Tipo de Norma: Instructivo

Nombre: Instructivo de buen uso de los recursos tecnológicos e información de la UTPL.

Código: VAD_IN_32_2014_V2_2020

Fecha	Versión	Cambios realizados
08/05/2014	V1	Creación del Documento
25/06/2020	V2	Reformas varias
Registro de gestión		
	Nombres y apellidos	**Cargo**
Elaboración	Ing. Julia Alexandra Pineda Arévalo	Coordinadora Técnica del Área de Seguridad, Riesgos y Auditoría-UGTI
Elaboración	Mgtr. María Paula Espinosa Vélez	Directora de operaciones y procesos
Elaboración	Mgtr. Carlos Gabriel Córdova Erréis	Gerente UGTI
Revisión	Mgtr. Cristina del Pilar Luzuriaga Montoya	Abogada / Procuraduría
Proponente	Dr. José María Sierra Carrizo	Vicerrector Administrativo
Aprobación	Ph. D. Santiago Acosta Aide	Rector

Registro manifestación de conformidad Abogado / Procuraduría	
Nombres y apellidos	**Cargo**
N/A	N/A

La universidad ha adoptado el lenguaje inclusivo en su Estatuto Orgánico. Sin embargo, la normativa institucional podría utilizar el género masculino para referirse a personas o cargos de manera general, siendo su alcance amplio, abarcando tanto a mujeres y hombres.

Ph. D. Carmen Eguiguren Eguiguren
Procuradora Universitaria

1. OBJETIVO

Establecer los lineamientos generales para el buen uso de los recursos tecnológicos e información de la UTPL, así como la gestión de accesos a los sistemas, que deben acatar empleados (administrativos, docentes) y estudiantes; así como el personal externo que por relación contractual o convencional tenga acceso a los sistemas de la Universidad.

2. TERMINOLOGÍA, DEFINICIÓN Y SÍMBOLOS

- **Dueño funcional del sistema:** persona responsable de velar por que el sistema funcione acorde a los procesos del negocio.
- **Administrador Técnico:** persona técnica que administra el sistema y ejecuta las solicitudes del dueño funcional.

3. DESCRIPCIÓN

CAPITULO I: GESTIÓN DE ACCESO A LOS SISTEMAS DE LA UTPL

Art 1.- Deberá existir un proceso formal para gestionar el control de acceso a los sistemas de información de la UTPL, estos procesos deben ser definidos por Dirección de Recursos Humanos y Desarrollo Personal, el dueño funcional del sistema y el administrador técnico, apoyado por el área de Seguridad Riesgos y Auditoría (Ver Anexo 1: Gestión de Accesos).

Art 2.- Registro de usuarios. - Todos los usuarios de los sistemas de información de la UTPL deberán tener asignado un identificador de usuario único y contraseña, así como tener un rol o perfil en cada sistema para que puedan acceder según las actividades que realizan en su ámbito de responsabilidad.

Art 3.- Para la creación, activación y desactivación de usuarios, el proceso será iniciado bajo el siguiente detalle:

Tipos de usuarios	Inicio del proceso
Empleados de UTPL	Solicitud de Dirección General de Recursos Humanos y Desarrollo Personal
Estudiantes	Haber realizado el pago de su matrícula y entrega de requisitos (en caso de ser necesario) en el ciclo vigente.
Personal externo Cuentas Genéricas	Solicitud de personal de UTPL anexando la debida justificación y aprobación del jefe inmediato, a excepción del Rector y Vicerrectorados que lo podrán solicitar directamente sin otra autorización

Art 4.- El nombre de usuario será creado según el estándar definido (Ver Anexo 2: Creación de cuentas).

Art 5.- La contraseña del usuario será creada según el estándar definido (Ver Anexo 3: Creación de cuentas).

Art 6.- Los administradores de servicios deberán otorgar acceso a los diferentes sistemas de información siempre que el solicitante tenga la respectiva autorización según se haya definido.

Art 7.- El otorgamiento de roles y perfiles de usuario se deberá realizar de acuerdo al principio del mínimo privilegio.

Art 8.- Los administradores de servicios deberán mantener un registro actualizado de usuarios y privilegios de acceso asignados, a fin de poder generar reportes y listados de los mismos.

Art 9.- Credenciales de acceso a los sistemas. - Los empleados (administrativos, docentes) y estudiantes de la Universidad; y personal externo que por relación contractual o convencional tenga acceso a los sistemas de la Universidad y se les haya entregado credenciales de usuario y contraseña, deben acatar las siguientes disposiciones de buen uso de las credenciales de acceso:

- ✓ El usuario al que se le otorgue credenciales de acceso a los sistemas deberá usarlas para el fin con el cual fueron entregadas.

- ✓ El usuario será responsable de mantener la confidencialidad de dichos datos, así como de todas las actividades realizadas en los sistemas desde su cuenta.
- ✓ Las credenciales de usuario y contraseña son intransferibles y de uso personal (no se puede compartir con otras personas o exponerlas a terceros.
- ✓ Las credenciales de usuario y contraseña solo deben ser utilizados para los fines asignados.
- ✓ Si existe sospecha de que la contraseña ha sido descubierta, se debe realizar el cambio inmediato de la misma, por medio de la página web https://gidentidad.utpl.edu.ec.
- ✓ Se debe realizar el cambio periódico de contraseña, tomando en cuenta el estándar recomendado de seguridad (ver Anexo 3). Todos los usuarios de la UTPL deberán mantener sus equipos de trabajo (PC o PORTATIL) bloqueados y con contraseña de acceso segura cuando no estén trabajando en ellas

Art 10.- Usuarios o contraseñas predefinidas. - Los usuarios o contraseñas predefinidas (usuarios / contraseñas por defecto) que se encuentren configurados en los sistemas de información, servidores o equipos de comunicación deberán cambiarse o eliminarse inmediatamente antes de que éstos empiecen a funcionar en un entorno productivo. Los administradores de servicios y el Oficial de Seguridad de la Información o quien haga sus veces deberán analizar el impacto, el riesgo y la factibilidad de cambiar o eliminar un usuario o contraseña por defecto.

Art 11.- El administrador técnico, deberá considera que para las contraseñas de los usuarios con permisos privilegiados (tales como root, sa, administrador y otros) deberán ser cambiadas al menos 1 vez al año y no deberán ser compartidas (El manejo de excepciones deberá estar debidamente documentado y aprobado por el Oficial de Seguridad de la Información).

Art 12.- Revisión de los privilegios de acceso de los usuarios. - Los administradores funcionales y técnicos de los sistemas serán responsables de ejecutar una revisión y actualización semestral de los derechos y privilegios de acceso que tienen sus colaboradores en todos los sistemas de información a los cuales tienen acceso.

Art 13.- Los administradores de servicios deberán validar trimestralmente con el Oficial de Seguridad los accesos que se han otorgado a los usuarios privilegiados en los activos de información esto con depurar privilegios en caso que deban ser revocados.

Art 14.- Los administradores funcionales y técnicos de los sistemas deben garantizar que los accesos que tienen los usuarios sean los estrictamente necesarios.

Art 15.- Seguridad mínima en los sistemas de información. - Todos los sistemas de información de la UTPL deberán contar con un módulo de seguridad, el cual deberá permitir como mínimo:

- ✓ Indicar al usuario el cambio obligatorio de su contraseña una vez que las credenciales de acceso le hayan sido entregadas por primera vez.
- ✓ Bloquear al usuario luego de 5 intentos de acceso fallidos, y 15 minutos después activarlo automáticamente.
- ✓ Verificar la robustez de las contraseñas según estándar.
- ✓ Proteger las claves de acceso mediante controles criptográficos.
- ✓ En los equipos computacionales de UTPL, bloquear la sesión de usuario y solicitar una nueva autenticación cuando exista un tiempo de inactividad de 15 minutos.

El Área de Seguridad debe coordinar y monitorear la implementación de estos requisitos en los sistemas de UTPL.

CAPITULO II: AUDITORIA

Art 16.- Los servicios de Tecnología de la Información (TI) serán auditados por el Área de Seguridad, Riesgos y Auditoría.

Art 17.- Se deberá activar el registro de auditoría en los servicios, servidores, equipos de comunicación y sistemas críticos, para aquellos usuarios que mantengan privilegios administrativos o para aquellos usuarios que por su función o responsabilidad tienen acceso a información o transacciones privilegiadas, tema que deberá ser previamente analizado por el Oficial de Seguridad de la Información.

Art 18.- Los registros de auditoría deberán ser respaldados mensualmente o antes de que sean eliminados o sobrescritos por el propio sistema de información y retenidos mínimamente por tres meses.

Art 19.- La factibilidad de habilitar los registros de auditoría en los sistemas de información deberá ser autorizados por el Oficial de Seguridad de la Información y los administradores de servicio a fin de que puedan evaluar el impacto en el procesamiento y tiempo de respuesta del sistema de información en el cual se activarán (o no) dichos registros de auditoría.

Art 20.- La Universidad se reserva el derecho de auditar los procesos académicos o administrativos, y los sistemas que están relacionados, dicha auditoría solo será realizada bajo autorización del Rectorado, Vicerrectorados y Direcciones Generales.

CAPITULO II: USO DEL CORREO ELECTRÓNICO

Los empleados (administrativos, docentes) y estudiantes de la Universidad; y personal externo que tenga asignado una cuenta de correo electrónico deben acatar los siguientes lineamientos de buen uso del correo electrónico:

Art 21.- Para el uso y creación de una cuenta de correo personal institucional bajo el dominio @utpl.edu.ec de debe considerar:

- ✓ ***Cuentas de correos institucionales personales (empleados/estudiantes):*** El usuario debe ser un estudiante de la Universidad o tener una relación laboral de dependencia con la Universidad.
- ✓ ***Cuentas de correos institucionales personales (personal externo):*** Este tipo de cuenta corresponde a proveedores que por el servicio que brinde a la Universidad requiere el acceso al correo. La activación de este tipo de cuentas debe ser justificada y autorizadas por el Área de Seguridad - UGTI.
- ✓ ***Cuentas de correo genérico:*** Cuentas solicitadas con una justificación académica o administrativas para la Universidad. Estas cuentas deben tener asignado un responsable por parte de la universidad. Las cuentas de correo genéricas no pueden ser usadas para otros fines que no sean los propios de la unidad a la que pertenece y que originaron su creación.

Art 22.- El uso del correo electrónico institucional es obligatorio para toda la comunidad universitaria, siendo el único canal de comunicación oficial para los fines relacionados con la actividad institucional.

En virtud de lo dispuesto, la comunicación relacionada con las actividades académicas **y** administrativas, como, solicitudes, disposiciones, información institucional y demás comunicaciones de la universidad, tendrán como remitente una cuenta institucional (@utpl.edu.ec) e irá dirigido a las cuentas institucionales de los empleados de la UTPL (docentes y administrativos) y estudiantes activos.

Art 23.- Los Vicerrectorados Académico y de Modalidad Abierta y a Distancia, Dirección de Comunicación y Dirección de Operaciones deberán definir el personal autorizado para realizar comunicaciones a los empleados, estudiantes o ex estudiantes de UTPL y personal interesado en estudiar en la universidad.

Art 24.- El correo electrónico debe ser utilizado únicamente para fines académicos o administrativos de la institución y para la difusión de convenios, beneficios a los usuarios de otras entidades que la Universidad haya autorizado; como, por ejemplo: la asociación de docentes y empleados. No se debe utilizar el correo con fines de propaganda, ventas de artículos, envío de cadenas, o actividades personales que no tengan relación con la institución.

Art 25.- Para el envío de correos masivos se debe tomar en cuenta las consideraciones definidas para el envío de correos masivos y personalizados a usuarios de la UTPL".

Art 26.- Vigencia de las cuentas

- ✓ Las *cuentas de correo personal* de los empleados estarán activas mientras dure la relación laboral.
- ✓ *Las cuentas de correos institucionales para personal externo* estarán activas mientras dure el servicio que esté prestando a la Universidad, luego de ello la cuenta será desactivada y transcurrido 3 meses la cuenta será eliminada.
- ✓ Para las *cuentas de correos genéricas*, en caso de que el responsable deje de laborar se debe asignar un nuevo responsable de la cuenta genérica quién deberá realizar el cambio inmediato de clave de la cuenta de correo.

CAPITULO IV: USO DE SISTEMAS E INFRMACIÓN DE LA UNIVERSIDAD

Art 27.- Los empleados (administrativos, docentes) y estudiantes de la Universidad; y personal externo que tenga asignado una cuenta de acceso a los sistemas de la Universidad deben acatar los siguientes lineamientos para el buen uso de los sistemas:

- ✓ La información es un activo importante de la UTPL, por lo que el acceso a la información no es permitido para su uso fuera de las responsabilidades laborales del usuario. La información y datos solamente deben ser utilizados para los asuntos legítimos de la UTPL.
- ✓ Los sistemas de la UTPL deben ser utilizados apropiadamente según los fines asignados a cada usuario. Está prohibido utilizar los sistemas para actos de bullying, actos que denigren a personas o a la institución, promocionar ventas, fiestas, pornografía, etc. En estos casos, se estará a lo dispuesto por el Reglamento de Ética y Régimen Disciplinario de la UTPL.
- ✓ Las actividades de los usuarios registradas en los sistemas son de responsabilidad única del dueño de la cuenta.
- ✓ La Universidad podrá interrumpir temporal o indefinidamente, el acceso del usuario a los sistemas, si detecta un uso contrario a lo autorizado.

Art 28.- Los empleados (administrativos, docentes) y estudiantes de la Universidad; y personal externo que tenga acceso a información de la Universidad deben acatar los siguientes lineamientos para el de buen uso de la información:

- ✓ El personal de la universidad debe implementar los mecanismos necesarios para mantener la confidencialidad de la información que tiene a su cargo en sus diferentes medio o formas.
- ✓ Las evaluaciones que se receptarán a los estudiantes son consideradas como información confidencial, por lo cual, las personas que tienen acceso a esta información deberán observarlas precauciones necesarias para evitar la fuga de información.
- ✓ El usuario se compromete a no distorsionar la información o dañar los datos en sus diferentes medios o formas.

- ✓ El usuario no intentará acceder a información que no le haya sido otorgada.
- ✓ Está prohibida la reproducción total o parcial de documentos, propiedad de la Universidad como: guías, evaluaciones, trabajos a distancia, paper's, documentos de investigación o cualquier otro documento que haya sido elaborado por esta, si no hay el expreso consentimiento, para el efecto.

CAPITULO V: GESTIÓN DE INCIDENTES DE SEGURIDAD

Art 29.- El Equipo de Respuesta a Incidentes de Seguridad Informática de la UTPL (CSIRT-UTPL) es el encargado de:

- ✓ Gestionar los incidentes de seguridad informáticos en los cuales esté involucrado un sistema o información de la Universidad.
- ✓ En coordinación con Dirección de Recursos Humanos y Desarrollo Personal y Unidad de Bienestar Universitario, concientizar a los empleados, estudiantes y personal externos sobre buenas prácticas de seguridad.
- ✓ Coordinar y ejecutar acción encaminadas en minimizar vulnerabilidades en los sistemas y monitorear la seguridad de los mismos.

Art 30.- Los empleados, estudiantes y personal externos, en caso de tener incidentes de seguridad con los sistemas de la Universidad como: suplantación de identidad, solicitudes de usuarios y contraseñas, correos sospechosos, robo de información, etc, deberán contactar con el (CSIRT-UTPL) (ver Anexo 4).

Art 31.- En caso de que el CSIRTUTPL detecte un incidente ya sea hacia una cuenta de un usuario o sistemas de la Universidad, este inmediatamente notificará al usuario o administrador técnico.

Art 32.- Para prevenir incidentes de seguridad sobre los sistemas de UTPL, el Área de Seguridad, Riesgos y Auditoría deberá realizar escaneos de vulnerabilidades cada 6 meses a los sistemas críticos y cada año a los sistemas no críticos, o lo que se defina en el plan operativo anual de seguridad.

Art 33.- El CSIRT-UTPL deberá recomendar planes de acción que ayuden a prevenir incidentes futuros en la Universidad y deberá ser entregado a las áreas correspondientes.

Art 34.- Toda la información relativa a los incidentes de seguridad será clasificada por defecto como "Reservada – Confidencial". Dicha clasificación será realizada de acuerdo a la "Política de Gestión de Activos de Información".

Art 35.- Todas las actividades concernientes al manejo de incidentes se realizarán siguiendo los protocolos y procedimientos formales definidos para el manejo de incidentes los cuales deberán permitir la obtención de evidencias que puedan ser legalmente aceptadas, de tal forma que, si la Universidad lo desea, pueda tomar las acciones legales correspondientes.

Art 36.- Por ningún motivo se utilizarán métodos ilegales para el tratamiento de un incidente, debiéndose tomar en cuenta que aquellos métodos autorizados que se utilicen no ocasionen riesgos legales que posteriormente podrían afectar a la Universidad.

Art 37.- El impacto de todos los incidentes de seguridad de la información deberá ser analizado con la participación y dictamen de la Procuraduría Universitaria, sin limitarse a los incidentes relacionados a suplantación de identidad y acceso a información reservada.

CAPITULO VI: CONTROL DE NAVEGACIÓN

Art 38.- La Gerencia de la Unidad de gestión de TI deberá implementar mecanismos que permitan realizar un bloqueo de contenido web inapropiado para el personal, los estudiantes y personal externos que se conecta a la red de la Universidad, como, por ejemplo:

- ✓ Filtrado Web por palabras clave a bloquear
- ✓ Filtrado Web por Lista Negra
- ✓ Filtrado Web por Lista Blanca

- ✓ Peticiones de Bloqueo por parte de usuarios
- ✓ Filtrado Web por Extensiones Prohibidas

Art 39.- Las categorías de sitios web consideradas inapropiadas y de alto riesgo para la Universidad serán bloqueadas, en coordinación con el Área de Seguridad, Riesgos y Auditoría de UGTI.

Art 40.- Los jefes de las áreas, departamentos, directores, vicerrectores, podrán solicitar a la Unidad de Gestión de TI el bloqueo o excepciones de bloqueos de las categorías de sitios web para sus áreas, según ellos crean conveniente y exista una justificación académica o administrativa para ello.

CAPITULO VII: CONTROL DE CUMPLIMIENTO Y SANCIONES

Art 41.- El área de Seguridad, Riesgos y Auditoría evaluará el cumplimiento del presente instructivo y entregará el informe del mismo al Comité de Seguridad para que este analicé la factibilidad de la implementación de las mejoras propuesta al Sistema de Gestión de Seguridad.

Art 42.- El incumplimiento de lo dispuesto en el presente Instructivo, así como el uso inapropiado del correo electrónico, difusión de contenido inadecuado, falsificación o suplantación de identidad, ingreso a sistema sin autorización, uso de la información de manera no autorizada, vulneración de los sistemas o información de UTPL, considerando, además, las faltas contempladas en el Reglamento de ética y Régimen Disciplinario, dará paso a los procesos sancionatorios contemplados en dicho Reglamento, sin perjuicio de las responsabilidades civiles y penales a las que hubiere lugar.

ANEXOS

ANEXO 1: GESTIÓN DE ACCESOS

Para la Gestión de acceso se deberá considerar:

- ✓ Definición de la Matriz de roles y privilegios
  - El rol está definido por la función que cumple un usuario dentro de un sistema.
  - El privilegio es la descripción detallada de las transacciones que un usuario puede realizar en un sistema, esto basado en los establecido en los procesos de la Universidad.
  - En la matriz de acceso de deberá identificar el rol del sistema con el perfil o cargo de los usuarios que van a tener dicho rol.
- ✓ Procedimiento de creación, baja y modificación de privilegios de usuarios, en la cual se especifique:
  - Personal autorizado a solicitar creaciones, bajas y modificaciones de privilegios de los usuarios.
  - Personal ejecutor.
  - Periodicidad en la ejecución de depuración de usuarios en el sistema.
- ✓ Procedimiento de entrega de credenciales de acceso.

ANEXO 2: CREACIÓN DE CUENTAS

La creación de cuentas para personas, deberá cumplir con los siguientes parámetros:

- ✓ Se tomará la primera letra del primer nombre seguido de la primera letra del segundo nombre en conjunto con el primer apellido configurado en minúscula (letrapnombre+letrasnombre+papellido). Ejemplo: si el nombre es Pablo Emilio Pérez Ruiz la cuenta de usuario será: peperez.

- ✓ Si la cuenta de usuario ya existe se deberá añadir aleatoriamente hasta dos números al final. Ejemplo: si el nombre es Juan Andrés Pérez Lima la cuenta del usuario quedará: japerez en caso de estar utilizado japerez32.
- ✓ Si el nombre del nuevo colaborador contiene "ñ" o tildes en su nombre o apellido éste se deberá reemplazar con una "n" o sin tildes. Ejemplo: si el nombre es Iván Leonardo Montañez la cuenta de usuario quedará: ilmontanez.

Las excepciones a estos parámetros serán autorizadas por la Gerencia de UGTI.

ANEXO 3: RECOMENDACIONES DE SEGURIDAD

Conformación de una contraseña:

- ✓ Para que una contraseña sea segura debe cumplir, al menos, tres de las siguientes características:
  - Tener números.
  - Tener Letras.
  - Tener mayúsculas y minúsculas.
  - Tener símbolos (&, %, @, *, etc.).

  Por ello todas las cuentas de usuarios de la Universidad deberán cumplir con este requerimiento.
- ✓ Además, debe cumplir los siguientes requisitos:
  - Su longitud debe ser mayor o igual a ocho caracteres.
  - No debe formarse con números o letras que estén adyacentes en el teclado. Ejemplo: 123456, 1q2w3e o 123QWEasd.
  - No debe contener información que sea fácil de averiguar, por ejemplo, nombre de usuario de la cuenta, información personal (cumpleaños, nombre de familiares, etc.).
  - No debe contener palabras existentes en diccionarios de algún idioma. Los ataques de diccionario prueban cada una de las palabras que figuran en el diccionario y/o palabras de uso común

Cambio de contraseña:

- ✓ Los usuarios deberán considerar que sus contraseñas de la Universidad deben ser cambiadas cada 3 meses, tomando en cuenta la conformación de una contraseña.
- ✓ Si se ha identificado que la contraseña ha sido descubierta se debe realizar el cambio inmediato de la misma, por medio de https://gidentidad.utpl.edu.ec.
- ✓ Si se presenta un inconveniente con el cambio de contraseña, se contactará con Mesa de Servicios Tecnológicos.

ANEXO 4: CONTACTO CON EL CSIRT-UTPL

Tipos de usuario	Canal	Contacto
Todos los usuarios	Portal CSIRT-UTPL	https://csirt.utpl.edu.ec/contact
Empleado UTPL	Teléfono	(593) 7 3701444 ext (3333)
	Correo	mst@utpl.edu.ec

Prospecto Estudiantes Exestudiante	Línea gratuita	1800 8875 88
	Buzón de consultas	https://buzon.utpl.edu.ec/
	Centros Universitarios	https://www.utpl.edu.ec/centros_utpl/