gen8	Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
	P2000 (ALMACENAMIENTO EXTERNO)	P200_G3_LFF	
	RACK CERRADO PISO 42U 213*60*100CM	42U 213*60*100CM	

Existen otros servicios como lo son las revistas científicas y el sistema de Ecuciencia, ambos usan servidores con las siguientes características:

- HPE Smart Buy Proliant DL160 Gen9 Intel Xeon E52609v4 Intel Xeon E5-2609v4 8-Core (1.70 GHz 20MB L3 Cache) Kit / 16GB (2x8GB) DDR4 2400MHz RDIMM / HP Integrated Matrox G200eH2 with 16MB Video RAM / HP Embedded Dual Port 361i Adapter / (x2) HPE 1TB 6G SATA 7.2K LFF SC STND HDD / Dynamic Smart Array B140i controller (RAID 0/1/1+0/5) SATA Only (No Cache) / (4) Hot Plug 3.5in Large From Factor Smart Carrier Hard Disk / (x1)HP 9.5mm SATA DVD-RW (Jack-Black) Gen9 Kit / Modular Battery: 1, PCIe 8x:1, Graphics: 1/1 x Non-Pluggable Non-Redundant 550W FIO Power Supply / (x1) HPE 3y NBD DL160 Gen9 FC SVC / Garantía 3 Year Parts / 1 Year Labour / 1 Year Onsite Warranty / HP 1U SFF Easy Install Rail Kit, HP Thumbscrew Ear Kit / Rack Mount (1U) SERIE: 2M274203LX.

La Universidad Técnica de Cotopaxi cuenta con una infraestructura de red con las siguientes características:

Como antecedente importante se tiene que la Universidad Técnica de Cotopaxi en la Sede Matriz, adquirió en el **año 2015** los siguientes equipos de conectividad:

Tabla 2. Infraestructura de Red de la Matriz.

EQUIPO	MODELO	UBICACIÓN	OBJETIVO
Security Appliance	MX400	Datacenter	Firewall / IPS, actualmente cumple funciones de backup (respaldo) al equipo Fortigate D1000, acceso VPN, filtrado de contenido
Switch Core	MS420-24P	Datacenter	Switch principal de la infraestructura de comunicación, encargada de gestión de Vlans, DHCP, enrutamiento de tráfico. En este switch se conectan los enlaces de fibra óptica hacia los siguientes edificios: Bloque A, Bloque B, Teatro (laboratorios de CIYA); de igual manera los enlaces de fibra óptica hacia Security Appliance MX400 y hacia el switch de datacenter.
Switch_Datacenter	MS320-24	Datacenter	Switch principal Edificio Administrativo, enlace de red interna

			hacia diferentes servidores de aplicaciones (académico, Moodle, financiero, investigación, etc)
Switch Distribución 1	MS320-24	Rack MDF 1-A Bloque A	Switch principal Bloque A, enlace hacia diferentes switches de acceso del edificio. Tiene los enlaces de fibra óptica desde los switches de Core y SDF 4-A
Switch Distribución 2	MS320-24	Rack MDF 1-B Bloque B	Switch principal Bloque B, enlace hacia switches de acceso del edificio. Tiene los enlaces de fibra óptica desde los switches de Core y MDF 1-C (Bloque Comedor)
Switch Distribución 3	MS320-24	Rack MDF 1-C Bloque Comedor	Switch principal Bloque Comedor, enlace hacia switches de acceso del edificio. Tiene el enlace de fibra óptica MDF 1-B (Bloque B). De igual manera actúa como switch de acceso de algunos puntos terminales de red del edificio.
Switch DMZ	MS220-24P	Datacenter	Switch que gestiona la conexión de la granja de servidores hacia los direccionamientos públicos.
Switch Acceso 1	MS220-48LP	Rack MDF 1-B Bloque B	Switch que contiene los diferentes puntos de red hacia equipos terminales del edificio (computadores, impresoras, Access Point, controles de acceso a aulas, etc.).
Switch Acceso 2	MS220-48LP	Rack MDF 1-B Bloque B	Switch que contiene los diferentes puntos de red hacia equipos terminales del edificio (computadores, impresoras, Access Point, controles de acceso a aulas, etc.).
Switch Acceso 3	MS220-48LP	Rack MDF 1-B Bloque B	Switch que contiene los diferentes puntos de red hacia equipos terminales del edificio (computadores, impresoras, Access Point, controles de acceso a aulas, etc.).
Switch Acceso 4	MS220-48LP	Rack MDF 1-B	Switch que contiene los diferentes puntos de red hacia equipos terminales del

		Bloque B	edificio (computadores, impresoras, Access Point, controles de acceso a aulas, etc.).
Switch Acceso 5	MS220-48LP	Rack MDF 1-B Bloque B	Switch que contiene los diferentes puntos de red hacia equipos terminales del edificio (computadores, impresoras, Access Point, controles de acceso a aulas, etc.).
Switch Acceso 6	MS220-48LP	Rack SDF 2-B Bloque B	Switch que contiene los diferentes puntos de red hacia equipos terminales del edificio (computadores, impresoras, Access Point, controles de acceso a aulas, etc.).
Switch Acceso 7	MS220-48LP	Datacenter	Switch que contiene los diferentes puntos de red hacia equipos terminales del edificio (computadores, impresoras, Access Point, controles de acceso a aulas, etc.).
Switch Acceso 8	MS220-48LP	Rack MDF 1-C Bloque Comedor	Switch que contiene los diferentes puntos de red hacia equipos terminales del edificio (computadores, impresoras, Access Point, controles de acceso a aulas, etc.).
Switch Acceso 9	MS220-48LP	Datacenter	Switch que contiene los diferentes puntos de red hacia equipos terminales del edificio (computadores, impresoras, Access Point, controles de acceso a aulas, etc.).
Switch Acceso 10	MS220-24P	Rack MDF 1-B Bloque B	Switch que contiene los diferentes puntos de red hacia equipos terminales del edificio (computadores, impresoras, Access Point, controles de acceso a aulas, etc.).
Switch Acceso 11	MS220-24P	Rack MDF 1-B Bloque B	Switch que contiene los diferentes puntos de red hacia equipos terminales del edificio (computadores, impresoras, Access Point, controles de acceso a aulas, etc.).

Switch Acceso 12	MS220-24P	Rack SDF 2-B Bloque B	Switch que contiene los diferentes puntos de red hacia equipos terminales del edificio (computadores, impresoras, Access Point, controles de acceso a aulas, etc.).

Otros equipamientos de conectividad en la MATRIZ, SALACHE Y LA MANÁ. el cual fue adquirido en el **año 2018**, como se observa en la tabla:

Tabla 3. Infraestructura de Red Salache y La Maná.

EQUIPO	MODELO	UBICACIÓN	OBJETIVO
Fortigate	1000D	Datacenter Sede Matriz	Firewall / IPS principal en la sede, controla todo lo referente a seguridad perimetral, seguridad de la intranet, seguridad de datos institucionales, gestión de VPN, filtrado de contenidos y filtrado de aplicaciones hacia internet, controladora de WIFI, enrutamiento, administración y gestión de red.
Fortigate	800D	Datacenter Sede Salache	Firewall / IPS principal en la sede, controla todo lo referente a seguridad perimetral, seguridad de la intranet, seguridad de datos institucionales, gestión de VPN, filtrado de contenidos y filtrado de aplicaciones hacia internet, controladora de WIFI, enrutamiento, administración y gestión de red.
Fortigate	800D	Datacenter Sede La Maná	Firewall / IPS principal en la sede, controla todo lo referente a seguridad perimetral, seguridad de la intranet, seguridad de datos institucionales, gestión de VPN, filtrado de contenidos y filtrado de aplicaciones hacia internet,

			controladora de WIFI, enrutamiento, administración y gestión de red.
Fortiauthenticator	1000D	Datacenter Sede Matriz	Gestión de autenticación de identidad y equipos en la red.
Fortiauthenticator	400E	Datacenter Sede Salache	Gestión de autenticación de identidad y equipos en la red.
Fortiauthenticator	400E	Datacenter Sede La Maná	Gestión de autenticación de identidad y equipos en la red.
Fortianalyzer	400E	Datacenter Sede Matriz	Análisis y gestión de logs. Análisis forense, vulnerabilidades, informes del estado de la red, consumo de ancho de banda, es un equipo esencial para conocer de manera oportuna y precisa el buen funcionamiento de la red y toma oportuna de decisiones.

La topología es de tipo árbol (una serie de redes en estrella interconectadas), se dispone de un cableado estructurado, en la figura se muestra el esquema general.

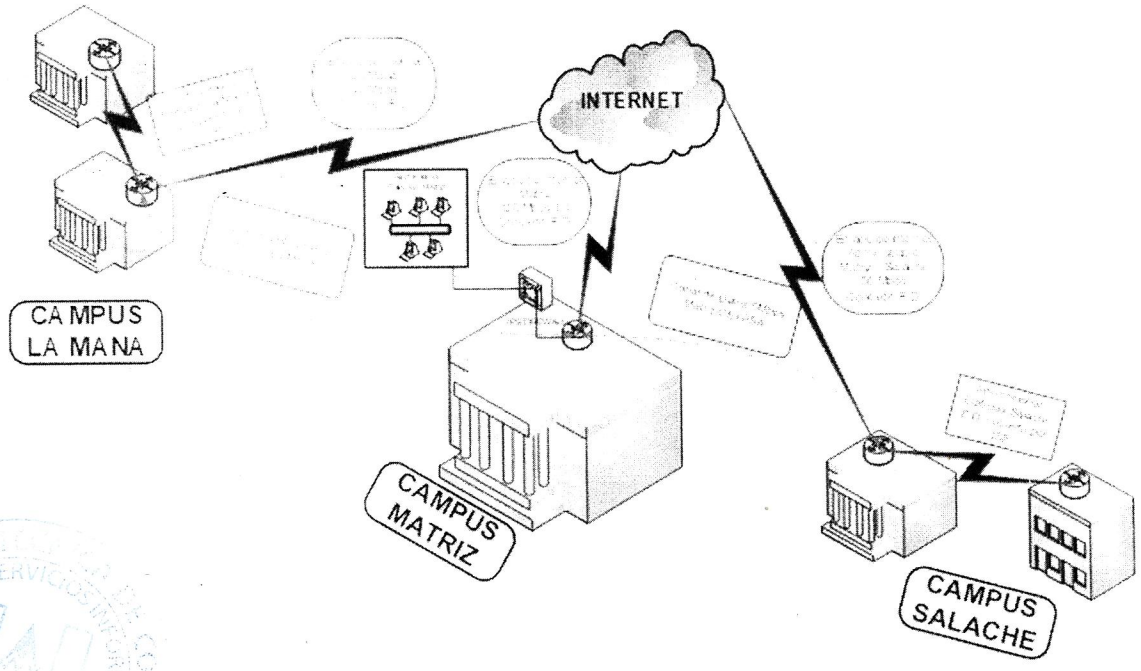


Figura 1. Esquema general de la Red-UTC.

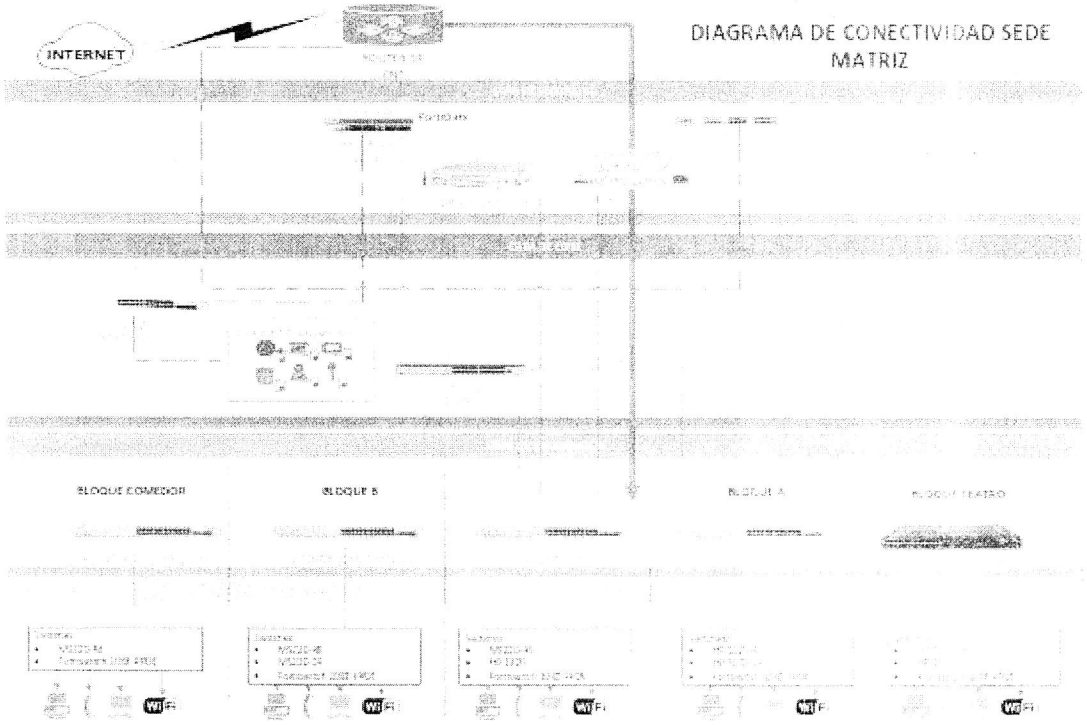


Figura 2. Diagrama de infraestructura de Red Sede Matriz.

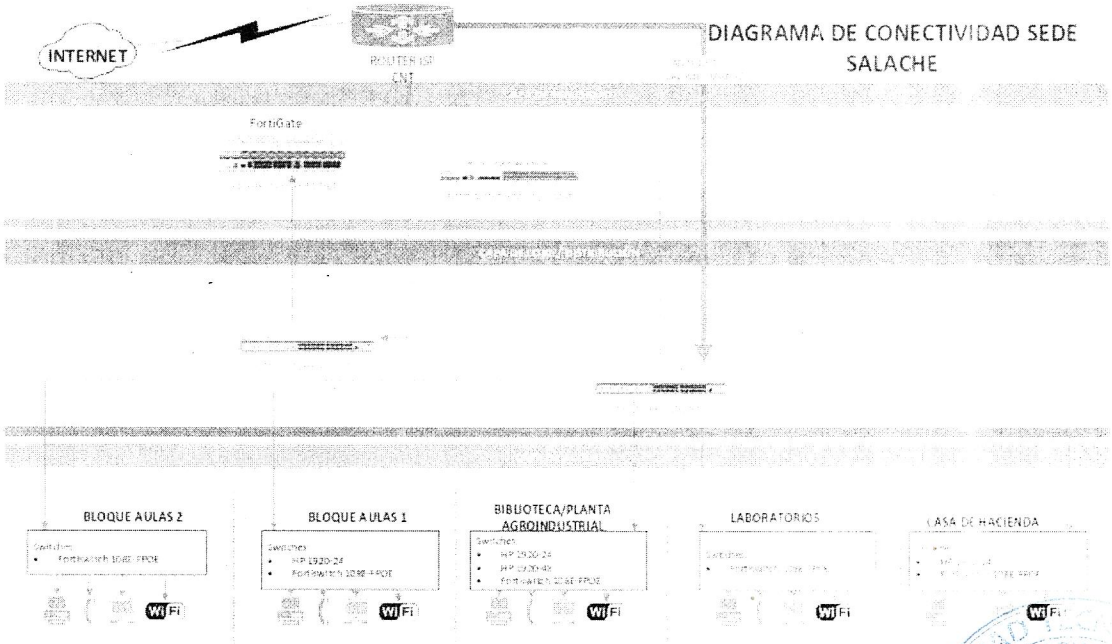


Figura 3. Diagrama de infraestructura de Red Campus Salache.

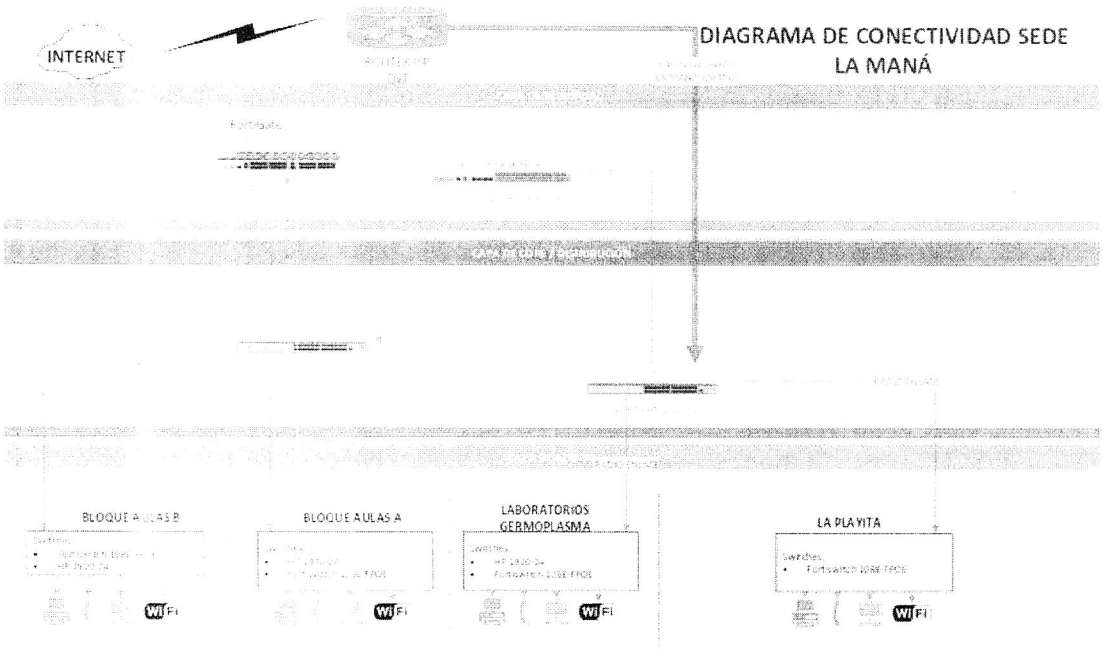


Figura 4. Diagrama de infraestructura de Red Extensión La Maná.

Aplicaciones en explotación.

1. Servicio Web.
2. Bases de datos.
3. Aplicaciones UTC (Talento Humano, Académico, Registros, SIG-UTC):
   - Informaciones generales de los trabajadores, docentes y otros.
   - Gestión de permisos.
   - Registros online de asistencia.
   - Registro de actividades.
   - Prematrículas y matrículas.
   - Gestión del silabo.
   - Otros.
4. Aulas virtuales (Moodle)
5. Correo.
6. Almacenamiento en la nube.
7. Antivirus.
8. Administración de servidores virtuales.
9. Monitoreo. Revisión. Configuración y actualizaciones de S.O del Servidor NAS y Synology.

10. Base de Datos Sistema de Facturación (Departamento Financiero).

En la figura se observa el esquema general y resumido del Sistema Integrado de Gestión:

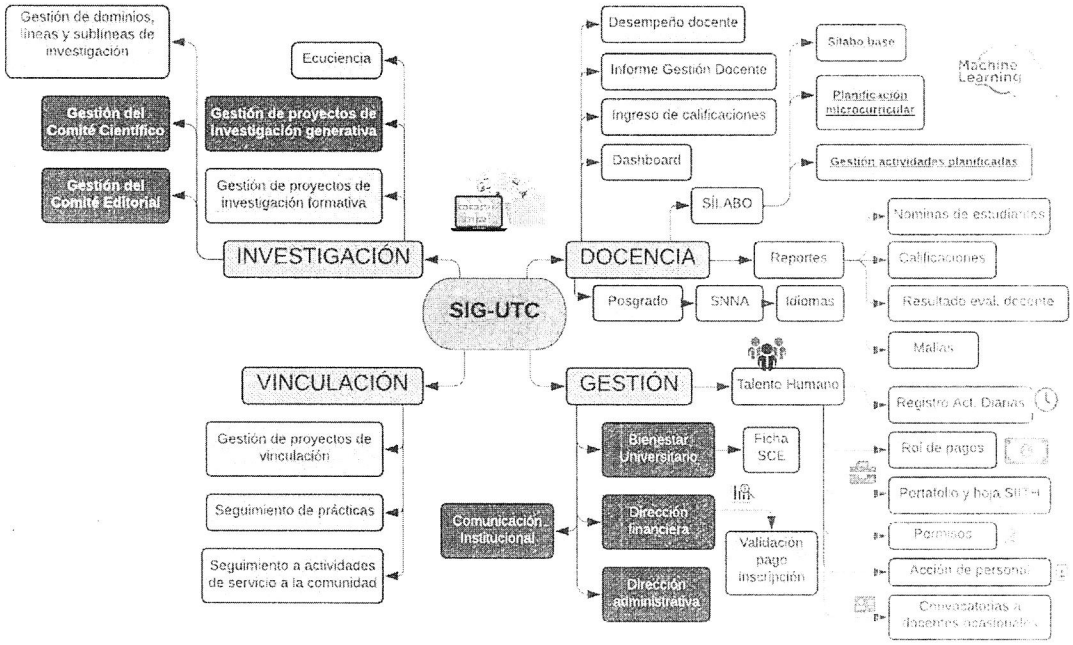


Figura 5. Esquema general del Sistema Integrado de Gestión de la UTC.

Servicios informáticos y de comunicaciones disponibles.

- Servicio de navegación por Internet.
- WIFI.
- Correo electrónico.
- Sistema Integrado de Gestión.
- Aulas Virtuales.
- Almacenamiento en la nube.
- Antivirus.
- Bitácoras.
- Bases de datos.
- Copias de seguridad.
- Soporte técnico.

La información que se produce y se intercambia tanto externa como interna se realiza básicamente a través del correo electrónico, sitio web institucional y dispositivos extraíbles USB dependiendo del tipo de información que se desee.

3. Resultados del Análisis de Riesgo:

Las amenazas más importantes a considerar de acuerdo al impacto que pudieran tener sobre la entidad son:

Actos originados por la criminalidad común:

- Divulgación de información.
- Perdidas de datos.
- Saturación de información.
- Procesamiento de datos ilegales.
- Robos de equipo.
- Destrucción de los equipos o medios.
- Códigos maliciosos.

Sucesos derivados de la negligencia de los usuarios:

- Falta de mantenimiento físico.
- Modificación de la información.
- Datos de fuentes no confiables.
- Cambio Hardware.
- Cambio Software.
- Falla de equipo.
- Falta de disponibilidad de los recursos humanos.
- Monitoreo del tráfico de la red.
- Uso de contraseñas débiles.
- Acceso a los archivos de contraseñas.

Sucesos de origen físico / Daños naturales:

- Sobrecarga eléctrica.
- Interrupción de fuentes de energía.
- Fenómeno climático.
- Fenómeno volcánico.
- Fenómeno sísmico.

- Fuego.
- Errores en los sistemas operativos.

Los bienes más importantes a proteger son:

- Todas las computadoras de la Institución.
- Los servidores del Data Center.
- Los equipos de red (interno y de borde) de todos los campus y extensiones.

El área de mayor peso de Riesgo es:

- Data Center.

4. Políticas de Seguridad Informática

Para la UTC se han considerado las siguientes políticas de seguridad informática:

- ✔ **PO-0** Políticas generales.
- ✔ **PO-1A** Política de control de acceso a recursos informáticos.
- ✔ **PO-1B** Política de administración de activos de tecnología de información.
- ✔ **PO-1C** Política de resguardo de la información.
- ✔ **PO-1D** Política de seguridad a componentes informáticos.
- ✔ **PO-1E** Política de uso adecuado de internet.
- ✔ **PO-1F** 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 manejan los distintos departamentos de la Universidad Técnica de Cotopaxi.

A. POLÍTICAS GENERALES

1. Alcance.

Aplica a todas las personas que conforman la comunidad de la Universidad Técnica de Cotopaxi, incluyendo consultores, contratistas, trabajadores temporales, socios estratégicos y entes autorizados por la institución para hacer uso de sus recursos informáticos.

2. Documentos de referencia.

N/A

3. Descripción de la Política.

a) De la propiedad y responsabilidad de uso de los Recursos TIC:

- Los Recursos TIC provistos por la Institución son de su propiedad o están debidamente licenciados a su nombre. Su utilización será dedicada exclusivamente para efectos laborales, académicos, de investigación, vinculación o de gestión.
- El uso de las TIC deberá estar acorde con el respeto a las leyes, regulaciones, reglamentos, estatutos y normas institucionales y nacionales.

b) De la limitación de la responsabilidad de la Institución:

- Los recursos tecnológicos son ofrecidos con el fin de facilitar el desarrollo de los procesos sustantivos universitarios. En este ofrecimiento de recursos tecnológicos, la Institución no asume ninguna responsabilidad hacia el usuario.
- Cuando la Institución así lo solicite o cuando finalice la relación laboral, profesional o académica con el usuario, él deberá devolver en buen estado todos los recursos tecnológicos que le fueron otorgados (equipo institucional, software institucional, comunicación electrónica, etc.).

c) Sobre Desarrollo de Software para la Universidad Técnica de Cotopaxi:

- Para buscar uniformidad, interoperabilidad, estandarización y homogeneidad en los aplicativos cualquiera que fueren y que se desarrollen para la UTC, se hace necesario que se cumplan los requerimientos asociados al tipo de Base de Datos, esta debe ser en Microsoft SQL, tecnología .NET y Window Server, en versiones acorde a lo desarrollado por la Dirección de TIC y que estos sean capaces de acoplarse al Sistema Integrado de Gestión de la Universidad Técnica de Cotopaxi, para garantizar continuidad y mantenimiento de los sistemas que los componen.

d) Del incumplimiento:

- La Institución hará responsable al usuario del conocimiento del presente documento de Políticas y de las consecuencias que se derivarán de su incumplimiento. Asimismo, el usuario deberá conocer estas Políticas desde su ingreso a la Institución.
- La Institución se reserva el derecho de evaluar periódicamente el cumplimiento de estas Políticas. Cualquier acción disciplinaria derivada del incumplimiento de las mismas, tales como llamadas de atención, suspensiones, expulsiones o despidos, será considerada de acuerdo con los procedimientos establecidos por la Institución y en estricto acatamiento de las estipulaciones legales vigentes.

- En materia de irregularidades o incumplimiento en el uso del software, el usuario que no cumpla con esta Política será directamente responsable de las sanciones legales, en que por responsabilidad laboral, penal o civil se incurra, derivadas de sus propios actos. Igualmente, será responsable de los costos y gastos en que pudiera incurrir la Institución derivados de la defensa por el uso no autorizado o indebido de licencias de software o su aplicación. En razón de lo anterior, no es permitido alegar ignorancia de estas Políticas, ni de documentación que en ellas se mencione, incluyendo las demás licencias en uso.

B. POLÍTICA DE CONTROL DE ACCESO A RECURSOS INFORMÁTICOS

1. Alcance.

Aplica a todas las personas que conforma la comunidad de la Universidad Técnica de Cotopaxi, incluyendo consultores, contratistas, trabajadores temporales, socios estratégicos y entes autorizados por la institución para hacer uso de sus recursos informáticos.

2. Documentos de referencia.

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

RE-02A. Creación de usuario de red.

3. Descripción de la Política.

El primordial y 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 firmado el documento correspondiente al RE-01A "Aceptación y cumplimiento de las políticas".

El uso de cualquier servicio informático y de equipos tecnológico de la UTC será autorizado, solo hasta después de haber sido informado al usuario lo establecido en el documento RE-01A y RE-02A, dejar establecido con el usuario que la información concedida por parte de la universidad solo pueden ser usados para propósitos previamente autorizados, cumpliendo los objetivos que la institución establezca.

El usuario deberá cumplir los siguientes lineamientos:

- Uso adecuado de los recursos obtenidos, el usuario y clave que será proporcionado por parte del área de tecnologías de la información a cada integrante de la institución, será solo para el

uso personal y exclusivo de sí mismo, queda determinantemente prohibido compartir, socializar, entregar estas credenciales a segundas o terceras personas, del usuario incurrir en esta violación considerada grave, será notificado a las autoridades para que sean aplicadas las medidas disciplinarias correspondiente acorde al reglamento de la UTC correspondiente para ello.

- Responsabilidad, entender que toda actividad que sea registrada al sistema con la clave y el usuario asignado, será de total responsabilidad del usuario al cual se le concedió dichos datos.
- Transparencia, llevar a cabo todos los procesos designados de forma legal, comunicando al inmediato superior cualquier tipo de situación que sea sospechosa o que ponga en peligro la información de la institución.
- Confidencialidad, las credenciales asignadas son de uso personal, por lo cual no pueden ser divulgadas a ninguna otra persona.
- Pro actividad, los usuarios tienen el deber de cumplir y apoyar todas las normas de seguridad dictadas en esta política.
- Seguridad, el usuario tiene la obligación de recordar sus credenciales asignadas, por lo cual tiene determinantemente prohibido escribirla en algún medio que pueda ser encontrado.
- En caso de que el usuario sospeche que ha ocurrido una eventualidad respecto a sus credenciales del Sistema Integrado de Gestión, correo institucional, aulas virtuales o cualquier otro de los sistemas que la institución implementare, deberá notificar urgentemente a la Dirección de TI.
- En caso de que el usuario olvidara o perdiera la contraseña de acceso a los diferentes sistemas informáticos, deberá utilizar la opción de generación de nuevas contraseñas, en caso de ser necesario acercarse a la Dirección de TIC.
- Toda persona que incumpla los reglamentos previamente señalados en esta política, deberá someterse a acciones disciplinarias según el reglamento de la institución.
- El usuario no deberá, sin permiso expreso y por escrito de la Dirección de TIC, hacer modificaciones a la Red Institucional, la Intranet o a sus recursos. No se permitirá ningún intento de vulnerar o de atentar contra los sistemas de protección o de seguridad de la Red.

Ante cualquier acción de este tipo, la Institución procederá a ejecutar cualquier acción de carácter administrativo, laboral, penal o civil que corresponda.

- Son expresamente prohibidas las siguientes acciones:
  i. Cambiar la configuración en las interfaces de la Red.
  ii. Cambiar o suplantar la identidad del equipo en la Red (número IP, dirección física, nombre de la máquina, dominio de red).
  iii. Cambiar la ubicación física de los cables de Red.
  iv. Acceder a los centros de cableados o manipular los dispositivos de comunicación de datos sin autorización.
  v. Ingresar o instalar en la Red de la UTC algún dispositivo de comunicación de datos (AP, Switch, Router o de cualquier otro tipo) sin autorización de la Dirección de TIC.

De este modo, se detalla las siguientes medidas de control a implementarse en el acceso de los recursos informáticos:

Acceso al Sistema Integrado de Gestión.

- Talento Humano tendrá la obligación de notificar a la Dirección de TI la creación de nuevos usuarios con relación de dependencia, para así ser utilizados en el Sistema Integrado de Gestión y del correo institucional, previa inducción de las políticas de seguridad informática y aceptación por parte del usuario.
- Las secretarías académicas de las facultades, posgrado y nivelación tendrán la obligación de notificar a la Dirección de TI la creación de nuevos usuarios estudiantes, para así ser utilizados en el Sistema Integrado de Gestión y del correo institucional, previa inducción de las políticas de seguridad informática y aceptación por parte del usuario.
- Los usuarios del Sistema Integrado de Gestión serán creados con el siguiente estándar: se usarán las credenciales de su cédula de identidad o pasaporte (1500727473), los cuales deberán cambiar sus contraseñas en su primer inicio de sesión.
- Todos los usuarios dispondrán de un usuario y contraseña únicos que le permita acceder a su equipo de cómputo asignado.
- Pasados los 5 minutos de inactividad en el equipo de cómputo asignado, se cerrará la sesión, protegiéndola de personas no autorizadas, utilizando el bloqueo de pantalla u otro método apropiado para el mismo.

- La clave designada tendrá un mínimo de 8 caracteres.
- La clave estará compuesta por letras (incluyendo mayúsculas), números y caracteres especiales.
- El usuario puede cambiar la clave de acceso designada cada 6 meses o en caso que presienta que ya no es confidencial.
- Pasados los 30 minutos de inactividad después de iniciar sesión en el Sistema Integrado de Gestión, se cerrará la sesión, protegiendo la cuenta de personas no autorizadas.
- Los usuarios del Sistema Integrado de Gestión tienen la obligación de cambiar la contraseña de acceso no menos de una vez cada tres (3) meses.

Correo electrónico.

- El Departamento de Tecnologías de la Información creará una contraseña temporal para el acceso al servicio de correo electrónico.
- Las cuentas de correo electrónico estarán estandarizadas de la siguiente forma: el primer nombre, punto, primer apellido y los 4 últimos dígitos de la cédula/pasaporte de identidad, ejemplo: (luis.lopez3358@utc.edu.ec).
- Están completamente prohibidas las siguientes actividades:
  1. Utilizar el Correo Electrónico para cualquier propósito comercial, fines de lucro, o actividades ajenas a las funciones institucionales.
  2. Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para nuestra Institución.
  3. Toda información o contenido que sea transmitido por las cuentas de correo, son responsabilidad únicamente del dueño de la cuenta, por lo que dichos contenidos no reflejan las preferencias o ideas de la institución.
  4. El correo electrónico institucional es de uso exclusivo para los intereses de la UTC, no deberá sobrepasar el límite de almacenamiento en la nube permitido por el proveedor.
  5. La unidad de Talento Humano deberá proveer a la Dirección de TIC el listado del personal que hayan culminado sus funciones de relación de dependencia con la institución, una vez entregada la información y ser notificado, el usuario tendrá un tiempo de un mes para respaldar

su información, luego de transcurrir este tiempo será desactivada su cuenta, hasta transcurrir 6 meses después de la fecha de desactivación, luego de esto será eliminada completamente.

6. Las secretarías académicas de las facultades, posgrado y nivelación tendrán la obligación de notificar a la Dirección de TI el listado de estudiantes graduados, culminado sus estudios o estudiantes que hayan decidido retirarse por el motivo que fuere. Estos estudiantes tendrán un tiempo máximo de 3 meses luego de su notificación para respaldar su información, inmediatamente de transcurrir este tiempo serán desactivadas sus cuentas, hasta transcurrir 6 meses después de la fecha de desactivación, luego de esto será eliminada completamente.
7. Cada usuario contará con una única cuenta de correo electrónico para cumplir con sus funciones.
8. Los usuarios del correo electrónico tienen la obligación de cambiar la contraseña de acceso no menos de una vez cada tres (3) meses.
9. Son expresamente prohibidas las siguientes acciones:

- El envío de mensajes que atenten contra la moral (de contenido vulgar, ofensivo, abusivo o insinuante).
- Enviar mensajes masivos que no estén debidamente autorizados o que no se trate de asuntos oficiales.
- Propagar cadenas de mensajes.
- Publicar anuncios personales sin autorización de la Institución (servicios, productos u otros).
- Utilizar o divulgar códigos, claves o contraseñas de acceso de otro usuario, así como abrir, borrar, modificar o recuperar archivos que no son de su propiedad; a menos que sea formalmente autorizado.

Usuarios para el aula virtual.

- El usuario de aula virtual será creado una vez suministrado el listado de los estudiantes y a petición de los docentes.
- Los Usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y su buzón asociado a nuestra Institución.
- Los usuarios de las aulas virtuales serán creados con el siguiente estándar: se usarán las credenciales de su cédula de identidad o pasaporte (1500727473), los cuales deberán cambiar sus contraseñas en su primer inicio de sesión.

- La contraseña que se establece temporalmente como valor inicial es su número de cédula, es obligatorio 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 6 meses, el sistema eliminará el usuario de forma permanente.
- Los usuarios de las aulas virtuales tienen la obligación de cambiar la contraseña de acceso no menos de una vez cada tres (3) meses.

Plataformas, equipos de conectividad e infraestructura de servidores.

- El Departamento de Tecnologías de la Información establecerá una contraseña para su uso o administración.
- El área de Tecnologías de la Información administrará todas las contraseñas de acceso a los diferentes servidores, aplicaciones, equipos informáticos y de conectividad.
- Los responsables de plataformas, equipos de conectividad e infraestructura de servidores contarán con un usuario y contraseña que deberá proteger y que será solo para el uso personal y exclusivo de sí mismo con el propósito de administrar, configurar, realizar respaldos, entre otros acorde a sus funciones; queda determinantemente prohibido compartir, socializar, entregar estas credenciales a segundas o terceras personas.
- Las credenciales para administrar las plataformas, equipos de conectividad e infraestructura de servidores niveles de seguridad alto, deberán de contener letras mayúsculas, minúsculas, números y caracteres especiales, con un mínimo de 8 caracteres.
- Las contraseñas deberán ser cambiadas al menos con una frecuencia de 6 meses, dejando evidencia en bitácora de lo realizado.
- Los responsables de las plataformas, equipos de conectividad e infraestructura de servidores deberán crear credenciales alternas con privilegio de superusuario o administradores solo con el propósito de enfrentar alguna contingencia.

- Los responsables de las plataformas, equipos de conectividad e infraestructura de servidores deberán, entregar las credenciales con privilegio de superusuario o administradores solo con el propósito de enfrentar alguna contingencia en un sobre sellado al Director de TI para su custodio, quien solo podrá abrir en casos de eventualidades, obligando el cambio inmediato de contraseñas.
- Se considerará que toda actividad registrada al sistema con las claves y usuario asignados a los responsables de las credenciales de las plataformas, equipos de conectividad e infraestructura de servidores, será de total responsabilidad de este.
- Transparencia, llevar a cabo todos los procesos designados de forma legal, comunicando al inmediato superior cualquier tipo de situación que sea sospechosa o que ponga en peligro la información de la institución.
- Pro actividad, los responsables de las plataformas, equipos de conectividad e infraestructura de servidores tienen el deber de cumplir y apoyar todas las normas de seguridad dictadas en esta política.
- En caso de que los responsables de las plataformas, equipos de conectividad e infraestructura de servidores sospechen que ha ocurrido una eventualidad respecto a sus credenciales, deberá notificar urgentemente a la Director de TI.

C. POLÍTICA DE ADMINISTRACIÓN DE ACTIVOS DE TECNOLOGÍA DE INFORMACIÓN

1. Alcance.

Aplica a todos los usuarios que operan con activos de la Universidad Técnica de Cotopaxi, incluyendo trabajadores temporales y cualquier ente autorizado por la institución para hacer uso de estos.

2. Documentos de referencia.

N/A.

3. Descripción de la Política.

- La Dirección de Tecnologías de la Información debe tener la competencia de designar equipos informáticos a los usuarios previamente creados.
- La Dirección de Tecnologías de la Información llevará un registro del inventario de equipos informáticos.

- De igual manera llevará un registro de inventario para el control de software.
- 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 de todas las actividades que realizó.
- El personal encargado del mantenimiento detallará las características del equipo al cual realizará dicho mantenimiento.
- Los mantenimientos preventivos serán realizados una vez por semestre y serán programados en común acuerdo con el usuario y según políticas estipuladas en el documento de procedimientos de mantenimiento de equipos de cómputo.
- Los mantenimientos correctivos serán atendidos de acuerdo con políticas estipuladas en el Documento de Procedimientos de Mantenimiento de Equipos de Cómputo.
- La Dirección de TIC está autorizado para realizar revisiones periódicas de hardware, software y actualizaciones en los equipos institucionales y espera la colaboración de los usuarios cuando se requiera la realización de tales revisiones.
- El usuario es el único responsable de respaldar toda la información personal y laboral guardada en el equipo institucional. La Dirección de TIC, en su proceso de mantenimiento, sólo hará respaldo de documentos relacionados con su función. Los archivos personales de música, fotos y vídeo personales no serán respaldados.
- Se prohíbe a los usuarios destapar los equipos e intercambiar, remover sus partes o colocar accesorios dentro de Unidad Central de Procesamiento.

D. POLÍTICA DE RESGUARDO DE LA INFORMACIÓN

1. Alcance.

Aplica en toda la infraestructura del área de Tics de la Universidad Técnica de Cotopaxi.

2. Documentos de referencia.

N/A

3. Descripción de la Política.

Impedir a toda costa la pérdida o filtración de la información dentro de la institución en caso de que exista algún evento accidental o catastrófico con el fin de garantizar y certificar la integridad y disponibilidad de dicha información para de esta forma, asegurar que toda la información afectada se consiga recuperarse en ocasión de un fallo, se debe considerar los elementos siguientes:

- ✔ Delimitar el nivel preciso y necesario de la información de respaldo.
- ✔ Ejecutar copias de seguridad completas de la información y establecer los procesos de restauración.
- ✔ Analizar que los soportes 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 una carpeta estandarizada a nivel de todas las PC de la institución, con la denominación de UTC_DEPENDENCIA / AÑO / MES / TIPO_DOC / … Ejemplo: UTC_TIC / 2022 / 09 / OFICIOS_ENVIADOS / RECTORADO / …
- ✔ El usuario deberá almacenar sólo 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 vez que el personal de Tecnologías de la Información lo solicite.

Departamento de Tecnologías de la Información.

- ✔ Proporcionar un espacio en el cual permita almacenar todos los respaldos necesarios que se realizarán del Sistema Integrado de Gestión.
- ✔ Implementar un software específico y de fácil uso que contribuya en la generación de respaldos periódicos a realizar.
- ✔ Establecer los espacios de almacenamiento en las PC de cada dependencia conforme a la posición que desempeñe cada usuario creado para sus respaldos.
- ✔ Registrar de forma automática los respaldos del Sistema Integrado de Gestión para así llevar un control adecuado mediante una bitácora de respaldos.
- ✔ Suscitar un cronograma de respaldo de archivos de la información de acuerdo a cada área o departamento existente en la Institución.

Bases de datos.

- ✔ Realizar 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.

E. POLÍTICA DE SEGURIDAD A COMPONENTES INFORMÁTICOS

1. Alcance.

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

2. Documentos de referencia.

N/A

3. Descripción de la Política.

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

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

Protección de equipos.

Antivirus.

- Las computadoras y servidores (tanto físicos como virtuales) pertenecientes a la institución, contarán con un software antivirus, el mismo que será administrado únicamente por el Departamento de Tecnología de Información.
- El seguimiento y control de estos antivirus serán gestionados por la Dirección de Tecnologías de la Información por medio de bitácoras.
- 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 de Información.
- El equipo infectado será retirado para su revisión pertinente.
- El Departamento de Tecnologías de Información 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.

Acceso a servidores.

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

F. POLÍTICA DE USO ADECUADO DE INTERNET

1. 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.

2. Documentos de referencia.

Anexo-01F. Categorías de Filtrado Web.

3. Descripción de la Política.

La Universidad, consciente de la significativa importancia de internet como un instrumento para el cumplimiento de las labores diarias, facilitará y suministrará los recursos necesarios para asegurar su acceso a los usuarios que requieran para el desarrollo de sus actividades institucionales.

Departamento de Tecnologías de la Información.

- ✔ La utilización de Internet está abierta a todas las dependencias institucionales, campus y extensiones por medio de una red física o inalámbrica, dentro de las restricciones propias de las laborales autorizadas.
- ✔ 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 por la Dirección de TIC, al igual que la instalación de estos por cuestiones de seguridad de la información, muchos ataques son perpetrados por virus, gusanos, ransomware, entre otros que pueden estar solapados por detrás de una aplicación. Todo software que fuere descargado previa autorización, debe pasar un período de cuarentena establecido por la Dirección de TIC.
- ✔ Queda prohibido el uso de los recursos de Internet en cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular.
- ✔ Queda prohibido el uso de los recursos de Internet para el acceso a lugares obscenos, que distribuyan libremente material pornográfico, o bien, materiales ofensivos en perjuicio de terceros.
- ✔ Queda prohibido el uso de los recursos de Internet para la descarga de archivos potencialmente peligrosos y que puedan afectar el software de los equipos de la red de área local.
- ✔ 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 o que no sea de carácter educativo.
- ✔ Tiene determinantemente prohibido implementar, poner a prueba o cualquier acción para hospedar blogs, páginas web, aplicaciones web o de cualquier otro tipo en proveedores de hosting y dominios externos sin una previa autorización de la dirección de TIC, quien tomará atribución de exigir que cualquier servicio de esta índole quede registrada como subdominio del dominio principal utc.edu.ec para garantizar continuidad en la identidad digital y la seguridad de la información de la UTC en estos escenarios.

4. Registros.

N/A.

5. Anexo.

- **Anexo-01F.** Categorías de Filtrado Web.

Anexo-01F. Categorías de Filtrado Web:

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 6. 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.

G. POLÍTICA DE USO ADECUADO DE LABORATORIOS DE COMPUTACIÓN

1. 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.

2. Documentos de referencia.

- **RE-01G** Registro de docentes por uso de laboratorios.
- **RE-02G** Registro de estudiantes por uso de laboratorios.

3. Descripción de la Política.

La presente política 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 Facultades Académicas a las que correspondan.

Sobre la administración:

- Los técnicos de los laboratorios serán los encargados de administrar el control de dichos lugares.
- Para realizar la administración de los laboratorios, el encargado utilizará 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.
- El técnico de cada laboratorio poseerá las siguientes funciones:
  - Regular el acceso 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 funcionamiento 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.
- Garantizar el soporte técnico en todo momento.
- Velar por el estricto cumplimiento de las políticas planteadas en el presente plan.
- Velar porque en los laboratorios no exista consumo de alimentos, bebidas alcohólicas o de cualquier otro tipo que pueda afectar o dañar el funcionamiento y la imagen institucional.

Unidades Académicas:

- Todos los horarios académicos serán planeados con anticipación por todas las unidades académicas en coordinación con los técnicos 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.
- La Dirección de TIC realizará el préstamo a entidades externas que requieran los espacios de los laboratorios de cómputo, previa a una autorización realizada por el Rector, siempre y cuando no afecte el normal desenvolvimiento de las actividades académicas de cada facultad o área implicada.

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 Académico y de Investigación.
- 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, áreas administrativas, o cualquier otro personal con relación de dependencia con la UTC que se encuentre justificado el préstamo acorde al trabajo que se realizará, la justificación deberá ser por escrito emitido y autorizado por el jefe inmediato superior, 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, previamente dando a conocer a la Jefatura de Control de Bienes.

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.
- El alumno tendrá la obligación de realizar su registro de manera adecuada, utilizando los detalles de sus credenciales para solicitar el equipo de cómputo en el cual será designado para usar las aplicaciones necesarias con un tiempo máximo de 2 horas.
- 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.
- Todo usuario tiene terminantemente prohibido consumir alimentos o bebidas dentro del laboratorio.

. Registros.

Tabla 7. Documentos de referencia para uso adecuado de laboratorios de computación.

Código	Nombre	Actualización
RE-01G	Registro de docentes por uso de laboratorios	Cada vez que un docente solicite el uso de los laboratorios
RE-02G	Registro de estudiantes por uso de laboratorios	Cada vez que un docente solicite el uso de los laboratorios

. Anexos.

/A.

Tabla 8. Registro de docentes por uso de laboratorios.

Campus: Ubicación: Facultad:

Fecha	Responsable	Software utilizado	Ciclo	Carrera	Hora Uso		Número de Equipos	LAB. N°.	Observaciones	Firma
					Entrada	Salida				

Tabla 9. Registro de estudiantes por uso de laboratorios

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

UNIVERSIDAD TÉCNICA DE COTOPAXI

DIRECCIÓN DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

Elaborado por:

PhD. Gustavo Rodríguez Bárcenas:

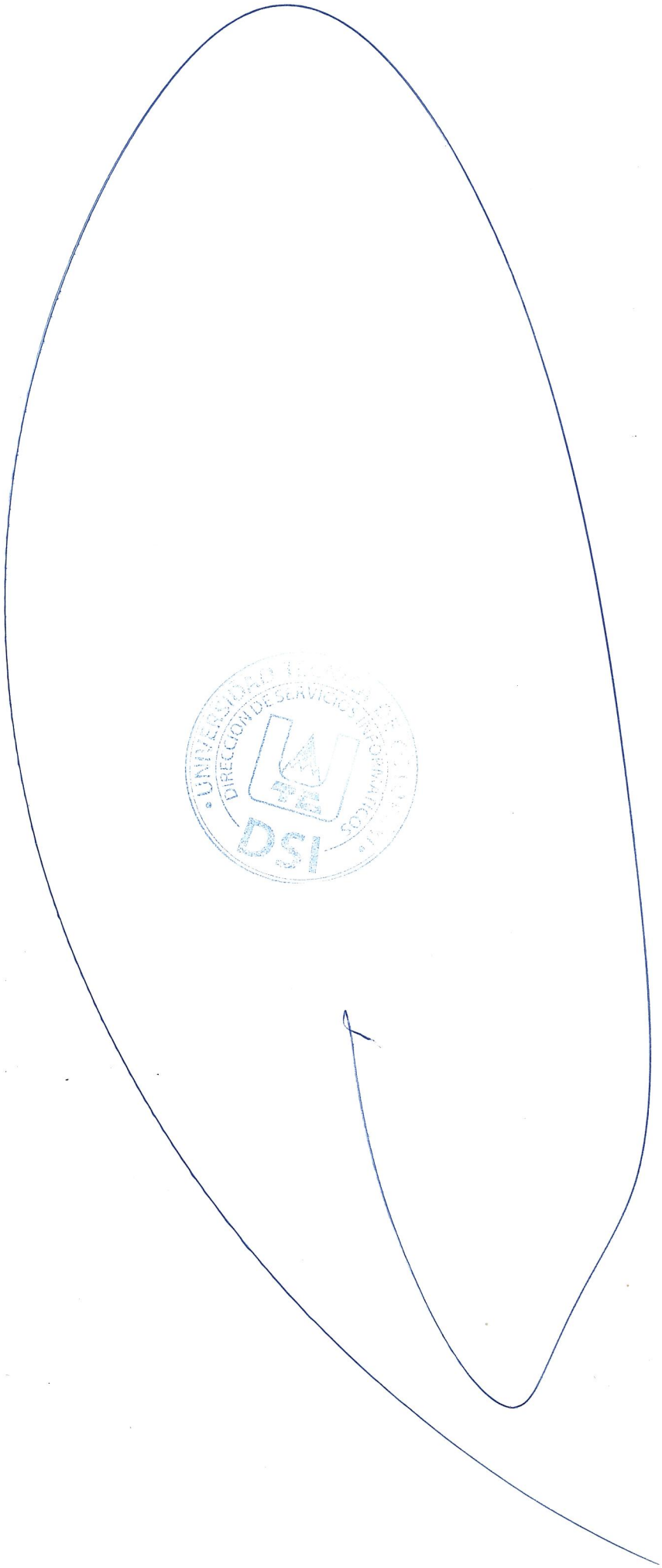
Director de Tecnologías de Información de la Universidad Técnica de Cotopaxi

Aprobado por: ING Hbastidas

Msc. Hernán Patricio Bastidas Pacheco:

Vicerrector Administrativo

UNIVERSIDAD TÉCNICA DE COTOPAXI
DIRECCIÓN DE SERVICIOS INFORMÁTICOS
DSI


DIRECCIÓN DE SERVICIOS INFORMÁTICOS
DSI