Portoviejo, 30 de noviembre de 2020 RHCU.UTM-No. 247-SO-07-2020
Of. No. 0499 HCU UTM

Doctora
María Hipatia Delgado Demera, PhD
Vicerrectora Académica de la Universidad
Ciudad

De mi consideración:

El H. Consejo Universitario en sesión ordinaria del jueves 26 de noviembre del presente año, consideró su Oficio No. UTM-VRAC-2020- 0824-OF del 24 de noviembre/2020, remitiendo para la correspondiente aprobación las Políticas de Tecnología de Información y Comunicación de la Universidad Técnica de Manabí 2020, una vez incluidos los cambios que han sido presentados.

Al respecto, este H. Órgano avocó conocimiento de esta comunicación y resolvió aprobar las Políticas de Tecnologías de Información y Comunicación de la Universidad Técnica de Manabí 2020, disponiendo se las remita a las diferentes unidades académicas y administrativas de la Universidad para la debida ejecución.

Particular que comunico para los fines pertinentes.

Atentamente,
PATRIA, TÉCNICA Y CULTURA

Firmado electrónicamente por:
VICENTE FELIX VELIZ
Rector-Presidente

Anexo Políticas Tecnologías
ABriones

POLÍTICAS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN
UNIVERSIDAD TÉCNICA DE MANABI
2020

1. INTRODUCCIÓN

El presente documento **Políticas de Tecnología de la Información y Comunicación,** representa una herramienta que servirá para garantizar el buen funcionamiento de los procesos de tecnología, optimizar los sistemas internos y garantizar la calidad en la prestación de servicios a la comunidad universitaria en particular.

Se define como Tecnologías de la Información y Comunicación (TIC) a las herramientas y métodos utilizados para recabar, retener, manipular o distribuir información, la cual por lo general se encuentra relacionada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones.

En los sistemas de información, la ética es una *conditio sine qua non* por tanto esperamos que este documento transparente y de idoneidad a los métodos y tecnologías que son utilizadas acceder, procesar y divulgar la información inherente a los diversos procesos administrativos, académicos, científicos y de extensión de la UTM. Cada acto que tenga que ver con las TIC y la información institucional tienen como responsables a la Dirección de Tecnología de la Información y Comunicación y a los usuarios de las mismas. Son estos últimos los que tendrán que responder por el buen o mal uso de las TIC ante las instancias correspondientes.

Para definir las Políticas de TIC, fue necesario asegurar una planeación estratégica tomando en cuenta las necesidades presentes y futuras de la institución, considerando como factor principal al talento humano con que cuenta esta IES. De esta manera se busca que sus funcionarios: servidores y trabajadores se identifiquen con las políticas establecidas, encausando sus esfuerzos en el fomento del trabajo en equipo, en la integración y en la coordinación de todas las áreas en una misma dirección.

Conscientes de que el uso de la tecnología está transformado a toda la humanidad, pretendemos encausar la administración de la tecnología de la información de nuestra institución, estableciendo políticas enfocadas a mejorar los procesos de la Universidad Técnica de Manabí, enmarcados en la normativa existente y las políticas institucionales.

El presente documento ha sido diseñado y validado de forma colaborativa mediante el consenso de los actores que conforman el ecosistema de TIC de la Dirección de Tecnología de la Información y Comunicación de la UTM.

2. NORMATIVA LEGAL

- Constitución de la República del Ecuador en sus artículos 16, inciso 2; artículo 347, inciso 8, y artículo 386.
- Ley Orgánica de la Contraloría General del Estado - ACUERDO 041-CG-2017: **EXPEDIR EL REGLAMENTO GENERAL PARA LA ADMINISTRACIÓN, UTILIZACIÓN, MANEJO Y CONTROL DE LOS BIENES E INVENTARIOS DEL SECTOR PÚBLICO - CAPÍTULO I - MANTENIMIENTO DE EQUIPOS INFORMÁTICOS**
- CGE - Normas de Control Interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos, 410 tecnologías de la información, desde su artículo 410-01 hasta 410-17.
- Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación,
- Apartado primero (del software de código cerrado y bases de datos) y segundo (de las tecnologías libres y formatos abiertos), Registro Oficial Nro. 899.

3 POLÍTICAS INFORMÁTICAS

3.1 GENERALIDADES

Art. 1.- Finalidad. - El objetivo de las Políticas de Tecnología de la Información y Comunicación es proteger la información de la institución y procurar el aprovechamiento de la tecnología en un entorno seguro, lo que contribuirá de manera eficiente al trabajo y continuidad de las operaciones de las Unidades Académicas y Administrativas del Universidad Técnica de Manabí

También se dejan establecidas las políticas de TIC que regirán el uso y mantenimiento de la plataforma tecnológica de la institución, con el propósito de asegurar su operatividad, de manera que los responsables de estas tecnologías aseguren el cumplimiento de esta normativa, con miras al desarrollo de un trabajo óptimo y de calidad.

Art 2. Alcance. - Las Políticas de Tecnología de la Información y Comunicación serán aplicadas de manera obligatoria por las y los funcionarios, servidores y trabajadores de las Unidades Académicas (AC) y Administrativas (AD) de la Universidad Técnica de Manabí (UTM).

Art. 3. Recursos tecnológicos. - Las Políticas de Tecnología de la Información y Comunicación regularán y estandarizarán el uso de los recursos informáticos que la Universidad Técnica de Manabí pone a disposición de los funcionarios, servidores y trabajadores para desarrollar sus actividades y cumplir con la misión de la Universidad Técnica de Manabí.

Art. 4.- Autorización y difusión. - Las Políticas de Tecnología de la Información y Comunicación de la Universidad Técnica de Manabí serán aprobadas por la máxima autoridad o su delegado.

Art. 5.- Glosario de Términos. - Se definen los siguientes términos:

- Administrador funcional del aplicativo: Persona quien tendrá la responsabilidad de generar los requerimientos funcionales y su aprobación respectiva.
- DGGA: Dirección General de Gestión Administrativa
- DTIC: Dirección de Tecnología de Información y Comunicación.
- DTIC: Dirección de Tecnologías Informáticas Comunicacionales
- Dueño de la información: Es la persona que crea un activo de información y por ende tiene la facultad de definir su clasificación y los derechos de acceso que tienen los demás usuarios.
- Ecosistema de TIC: Conjunto de actores especializados en el tratamiento de los sistemas de información.
- EP: Empresa Pública
- Hardware: conjunto de componentes que integran la parte material de una computadora, impresora o equipo de comunicación.
- In house: Desarrollo de software con personal propio de la Entidad.
- Internet: Red informática de comunicación internacional que permite el intercambio de todo tipo de información entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas International Network (red internacional).
- LONSCP: Ley Orgánica Nacional del Sistema de Compras Públicas.
- Normativa: Conjunto de normas aplicables a una determinada materia o actividad.
- Password: Traducido del inglés representa a la Clave de acceso o ingreso.
- POA: Plan Operativo Anual
- Recuperación: Es la tarea que se lleva a cabo cuando es necesario volver al estado de la aplicación al momento del último respaldo, a partir de los datos de la última copia de seguridad realizada.
- Respaldo: Es la obtención de una copia de los datos en otro medio magnético, de tal modo que a partir de dicha copia es posible restaurar el sistema o la información.
- Seguridad lógica: Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

- Software libre: Es el software que permite a los usuarios la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software.
- Software: Es un término genérico que designa al conjunto de programas de distinto tipo (sistema operativo y aplicaciones diversas) que hacen posible el funcionamiento y la operación del computador.
- Soporte 1er Nivel: Mantenimiento preventivo y/o correctivo de primera instancia.
- Técnico informático: Servidor que realiza actividades en equipos y/o sistemas informáticos.
- TIC: Tecnologías de Información y Comunicación.
- U. AC.- Unidad Académica o Facultad
- U. AC/AD. - Unidades Académicas y Administrativas
- U. AD.- Unidad Administrativa
- UTM: Universidad Técnica de Manabí.
- Virus: Es un programa informático que se ejecuta en el ordenador sin previo aviso y que puede corromper el resto de los programas, archivos de datos e incluso el mismo sistema operativo.

3.2 POLÍTICA PARA EL USO ADECUADO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Art. 6.- Generales. – En aras del uso adecuado de los recursos tecnológicos, los servidores y funcionarios de la institución tomarán en cuenta las siguientes disposiciones:

1) El personal de la DTIC, es el único autorizado para realizar las actividades de soporte técnico, mantenimiento y cambios de configuración en el equipo de cómputo (equipos, impresoras, escáneres, servidores y demás recursos tecnológicos) de propiedad de la UTM.

En el caso de actividades de mantenimiento efectuadas por terceros, éstas serán previamente aprobadas por la DTIC.

2) Los técnicos informáticos en las U. AC/AD deberán efectuar labores de soporte técnico enmarcados en los procedimientos y lineamientos de la DTIC.

3) La DTIC, debe mantener un inventario actualizado de los recursos informáticos de la UTM.

5) El acceso a los Data Center, cuartos de procesamiento y/o de telecomunicaciones de la UTM será restringido para todo el personal, salvo aquel personal debidamente autorizado asignado a la DTIC

6) La información de trabajo se almacenará en las máquinas asignadas, o en su defecto en las carpetas compartidas institucionales, bajo custodia de la DTIC

7) Las y los usuarios autorizados de los sistemas informáticos de la UTM, no harán uso indebido de la información institucional, datos en general y datos confidenciales.

8) Los sistemas internos, así como, las bases de datos bajo custodia de la DTIC estarán centralizadas en el Data Center Institucional, salvo en casos debidamente justificados y motivados y autorizados expresamente por la DTIC. De existir sistemas y bases de datos aisladas o no compatibles con la infraestructura tecnológica de la DTIC, las unidades a cargo de estos, deberán promover proyectos de integración y/o migración en coordinación con la DTIC, los cuales no pueden ser implementados hasta tener informe favorable de DTIC.

9) El acceso a las bases de datos de la UTM debe contar con la autorización de la Autoridad Nominadora.

10) La entrega de información a entidades externas gubernamentales o privadas, contará con la autorización de la Autoridad Nominadora.

11) Para el caso de conexiones inalámbricas de personas ajenas a la institución, por defecto se otorgará un acceso a la red pública de invitados. Si se requieren accesos puntales a la red privada o a una red específica, los accesos se otorgarán solamente a través de la red cableada, en conocimiento y disposición de la DTIC

12) Todos los computadores de las Unidades AC/AD, se sujetarán a la versión de software antivirus institucional que determine la DTIC; este software tendrá activada la protección en tiempo real al sistema operativo y mantendrá instalada la última definición de virus. La actualización de las definiciones de antivirus se realizará preferiblemente de manera automática, caso contrario de manera manual.

13) Los lugares de trabajo de los funcionarios de la UTM y del personal externo que preste servicios en la institución deben localizarse preferentemente en sitios que restrinjan el acceso de personas ajenas a esos procesos. De esta forma se protege tanto el equipamiento tecnológico como los documentos que pudiera utilizar el servidor.

14) Las estaciones de trabajo y equipos portátiles deben tener aplicado el estándar relativo a protector de pantalla, de forma que se active ante un tiempo sin uso.

15) El personal de la UTM deben aplicar la política de puesto de trabajo despejado y pantalla limpia.

16) El proceso de publicación de comunicaciones por medios electrónicos estará regulado por la DTIC y la Dirección de Comunicación.

Art. 7.- Hardware. - El hardware de propiedad de la UTM, así como el arrendado, se utilizará únicamente para actividades relacionadas con los objetivos y metas de la institución, para lo cual se observará lo siguiente:

1) Para el correcto funcionamiento del hardware se realizará el mantenimiento preventivo, de acuerdo al plan de mantenimiento preventivo anual de equipo de cómputo. Para Unidades AC/AD que cuenten con técnicos informáticos, estos deberán remitir su cronograma de mantenimientos a la DTIC a principios de cada año.

2) Cuando exista algún siniestro (robo, extravío, daño físico) que afecte de manera directa al hardware de las Unidades AC/AD, previa revisión de la DTIC en primera instancia, se notificará a la Dirección General Administrativa y Procuraduría General Institucional, según corresponda a los fines de ley consiguientes.

3) Solamente el personal de la DTIC, está facultado para abrir las carcasas de los computadores personales o de cualquier otro equipo de cómputo institucional que NO cuente con garantía técnica vigente.
Para los equipos cuya garantía técnica aún se encuentre vigente, esa acción lo efectuará únicamente el personal técnico calificado de la contratista, previa coordinación con el funcionario administrador del contrato designado por la UTM.

Para los equipos de cómputo en esquema de arrendamiento, la empresa arrendadora es la única autorizada para abrir las carcasas de dichos equipos o en su caso consentirá la apertura de ellos, previa coordinación con el funcionario administrador del contrato designado por la UTM.

Art. 8.- Data Center. - En los Data Centers de la UTM se alojarán los servidores y equipos de comunicación necesarios para la operación de las actividades informáticas de la institución; en general se observará lo siguiente:

1) Para todas las Unidades AC/AD, el Data Center Institucional será la primera opción para instalar infraestructura de servidores y aplicaciones informáticas, previo a un informe de técnico justificado y motivado por la unidad solicitante y autorizado por la DTIC. En los casos en los cuales no exista compatibilidad o capacidad a nivel de tecnología, la DTIC emitirá a la unidad solicitante un informe técnico con las alternativas.

2) No se permitirá la construcción de Data Centers adicionales, posterior a la fecha de publicación de la Política de Tecnología de la Información y Comunicación, salvo en casos debidamente justificados y motivados por las unidades solicitantes y autorizadas expresamente por DTIC.

3) El acceso físico a cualquier Data Center en general será restringido, y sólo será autorizado a los técnicos de la DTIC.

4) El acceso lógico a los equipos ubicados en el Data Center institucional, ya sea usando la consola de administración local o una consola de administración remota es restringido. Solo se permitirá ingresar al personal autorizado por la DTIC, El intento de conexión por alguna persona no autorizada a cualquier consola de administración sin la debida autorización se considera una violación a las políticas de seguridad.

Art. 9.- Propiedad de la Información. - Las y los usuarios de cualquier equipo de cómputo de la UTM deben estar informados y conocer que los datos que ellos crean y manipulan en los sistemas, aplicaciones y cualquier medio de procesamiento electrónico durante el desarrollo normal de sus actividades laborales, son de propiedad y responsabilidad de la UTM, para lo cual se respetará lo siguiente:

1) Los derechos patrimoniales de un programa de computación, hojas de cálculo de Word, macros, etc., y su documentación, creados por uno o varios empleados en el ejercicio de sus actividades laborales pertenecen a la UTM.

2) Los respaldos que contengan información de la UTM, que fueron realizados o solicitados por el usuario de equipo de cómputo, se tendrán exclusivamente bajo resguardo; no se permitirá su distribución o publicación a terceros sin la debida autorización de la DTIC.

3) Al finalizar su relación laboral con la institución, los respaldos de información del equipo de cómputo a cargo del usuario deberán ser entregados a su jefe inmediato superior, previo a la respectiva acta entrega recepción.

Art.10.- Usos inadecuados. - Las siguientes actividades están prohibidas:

1) Violar los derechos de cualquier persona o institución en relación con los derechos de autor, patentes o cualquier otra forma de propiedad intelectual.

2) Difundir información identificada como confidencial a través de medios que involucren el uso de la Tecnología de Información.

3) Introducir software malicioso en la red o en los servidores (virus, gusanos, troyanos, ráfagas de correo electrónico, etc.).

4) Utilizar la infraestructura de la UTM para conseguir o transmitir material con ánimo de lucro.

5) Utilizar el sistema de comunicaciones de la UTM con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.

6) Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios de la UTM

7) Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.

8) Monitorear puertos o realizar análisis de tráfico de la red con el propósito de evaluar vulnerabilidades de seguridad. El personal de la DTIC responsable de la Seguridad Informática puede realizar estas actividades siempre y cuando cuente con la aprobación del Jefe de la Unidad AC/AD.

9) Burlar mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.

10) Interferir o negar el servicio a usuarios autorizados con el propósito de afectar la prestación o, deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (internet, intranet).
11) Usar comando o programas de envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (intranet, internet)

12) Queda estrictamente prohibido compartir un repositorio de información sin restricciones de usuario. La DTIC puede cambiar permisos de recursos compartidos por los usuarios si detecta que éstos no cumplen con las mejores prácticas de gestión de la información y las tecnologías.

3.3 POLITICA DE GESTION DE PROYECTOS TECNOLÓGICOS

Art. 11.- Generales. - Para la gestión de proyectos tecnológicos será la DTIC quien defina los mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conforman la institución, para lo cual se observarán las siguientes condiciones previas a la ejecución de un proyecto.

1.-) La propuesta de proyecto contendrá la descripción de la naturaleza, objetivos y alcance, su relación con otros proyectos institucionales, niveles de compromiso, participación y aceptación de los usuarios interesados, así como los cronogramas de actividades para cada uno de los participantes en el proyecto.

2.-) La formulación considerará el Costo Total de Propiedad, que incluya los costos de adquisiciones así como los de operación.

3.-) En el caso de proyectos interdisciplinarios, se establecerá un responsable del proyecto y un responsable funcional.

4) La gestión de proyectos se realizará enmarcada en las mejores prácticas (control por fases, documentación y control de riesgos) y los procedimientos y formatos establecidos por la DTIC.

3.4 POLITICA DE LA CALIDAD DE LOS DATOS E INFORMACIÓN

Art. 12.- Definición. - La calidad se la define como el conjunto de propiedades o características de un producto o servicio que le confieren aptitud para satisfacer unas necesidades expresas o implícitas. Por otro lado, la veracidad de la información se refiere a que la información ingresada por el usuario funcional del sistema o dueño de la información sea correcta.

Art. 13.- La calidad de los datos e información. - La calidad de los datos y de la información que almacena la UTM en el Data Center de la DTIC, estará determinada tanto por la calidad y veracidad de la información ingresada, así como, por la calidad de la información almacenada en las bases de datos y la calidad de la presentación de los datos.

Art. 14.- Integridad de los datos e información. - La DTIC velará para que las bases de datos e información almacenada en el Data Center, no sufra descomposición por efectos de virus, malwares u otros factores que afecten su integridad, veracidad y disponibilidad. Entre las acciones previstas mantendrá respaldos de la información y datos para recuperarlos en caso de daños físicos o incidencia de otros factores.

Art. 15.- Exclusiones de responsabilidad. - La DTIC excluye dentro de su responsabilidad, la calidad y veracidad de la información ingresada en la base de datos y/o de la información almacenada en aplicativos. Datos erróneos, desactualizados, equivocados, e incompletos son responsabilidad de los usuarios.

El usuario acepta que la DTIC no será responsable por la calidad veracidad de la información cargada dentro de bases de datos o aplicativos. El usuario será el responsable de comprobar que en las bases de datos la información almacenada sea correcta, confiable y exacta.

3.5 POLÍTICA DE CONTRASEÑAS

Art. 16.- Generales. - El acceso a los aplicativos informáticos solo será ejecutado por personal autorizado; además, equipos, sistemas y datos, utilizarán mecanismos de contraseñas para controlar el acceso. Tales mecanismos se aplicarán al inicio de sesión en la computadora, ingreso a la red institucional, uso de sistemas internos y externos, correo electrónico, entre otros.

Art. 17.- Administración. - se acatará lo siguiente:

1) Todos los usuarios internos de la UTM requieren de un nombre de usuario y una contraseña para utilizar el equipo de cómputo que tiene asignado y servicios de red como correo electrónico, impresión, archivos compartidos, intranet, internet, etc.
2) Todas las contraseñas son personales e intransferibles. Se prohíbe a los usuarios dar a conocer a terceras personas su contraseña. Quien así lo hiciere debe considerar que sigue siendo el único responsable de las actividades que se realicen con su identificación de usuario y contraseña.
3) Todas las contraseñas del sistema (cuenta de administrador, cuentas de aplicaciones, etc.) se cambiarán con una periodicidad de al menos una vez en el año.
4) Todas las contraseñas del usuario (cuentas de usuario, cuentas de servicio web, etc.) se cambiarán al menos una vez en el año.
5) En caso de que el usuario sospeche que su contraseña ha sido comprometida deberá cambiarla o solicitar al responsable informático el cambio respectivo.
6) En caso de olvido o bloqueo de su contraseña, el usuario debe coordinar el restablecimiento de la misma con el responsable informático de la DTIC.
7) Las contraseñas de los usuarios deben cumplir con ciertos requerimientos de seguridad los cuales definirá la DTIC con el objeto de evitar que los usuarios elijan contraseñas débiles.
8) Las contraseñas para acceso al correo electrónico será la misma de usuario de la máquina y será modificada por el usuario la primera vez que acceda a su cuenta.
9) Las contraseñas de los sistemas internos contarán con contraseñas independientes de la utilizada para iniciar sesión en la red institucional. El responsable de la administración funcional, autorizará la creación de usuarios y contraseñas de los sistemas internos, mismos que serán creados y entregados por parte de la DTIC.
10) Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación del negocio, operación de sistema, desarrollo y mantenimiento) debe ser identificable de manera única.
11) Cuando un usuario se desvincule de la Institución o se le asigne un rol diferente para el que tiene permisos de acceso, la Dirección de Administración de Talento Humano o en su defecto su jefe inmediato, deberá notificar a la DTIC para suspender o modificar los permisos de red a los sistemas institucionales, etc.
12) Las y los funcionarios, servidores y trabajadores, deberán suscribir un compromiso de responsabilidad de seguridad y uso de usuario y claves de acceso a la información de recursos tecnológicos de la DTIC.
Art. 18.- Prohibiciones. - Las actividades que se detallan a continuación están prohibidas:
1) Revelar o compartir su contraseña de cualquier forma.
2) Escribir la contraseña o almacenarla en archivos sin que sean encriptados, comunicarla en el texto de mensajes, o cualquier otro medio.
3) Comunicar las contraseñas en conversaciones electrónicas.

3.6 POLITICA DE USO DE CORREO ELECTRONICO

Art. 19.- Generales. - El correo electrónico institucional es un recurso que la UTM pone a disposición de las y los funcionarios, servidores y trabajadores, como una herramienta de comunicación, colaboración e intercambio de información oficial. El acceso ay uso de este recurso está condicionado a la presente política de uso.
1) El acceso a este servicio, se lo realiza por medio del cliente de correo electrónico, intranet o de la página web institucional https://mail.utm.edu.ec/ . Las comunicaciones institucionales efectuadas por correo electrónico, solo se realizarán mediante las cuentas institucionales.
2) Las cuentas de correo asignado a los funcionarios, servidores y trabajadores de cada área, serán utilizadas solo para actividades laborales, relacionadas con los propósitos y funciones institucionales.

3) Los buzones de correo electrónico, creados para las y los funcionarios, servidores y trabajadores de la UTM, y toda la información contenida en los mismos, son de propiedad exclusiva de la institución.
4) La DTIC se reserva el derecho para modificar las condiciones de uso establecidas cuando lo considere necesario. También podrá modificar o bloquear servicios relacionados al servicio de correo electrónico cuando sea necesario, por razones administrativas, de mantenimiento, por causas de fuerza mayor o por necesidad institucional.
5) La DTIC puede, en cualquier momento, cancelar o inhabilitar la cuenta de cualquier usuario sin previo aviso e incluso eliminar ésta por falta de uso, o bien si considera que el usuario ha contravenido las reglas aquí mencionadas. En tales casos la DTIC no se hace responsable de la información ni de eventuales repercusiones por dicha cancelación o inhabilitación.

Art. 20.- Tipos de Cuentas. - Se definen los siguientes tipos:

1) **Cuentas personales**: El personal de la UTM contará con una cuenta de correo en el servidor de la Institución con capacidad de bandeja asignada, cuya dirección electrónica estará formada por la primera letra del nombre o nombre completo, apellido según el siguiente formato: (letra del nombre.apellido@utm.edu.ec).
2) **Cuentas temporales**: Estas cuentas se crearán bajo propósitos específicos, que serán detallados en el campo de texto "notas) al momento de crearlas. Además, se especificará el tiempo de validez, para que sea borrada una vez que ya no se la necesite. El formato de este tipo de cuenta será: propósito@utm.edu.ec
3) **Cuentas departamentales**: Estas cuentas serán creadas, con el objetivo de comunicar a todos los miembros de una determinada dirección o lista de usuarios específicos, el formato de este tipo de cuenta será: nombredelarea@utm.edu.ec

4) **Cuentas de servicios.** - Estas cuentas están asociadas a los servicios que tiene implementada la UTM, para que se envíen comunicados hacia los usuarios de los mismos. El formato de este tipo de cuenta es notificaciones.nombredelservicio@utm.edu.ec

Art. 21.- Responsabilidades. – Las responsabilidades para el uso de correos electrónicos serán:

1) Los servicios de correo electrónico serán administrados por la DTIC y será la responsable de velar por el correcto funcionamiento y operación del servicio.
2) La Dirección de Talento Humano y/o coordinadores departamentales de las facultades deberá comunicar a la DTIC, sobre las entradas, movimientos y salidas de personal en la institución, para la activación, modificación o desactivación respectiva.
3) Los usuarios son los únicos responsables de todas las actividades realizadas desde su cuenta de correo.
4) La Información transmitida mediante el servicio de correo electrónico es responsabilidad única y exclusiva de cada usuario. La Universidad Técnica de Manabí no garantiza la veracidad, integridad o calidad de los contenidos de los mensajes enviados mediante este servicio.
5) La cuenta de correo es intransferible por lo que la información será responsabilidad exclusiva de cada usuario.
6) La información que se recibe de manera personal y confidencial por correo electrónico, no se puede reenviar a otra persona sin la autorización del remitente.

Art. 22.- Gestión del buzón de correo. - Se define lo siguiente:

1) Los usuarios son responsables de mover recurrentemente los correos electrónicos del buzón al archivo de almacenamiento local, en el caso de estar disponible. Esta acción debe tomarse recurrentemente con el objetivo de evitar que se llene el buzón de correo institucional.
2) La gestión de la información contenida en su cuenta de correo electrónico debe ser adecuada, por lo que periódicamente debe revisar su bandeja de entrada y su capacidad disponible, etc. Se recomienda eliminar los mensajes que no deban conservarse y archivar el resto en la carpeta o subcarpeta apropiada de su archivo de almacenamiento local.
3) Resguardar la seguridad del buzón del correo, por lo cual deberán evitar la recepción de correo cuando se desconozca al remitente ya que en ocasiones este puede ser un mensaje con contenido potencialmente peligroso (virus, malware, etc.)

4) La DTIC definirá el espacio del buzón de correo electrónico, según las necesidades laborales e institucionales.

Art. 23.- Uso inaceptable. - Se considera como mal uso o de uso inaceptable del correo electrónico las siguientes actividades:

1) Utilizar el correo electrónico para actividades ajenas a la institución.
2) Participar en la propagación de cadenas, esquemas piramidales y otros similares de envío con el correo institucional.
3) Enviar o reenviar mensajes con contenido difamatorio, ofensivo, racista, discriminatorio u obsceno.
4) Enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.
5) Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor del correo electrónico.
6) Distribuir mensajes con contenidos definidos como inapropiados y/o lesivos que atenten contra la moral o las buenas costumbres. Son considerados contenidos inadecuados todos aquellos que constituyan complicidad con hechos delictivos, por ejemplo: apología al terrorismo, uso y/o distribución de programas piratas, todo tipo de pornografía, amenazas, estafas, esquemas de enriquecimiento ilícito, lenguaje obsceno, virus o código hostil, etc.
7) Apropiarse de alguna(s) cuenta(s) de correo electrónico diferente a la asignada.
8) Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado “spam”.
9) Dirigir a un usuario o al propio sistema de correo electrónico, mensajes que tengan el objetivo de paralizar el servicio por saturación de la capacidad del servidor de correo o del espacio en disco de usuario.

3.7 POLITICA DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN

Las Unidades AC/AD de la Universidad Técnica de Manabí que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, sensible y confidencial, deberán aplicar la Política de Tecnología de Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera.

Art. 24.- Generales. - Las y los usuarios internos cumplirán las siguientes recomendaciones:

1) Si no va estar en su puesto de trabajo por algún motivo, el equipo deberá ser bloqueado.
2) No modificar las configuraciones de dirección IP, DNS, hora, nombre de equipos y demás. En el caso de requerir algún cambio deberá ser solicitado a la DTIC.
3) No modificar configuraciones del equipo como fondo de pantalla y protector de pantalla, así como la configuración de software y hardware establecidos por la DTIC. Si en su equipo se han realizado modificaciones, deben notificar a la DTIC, para que se realice la reconfiguración del mismo.
4) En caso de funcionarios y/o servidores que tengan a su cargo computadores portátiles, estos deberán permanecer con el candado de seguridad durante todo el tiempo que el computador esté sin supervisión. En caso de no disponer de candado, se deberá gestionar la adquisición del mismo a través de la jefatura en la que labora el funcionario, servidor o trabajador.
5) Para evitar pérdida de información, el usuario es responsable de respaldar su información periódicamente en medios magnéticos externos y verificar que los respaldos generados se encuentren íntegros y disponibles en el caso de ser requeridos.
6) No pueden moverse los equipos o reubicarlos sin permiso. En caso de necesitar moverlos fuera de la institución se requiere autorización de la DGGA, a solicitarse en los formularios previstos en página web UTM
7) Está prohibido poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios y/o dañar o alterar la información de la institución.
8) Todo el personal que acceda a los sistemas de información de la UTM debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de uso.
9) Queda estrictamente prohibido la explotación de vulnerabilidades de cualquier tipo a los recursos de la UTM, en caso que un funcionario, servidor o trabajador detecte alguna vulnerabilidad deberá reportarla a las autoridades pertinentes de la Seguridad Informática de la DTIC,

Art. 25.- Responsables de la seguridad. - La DTIC estará a cargo de la seguridad informática, mientras que las Unidades AC/AD serán las responsables de la seguridad de la información. En el cumplimiento de sus funciones en los aspectos relacionados a la seguridad, estas Unidades deben observar lo siguiente:
1) Controlar la existencia de documentación física o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas.
2) Evaluar el posible impacto operativo a nivel de seguridad de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.
3) Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
4) Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad para soportar potenciales amenazas a la seguridad de la información que procesan.
5) Controlar la obtención de copias de resguardo de información de sistemas tecnológicos, así como, la prueba periódica de su restauración.
6) Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, con el propósito de tomar medidas correctivas.
7) Implementar los controles de seguridad informática definidos en base al análisis de riesgos (ej., evitar software malicioso, accesos no autorizados, etc.).
8) Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento (ej., cintas, discos, etc.), y la eliminación o destrucción segura de los mismos, cuando proceda.
9) Gestionar los incidentes de seguridad de la información de acuerdo a los procedimientos establecidos.

Art. 26.- Excepciones de seguridad. - Para propósitos de mantenimiento y pruebas de seguridad de la red de la UTM, el personal debidamente autorizado, estará exento de seguir algunas de las restricciones anteriores. Estos privilegios de acceso deberán ser solicitados a la DTIC, anexando la justificación respectiva de forma escrita. Solo se procederá si ha sido debidamente autorizado.

Art. 27.- Responsables de la Información. - Los responsables de la información se definen para asegurar adecuadamente la pertenencia, custodia y salvaguarda de los recursos, teniendo en cuenta una correcta distribución de funciones, para lo cual hemos hecho una diferenciación entre los Responsables Directos y los Responsables Secundarios y Custodios.

Responsables directos: Son aquellos que por la naturaleza de su posición en la institución conocen el tipo de información que se genera, comunica o ingrese en los diferentes sistemas o aplicativos. Son responsables de:

- La clasificación directa de la información, de la organización y autorización del acceso a la información.
- Manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso.
- Monitoreo del uso de la información por parte del personal a su cargo.
- Asignar a los responsables del uso y manejo de la información.

Responsable secundarios: Son aquellos que por la naturaleza de su cargo en la institución deben acceder, modificar o almacenar información. Son responsables de:

- Manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso.

Custodios: los custodios de la información son aquellos que por la naturaleza de su cargo en la Universidad Técnica de Manabí deben custodiar, respaldar o almacenar la información. Se convierten en custodios el personal que tenga acceso a bases de información. Entre sus responsabilidades están:

- El manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso.
- Mantener la disponibilidad e integridad de la información custodiada.
- Mantener el acceso y permisos de acceso a la información custodiada.
- Brindar soporte para evaluar e identificar la información para su clasificación.

Monitorear el uso de la información por parte de los responsables directos: los responsables directos de la información por tener una relación directa en el manejo de la información serán responsables de monitorear el uso que le dé el personal a su cargo.

Responsabilidades:

- Definir procedimientos para el control de cambios a los procesos operativos y verificar su cumplimiento, de manera que no afecte la seguridad de la información.
- Controlar los mecanismos de distribución y difusión de información dentro y fuera de la institución.
- Desarrollar procedimientos adecuados de concienciación de usuarios en materia de seguridad de la información.
- Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.
- Coordinar la gestión de eventos de seguridad con la DTIC.

Art. 28.- Acuerdo de Confidencialidad. - Las y los servidores de la institución deben firmar acuerdos de confidencialidad y de no-divulgación de información de conformidad con lo dispuesto en la Constitución, las leyes y las necesidades de protección de información de la institución.

La DTIC será la encargada de controlar que los acuerdos de confidencialidad de la información, documento físico o electrónico, sea firmado por el personal de la institución, sin excepción; gestionar la custodia de los compromisos firmados en los expedientes físico o electrónicos, de cada funcionario y/o servidor, y controlar que la firma de los compromisos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios y/o servidores a la institución, sin excepción.
El personal de otras entidades públicas o privadas que requiera ingresar a los equipos y/o los sistemas de la UTM, deberá, de igual manera, suscribir un acuerdo de confidencialidad previo a acceder a la información. Esta acción será gestionada por la DTIC.

Art. 29.- Clasificación de la Información. - Los Responsables de la información clasificarán adecuadamente la información bajo su responsabilidad y se asegurarán de que se respete el acceso a la misma por parte del personal a su cargo.

Los activos de información de la organización deben ser clasificados en una de las categorías definidas en el punto *Niveles de clasificación de Información* de la Política de Seguridad de la Información.

Para clasificar la información dentro de uno de los niveles determinados o cambiar su categoría, se deben utilizar criterios de clasificación de información la Política de Seguridad de la Información.

La información será rotulada claramente con la clasificación que sea otorgada. Esta rotulación debe ser clara y visible.

Toda la información generada en la organización y que no se le dé una clasificación específica, mantendrá carácter de PRIVADA y deberá ser tratada como tal.

1) Los criterios de clasificación. - Son:

Valor: Es el principal criterio de clasificación. Está basada en el valor del activo desde el punto de vista del negocio (valor propio del activo o producto del mismo).
Tiempo: En virtud de su antigüedad puede cambiar si el valor de la información se reduce.
Vida útil: Cuando la información se vuelve obsoleta en base a nueva información generada, cambios organizacionales u otros motivos.

2) Los niveles de clasificación de la información.

Pública. - Es la información que, por su naturaleza, puede ser visible o divulgada por el personal general de la organización, usuarios o el público en general, sin riesgo de que su contenido pueda afectar en ningún sentido la integridad o economía de la institución. Esta información puede ser, entre otras, publicaciones, anuncios de prensa o medios de comunicación, página web institucional, etc.

Sensible: Solo para uso interno, destinada al uso exclusivo por parte de los funcionarios, servidores y trabajadores de la Institución en el desarrollo rutinario de los procesos. Esta información puede ser, entre otras: memorandos, avisos, comunicaciones, informativos, etc.
Confidencial: Es la información considerada como sensible y está destinada a uso interno y por parte del personal específico que debe tener permisos y autorización para su visualización y/o manejo. La divulgación o visualización no autorizada causaría violación de la privacidad de las personas o produciría un daño grave o irreparable a la imagen de la institución.

3) Acceso a recursos y privilegios. - Los usuarios deberán tener sólo los privilegios que son esenciales para acceder a las aplicaciones y realizar las actividades diarias a su cargo; por defecto se cumplirá el principio de privilegio mínimo al configurar los perfiles de acceso a recursos y sistemas institucionales.

4) Gestión de Incidentes de seguridad. - La gestión de incidentes de seguridad debe realizarse considerando los siguientes tres objetivos básicos:

- Responder rápida y efectivamente,
- Contener y reparar el daño causado por los incidentes,
- Prevenir daños futuros.

5) **Segregación funcional**. - Ningún proceso crítico debe ser conocido y ejecutado por una sola persona o que una misma persona tenga privilegios o accesos en diferentes fases de un proceso. Los distintos procesos deben ser claramente descritos

Art. 30.- Conducta del Usuario Interno. - El usuario interno deberá acogerse a lo dispuesto en estas políticas de uso de TIC, de la información y del conocimiento:

1) El usuario es el único responsable del contenido de transmisiones a través de cualquier servicio
2) El usuario debe cumplir con las leyes de transmisión de datos técnicos desde los cuales y hacia donde se envían los mensajes de correo electrónico.
3) El usuario no debe usar el servicio para propósitos ilegales.
4) El usuario debe cumplir con todas las regulaciones, políticas y procedimientos de uso de internet de la institución.
5) La comunicación de los usuarios se debe conducir con respeto y consideración, evitando los abusos y el uso del lenguaje inapropiado.
6) Se prohíbe el acceso a cualquier fuente de información cuyo contenido no se encuentre relacionado con las actividades laborales dentro de los ámbitos de competencia de la UTM.

Art. 31.- Respaldo de la Información tecnológica. - La DTIC, así como las Unidades AC/AD responsables de la información, según correspondan, determinarán el procedimiento de resguardo y contención de la información obtenida de los sistemas y/o aplicativos informáticos, considerando al menos los siguientes puntos:

1) Etiquetado de las copias de respaldo, contenido, periodicidad y retención
2) Extensión (completo/diferencial) y frecuencia de respaldos, de acuerdo a los requisitos institucionales.
3) Vida útil recomendada por el proveedor y la destrucción de estos medios magnéticos
4) Resguardo de los respaldos en un sitio lejano, a una distancia suficiente para evitar cualquier daño debido a desastres.
5) Grado apropiado de protección física y ambiental.
6) Eventos regulares de verificación y restauración de los medios de respaldo para garantizar sean confiables para uso de emergencia
7) Protección de la información confidencial por medio de encriptación
8) Generación de respaldos a discos duros y en el mismo sitio si se tiene suficientes recursos, ya que, en caso de mantenimientos de los sistemas de información, es más rápida su recuperación.

Art. 32.- Retiro de privilegios. - La DTIC retirará los privilegios de acceso a los activos de información y a los servicios de procesamiento de información (ej., sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, etc.,) inmediatamente luego de que se comunique formalmente a la DTIC

la terminación de la relación laboral del funcionario, servidor o trabajador municipal por parte de la Dirección de Recursos Humanos del UTM.

3.8 POLÍTICA DE CONTINUIDAD DE LOS SERVICIOS INFORMÁTICOS

La DTIC establecerá, documentará y socializará el Plan de Continuidad de los Servicios Informáticos, a fin de minimizar el riesgo de ocurrencia de la pérdida de la disponibilidad de los servicios críticos.
Este plan de continuidad será mantenido y revisado por la unidad pertinente dentro de la DTIC.

3.9 POLÍTICA DE USO DE SOFTWARE

Art. 33.- Administración. - La DTIC, es la entidad responsable de la administración, instalación, soporte y funcionamiento del software instalado en las Unidades AC/AD. Adicionalmente, según corresponda, tendrán la responsabilidad de:
1) Mantener un consolidado de licencias de uso de software.
2) Mantener actualizado el catálogo de software de la unidad.
3) Generar los estándares de software institucional.
4) Establecer los procedimientos para el uso de software.
5) Realizar el análisis de necesidades y requerimientos con la finalidad de planificar la adquisición o desarrollo de una solución de software.

Art. 34.- Uso/instalación de Software. - Para el uso e instalación del software se observará lo siguiente:

1) La DTIC es la única entidad autorizada para realizar la instalación de software y proporcionar soporte técnico del mismo en las computadoras de la institución.
2) El software utilizado por las unidades, deberá ajustarse a los estándares y especificaciones técnicas definidos por la DTIC. Se exceptuarán los casos debidamente justificados mediante informe técnico del requirente y autorizado expresamente por la DTIC.
3) Para el uso/instalación de software se debe tener licencia de uso o en su defecto los derechos de autor a nombre del UTM.

Art. 35.- Restricciones. - Se prohíbe la instalación y/o uso de software que no se haya identificado como institucional, y software adquirido para uso personal del usuario (sin fines institucionales).

Art. 36.- Requerimientos de Software. - Todo usuario interno que requiere la instalación de un determinado software para sus actividades diarias, deberá solicitarlo a la DTIC, de acuerdo a los procedimientos y formatos que para el efecto se establezcan.

De acuerdo a las características del software, si existe posibilidad de atender el requerimiento con el software existente, o en su caso, si se cuenta con el software alterno para atender las necesidades del usuario, este será instalado. En el caso de que no se pueda atender el requerimiento, por no contar con el software necesario, los técnicos informáticos remitirán a la DTIC un informe de necesidad.

La DTIC será la encargada de remitir las especificaciones técnicas generales y específicas del software requerido, así como un presupuesto aproximado para la compra por parte del requirente. En el caso de conseguir los fondos necesarios para la continuación del trámite respectivo, el requirente procederá con el procedimiento de contratación de conformidad con la Ley Orgánica del Sistema Nacional de Contratación Pública, su Reglamento General y resoluciones del Servicio Nacional de Contratación Pública.

Art. 37.- Registro de derechos de autor. - Para software, aplicaciones o sistemas desarrollados directamente o a través de terceros (contratados) dentro de la institución, la DTIC, o en su defecto, los técnicos de departamentos informáticos, serán los responsables de gestionar el registro de derechos de autor a nombre de la UTM, en cumplimiento de las disposiciones, leyes y normas vigentes sobre Propiedad Intelectual.

3.10 POLITICA DE DESARROLLO DE APLICACIONES

Art. 38.- Generales. - Para el desarrollo de software se establece que:

1) Todo proyecto tecnológico que esté orientado al desarrollo deberá seguir el procedimiento establecido en la Metodología de la DTIC, mediante la cual la unidad requirente solicitará un informe de factibilidad del proyecto.
2) Todos los sistemas deberán ser versionados en la herramienta que para el efecto posee la DTIC, con el propósito de garantizar la disponibilidad del código fuente y/o ejecutable.
3) Las unidades que poseen su propia infraestructura deberán garantizar el cumplimiento de la metodología generada por la DTIC, para la atención de requerimientos y/o incidentes.
4) La implementación y mantenimiento de aplicativos debe seguir las normas, estándares y arquitectura para desarrollo de aplicaciones y aseguramiento de la calidad establecidos por la DTIC.
5) La Unidad requirente debe nombrar un usuario administrador funcional del aplicativo, quien tendrá la responsabilidad de generar los requerimientos funcionales y su aprobación respectiva,
6) La Unidad requirente previo a la operación de un sistema deberá nombrar a un administrador del sistema, quien ejercerá el control, parametrización y administración del sistema en operación

Art. 39.- Tipo de desarrollo/mantenimiento de aplicaciones. - La DTIC ha definido los siguientes tipos de desarrollo/mantenimiento de aplicaciones:

- **Desarrollo/Mantenimiento Centralizado**: Son aplicativos que por sus requerimientos especializados es mejor desarrollarlos con los recursos propios de la DTIC, considerando que para proyectos nuevos se debería incrementar recursos nuevos que están considerados dentro del costo del proyecto.
- **Desarrollo/Mantenimiento Descentralizado**: Se considera a los sistemas que están alojados o no en la DTIC, y que la unidad requirente posee personal informático que entre sus actividades tienen el desarrollo y/o mantenimiento de aplicaciones.
- **Desarrollo a Medida realizado por Proveedores**: Son aplicativos cuyo desarrollo es contratado a terceros (proveedores externos)
- **Mantenimiento de aplicaciones desarrollado a Medida por Proveedores:** Mantenimiento a los aplicativos desarrollados por proveedores externos.
- **Desarrollo/Mantenimiento de aplicaciones personalizadas:** Son aplicativos desarrollados por terceros y que el área requirente contrata su implementación y personalización, incluido el código fuente.
- **Implementación de aplicaciones Cerradas:** Son aplicativos que requieren contratación de terceros para su implementación, no incluido el código fuente (Ejm. Paquetes comerciales como SPSS).
- **Donación de Aplicaciones:** Son aplicativos que, por convenios, acuerdos, etc. institucionales son donado. Estos aplicativos son de interés institucional por lo tanto la UTM debe asumir su implementación. Según la categorización que se determine, se deberá seguir los lineamientos y directrices de los estándares y procedimientos establecidos por la DTIC.

Art. 40.- Entorno de Trabajo. - La DTIC utilizará los siguientes ambientes para el proceso de desarrollo de aplicaciones:

1) **Desarrollo**. - Ambiente utilizado para la construcción de las aplicaciones. El ambiente es administrado por el área de Ingeniería de Soluciones (IS).

2) **Preproducción (pruebas).** - Establecido como un ambiente similar al de producción, utilizado para el Aseguramiento de calidad y pruebas del aplicativo. Este ambiente es administrado por el área de Aseguramiento de la Calidad (QA).

3) **Producción**. - Ambiente utilizado para la operación de los aplicativos. El ambiente es administrado por el área de Infraestructura.

De la Implantación de un aplicativo en ambiente de producción, alojado en la DTIC, se procederá:

4) El área de Desarrollo, conjuntamente con el área de Aseguramiento de la Calidad (QA) y el área de Infraestructura, seguirán el procedimiento determinado y aprobado por la DTIC para la implantación o modificaciones de los aplicativos que se encuentran en ambiente de producción.

5) La Implantación o modificaciones de los aplicativos desarrollados por la DTIC debe ser validada y aprobada formalmente por el área del negocio requirente, previamente a la liberación en el ambiente de producción.

3.11. POLITICA PARA LA ADQUISICIÓN DE INFRAESTRUCTURA Y CONTRATACIÓN DE SERVICIOS TECNOLÓGICOS

Art. 41.- Generales- En lo concerniente a este punto se tendrá en cuenta lo siguiente:

1) La DTIC será la entidad encargada de aprobar los proyectos de adquisición de infraestructura alineada a los objetivos de la organización, basándose para ello en principios de calidad de servicios, portafolios de proyectos y servicios.

2) La adquisición de bienes tecnológicos y licencias, y la contratación de servicios de soporte técnico y/o mantenimiento se llevará a cabo de acuerdo con los lineamientos y estándares que emita la DTIC, basándose en la necesidad institucional y la normativa vigente sobre la materia.

3) La DTIC será la única responsable de emitir informes sobre pertinencia de adquisición de infraestructura y servicios tecnológicos en el Universidad Técnica de Manabí.

Art. 42.- Dimensionamiento de la capacidad. - Para la optimización de recursos:

1) La DTIC debe elaborar informes anuales sobre las necesidades de incremento de capacidades, en los cuales se realice la evaluación de riesgos tecnológicos, costos y vida útil de los equipos para futuras actualizaciones.
2) Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información.

3.12 POLÍTICA DE GESTÓN DE CAMBIOS A LOS SISTEMAS

Art. 43.- Generales. - Para los sistemas administrados por la DTIC, la unidad Institucional requirente deberá realizar el pedido formal de cambio a los sistemas a través de un requerimiento funcional, que incluya la prefactibilidad en el ámbito legal y el análisis de riesgo sobre el cambio. Una vez, ingresado el requerimiento, la DTIC procederá con el procedimiento establecido para la gestión de cambio a los sistemas.
En los sistemas que no sean administrados por la DTIC, para realizar el cambio sobre los sistemas, se coordinará con la DTIC para el establecimiento de los lineamientos que deberán ser aplicados para una adecuada modificación.

3.13 POLÍTICA DE USO DE INTERNET E INTRANET

Art. 44.- Generales. - Los servicios de Internet e Intranet son recursos que la institución pone a disposición de las y los funcionarios, servidores y demás trabajadores de las Unidades AC/AD, como una herramienta de consulta de información, investigación y acceso a los sistemas institucionales, facilitando la realización de las labores cotidianas, tomando en cuenta lo siguiente:

1) El acceso y uso de los servicios de Internet e Intranet está condicionado a la aceptación de las políticas de este instrumento normativo.
2) El uso de servicio de Internet e Intranet está limitado a la realización de actividades laborales que estén relacionadas con los propósitos y funciones institucionales.
3) Para el uso de servicios institucionales se procederá a la creación de un usuario, con su respectivo perfil de acceso, La configuración del usuario en el dispositivo asignado será responsabilidad de la DTIC.

4) Para los usuarios externos, ajenos a la institución, que requieran el acceso al servicio de internet, se ingresará a la red pública de invitados, la cual tienen un perfil limitado.
5) El intercambio de información entre las Unidades AC/AD, se podrá realizar a través de la red local, intranet, conexión de datos o una conexión privada virtual.

Art. 45.- Responsabilidades. - Los servicios de enlaces de datos y de Internet e Intranet son administrados por el personal de la DTIC a través del área de Infraestructura. El proveedor de servicios de enlaces de datos y de Internet es responsable de garantizar la disponibilidad y los anchos de banda del enlace, con base en los acuerdos de nivel de servicio contratados, tomando en cuenta lo siguiente:

1) La DTIC es la entidad responsable de monitorear periódicamente el uso de Internet e Intranet de la UTM, con la finalidad de vigilar el cumplimiento de las presentes políticas, manteniendo la confidencialidad de la información,
2) La información y mensajes que se envíen a través de internet, será de completa responsabilidad del usuario emisor. En ningún momento dichos mensajes podrán atentar contra la imagen y reputación de la institución.
3) El usuario será el único responsable por los sitios web visitados desde su perfil de acceso a internet, por lo tanto, será también responsable de mantener en privado las credenciales de su cuenta.

Art. 46.- Prohibiciones.

1) Utilizar el internet como medio para realizar cualquier actividad comercial o lucrativa de carácter individual o la participación y distribución de actividades o materiales que vayan en contra de la ley,
2) Utilizar el internet para propósitos que puedan influir negativamente en la imagen del
Universidad Técnica de Manabí, de sus autoridades o funcionarios,
3) Realizar cualquier actividad que pueda comprometer la seguridad de los servidores y recursos informáticos de la institución,
4) Accesos a sitios web que puedan ser percibidos como obscenos, que distribuyan, emitan o promocionen material pornográfico, material ofensivo o con humor inapropiado; que atente a la moral y buenas costumbres, entre otros,
5) Acceso a sitios de juegos y actividades recreativas o de promoción de intereses personal, tales como: chats, concursos, entre otros,
6) Transmitir amenazas, material indecente o de hostigamiento, así como, intimidar, insultar difamar, ofender, acosar a otras personas o interferir en el trabajo de otros usuarios,
7) Distribuir por internet material que cause daño, como piratería, el sabotaje específicamente la distribución de software malicioso,
8) Descargar e instalar programas o archivos vía internet. Únicamente se podrá llevar a cabo esta tarea en situaciones previamente autorizadas por la DTIC,
9) Congestionar, afectar, interferir o paralizar el uso del servicio de internet,
10) La instalación o uso de programas P2P,
11) Descargar música, fotos, videos u otro material que no esté relacionado con las actividades o propósitos laborales.

3.14 POLÍTICA DE USO DE FIRMAS ELECTRONICAS

Art. 47.- Definición. - Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Art. 48.- Ámbito. - El uso de firmas electrónicas dentro de la UTM estará amparado en la Ley de Comercio Electrónico, firmas y mensajes de datos, el Reglamento General de la Ley de Comercio Electrónico, Firmas y mensajes de datos; sin perjuicio de nuevas reformas que fortalezcan el desarrollo y aplicación efectiva del comercio electrónico.

Art. 49.- Efectos de la firma electrónica. - La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio.

Art. 50.- Instrumentos públicos electrónicos. - Se reconocerá la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmada electrónicamente. Dichos instrumentos públicos electrónicos deberán observar los requisitos, formalidades y solemnidades exigidos por la ley y demás normas aplicables.

Art. 51.- De las infracciones al uso de firmas electrónicas. - Los delitos o infracciones informáticas relacionadas al uso de firmas electrónicas serán sancionadas acorde a lo establecido en la Ley de Comercio Electrónico, Firmas y mensajes de datos (Ley No. 67 R.O. Suplemento 557 de 17 de abril de 2002).

3.16 SANCIONES

Art. 52.- Incumplimiento de las Políticas. - Ante el incumplimiento de las obligaciones contempladas en este instrumento, se iniciarán las respectivas acciones y procedimientos administrativos y jurisdiccionales, de conformidad a las normas que las regulan, a fin de que se determine la responsabilidad civil, administrativa y penal, a que haya lugar, en contra de las personas imputables. La Universidad Técnica de Manabí podrá iniciar las acciones de oficio o a petición de parte, a través de los órganos competentes.

4 DISPOSICIONES
4.1 DISPOSICIONES GENERALES

PRIMERA. - La Dirección de Tecnologías de la Información y Comunicación, será el único responsable de formular y difundir políticas, estrategias, normas técnicas, objetivos y fijar estándares en lo relacionado a la infraestructura informática y sistemas de información para las Unidades AC/AD de la UTM.

SEGUNDA. - La Dirección de Tecnologías de la Información y Comunicación, será responsable de aprobar y difundir los reglamentos pertinentes que regulen la administración y uso de los recursos informáticos para todas las Unidades AC/AD.

TERCERA. - La DTIC estará facultada para aprobar procedimientos y estándares específicos que se requieran para la aplicación de las presentes políticas que regulen las actividades relacionadas con el uso de Tecnologías de la Información y Comunicaciones.
CUARTA. - La DTIC será la encargada de establecer y socializar procedimientos e instructivos que regulen las actividades relacionadas con tecnologías de información para las Unidades AC/AD.

QUINTA. - Los Analistas de Desarrollo de Software y de Mantenimiento Informático responderán a las directrices y lineamientos expresados en la presente Política de Tecnología de la Información y Comunicación.

4.2 DISPOSICIÓN TRANSITORIA

PRIMERA. - En el plazo de 60 días a partir de la entrada en vigencia del presente documento, los Analistas y Asistentes de Mantenimiento Informático que cumplen funciones en las Unidades AC/AD, coordinarán con la Dirección de Tecnología de la Información y Comunicación la información correspondiente de los inventarios de software y hardware de cada una de sus unidades.

SEGUNDA. - En el plazo de 60 días a partir de la entrada en vigencia del presente documento, Analistas y Asistentes de Mantenimiento Informático que cumplen funciones en las Unidades AC/AD, continuarán administrativamente en sus puestos de trabajo, pudiendo ser rotados a petición de Jefe de Tecnología.

TERCERA. - En el plazo de 90 días a partir de la entrada en vigencia del presente documento, las Unidades AC/AD que posean aplicaciones o software adquiridos, desarrollados o donados, deberán realizar el respectivo inventario y reportarlo ante la Dirección de Tecnología de la Información y Comunicación.

CUARTA. – En el plazo de 90 días a partir de la entrada en vigencia del presente documento, las Unidades AC/AD que posean Data Center aislados, deberán presentar un plan de integración de los equipos informáticos.

4.3 DISPOSICIÓN FINAL

DISPOSICIÓN FINAL. - Las Políticas de Informática y Comunicación entrará en vigencia a partir de su aprobación, por parte del máximo organismo de la Universidad Técnica de Manabí.

Dado y firmado por el H. Consejo Universitario en sesión ordinaria efectuada a través de la plataforma virtual Zoom, a los veintiséis días del mes de noviembre de dos mil veinte.

Firmado electrónicamente por:
VICENTE FELIX VELIZ

Rector-Presidente

Firmado electrónicamente por:
GARY OSWALDO LOOR FERNANDEZ

Secretario General (e)