TABLA DE CONTENIDO

INTRODUCCIÓN 2

OBJETIVO 2

ALCANCE 2

DEFINICIONES 3

DISPOSITIVOS MÓVILES. 12
CORREO ELECTRÓNICO INSTITUCIONAL. 14
CONTROL DE ACCESO. 18
ACCESO A REDES Y A SERVICIOS EN RED 21
USO DE CONTROLES CRIPTOGRÁFICOS 23
PANTALLAS, ESCRITORIOS LIMPIOS Y EQUIPOS DESATENDIDOS. 24
PROTECCIÓN CONTRA SOFTWARE MALICIOSO. 29
RESPALDO DE LA INFORMACIÓN. 31
TRANSFERENCIA DE INFORMACIÓN. 34
DESARROLLO SEGURO DE SOFTWARE 35
RELACIONES CON TERCEROS Y EL PERSONAL QUE PRESTA SERVICIOS 37
PROTECCIÓN DE DATOS PERSONALES 41
DATOS ABIERTOS 55
USO DE LA RED DE DATOS INSTITUCIONAL 57

INTRODUCCIÓN

Las directrices de seguridad de la información de la Universidad Tecnológica de Pereira van dirigidas a preservar la confidencialidad, integridad y disponibilidad de todos los activos de información, a través de mecanismos de control para la identificación, evaluación, impacto y control de los riesgos relacionados con la información, a fin de implementar y mantener el Sistema de Gestión de Seguridad de la Información - SGSI.

De esta forma, la Institución se basa en la definición de responsabilidades frente a la protección de la información para el desarrollo y cumplimiento de su modelo de seguridad de la información; el cumplimiento de los requerimientos legales y normativos, aplicables a los activos de información y a la Universidad; la existencia de mecanismos de concientización en temas de seguridad de la información; el reporte e investigación de los incidentes de seguridad y la continuidad en la prestación de sus servicios. El manual de directrices representa la Política de Seguridad de la Información de la Universidad Tecnológica de Pereira.

Las directrices expresadas en este manual son la base para la implantación de procedimientos, que también son parte esencial del modelo de Seguridad de Información mediante la arquitectura de tecnología informática, un ambiente de administración y controles efectivos, que garanticen la seguridad de la información en la Universidad.

El cumplimiento de las directrices es un deber de las personas que laboran o prestan sus servicios a la Universidad y que tienen acceso a la información.

OBJETIVO

Establecer las directrices de Seguridad de la Información en la Universidad Tecnológica de Pereira, con el fin de generar conciencia y buenas prácticas de la seguridad de la información al interior de la entidad, a través de su cumplimiento e interiorización.

ALCANCE

Las Directrices de Seguridad de la Información son aplicables a todos los procesos del alcance del Sistema de Gestión de Seguridad de la Información y buscan la protección de las características de Confidencialidad, Integridad y Disponibilidad de la información en la Universidad, mediante las

medidas preventivas y correctivas necesarias para el logro del objetivo y la finalidad de cada directriz.

DEFINICIONES

Para efectos de este manual se tendrán en cuenta las siguientes definiciones:

- **Activo de información**: Todo bien tangible o intangible que posee valor para la organización y que representa, contiene, almacena o transmite información.
- **Algoritmo de cifrado:** Procedimiento sistemático para implementar la criptografía.
- **Almacenamiento en la nube:** Es un modelo de almacenamiento de datos basado en redes, donde los datos están alojados en espacios virtualizados, por lo general aportados por terceros.
- **Ambiente de desarrollo:** Entorno o ambiente orientado exclusivamente al desarrollo y diseño de nuevas clases de proceso. Al estar ubicado en instalaciones independientes, se garantiza su imparcialidad hasta que sean comprobados en el ambiente de pruebas antes de sincronizarlos con el ambiente de Producción.
- **Ambiente de producción:** Ambiente donde los usuarios trabajan diariamente en los procesos misionales introduciendo y consultando los datos reales de la organización.
- **Ambiente de pruebas**: Entorno o ambiente donde se comprueban y certifican los nuevos desarrollos antes de pasarlos al ambiente de producción.
- **Anonimizar:** Proceso para remover datos personales de una base de datos, buscando la publicación segura de datos para el reúso.
- **Antimalware:** Software que ayuda en la detección y eliminación de toda clase de software malicioso.
- **Antispam:** Software o dispositivo que ayuda a prevenir el correo no deseado.
- **Antispyware:** Software que se encarga de buscar, detectar y eliminar spyware o espías en el sistema.
- **Antivirus:** Programas cuyo objetivo es detectar o eliminar virus informáticos.
- **Arquitectura de software:** Es un conjunto de patrones que proporciona un marco de referencia necesario para guiar la construcción de un software, permitiendo a los programadores, analistas

y todo el conjunto de desarrolladores compartir una misma línea de trabajo y cubrir todos los objetivos y restricciones de la aplicación. Es considerada el nivel más alto en el diseño de la arquitectura de un sistema, puesto que establece la estructura, funcionamiento e interacción entre las partes del software.

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- **Aviso de Privacidad:** comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de laexistencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
- **Banco de datos:** Es un centro de acopio y de intercambio de información, el cual puede ser digital o física.
- **Base de datos de conocimiento:** Es un tipo especial de base de datos para la gestión del conocimiento. Provee los medios para la recolección, organización y recuperación computarizada de conocimiento.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
- **Bloqueo dispositivo móvil:** Método de bloque de los dispositivos móviles (contraseña, biométrico, patrón o reconocimiento de voz.)
- **Causahabiente:** persona que ha sucedido a otra por causa del fallecimiento de ésta (heredero).
- **Centro de datos:** Es la ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.
- **Certificado digital:** Es un archivo generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet. Su función principal es la de asegurar y autenticar las comunicaciones que se realicen.
- **Clave pública, clave privada:** Método criptográfico que usa un par de claves para el envío de mensajes. Una clave (pública) se entrega a cualquier persona, la otra (privada) debe ser guardada de modo que nadie tenga acceso a ella**.**
- **Clave:** Mecanismo de seguridad implementado para garantizar la identidad del usuario y de esta manera brindarle acceso a los sistemas de información.

- **Confidencialidad:** Es la propiedad que impide la divulgación de información a personas osistemas no autorizados, deben tener acceso a la información únicamente aquellas personas quecuenten con la debida autorización.

- **Conjunto de datos (Dataset):** Unidad mínima de información sujeta a carga, publicación, transformación y descarga en la plataforma.

- **Contrato:** Acuerdo de voluntades sobre la adquisición de bienes y/o servicios celebrado entre la Universidad y el contratista, en el cual se establece el objeto del mismo, los valores, las cantidades, las reglas que rigen la naturaleza de los trabajos o actividades, los derechos y las obligaciones de las partes y los plazos para su cumplimiento y liquidación.

- **Control de acceso:** Práctica de restringir el acceso mediante diferentes mecanismos a los distintos sistemas de información.

- **Copia de respaldo:** Copia de los datos originales de un sistema de información que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

- **Criptografía:** Técnicas destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

- **CSV (Valores separados por coma):** Formato abierto y sencillo para representar datos enformato de tabla, en columnas separadas por comas (o punto y coma, donde la coma es el separador decimal) y las filas son saltos de línea. Los campos que tienen una coma, un salto de línea o una comilla doble, deben cerrarse entre comillas dobles. Las extensiones que se utilizan son .csv y .txt.

- **Dato personal**: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **Dato personal privado:** Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización expresa.

- **Dato personal semiprivado:** Son datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Para su tratamiento se requiere la autorización expresa del titular de la información, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV" de la Ley 1266.

- **Dato Público:** es el dato que no sea semiprivado, privado y sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y

a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

- **Dato sensible**: datos que afectan la intimidad de una persona natural o cuyo uso indebido puede generar su discriminación , tales como aquellos que revelen el origen racial, étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, o que promueva intereses de cualquier partido político o que garanticen los derechos o garantías de partidos políticos de oposición así como los relativos a la salud, la vida sexual y los datos biométricos. Es información catalogada como reservada o clasificada la cual es de primordial importancia para el funcionamiento de la universidad Tecnológica de Pereira.

- **Datos Abiertos:** Son todos aquello datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

- **Datos estructurados:** Método de publicación de datos para que puedan ser interconectados y más útiles.

- **Datos indispensables:** se entienden como aquellos datos personales de los titulares imprescindibles para llevar a cabo la actividad de educación superior en docencia, investigación, extensión, responsabilidad social y bienestar universitario. Los datos de naturaleza indispensable deberán ser proporcionados por los titulares de los mismos o los legitimados para el ejercicio de estos derechos.

- **Dispositivos móviles:** Computadores portátiles, tabletas, teléfonos inteligentes y dispositivos de almacenamiento.

- **Efecto mosaico:** Combinación de información disponible de bases anonimizadas que permite la identificación de los individuos. Es importante evitar este efecto para proteger los datos de las personas.

- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

- **Entidad:** Organismos establecidos por la legislación colombiana, los cuales tienen la facultad de definir inventarios de datos y conjuntos de datos a publicar.

- **Equipo desatendido:** Es la protección que se deriva del control que se tenga sobre la computadora y portátiles, tabletas u otros dispositivos similares que sean de propiedad de la Universidad, aun cuando el usuario no se encuentre frente a estos. Consiste en un bloqueo de pantalla o desconexión cuando no está siendo atendido.

- **Equipos de cómputo:** Computadores de escritorio, portátiles y tabletas que pertenezcan a la Universidad Tecnológica de Pereira.

- **Escritorio limpio:** Es la protección que se deriva del control frente al uso y ubicación de papeles y medios removibles de almacenamiento de información que son manipulados en las estaciones de trabajo. Consiste en evitar la pérdida, daño o acceso no autorizado a la información durante y fuera de las horas laborales.

- **Formatos libres:** Son formatos de archivo que se pueden crear y manipular para cualquier software, libre de restricciones legales.

- **Formatos propietarios:** Son formatos de archivo que requieren herramientas que no son públicas.

- **Fuentes de datos**: Se refiere a todas las unidades organizacionales que son fuentes primarias de información que son susceptibles de identificar datos abiertos a cargarse en la plataforma de datos abiertos.

- **Fuentes desconocidas:** Aplicaciones que no provienen de las tiendas oficiales de aplicaciones de los diferentes sistemas operativos.

- **Gestión de cambios:** Es un conjunto de procedimientos que se emplea para garantizar que se apliquen cambios necesarios en forma ordenada, controlada y sistemática para lograr el cambio esperado.

- **Gestión de entrega y despliegue**: Se encarga de asegurar que los paquetes de software o hardware ofrecidos cumplen las especificaciones detalladas en la RFC (definición de técnicas, procedimientos y protocolos). Además, con este proceso se realizará toda la configuración.

- **Grupo:** Se crea como una dirección de correo electrónico, a la cual tendrán acceso las cuentas de correo asociadas a este. Permite manejar bandeja de entrada de uso compartido. Dicho "grupo" no tiene asociada una clave de acceso. También puede usarse como lista de distribución de correos.

- **Habeas data:** derecho de cualquier persona a conocer, actualizar y rectificar la información que han sido suministrados y que se han incorporado en distintas bases o bancos de datos, o en repositorios electrónicos de todo tipo con que cuenta la Universidad Tecnológica de Pereira.

- **Información pública clasificada.** Es aquella información que estando en poder o custodia de la Universidad, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

- **Información pública reservada:** Es aquella información que estando en poder o custodia de la Universidad, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014 y el artículo 24 de la Ley 1755 de 2015.

- **Información pública**: Información que puede ser entregada o publicada por personas autorizadas sin restricciones

- **Información**: Toda comunicación o representación de conocimiento, como datos, en cualquier forma, con inclusión de forma textual, numérica, gráfica, cartográfica, narrativa o audiovisual, y en cualquier medio, ya sea digital, papel, pantalla de computadora, audiovisual u otro.

- **Integridad:** Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas, permitiendo mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

- **Interventor:** Persona natural o jurídica contratada por la Universidad para realizar el seguimiento, vigilancia y control de carácter administrativo, técnico, financiero o legal que sobre el cumplimiento del contrato, convenio o proyecto.

- **Lugar seguro**: Aquel lugar que protege el activo de información de acceso de personas no autorizadas (por ejemplo: archivador, cajonero, oficina con llave, caja fuerte, entre otros).

- **Malware:** Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

- **Medios de almacenamiento:** CD, DVD, cintas, discos duros modificados, discos duros externos, almacenamiento en la nube.

- **Metadato:** Los metadatos son "datos sobre datos" - es decir, los datos que describen los aspectos básicos de un conjunto de datos, por ejemplo, cuándo se creó el conjunto de datos, cuál es la unidad organizacional responsable de la base de datos, el formato de los datos, etc.

- **Niveles de acuerdo de servicio (SLA):** Los SLA establecen la relación entre ambas partes: proveedor y cliente, identifica y define las necesidades del cliente a la vez que controla sus expectativas de servicio en relación a la capacidad del proveedor, proporciona un marco de entendimiento, simplifica asuntos complicados, reduce las áreas de conflicto y favorece el diálogo ante la disputa.

- **Pantalla limpia:** Control frente al uso y ubicación de información que son manipulados computadora y pc portátiles, tabletas u otros dispositivos similares que sean de propiedad de la Universidad. Consiste en evitar la pérdida, daño o acceso no autorizado a la información durante y fuera de las horas laborales.

- **Personal que labora**: Administrativos (planta y transitorios), docentes (planta, transitorio, cátedra).

- **Personal que presta servicios:** Contratistas (órdenes de trabajo, prestación de servicios) y personal vinculado a través de la administradora de nómina.

- **Petición de solicitud de cambio (RFC):** Propuesta formal para que se realice un cambio, la cual incluye detalles del cambio propuesto, y puede registrarse en papel o electrónicamente.

- **Petición:** Solicitud de algún requerimiento que el Titular necesite o de algún comentario que desee manifestar a la institución. Por lo anterior la petición puede ser: comentario, información, inquietud, solicitud, sugerencia, agradecimiento o felicitación

- **Reclamo:** Es la manera de exigirle a la entidad que corrija la situación que impide o atropella el ejercicio de los derechos en relación con el tratamiento de los datos personales.

- **Redes de datos**: Conjunto de equipos informáticos y software conectados entre sí por mediode dispositivos físicos que intercambian información.

- **Registro Nacional de Bases de Datos:** es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.

- **Repositorio electrónico:** Es un sitio centralizado donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos.

- **Requisito funcional:** Un requisito funcional define una función del sistema de software o sus componentes. Una función es descrita como un conjunto de entradas, comportamientos y salidas. Los requisitos funcionales pueden ser: cálculos, detalles técnicos, manipulación de datos y otras funcionalidades específicas que se supone, un sistema debe cumplir.

- **Requisito no funcional:** Un requisito no funcional o atributo de calidad es, en la ingeniería de sistemas y la ingeniería de software, un requisito que especifica criterios que pueden usarse para juzgar la operación de un sistema en lugar de sus comportamientos específicos, ya que éstos corresponden a los requisitos funcionales. Por tanto, se refieren a todos los requisitos que no describen información a guardar, ni funciones a realizar.

- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos o el Tratamiento de los datos.

- **Reutilización de datos:** Producto que se elabora a partir de los datos públicos, puede ser una visualización, una aplicación web, un servicio, un cuadro de mandos, una noticia o una información, una gráfica, un dibujo, una gráfica dinámica, entre otras cosas.

- **Reutilizadores de datos:** Aquellas personas que con los Datos Abiertos como materia prima elaboran productos o servicios, pueden ser tales como emprendedores, empresas, ONG, periodistas, hackers cívicos, o cualquier persona que tenga conocimientos del tratamiento y la manipulación de los datos.

- **Rol:** Grupo en el cual se encuentran uno o más usuarios y al que se le definen los controles de acceso.

- **Servidor:** Es un computador u otro tipo de dispositivo que suministra una información requerida por unos clientes (que pueden ser personas, o también pueden ser otros dispositivos como computadores móviles, impresoras, entre otros).

- **Sistema de información:** Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo

- **Spam:** Mensajes electrónicos no solicitados, no deseados o con remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor.

- **Spyware:** Software que recopila información de un computador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

- **Supervisor de contrato:** Servidor vinculado a la Universidad y que realiza la tarea de seguimiento vigilancia y control de carácter administrativo, técnico, financiero o legal que sobre el cumplimiento del objeto del contrato, cuando para la ejecución de dichas labores no se requieren conocimientos especializados.

- **Tercero:** Persona natural o jurídica que suministra un bien o servicio a la Universidad o desarrolla trabajos para la entidad, que incluyan algún tipo de contacto con la información o sistemas de información de la entidad.

- **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento. Se consideran titular de información a los estudiantes, egresados, docentes, funcionarios públicos, jubilados, contratistas, proveedores y en general a cualquier persona que suministre datos personales a la Universidad.

- **Transferencia:** la transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

- **Transmisión:** tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

- **Virus informáticos:** Un virus informático es un software que tiene por objetivo alterar el normal funcionamiento del computador, sin el permiso o el conocimiento del usuario.

- **VPN:** Conexión segura que permite tener acceso a un recurso interno desde fuera de la Institución.

DIRECTRICES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Universidad Tecnológica de Pereira está comprometida con la implementación de estrategias de seguridad de la información, por lo cual se establecen las siguientes directrices:

DISPOSITIVOS MÓVILES.

Declaración Institucional

Se debe gestionar el riesgo de pérdida o daño de la información, identificada como pública, clasificada o reservada, por el uso de dispositivos móviles institucionales dentro y fuera del Campus.

Objetivo

Reducir el riesgo de pérdida, daño o divulgación de la información pública, clasificada o reservada por el uso de dispositivos móviles.

Alcance

Estas directrices serán aplicadas para uso de los dispositivos móviles institucionales que estén bajo responsabilidad individual. No aplican para dispositivos destinados para uso común o préstamo.

Responsabilidad

- **Comité de Sistema Integral de Gestión:** Revisar y aprobar los cambios que requiera la presente directriz.
- **Grupo Técnico de Gestión de Seguridad de la Información:** Recomendar ajustes a la presente directriz.
- **Jefes de dependencia o área:** Socializar e implementar la presente directriz en su área.
- **Personal que labora o presta servicios y terceros:** Aplicar la presente directriz y mientras tengan la información bajo su control, mantener los niveles de protección y clasificación establecidos para la misma haciendo uso adecuado de los recursos puestos a su disposición.
- **Administración de Servicios Informáticos:**
  - ✓ Realizar la configuración inicial del dispositivo e instalar el software inicial en los dispositivos móviles.
  - ✓ Establecer un método de bloqueo para los dispositivos móviles institucionales antes de ser entregados.
  - ✓ Establecer la opción de cifrado en la memoria de almacenamiento de los dispositivos móviles.

- ✓ Activar la opción de borrado remoto de información en los dispositivos móviles institucionales y realizar una restauración de fábrica remotamente, en los casos que sea posible.

- **Almacén General:** Solicitar a la Administración de Servicios Informáticos la configuración inicial de los dispositivos móviles que lleguen directamente al almacén general.

Directrices

1. Configuración de dispositivos móviles

- No se deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

- No se permite la instalación de software desde fuentes desconocidas.

- Cada vez que el sistema operativo de los dispositivos móviles institucionales notifique que existe una actualización disponible, se debe aceptar y aplicar dicha actualización.

2. Uso de Dispositivos Móviles

- Los dispositivos móviles institucionales no deben ser conectados a redes inalámbricas o equipos de cómputo públicos que no tengan ningún tipo de seguridad.

- Cuando sea necesario retirar un computador portátil de la Universidad, es necesario tramitar la salida del equipo ante Gestión de Servicios Institucionales.

- En caso de pérdida de un dispositivo móvil institucional, el responsable del mismo deberá notificar al Jefe inmediato, Centro de Soluciones y a Gestión de Servicios Institucionales.

- Los dispositivos móviles institucionales deben ser usados exclusivamente para labores institucionales y sistemas operativos y software totalmente licenciados.

CORREO ELECTRÓNICO INSTITUCIONAL.

Declaración Institucional

Se aplica para la creación, uso o eliminación de las cuentas de correo electrónico institucional.

Objetivo

Definir las reglas para la creación, uso y eliminación de las cuentas de correo electrónico institucionales.

Alcance

Las disposiciones contenidas en la presente directriz serán aplicables a todos los usuarios de correo electrónico de la Universidad.

Se entiende por usuario de correo electrónico de la Universidad a:

- Servidores públicos (docentes y administrativos planta) y trabajadores oficiales de la Universidad.
- Administrativos y docentes transitorios.
- Docentes de hora cátedra.
- Personal ocasional por proyecto.
- Contratistas (con previa solicitud por escrito del supervisor o interventor)
- Estudiantes de pregrado y posgrado.
- Egresados.
- Jubilados y pensionados.
- Estudiantes en práctica de otras instituciones.

Responsabilidad

- **Comité del Sistema Integral de Gestión:** revisar y aprobar los cambios que requiera la presente directriz.
- **Grupo Técnico para el Sistema de Gestión de Seguridad de la Información:** recomendar ajustes a la presente directriz, respecto al uso del correo electrónico institucional.
- **Jefes de dependencia o área:** Socializar e implementar la presente directriz en su área.
- **Personal que labora o presta servicios y terceros:** Aplicar la presente directriz.

Directrices

1. Disposiciones generales

- Todos los usuarios que hacen parte de la comunidad universitaria, deben tener correo electrónico institucional.

- La cuenta de correo electrónico es personal e intransferible.

- El correo electrónico institucional será el correo oficial de contacto para la Universidad Tecnológica de Pereira; razón por la cual, la información emitida por la institución será comunicada a los usuarios a través de este medio.

- El usuario asignado para acceder a los diversos sistemas de información de la institución será el mismo usuario para el correo electrónico.

- Si un egresado, jubilado o pensionado requiere la eliminación de la cuenta de correo institucional se debe enviar la solicitud a la dependencia Administración de Redes y Seguridad de la Información siguiendo el procedimiento para la eliminación de cuentas de correo para Egresados, pensionados y jubilados. Es de aclarar que solo se eliminará el servicio de correo electrónico, el usuario y sus credenciales seguirán existiendo en el sistema de autenticación de la universidad administrado por Gestión de Tecnologías Informáticas y Sistemas de Información.

- Los parámetros para asignar el nombre de usuario y contraseña, se documentará en el procedimiento (Administración de servicio correo electrónico, aplicaciones google, recursos IPy dominio) que será realizado por la Administración de Redes y Seguridad de la Información.

- El correo estará activo siempre y cuando el usuario se encuentre vinculado a la institución.

- Se exceptúa de la disposición establecida en el punto anterior, a las cuentas de correo institucional de los egresados, el personal jubilado y pensionado de la Universidad las cuales estarán activas por un periodo indefinido.

- La Administración de Redes y Seguridad de la Información bloqueará las cuentas de correo electrónico a través de las cuales se infrinja alguno de los puntos de esta directriz.

- Todos los usuarios tienen el deber de denunciar ante la Administración de Redes y Seguridad de

la Información a los usuarios que violen las directrices.

- Cada usuario será responsable de generar la copia de seguridad de sus mensajes de correo electrónico.

2. Uso del correo electrónico

- La clave de acceso asignada es personal y no debe ser divulgada, en razón a que los usuarios son responsables por la información que se envíe o divulgue a través de su correo electrónico y de los trámites o acciones realizadas en los portales y aplicativos a los cuales tiene acceso.

- En el caso del personal administrativo (planta y transitorios), docentes (planta, transitorio, cátedra), contratistas y personal ocasional de proyectos deberán utilizar el correo electrónico para fines académicos o laborales acorde a las funciones y responsabilidades de su cargo. El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo institucional y no se debe emplear para uso personal.

- En caso de acceso no autorizado por parte de terceros a su cuenta de correo institucional el usuario se compromete a notificar a la Administración de Redes y Seguridad de la Información.

- El envío de correos masivos estará regulado por las políticas de envío del proveedor de servicios de correo.

- Para evitar que se incluyan en la firma cualquier tipo de información no institucional (logos, frases, emoticones, entre otros), se debe hacer uso del generador de firmas de correo electrónico suministrado por Recursos Informáticos y Educativos. https://crie.utp.edu.co/crie/firma.html.

- Se debe excluir de los correos toda presentación de fondos personales y predeterminados no institucionales.

- La información que se envíe a través del correo electrónico, no podrá vulnerar derechos humanos ni contener datos contrarios a la moral, al buen nombre y las buenas costumbres.

- Se debeimplementarel uso de la opción concopiaoculta“CCOo BCC” cuando se realice envíos a más de cinco cuentas de correo electrónicos.

3. Se restringe

- El envío de material gráfico con contenido pornográfico o cualquier otro contenido sexual a través de los correos institucionales.

- Las amenazas a personas naturales y jurídicas o la organización de actos violentos. Al igual que la planificación, promoción y celebración de acciones que provoquen pérdidas financieras a terceros, incluidos los robos y los actos de vandalismo.

- El envío de mensajes acosadores o que contengan lenguaje ofensivo, resulte intimidatorio, incite al odio o a la discriminación de personas.

- La lectura de correos ajenos, generación o envío de correos electrónicos a nombre de otra persona sin autorización o suplantándola.

- La trasmisión de malware, programas de uso mal intencionado o introducción de software malicioso en la red o en los servidores.

- El envío de correos con material publicitario o cualquier otro tipo de anuncio comercial que no sea institucional.

4. Suspensión del correo Institucional

- Se suspenderán los correos electrónicos a los contratistas cuando el supervisor solicite la suspensión o si transcurridos 3 meses y no se ha renovado el contrato.

- Cuando se infrinjan las directrices del uso de correo electrónico, se suspenderá hasta que sea aclarado el motivo de la infracción por parte del propietario de la cuenta.

4.1 Cuentas de correo de estudiantes de pregrado y postgrado

El correo institucional de los estudiantes se suspenderá en algunas de las siguientes situaciones:

- Si el estudiante es expulsado definitivamente de acuerdo al reglamento estudiantil.

- Si el estudiante no se matricula por más de dos semestres académicos consecutivos.

5. Casos Especiales

- Si una dependencia académica o administrativa requiere una cuenta de correo adicional cuya finalidad sea estricta y explícitamente académica o laboral, se creará un "grupo" y se asociará a la cuenta de correo del solicitante o las que se determinen. Este "grupo" deberá ser solicitado por escrito o a través del correo electrónico por parte del jefe de dependencia u ordenador del gasto.
  Grupo: Se crea como una dirección de correo electrónico, a la cual tendrán acceso las cuentas de correo asociadas a este. Permite manejar bandeja de entrada de uso compartido. Dicho "grupo" no tiene asociada una clave de acceso.

- Para las listas de distribución también se utilizará el "grupo", el cual deberá ser solicitado por escrito o a través del correo electrónico por parte del jefe de dependencia u ordenador del gasto.

- Si actualmente un empleado administrativo (planta y transitorio), empleado docente (planta, transitorio, cátedra) no posee correo electrónico institucional debe tramitar la apertura de su cuenta con la Administración de Redes y Seguridad de la Información presentando su documento de identidad.

- El usuario del correo electrónico se cambiará únicamente cuando se demuestre que atenta contra la integridad y buen nombre de la persona, en tal caso el usuario se debe acercar con su documento de identidad a la Administración de Redes y Seguridad de la Información.

<u>CONTROL DE ACCESO.</u>

Declaración Institucional

Los activos de información contemplados en el alcance del Sistema de Gestión de Seguridad de la Información deben ser controlados de una manera adecuada permitiendo o restringiendo el acceso a los mismos según sea el caso. Con estas directrices se pretende que la información solo sea administrada por las personas adecuadas y definir los niveles de acceso.

Objetivo

Proteger los activos de información con el fin de controlar el acceso, modificación o divulgación no autorizada.

Alcance

Estas directrices deben ser aplicadas por los procesos que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información.

Cuando en esta directriz se emplee la palabra "usuario" se refiere a:

- Servidores públicos (docentes y administrativos planta) y trabajadores oficiales de la Universidad.
- Administrativos y docentes transitorios.
- Docentes de hora cátedra.
- Personal ocasional por proyecto.
- Contratistas (con previa solicitud por escrito del supervisor o interventor)
- Estudiantes de pregrado y posgrado.
- Egresados.
- Jubilados y pensionados.
- Estudiantes en práctica de otras instituciones.

Responsabilidad

- **Comité del Sistema Integral de Gestión:** Revisar y aprobar los cambios que requiera la presente directriz.
- **Grupo Técnico de Gestión de Seguridad de la Información:** Recomendar ajustes a la presente directriz.
- **Jefe de dependencia o área:** Definir los roles y los cargos que desempeñarán, así como los niveles de acceso a los activos de información que serán administrados haciendo revisiones periódicas.
- **Personal que labora o presta servicios:** Salvaguardar su información de ingreso a los diferentes sistemas (usuario y clave) y no difundir la información a la cual tienen acceso y haya sido restringida al público en general.
- **Recursos Informáticos y Educativos y Gestión de Tecnologías Informáticas Y Sistemas de Información:** Son responsables de administrar la infraestructura y herramientas necesarias para implementar el control de acceso a los activos de información.

Directrices

1. Usuarios

- Deben tener asignado un usuario y una clave que le permitirá ingresar a las aplicaciones que requieran.

- La creación de las cuentas de usuario se realizará desde las áreas que efectúan tareas de contratación o vinculación de usuarios de algún tipo.

- La estructura de la cuenta de usuario y el tiempo de vigencia, están definidas en la directriz de creación de cuentas de correo electrónico.

2. Claves

- Cada usuario debe contar con una clave para el ingreso a los servicios institucionales.

- La complejidad de las claves están definidas en el procedimiento control de acceso.

3. Generales

- Todo usuario que haga uso de los servicios institucionales debe identificarse con una cuenta y una clave intransferible, con el fin de garantizar el acceso a la información pertinente a sus labores.

- Se deben administrar los roles según requerimientos de los jefes de proceso cuando un usuario cambie de labores, ya sea en su mismo proceso o pase a realizar otras funciones en otra área.

- Las aplicaciones deben diseñarse teniendo en cuenta los activos de información y el acceso que requieran, para esto se deben definir los diferentes roles del sistema y las acciones que se podrán o no ejecutar con cada uno de ellos.

- Un usuario podrá pertenecer a diferentes roles siempre y cuando el jefe de dependencia o área, dueño del activo de información afectado por el rol así lo apruebe.

- Los servicios institucionales deben contar con mecanismos que permitan un cierre de sesión a aquellos usuarios que dejen inactiva su terminal después de un determinado tiempo.

- Cada usuario será responsable de la información que tenga bajo su cargo.

ACCESO A REDES Y A SERVICIOS EN RED.

Declaración Institucional

Los diferentes recursos de red contemplados en el alcance del Sistema de Gestión de Seguridad de la Información deben ser controlados de una manera adecuada permitiendo o restringiendo el acceso a los mismos según sea el caso.

Objetivo

Proteger de accesos no autorizados las diferentes redes y sus servicios, brindando así un entorno de trabajo confiable y con un alto nivel de disponibilidad.

Alcance

Estas directrices deben ser aplicadas por los procesos del alcance del Sistema de Gestión de Seguridad de la Información.

Cuando en esta directriz se emplee la palabra "usuario" se refiere a:

- Servidores públicos (docentes y administrativos planta) y trabajadores oficiales de la Universidad.
- Administrativos y docentes transitorios.
- Docentes de hora cátedra.
- Personal ocasional por proyecto.
- Contratistas (con previa solicitud por escrito del supervisor o interventor)
- Estudiantes de pregrado y posgrado.
- Egresados.
- Jubilados y pensionados.
- Estudiantes en práctica de otras instituciones.

Responsabilidad

- **Comité del Sistema Integral de Gestión:** Revisar y aprobar los cambios que requiera la presente directriz.
- **Personal que labora o presta servicios:** Hacer un uso adecuado de la infraestructura de red y de la información que intercambian con terceros.
- **Administración de Redes y Seguridad de la Información:** Administrar la infraestructura de redes velando por un adecuado funcionamiento.

Directrices

1. Se deben prevenir y controlar el acceso no autorizado a los recursos de red mediante la implementación de políticas y equipos de seguridad.

2. La red debe estar segmentada según la arquitectura de red definida por el área de Recursos Informáticos y Educativos para controlar el acceso a la información.

3. Si los usuarios requieren acceso desde fuera de la Universidad a los sistemas que no están públicos, el jefe de cada dependencia deberá gestionar ante Recursos Informáticos y Educativos el permiso de acceso y se habilitará su usuario para ingreso por VPN.

4. Todos los visitantes deberán estar aislados de la red institucional, si requieren acceso a algún servicio institucional, deben gestionar un permiso ante Recursos Informáticos y Educativos que les proporcionará el acceso adecuado según el requerimiento.

5. Se debe contar con equipos de seguridad perimetral tanto en el ámbito externo como interno para mitigar posibles ataques o intrusiones a la red.

6. Los canales de comunicación con entidades externas se realizarán siempre y cuando exista un documento para el manejo de la información (en cumplimiento de las normas legales vigentes) y se haya llegado a un acuerdo en los parámetros de comunicación.

7. Se deben identificar y administrar los puertos de acceso a los diferentes servicios informáticos con el fin de restringir el acceso solo a los servicios requeridos.

8. Se deben cambiar los puertos por defecto de los servicios de administración y gestión de redes cuando técnicamente sea posible realizarlo.

9. Se debe emplear un sistema de monitoreo tanto a nivel de redes como de servicios mediante herramientas y protocolos orientados a este fin.

10. El cableado que compone la red debe estar debidamente etiquetado, identificado y actualizado tanto a nivel físico como a nivel lógico, independientemente de la herramienta que se utilice.

11. Se debe contar con un sistema de registro de eventos donde se evidencie las accionesrealizadas en un momento determinado.

12. Servicios como voz sobre IP y video en streaming deben contar con la configuración de calidad de servicio.

USO DE CONTROLES CRIPTOGRÁFICOS

Declaración Institucional

Los activos de información contemplados en el alcance del Sistema de Gestión de Seguridad de la Información deben ser asegurados de una manera adecuada para su uso o intercambio con usuarios y terceros.

Objetivo

Proteger los activos de información y los medios por los cuales se transmiten o almacenan con el fin de evitar el acceso, la modificación o divulgación no autorizada.

Alcance

Estas directrices deben ser aplicadas por los procesos del alcance del Sistema de Gestión de Seguridad de la Información.

Cuando en esta directriz se emplee la palabra “usuario” se refiere a:

- Servidores públicos (docentes y administrativos planta) y trabajadores oficiales de la Universidad.
- Administrativos y docentes transitorios.
- Docentes de hora cátedra.
- Personal ocasional por proyecto.
- Contratistas (con previa solicitud por escrito del supervisor o interventor)
- Estudiantes de pregrado y posgrado.
- Egresados.
- Jubilados y pensionados.
- Estudiantes en práctica de otras instituciones.

Responsabilidad

- **Comité del Sistema Integral de Gestión:** Revisar y aprobar los cambios que requiera la presente directriz.

- **Jefe de dependencia o área:** Definir cuándo y cuáles activos identificados como reservados requieren el cifrado al momento de almacenar o distribuir.
- **Personal que labora o presta servicios:** Hacer uso de los mecanismos de cifrado para proteger los activos que lo requieran.
- **Recursos Informáticos y Educativos** y **Gestión de Tecnologías Informáticas Y Sistemas de Información:** Implementar los algoritmos de cifrado en servidores y canales de comunicación.

Directrices

Se deben usar algoritmos vigentes y seguros al momento de hacer uso de cifrado de información o comunicaciones.

1. Cualquier acceso que implique digitar clave o usuario debe estar cifrado.

2. Las comunicaciones o la transferencia de información que no sea de destino público y cuyo contenido esté identificado como restringido, debe ser protegido por mecanismos de cifrado.

3. Se deben emplear técnicas de criptografía para controlar la integridad de los mensajes que se transmiten en medios seguros.

4. La información que no sea pública, se debe almacenar cifrada para prevenir el acceso no autorizado a la misma.

5. Los equipos que contengan información sensible y constantemente salgan del perímetro de control de la Universidad, deben tener su información cifrada.

PANTALLAS, ESCRITORIOS LIMPIOS Y EQUIPOS DESATENDIDOS.

Declaración Institucional

Se aplica para la protección de la información que ha sido identificada como pública, clasificada o reservada que se encuentre en cualquier medio de conservación (Físico o digital) y que pueden estar dispuestas en los escritorios, estaciones de trabajo, computadores, medios removibles, documentos en papel y que pueden ser utilizados por personal autorizado que labora o presta servicios en la Institución en el desempeño de sus funciones o actividades en la Universidad Tecnológica de Pereira.

La declaración define como buena práctica mantener las pantallas y escritorios limpios y ordenados reduciendo el riesgo de que información sensible pueda ser dañada, deteriorada, extraviada o conocida por personas no acreditadas; asegurando de este modo la protección debida a la misma, que garantiza su confidencialidad, integridad y disponibilidad.

Objetivo

Reducir los riesgos potenciales de acceso no autorizado, pérdida o daño de la información y que son asociados al accionar cotidiano, ya sea de manera accidental o intencionada.

Alcance

La presente directriz debe ser aplicada por todos los usuarios de la Universidad Tecnológica de Pereira y que tiene acceso a información o a sus sistemas de información.

Aplica para computadores donde se procese información, papeles y medios de almacenamiento removibles.

Cuando en esta directriz se emplee la palabra “usuario” se refiere a:

- Servidores públicos (docentes y administrativos planta) y trabajadores oficiales de la Universidad.
- Administrativos y docentes transitorios.
- Docentes de hora cátedra.
- Personal ocasional por proyecto.
- Contratistas (con previa solicitud por escrito del supervisor o interventor)
- Estudiantes de pregrado y posgrado.
- Egresados.
- Jubilados y pensionados.
- Estudiantes en práctica de otras instituciones.

Responsabilidad

- **Comité del Sistema Integral de Gestión:** Revisar y aprobar los cambios que requiera la presente directriz.
- **Grupo Técnico para el Sistema de Gestión de Seguridad de la Información:** Recomendar ajustes a la presente directriz respecto a cómo tratar la información que se maneja en los escritorios y pantallas del personal que labora o presta los servicios en la Universidad.
- **Jefe de dependencia o área:** Son responsables de socializar e implementar la directriz de escritorio y pantalla limpia en su proceso.

- **Personal que labora o presta servicios:** Son responsables de aplicar la presente directriz; así mismo, mientras tengan la información bajo su control, de mantener los niveles de protección y clasificación establecidos para la misma haciendo uso adecuado de los recursos puestos a su disposición. De igual manera, son responsables de identificar y tratar los riesgos asociados respecto a disponer la información en su puesto de trabajo.

Directrices

1. Ubicación de escritorios y pantallas.

- Las oficinas deben contar con restricción de acceso, que impidan la entrada a personas externas o no autorizadas.
- Las estaciones de trabajo del personal que labora o que presta sus servicios deben localizarse preferiblemente en ubicaciones donde no queden expuestas al acceso de personal no autorizado.

- Los equipos que queden ubicados cerca a zonas de atención al público o tránsito de personas, deberán ubicarse o protegerse de tal forma que las pantallas no puedan ser visualizadas por personas no autorizadas.

2. Escritorios limpios

- El personal que labora o presta sus servicios en la Universidad debe conservar su escritorio libre de información propia de la Institución, con el fin de evitar que personal no autorizado tenga acceso a la misma, pudiéndola conocer, reproducir o utilizar para fines diferentes a los de la Entidad.

- Los medios removibles de almacenamiento deberán ser adecuadamente protegidos, teniendo presente que se deben guardar en los cajones bajo llave, en todo momento que no estén siendo utilizados.

- Los documentos con información identificada como clasificada o reservada, deben ser protegidos de tal forma que no sean de fácil acceso o dejados a la vista. Cuando la persona responsable de la información se ausente de su lugar de trabajo, debe guardar cualquier documento que contenga información sensible.

- No se deben publicar ni dejar a la vista los siguientes datos sensibles:

  - Nombres de usuario y contraseñas (Password)
  - Números de cuenta
  - Datos de personas con los que la Universidad tenga relación académica, laboral, contractual u otras.
  - Propiedad intelectual.
  - Documentos de carácter contractual o legal.

- Los usuarios de los equipos, al terminar sus tareas de oficina, debe asegurarse de:

  - Recoger y guardar en lugar seguro el material con información sensible o cuyo contenido se haya identificado como clasificado o reservado.
  - Cerrar bajo llave los gabinetes, cajones y escritorios que contengan documentos o medios removibles con información de uso interno.
  - Guardar las llaves de gabinetes, cajones y escritorios en un lugar seguro.
  - Asegurar los equipos portátiles.

3. Equipos desatendidos

- Los responsables de computadores y portátiles deberán asegurarse de mantener el control cuando no se encuentre frente a ellos, para lo cual deben bloquear la sesión de usuario cuando se aleje de su estación de trabajo, ya sea por poco tiempo, con el fin de proteger el acceso a las aplicaciones y a la información.

- La Universidad establecerá el bloqueo automático de sesión a los computadores y portátiles, que deberá activarse ante un tiempo determinado sin uso (5 minutos). Esta acción es un complemento al deber del usuario de bloquear la sesión.

- La Universidad establecerá el modo de hibernación de los PC, después de un tiempo determinado sin uso (30 minutos). Después del cual se apagará la pantalla y el equipo pasará a ahorro de energía.

- Para las tabletas u otros dispositivos similares de propiedad de la Universidad, el usuario deberá asegurarse de mantener bloqueado el acceso, cuando no lo esté utilizando.

- Siempre que la pantalla se encuentre bloqueada el usuario debe autenticarse mediante usuario y contraseña para ingresar al equipo.

- Los usuarios de los equipos, al terminar sus tareas de oficina, debe asegurarse de apagar los computadores y no solo limitarse a apagar la pantalla.

- Cuando medie autorización por superior inmediato para la conexión de escritorio remoto, el personal podrá dejar su computador encendido fuera de las horas laborales; sin embargo, deberá tener presente apagar la pantalla y bloquear la sesión.

4. Pantalla limpia

- El usuario de los equipos no debe almacenar documentos con información identificada como clasificada o reservada o que contenga datos sensibles en el escritorio (pantalla inicial) de su computador; por lo cual deberá crear carpetas con los respectivos controles de seguridad que se requieran.

5. Equipos de reproducción de información

- Los equipos de reproducción de información (Impresoras, escáner o fotocopiadoras) deben ser ubicados en sitios con acceso controlado.

- Al momento de reproducir documentos con información identificada como clasificada o sensible deberá ser retirada inmediatamente de los equipos de copiado (impresoras, escáner, equipos de fax).

- No se deben utilizar fotocopiadoras, escáneres, equipos de fax y en general equipos tecnológicos que se encuentren desatendidos.

6. Salas y tableros limpios

- Las salas o lugares donde se lleven a cabo reuniones, conferencias o capacitaciones, deben quedar limpios, por lo cual el responsable de la citación debe recoger y disponer de manera segura el material impreso utilizado.

- Los tableros de las salas o lugares de reuniones, conferencias o capacitaciones deben ser borrados una vez termine el evento realizado. Se debe asegurar que no quede expuesta información que se haya escrito en ellos.

- En caso de que se utilice un computador o portátil de uso común para proyección de información o registro de la misma, el responsable de la información debe asegurarse de eliminar los archivos correspondientes, teniendo en cuenta borrarlos de la papelera de reciclaje.

- Se debe cerrar la sesión de los aplicativos o cuentas de correo electrónico que haya utilizado en el computador o portátil de uso común.

- Los equipos utilizados deben ser apagados, junto con sus pantallas.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO.

Declaración Institucional

Se proporcionarán los mecanismos necesarios que mejoren la protección a los equipos de cómputo ante posibles contagios de software malicioso que puedan afectar (divulgar, dañar parcial o totalmente) la información identificada como publica, clasificada o reservada, por lo cual se deben establecer medidas para evitar dicho contagio.

Objetivo

Reducir el riesgo de contagio de software malicioso en los equipos de cómputo.

Alcance

La presente directriz debe ser aplicada por el personal que labora, presta servicios y terceros de la Universidad Tecnológica de Pereira.

Responsabilidades

- **Comité del Sistema Integral de Gestión:** Revisar y aprobar los cambios que requiera la presente directriz.
- **Grupo Técnico para el Sistema de Gestión de Seguridad de la Información:** Recomendar ajustes a la presente directriz.

- **Jefe de dependencia o área:** Son responsables de socializar e implementar la presente directriz en su proceso.
- **Personal que labora, presta servicios y terceros:** Son responsables de aplicar la presente directriz; así mismo, mientras tengan la información bajo su control, de mantener los niveles de protección y clasificación establecidos para la misma haciendo uso adecuado de los recursos puestos a su disposición.
- **Administración de Servicios Informáticos:** Es responsable de proveer e instalar las herramientas necesarias como antivirus, antimalware, antispyware y antispam que permitan reducir el riesgo de contagio de software malicioso en los equipos de cómputo, como también de garantizar que dichas herramientas cuenten con su licencia de funcionamiento y la disponibilidad de actualización tanto del software como de sus bases de datos.

Directrices

1. **Instalación, configuración y modificación de software de los equipos de cómputo**

- Solo se instalará en los equipos de cómputo el software provisto por la oficina de Administración de Servicios Informáticos, quienes serán los únicos autorizados para instalarlo, modificarlo o actualizarlo.

- Los sistemas operativos instalados en los equipos de cómputo que pertenezcan a la Universidad Tecnológica de Pereira deben tener instalados los parches y las últimas actualizaciones para bloquear las vulnerabilidades de seguridad conocidas.

- El personal que labora, presta servicios y terceros no podrán cambiar o eliminar la configuración del software antivirus, antispyware, antimalware y antispam, por lo tanto, solo podrán realizar tareas de escaneo.

2. **Instalación, configuración y modificación de software de servidores**

La seguridad ante el contagio de software de código malicioso en los servidores se hará a través de los dispositivos de seguridad perimetral que posea la Universidad Tecnológica de Pereira.

3. **Manejo del software contra código malicioso**

- El personal que labora, presta servicios y terceros que sospechen o detecten alguna infección

por software malicioso deben intentar erradicarlo con las herramientas instaladas para tal fin; en caso de no lograrlo debe comunicarse al Centro de Soluciones para su detección y eliminación.

- El software de antivirus, antimalware, antispyware debe utilizarse para examinar los medios de almacenamientos antes de realizar el intercambio de información.

- Los archivos adjuntos en los correos electrónicos deben ser analizados en busca de algún tipo de software malicioso.

RESPALDO DE LA INFORMACIÓN.

Declaración Institucional

Se debe garantizar el respaldo de la información identificada como pública, clasificada o reservada, estableciendo procedimientos y mecanismos necesarios para generar copias de respaldo de dicha información.

Estas directrices definen unas buenas prácticas para la administración de copias de respaldo de los sistemas de información y servidores de la Universidad Tecnológica de Pereira, como también de la información almacenada en computadores de escritorio de los usuarios.

Objetivo

Reducir el riesgo de la pérdida de información identificada como clasificada o reservada de los sistemas de información, servidores y equipos de cómputo de usuarios.

Alcance

Estas directrices serán aplicadas por Gestión de Tecnologías Informáticas y Sistemas de Información y por Recursos Informáticos y Educativos, con respecto a administrar los sistemas de información y servidores. Así mismo serán aplicadas por el personal que labora, presta servicios y terceros en relación a los equipos de cómputo que están a su cargo.

Cuando en esta directriz se emplee la palabra “usuario” se refiere a:

- Servidores públicos (docentes y administrativos planta) y trabajadores oficiales de la Universidad.

- Administrativos y docentes transitorios.
- Docentes de hora cátedra.
- Personal ocasional por proyecto.
- Contratistas (con previa solicitud por escrito del supervisor o interventor)
- Estudiantes de pregrado y posgrado.
- Egresados.
- Jubilados y pensionados.
- Estudiantes en práctica de otras instituciones.

Responsabilidad

- **Comité del Sistema Integral de Gestión:** Revisar y aprobar los cambios que requiera la presente directriz.

- **Grupo Técnico para el Sistema de Gestión de Seguridad de la Información:** Recomendar ajustes al presente directriz respecto a cómo tratar las copias de respaldo de los servidores y de los equipos de cómputo de la Universidad.

- **Jefe de dependencia o área:** Socializar e implementar la presente directriz en su proceso.

- **Personal que labora o presta servicios:** Aplicar la presente directriz; así mismo, mientras tengan la información bajo su control, de mantener los niveles de protección y clasificación establecidos para la misma haciendo uso adecuado de los recursos puestos a su disposición. Así como también serán responsables de realizar las copias de respaldo de la información identificada como pública, clasificada o reservada que estén bajo su responsabilidad.

- **Recursos Informáticos y Educativos** y **Gestión de Tecnologías Informáticas Y Sistemas de Información:** Realizar las copias de respaldo de los sistemas de información y servidores que estén a su cargo.

Directrices

1. **Copias de respaldo para sistemas de información y servidores.**

- Se debe contar con un sistema de generación de copias de respaldo (en disco, en cintas, almacenamiento en la nube), o en su defecto un procedimiento el cual permita crear,

salvaguardar y recuperar copias de respaldo de los datos de los sistemas de información y servidores.

- Se podrá respaldar los datos sensibles de los sistemas de información y servidores en medios de almacenamiento.

- Los archivos de configuración de servidores, servicios, bases de datos institucionales y código fuente de aplicaciones deben ser respaldados por lo menos una vez a la semana.

- Las copias de respaldo deberán estar claramente identificadas, con etiquetas que indiquen como mínimo a que sistema de información o servidor pertenece, fecha y hora de la realización de la copia.

- Las copias de respaldo deben estar almacenadas en un área con control de acceso físico y ambiental.

- Las copias de respaldo se deberán almacenar dentro de la universidad y en un lugar remoto (físico o lógico).

- El administrador del sistema de información o servidor definirá cual va a hacer el tiempo de retención de la copia de respaldo, la cual debe ser mínimo un mes.

- Se deben efectuar pruebas de recuperación de datos por lo menos una vez cada semestre, esto con el fin de verificar la integridad de los datos almacenados en dicha copia de respaldo.

- Los medios de almacenamiento que contengan copias de respaldo y vayan a ser eliminados deben pasar por un proceso de borrado seguro y posterior eliminación o destrucción.

2. Copia de respaldo para el personal que labora, presta servicios y terceros.

- Las copias de respaldo se deberán guardar en un lugar que cuente con algún tipo de control de acceso, acorde a la directriz de escritorio y pantalla limpia.

- El personal administrativo (planta y transitorios), docente (planta, transitorio, catedra) serán los responsables de la disponibilidad e integridad de las copias de respaldo.

TRANSFERENCIA DE INFORMACIÓN.

Declaración Institucional

El intercambio de información entre áreas, entidades o personas externas contempladas en el alcance del Sistema de Gestión de Seguridad de la Información debe garantizar que se cumpla con los criterios de disponibilidad, confidencialidad e integridad.

Objetivo

Definir las directrices y procedimientos para el intercambio de información entre las áreas del alcance del sistema de Gestión de la Seguridad de la Información y cualquier otra entidad o persona externa con la cual se tenga alguna relación.

Alcance

Estas directrices deben ser aplicadas por los procesos del alcance del Sistema de Gestión de Seguridad de la Información.

Responsabilidad

- **Comité del Sistema Integral de Gestión:** Revisar y aprobar los cambios que requiera la presente directriz.
- **Jefes de los procesos de Recursos Informáticos y Educativos** y **Gestión de Tecnologías Informáticas** y **Sistemas de Información:** Definir y hacer cumplir los procedimientos de intercambio de información.
- **Entidades Externas:** Cumplir los procedimientos de intercambio de información y su uso.
- **Recursos Informáticos y Educativos** y **Gestión de Gestión de Tecnologías Informáticas** y **Sistemas de Información:** Implementa las herramientas necesarias para asegurar el intercambio de información y definirán o participarán en la definición de los documentos de intercambio de información con tercero en base a la necesidad

Directrices

1. Para que se pueda realizar el intercambio de información debe existir un documento de aceptación de las políticas de seguridad y uso adecuado de información entre las partes que garantice la disponibilidad, confidencialidad e integridad.

2. Los terceros, con excepción de entidades gubernamentales, deberán firmar las cláusulas de confidencialidad que se adecuarán al documento.

3. Para el intercambio de información establecida por ley con entidades gubernamentales, se debe registrar la norma que aplique y un documento formal de trabajo que se realizará en conjunto para tal fin, en el cual se deben definir los mecanismos o protocolos a usar.
4. Para el intercambio de información sensible, se deben emplear controles criptográficos. (Ver directriz de Controles Criptográficos)

5. La Secretaría General reportará ante la Súper Intendencia de Industria y Comercio (SIC), al tercero que incumpla los acuerdos de uso de la información que le fue suministrada.

6. Se deberán seguir las normas y lineamientos definidos por GTISI en referencia al desarrollo de software para intercambio de información de aplicativos con terceros.

DESARROLLO SEGURO DE SOFTWARE

Declaración Institucional

El desarrollo de software contemplado en el alcance del Sistema de Gestión de Seguridad de la Información debe garantizar que los aplicativos cumplan con los requerimientos de los usuarios, con una arquitectura que permita un sistema unificado, flexible, robusto y cumpla con los atributos de calidad que cada sistema o subsistema amerite.

Objetivo

Definir las directrices para el desarrollo de software institucional que garanticen el cumplimiento de las necesidades de los usuarios, con criterios de calidad del producto, tiempos justos y garantizando los principios de seguridad de la información.

Alcance

Estas directrices deben ser aplicadas por los procesos del alcance del Sistema de Gestión de Seguridad de la Información.

Responsabilidad

- **Comité del Sistema Integral de Gestión:** revisar los cambios que requiera la presente directriz.

- **Jefes de proceso de Recursos Informáticos y Educativos** y **Gestión de Tecnologías Informáticas y Sistemas de Información:** Definir y hacer cumplir las normas, lineamientos, procedimientos de desarrollo y soporte de aplicaciones.
- **Usuarios de las aplicaciones:** Informar de cualquier anormalidad en el manejo de losaplicativos que afecten la prestación correcta del servicio al centro de soporte. También pueden realizar solicitudes de petición de cambios (RFC).
- **Recursos Informáticos y Educativos** y **Gestión de Tecnologías Informáticas y Sistemas de Información:** Serán las encargadas de definir las normas, lineamientos, procedimientos, parámetros generales y estándares en tecnologías en el desarrollo de aplicaciones institucionales (desarrollo interno o contratado con un tercero), velando por el cumplimiento de la ley, disposiciones internas y teniendo siempre presente la seguridad de la información.
- **Gestión de Tecnologías Informáticas y Sistemas de Información:** Desarrollar o contratar con terceros para mantener los aplicativos que requieran los usuarios en base a una programación de necesidades a ser resueltas.
- **Recursos informáticos y educativos**: Debe definir las normas y directrices para desarrollo de páginas web relacionadas con el portal web institucional conservando la identidad, imagen, presentación, estilo y marca Universidad.

Directrices

1. Todo desarrollo de software de misión institucional, ya sea interno o a través de un tercero, debe cumplir con las normas de desarrollo definidas por GTISI.

2. Todas las aplicaciones de misión institucional deben están alojadas en el centro de datos o donde lo defina el área encargada.

3. Se deben tener dos ambientes: producción y desarrollo.

4. Se deben implementar planes de capacitación en herramientas de desarrollo y paradigmas de innovación tecnológica.

5. Los aplicativos que manejen información sensible deben implementar sistema de auditorías.

6. Todo el software usado en el desarrollo de aplicaciones debe estar licenciado o contar con la debida autorización del proveedor.

7. Se deben tener acuerdos de licencias o propiedad de código o cesión de derechos de propiedad intelectual con las empresas y personal que desarrollen software para la Universidad.

8. La interconexión con sistemas internos o externos deberá cumplir con los criterios de confidencialidad, integridad y disponibilidad, además de definir los niveles de acuerdo del servicio.

9. Todas las aplicaciones deben pasar por pruebas de seguridad, de las cuales se deben dejar registros o evidencias de las mismas.

RELACIONES CON TERCEROS Y EL PERSONAL QUE PRESTA SERVICIOS

Declaración Institucional

Se aplica para la protección de la información y de los sistemas de información y que pueden ser accedidos o utilizados por proveedores o terceros de la Institución en el cumplimiento de su objeto contractual o en el desarrollo de las actividades de su contrato.

La declaración define como buena práctica la existencia de un contrato y cláusulas de confidencialidad detalladas para los proveedores o terceros que especifiquen los niveles de riesgos asociados con el manejo de la información de propiedad de la Universidad, dado que los terceroso proveedores pueden llegar a manipular información clasificada o reservada o pueden adquirir conocimientos de la administración, infraestructura y salvaguarda de los sistemas de información.

Objetivo

Preservar la seguridad de la información a la cual tienen acceso los proveedores o terceros que prestan sus servicios a la Universidad Tecnológica de Pereira y que han sido debidamente autorizados.

Alcance

La presente directriz debe ser aplicada por los proveedores y terceros que tengan alguna relación con la Universidad Tecnológica de Pereira y que tiene acceso a su información o a sus sistemas de información.

Responsabilidad

- **Comité del Sistema Integral de Gestión:** Revisar y aprobar los cambios que requiera la presente directriz.
- **Grupo Técnico para el Sistema de Gestión de Seguridad de la Información:** Recomendar ajustes a la presente directriz cuando se presenten eventos que obliguen a su actualización.
- **Jefe de dependencia o área:** Son responsables de determinar el acceso a la información que requieran los proveedores o terceros. Además, evaluar y tratar los riesgos asociados en la contratación de servicios de procesamiento o manejo de información con proveedores y terceros.
- **Personal que labora o presta servicios:** Reportar a los interventores de los contratos las fallas en la prestación de servicios contratados con proveedores o terceros, en especial las relacionadas con el uso de la información.
- **Supervisores de contrato:** Hacer seguimiento, revisar y verificar la prestación del servicio contratado con los proveedores o terceros, sin perjuicio de las demás obligaciones que del contrato se deriven.
- **Terceros y personal que presta servicios:** Cumplir con las directrices de seguridad de la información establecidas por la Universidad. Así mismo, deberán asegurar de manerarazonable que se tomarán las medidas que garanticen la protección de la información que está a su disposición, manteniendo los niveles de protección y clasificación establecidos para lamisma.

Directrices

1. Condiciones generales

- Los terceros o el personal que presta servicios a la Universidad y que en función de su contrato requiera la administración, acceso, uso, procesamiento, almacenamiento o transmisión de información, deben conocer, aceptar y cumplir las políticas de seguridad de la información definidas en el Sistema de Gestión de Seguridad de la Información. Así mismo, deberán cumplir con la reglamentación en materia de derechos de autor y propiedad intelectual y los relacionados con la protección de datos personales.

- Se deberá concertar con los terceros o el personal que presta servicios los requisitos sobre la seguridad de la información; estos deberán ser documentados y formalizados antes del inicio del contrato e incluirán los niveles de servicios en seguridad de la información, en el que se detallen

los compromisos en el cuidado de la información y los sistemas de Información y las sanciones en caso de incumplimiento.

- En caso de conflicto entre las políticas de seguridad de la Información de la Universidad y las políticas de seguridad de los terceros, se acordarán políticas comunes y se formalizarán mediante un documento anexo al contrato, que permitan cumplir los requisitos necesarios para garantizar la protección de la confidencialidad, integridad y disponibilidad de la información.

- Los terceros o el personal que presta servicios solo debe tener acceso a la información, sistemas de información o instalaciones que son indispensables para el cumplimiento de sus objetos contractuales.

2. Gestión de la prestación de servicios

- Cada servicio contratado con un tercero deberá tener un interventor o supervisor encargado de hacer seguimiento, revisar y verificar el cumplimiento del objeto contractual.

- El cumplimiento de los niveles de servicios contratados para asuntos de seguridad de la información debe ser verificado y controlado permanentemente por quienes ejerzan las funciones de supervisión e interventoría.

- Se deberá dejar explicita la obligación de los interventores o supervisores relacionada con la seguridad de la información en los contratos que la Universidad suscriba con terceros o personal que presta servicios.

- Los cambios en la prestación de servicios por parte de terceros o personal que presta servicios, se gestionarán teniendo en cuenta los niveles de criticidad de la información, sistemas y procesos que intervienen y la valoración de los riesgos.

- Al finalizar sus contratos los terceros o el personal que presta servicios deberán efectuar la devolución de información o activos de información que estuvieron bajo su responsabilidad y que son propiedad de la Universidad. De igual manera, se deberá procurar la destrucción o borrado seguro de información clasificada o reservada conocida en razón de su actividad.

3. Usos no autorizados

- Los terceros o el personal que presta servicios no están autorizados para utilizar la información y los sistemas de información para fines diferentes a los requeridos en el cumplimiento del contrato suscrito con la Universidad.

- No están autorizados los cambios o modificaciones sobre la infraestructura, sistemas de información y comunicaciones, controles de seguridad de la Universidad sin contar con la autorización formal y expresa del responsable de GTYSI y Recursos Informáticos y Educativos según corresponda.

4. Tratamiento del riesgo dentro de acuerdos

- En el desarrollo de un contrato con un tercero o personal que presta servicios se deberá concertar los requisitos de seguridad de la información para la prevención y mitigación de los riesgos asociados con el acceso a los activos de información o el suministro de infraestructura tecnológica para los sistemas de información

- Los requisitos de seguridad de la información pertinentes serán establecidos y acordados con cada tercero o personal que presta servicios que pueda acceder, procesar, almacenar, comunicar, transferir o proporcionar los componentes de infraestructura de tecnología de información.

- Para el acceso a cualquier tipo de información o sistema de información, los terceros o el personal que presta servicios deberán suscribir acuerdos de confidencialidad los cuales estarán anexos a los contratos, con el fin reducir los riesgos de divulgación de información con carácter reservado y clasificado.
- En los contratos asociados con los servicios de tecnologías de información y comunicación y los relacionados con el suministro de productos o infraestructura requeridos para los sistemas de información o redes, se deberá tener en cuenta la identificación, análisis, valoración y tratamiento de los riesgos de seguridad de la información que implique la contratación.

PROTECCIÓN DE DATOS PERSONALES.

Declaración Institucional

Dar cumplimiento a lo dispuesto en la Ley estatutaria 1581 de 2012 y a su Decreto Reglamentario 1377 de 2013.

Objetivo

Establecer las directrices para garantizar la protección de los datos personales que han sido suministrados y que se han incorporado en distintas bases o bancos de datos, o en repositorios electrónicos de todo tipo con que cuenta la Universidad Tecnológica de Pereira, garantizando con ello, el derecho constitucional que tienen todas las personas a conocer, actualizar, rectificar y eliminar su información.

Alcance

La directriz de tratamiento de protección de datos personales aplica para todas las unidades organizacionales y titulares de la información.

Responsabilidad

- **Secretaria General:** Atender las peticiones, consultas y reclamos en relación con la protección de datos personales.
- **Comité del Sistema Integral de Gestión:** Revisar y aprobar los cambios que requiera la presente directriz.
- **Grupo Técnico de Gestión de Seguridad de la Información:** Recomendar ajustes a la presente directriz y apoyar a la Secretaria General en la atención a las peticiones, consultas y reclamos en relación con la protección de datos personales.
- **Jefe de dependencia o área:** Socializar e implementar la presente directriz en su área; apoyar a la Secretaria General en la atención a las peticiones, consultas y reclamos en relación con la protección de datos personales a su cargo; administrar y registrar ante la SIC las bases de datos o repositorios a su cargo que contengan datos personales.
- **Proyectos especiales:** Socializar e implementar la presente directriz en su área; apoyar a la Secretaria General en la atención a las peticiones, consultas y reclamos en relación con la protección de datos personales a su cargo; administrar y registrar ante la SIC las bases de datos o repositorios a su cargo que contengan datos personales
- **Personal que labora o presta servicios y terceros:** Aplicar la presente directriz y dar el uso adecuado a los datos personales que estén bajo su custodia, control y protección.

Principios

- **Legalidad:** el tratamiento de datos es una actividad regulada que debe sujetarse a lo establecido en la presente política, en la Ley 1581 de 2012 y en las demás disposiciones que ladesarrollen.
- **Finalidad:** El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.
- **Libertad:** El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
- **Veracidad y calidad:** La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- **Transparencia:** En el tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
- **Acceso y circulación restringida:** El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente política, Ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la Ley.
- **Seguridad:** La información sujeta a tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- **Confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la Ley.

Directrices

1. Información responsable de los datos personales

La UNIVERSIDAD TECNOLÓGICA DE PEREIRA identificada con NIT: 891.480.035-9, es una Institución de Educación Superior del orden nacional, con personería jurídica, autonomía administrativa y patrimonio independiente, adscrito al Ministerio de Educación Nacional.

Se encuentra ubicada en la carrera 27 # 10- 02 Los Álamos, código postal 660003, municipio de Pereira, Risaralda.

2. Canales habilitados para interponer peticiones, consultas y reclamos

Se dispondrá del correo electrónico datospersonales@utp.edu.co y la línea telefónica 3137517 para que los titulares de la información puedan interponer sus peticiones, consultas y reclamos; como realizar cualquier solicitud de actualización, rectificación y supresión de datos personales, de acuerdo a las directrices aquí descritas y las contenidas en la Ley 1581 de 2013 y las normas que lo modifiquen. Dichos canales serán administrados por la Secretaría General.

3. Derechos que le asisten al titular de la información

3.1 Derechos de los titulares de los datos personales tratados por la Universidad Tecnológica de Pereira.

a. Conocer, actualizar y rectificar en cualquier momento sus datos personales frente a la Universidad en su condición de responsable de tratamiento de datos. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

b. Solicitar prueba de la autorización otorgada a la Universidad Tecnológica de Pereira salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.

c. Ser informado por la Universidad Tecnológica de Pereira, previa solicitud, respecto del uso que les ha dado a sus datos personales.

d. Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente directriz o en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.

e. Revocar la autorización o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

f. Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

3.2 Derechos niños y adolescentes.

En el tratamiento de datos personales se asegurará el respeto a los derechos prevalentes de los menores[1]. La Universidad Tecnológica de Pereira, garantizará el tratamiento de los datos personales de niños, niñas y adolescentes, por lo cual deberá velar por el uso adecuado de los mismos, de acuerdo a lo contenido en esta política y lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013.

Queda proscrito el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.

Será posible de manera excepcional el tratamiento de datos personales de los niños, niñas y adolescentes cuando se cumplan los siguientes criterios:

a) La finalidad del tratamiento responda al interés superior de los niños, niñas y adolescentes
b) Se asegure el respeto de sus derechos fundamentales de los niños, niñas y adolescentes.
c) De acuerdo con la madurez del niño, niña o adolescente se tenga en cuenta su opinión.
d) Se cumpla con los requisitos previstos en la Ley 1581 de 2012 para el tratamiento de datos personales.

Los derechos de los niños, niñas o adolescentes en relación con el tratamiento de los datos personales se ejercerán por las personas que estén facultadas para representarlos.

La Universidad deberá proveer información o capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

3.3 Legitimación para el ejercicio del derecho del titular

Los derechos de los Titulares, podrán ejercerse por las siguientes personas:

a) Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición la Universidad Tecnológica de Pereira.
b) Por sus causahabientes, quienes deberán acreditar tal calidad.

[1]Corte Constitucional, Sentencia C-748 de 2011, Magistrado Ponente: Jorge IgnacioPreteltChaljub.

c) Por el representante o apoderado del Titular, previa acreditación de la representación o apoderamiento.
d) Por estipulación a favor de otro o para otro.

4 Generalidades del Tratamiento de los datos personales

4.1 Tratamiento y finalidad al cual serán sometidos los datos personales:

El tratamiento de los datos personales de estudiantes, aspirantes, graduados, egresados, profesores, empleados, ex empleados, jubilados, proveedores, contratistas, o de cualquier persona con la cual la Universidad tuviere establecida o estableciera una relación, permanente u ocasional, lo realizará en el marco legal que regula la materia y en virtud de su condición de Institución de Educación Superior, y serán todos los necesarios para el cumplimiento de la misión institucional.

En todo caso, los datos personales podrán ser recolectados, almacenados, usados, compartidos, procesados y dárseles tratamiento para los siguientes fines:

a) Desarrollar la legítima misión educativa conforme a los estatutos de la Universidad.
b) Cumplir las leyes aplicables a la educación pública en Colombia.
c) Realizar las gestiones necesarias para dar cumplimiento a las obligaciones inherentes a los servicios que presta la Universidad y que están enmarcados en su misión.
d) Realizar estudios estadísticos poblacionales con el fin de estandarizar e identificar posicionamiento de la Universidad y de los programas en el medio, sin el uso de los datos que identifiquen la persona.
e) Evaluar la calidad de los servicios prestados, calidad y pertinencia de programas académicos y proyectos especiales, entre otros, con miras al mejoramiento continuo de la Institución.
f) Realizar mercadeo de sus programas institucionales, incluyendo los académicos, de extensión e investigación.
g) Realizar mercadeo y venta de productos a través de diferentes canales.
h) Enviar información y comunicados sobre oferta educativa, de extensión, servicios, beneficios y noticias de la Universidad a los diferentes grupos de interés, así como invitaciones a eventos.
i) Fomentar la investigación en todos los campos incluyendo el científico.
j) Proteger los derechos de propiedad intelectual de la Universidad.
k) Prestar asistencia, servicio y soporte técnico de nuestros productos y servicios.
l) Realizar encuestas afines a la educación, y a los servicios administrativos, de extensión e investigación que presta la Universidad, a quienes voluntariamente quieran participar.
m) Desarrollar programas sociales conforme a los estatutos.
n) Determinar los perfiles genéticos y estudios de filiación, en el caso del Laboratorio de Genética médica.

o) Determinar el gen asociado al Covid-19 a través de la prueba del PCR, para informar a la Secretaria de Salud Departamental y al Ministerio de Salud Nacional, esto lo realiza el Laboratorio de Biología Molecular y Biotecnología.
p) Recolección de datos para el agendamiento de la vacunación por Covid-19.
q) Desarrollar los diferentes programas de bienestar institucional, en lo concerniente a los estudios psicosociales, entrega de beneficios y las historias médicas de los estudiantes.
r) Procurar mantener en contacto con los egresados de la institución en lo relacionado a la gestión de los mismos.
s) Informar sobre oportunidades de empleos, ferias, seminarios u otros estudios a nivel local e internacional.
t) Suministrar a las autoridades competentes u organismos de control, la información que sea requerida en los cumplimientos de las leyes, regulaciones, procesos disciplinarios, fiscales, judiciales y administrativos.
u) Informar sobre cambios en los servicios de la Universidad.
v) Cumplir las leyes aplicables a ex empleados, empleados actuales y candidatos a futuro empleo, incluyendo, pero sin limitarse a las laborales y de seguridad social.
w) Desarrollar el Sistema de Gestión de Seguridad y Salud en el Trabajo, en lo concerniente a las historias médicas de los empleados.
x) Cumplir las leyes aplicables a proveedores, incluyendo, pero sin limitarse a las tributarias.
y) Cumplir todos sus compromisos contractuales.
z) Los datos obtenidos de dispositivos móviles como georeferención, cámara, sistemas de almacenamiento, notificaciones y permisos para hacer llamadas, se usarán únicamente para el funcionamiento de la aplicación 'UTP Móvil.

La Universidad Tecnológica de Pereira a través de su Sistema de Gestión de Seguridad de la Información adoptará los controles y medidas tecnológicas, humanas y administrativas que sean necesarias para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

4.2 Condiciones para el tratamiento de los datos.

La Universidad Tecnológica de Pereira, con el fin de garantizar el derecho a la intimidad que les asiste a todos los Titulares de datos personales, aplica las siguientes condiciones:

a) La Universidad Tecnológica de Pereira es la titular de las bases de datos o bancos de datos y de los repositorios electrónicos que usa para el desarrollo de sus actividades, para lo cual se sujeta plenamente a las normas sobre protección de datos personales y Habeas Data.
b) Los Titulares son los únicos responsables de que la información suministrada sea actual, exacta y veraz; y reconocen su obligación de mantener, en todo momento, actualizados los datos.
c) Toda información relativa al Titular de los datos no podrá ser consultada, accedida o solicitada sino por el Titular de la misma, el representante legal o un apoderado debidamente facultado.

d) Al autorizar la recolección de datos de carácter personal a la Universidad Tecnológica de Pereira, los Titulares declaran aceptar plenamente y sin reservas la incorporación de los datos facilitados y su tratamiento, en los términos estipulados en la presente directriz.
e) Para los casos del Titular de los datos de menores de edad, en virtud de la patria potestad dicha información podrá ser consultada por sus padres o representantes legales.
f) El Titular de la información podrá acceder en cualquier momento a sus datos que reposen en la Universidad Tecnológica de Pereira.
g) En todo caso el Titular de los datos podrá solicitar la respectiva actualización, o rectificación que pueda proceder.
h) La información sobre datos personales deberá conservarse con diligencia y cuidado, de acuerdo a las políticas de seguridad de la información que la Universidad implemente, ya sea que está se encuentre en medio digital o físico.
i) En caso de pérdida de los datos, la Universidad Tecnológica de Pereira, deberá informar dicha situación, en todo caso en la medida de lo posible debe guardar registro de toda la información.
j) El Titular reconoce que el ingreso de información personal lo realiza de manera voluntaria y acepta que a través de cualquier trámite por los canales habilitados para ello por la Universidad Tecnológica de Pereira pueden recogerse datos personales, los cuales no se cederán a terceros sin su conocimiento, salvo que se trate de un requerimiento de autoridad judicial o administrativa, o en el caso de los estudiantes, que medie un convenio de cooperación interadministrativo que lo haga necesario.
k) Todas y cada una de las personas que administran, manejen, actualicen o tengan acceso a información de cualquier tipo que se encuentre en bases de datos o bancos de datos y de los repositorios electrónicos de las cuales la Universidad Tecnológica de Pereira es la titular, se comprometen a conservarla y mantenerla de manera estrictamente confidencial y no revelarla a terceros.
l) Sin menoscabo de los derechos constitucionales y las disposiciones legales y reglamentarias, la Universidad Tecnológica de Pereira se reserva el derecho de modificar en cualquier momento las directrices de tratamiento de datos personales.

4.3 Autorización para el tratamiento de la información.

Sin perjuicio de las excepciones consagradas en la Ley 1581 de 2012, para realizar el tratamiento de la información la Universidad, requiere autorización previa e informada del titular. La autorización del titular no será necesaria cuando se trate de:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
b) Información requerida por terceros autorizados por el Titular o por la ley.
c) Datos de naturaleza pública.
d) Casos de urgencia médica o sanitaria.
e) Tratamiento de información autorizada por la ley para fines históricos, estadísticos o científicos.

f) Datos relacionados con el registro civil de las personas.

Para el caso de datos personales sensibles, se podrá hacer uso y tratamiento de ellos cuando:

- El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- El tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

4.4 Medios para la autorización del tratamiento de datos personales.

La Universidad solicitará de manera previa al Titular de los datos personales la autorización y consentimiento para el tratamiento de los mismos, mediante diferentes medios que pueda ser objeto de consulta posterior, entre ellos: el documento físico o un mensaje de datos que en todo caso permita la obtención del consentimiento mediante conductas inequívocas a través de las cuales se concluya que de no haberse surtido la misma por parte del Titular o de la persona legitimada para ello, los datos no se hubieran almacenado o capturado en la base de datos.

Para cumplir con lo anterior, se dispondrán de los medios requeridos, así:

- Los aspirantes y estudiantes: la autorización y consentimiento se hará al momento de la inscripción para aspirar a algún programa académico o en la respectiva matrícula.
- Docentes y administrativos de planta: al momento de su vinculación.
- El personal docente y administrativo transitorio, docentes hora cátedra: se hará al momento de legalización del contrato.
- Contratistas y proveedores: al momento del registro como proponente o de la legalización del contrato.
- Personas que acceden a servicios de extensión: la autorización y consentimiento se hará al momento de la inscripción o suscripción del servicio.
- Egresados: Esta autorización se obtuvo al momento de la matrícula como estudiante.

La Universidad conservará la prueba de la autorización otorgada por los Titulares de los datos personales para su tratamiento, para lo cual utilizará los mecanismos disponibles a su alcance, al igual que adoptará las acciones necesarias para mantener el registro de la forma y fecha en la que se obtuvo. En consecuencia, la Universidad podrá establecer archivos físicos o repositorios electrónicos realizados de manera directa o a través de terceros contratados para tal fin.

4.5 Revocatoria de la autorización o supresión del dato.

Los Titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, para ello la Universidad Tecnológica de Pereira a dispuesto el correo electrónico datospersonales@utp.edu.co.

El Titular de los datos personales tiene el derecho a solicitar a la Universidad su supresión o eliminación en cualquiera de los siguientes eventos:

a) Considere que los mismos no están siendo tratados conforme a los principios, deberes, y obligaciones previstas en la normatividad vigente.
b) Hayan dejado de ser necesarias o pertinentes para la finalidad para la cual fueron recabados.
c) Se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recabados.

La supresión de datos, implica la eliminación total o parcial de la información personal de acuerdo con lo solicitado por el titular en los registros, archivos, bases de datos o tratamientos realizados por la Universidad. Sin embargo, este derecho del titular no es absoluto y en consecuencia la Universidad podrá negar el ejercicio del mismo cuando:

1. El titular tenga un deber legal o contractual de permanecer en la base de datos.

2. La eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
3. Los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular, para realizar la acción en función del interés público o para cumplir con una obligación legalmente adquirida por el titular.

5. Transferencia y transmisión de datos personales e información personal por parte de la Universidad

La UNIVERSIDAD podrá efectuar transferencia y trasmisión de datos personales de los titulares, en cumplimiento de la Ley, la misión institucional y en consideración de sus vínculos permanentes u ocasionales de carácter académico y administrativo con instituciones internacionales, con entidades gubernamentales internacionales, con agencias de cooperación internacional

Para la transferencia internacional de datos personales de los Titulares, LA UNIVERSIDAD tomará las medidas necesarias para que terceros conozcan y se comprometan a observar esta política, en el entendido que la información personal que reciban únicamente podrá ser utilizada para asuntos

directamente relacionados con LA UNIVERSIDAD y solamente mientras esta exista, y no podrá ser usada o destinada para propósito o para fin diferente.

Para la Transferencia internacional de datos personales se observará lo previsto en el artículo 26 de la Ley 1581 de 2012.

Las transmisiones nacionales e internacionales de datos personales que efectúe la universidad no requerirán ser informadas al Titular, ni contar con su consentimiento cuando medie un contrato de trasmisión de datos personales, de conformidad con el artículo 25 del Decreto 1377 de 2013.

6. Deberes en el Tratamiento de los datos personales

6.1 Deberes de la Universidad Tecnológica de Pereira.

Como responsable del tratamiento de datos la Universidad tiene los siguientes deberes:

a. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b. Solicitar y conservar, en las condiciones previstas en la ley 1581 de 2012, copia de la respectiva autorización otorgada por el Titular.
c. Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
d. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
e. Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
f. Solicitar la actualización de la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.
g. Solicitar la rectificación de la información cuando sea incorrecta al encargado del Tratamiento.
h. Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la presente directriz.
i. Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
j. Tramitar las consultas y reclamos formulados en los términos señalados en la presente política.
k. Adoptar el presente manual interno de directrices y procedimientos para garantizar el adecuado cumplimiento la ley 1581 de 2012 y en especial, para la atención de consultas y reclamos.

l. Publicar en lugar visible las directrices y procedimientos para el uso y tratamiento de los datos personales e informar sobre ellas a los titulares de la información. Al momento de realizar cambios o modificaciones al manual deberá informarlo a los Titulares de la Información por medio de los medios de comunicación con que cuente la Universidad.
m. Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
n. Informar a solicitud del Titular sobre el uso dado a sus datos.
o. Proveer información a los representantes legales y tutores de los menores de edad sobre los eventuales riesgos a los que se enfrentan respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.
p. Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
q. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

6.2 Deberes de las unidades organizacionales o proyectos especiales responsable de las bases de datos en la Universidad Tecnológica de Pereira.

a) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la ley 1581 de 2012.
b) Actualizar la información reportada por el Titular dentro de los cinco (5) días hábiles contados a partir de su recibo.
c) Tramitar conjuntamente con la Secretaría General las consultas y los reclamos formulados por los Titulares en los términos señalados por la ley 1581 de 2012.
d) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
e) Permitir el acceso a la información únicamente a las personas que pueden tener accesoa ella.
f) Realizar el registro de las bases de datos a su cargo (RNBD).
g) Cumplir los procedimientos, instrucciones y requerimientos que establezca la Universidad tecnológica de Pereira en relación con las políticas de tratamiento de datos personales.

6.3 Aviso de privacidad

La Universidad Tecnológica de Pereira cuenta con un Aviso de Privacidad para informar a los Titulares sobre el tratamiento y uso dado a sus datos personales y la existencia de la presente directriz. Este aviso deberá ser remitido al momento de solicitar la información al Titular.

Aviso de Privacidad:

La Universidad Tecnológica de Pereira, *con domicilio en la Ciudad de Pereira, Risaralda Colombia, quien es Responsable del Tratamiento de los Datos Personales informa que sus datos personales serán incluidos en nuestras bases o bancos de datos y/o repositorios electrónicos y estos serán utilizados de manera directa o a través de terceros debidamente designados para:*

i. Cumplir con la misión y los objetivos institucionales y demás funciones propias de la Universidad como Institución de Educación Superior.
ii. Lograr una efectiva comunicación en relación con nuestros servicios y actividades de docencia, extensión, investigación y administración; así mismo, sobre alianzas, estudios
iii. Lograr una adecuada gestión, administración, mejora de los distintos servicios de nuestra Universidad que puedan contribuir con el bienestar de la comunidad Universitaria.
iv. Dar cumplimiento a obligaciones contraídas con nuestros estudiantes, docentes, empleados, contratistas, contratantes, clientes y proveedores.
v. Informar sobre los cambios de los procesos, trámites y servicios de la Universidad.
vi. Dar cumplimiento a las obligaciones contraídas en razón a convenios firmados con instituciones internacionales, siempre y cuando se cumpla lo establecido en la Ley 1581 de 2012.
vii. Dar cumplimiento a las normas legales en cuanto a los requerimientos de los entes de control y/o otras entidades públicas, en el ejercicio de sus funciones.

Para mayor información sobre el tratamiento dado a los datos personales por la Universidad Tecnológica de Pereira visitar el siguiente link: https://bit.ly/2OEj7RN.
Si tiene alguna inquietud sobre el tratamiento de sus datos nos puede contactar en:
*Dirección: Secretaria General, Edificio 1, segundo piso. C*arrera 27 # 10- 02 Los Álamos, código postal 660003*, Pereira Risaralda, Colombia.*
Correo electrónico: datospersonales@utp.edu.co
Teléfono: 3137517

6.4 Registro Nacional de bases de datos

La Universidad Tecnológica de Pereira registrará sus bases de datos de acuerdo a lo establecido por la Superintendencia de Industria y Comercio, conforme a lo dispuesto por la Ley 1581 de 2012 y según el instructivo “1313-SGC-INT-03 Instructivo Registro Nacional Bases de Datos (RNBD)”.

7. Procedimientos relacionados con el tratamiento de datos personales

7.1 Identificación

En cada una de las unidades organizacionales o proyectos especiales de la Universidad Tecnológica de Pereira se deben identificar los datos personales que se encuentran bajo su manejo y custodia.

7.2 Atención de consultas

Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en la Universidad Tecnológica de Pereira quien suministrará toda la información que esté vinculada con la identificación del Titular. La consulta se formulará a través del correo datospersonales@utp.edu.co

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma.

Cuando no fuere posible atender la consulta dentro de dicho término, la Secretaría General informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

7.3 Atención de reclamos o peticiones

El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la directriz o en la ley, podrán presentar una petición o reclamo según corresponda ante la Universidad Tecnológica de Pereira, a través del correo datospersonales@utp.edu.co. Para ello deberá:

a) El reclamo o la petición se formularán mediante solicitud dirigida al Secretario General de la Universidad Tecnológica de Pereira, en el cual deberá informar:

- Identificación del Titular (Nombre y apellidos, documento de identificación)
- Identificar si es reclamo o petición
- Descripción de los hechos que dan lugar al reclamo o petición,
- Dirección o correo electrónico donde desea recibir la respuesta
- Anexar documentos que se quiera hacer valer en el reclamo o que soporten su petición.

b) Si el reclamo o la petición resulta incompleta, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del mismo para que subsane las fallas. Transcurridos dos (2)

meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo o la petición.

c) El Secretario General, en caso de requerirse dará traslado a las unidades organizacionales o proyectos especiales responsable de las bases de datos en la Universidad o al Encargado del Tratamiento que corresponda, en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

7.4 Petición de supresión de datos

Los Titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos a través del correo electrónico datospersonales@utp.edu.co.

La supresión de datos personales se realizará siempre y cuando no lo impida una disposición legal o contractual, situación en la cual se le informará de la situación al Titular de la información en un plazo de quince (15) días hábiles, contados a partir de la fecha de recibido de la solicitud.

Para la revocatoria de la autorización y/o supresión del dato el Titular podrá hacerlo mediante la presentación de una petición o reclamo, para lo cual se seguirá lo establecido en el numeral 3.6.

7.5 Datos recolectados antes de la expedición del decreto 1377 de 2013

Para los datos suministrados a la Universidad con anterioridad del Decreto 1377 de 2013 se tendrá en cuenta el siguiente procedimiento:

a) Se solicitará de manera escrita al correo electrónico que se encuentre registrado en la base o banco de datos o mediante publicación en los medios de comunicación con cuente la Universidad, la autorización y/o consentimiento de los Titulares para continuar con el

tratamiento de los datos personales conforme a lo establecido en la Ley 1581 de 2012 y las normas que lo reglamente.

b) La Universidad dará a conocer las directrices que sobre el tratamiento de los datos personales implemente, para lo cual las publicará en su página Web.

c) El Titular de la información contará con el término de treinta (30) días hábiles, contados a partir del envío o publicación del comunicado, para solicitar la supresión de sus datos personales, de lo contrario la Universidad podrá continuar realizando el tratamiento de los datos contenidos en sus bases de datos de acuerdo a lo establecido en la presente política

d) El Titular tiene el derecho en cualquier momento de solicitar mediante reclamo o petición la eliminación o supresión del dato.

DATOS ABIERTOS

Declaración Institucional

Dar cumplimiento a lo dispuesto en la Ley 1712 de 2014, la Universidad Tecnológica de Pereira establece las directrices para la publicación de datos abiertos.

Objetivo

Establecer las directrices para garantizar la publicación de datos abiertos según la normatividad vigente y que la Universidad Tecnológica de Pereira considere de interés para la comunidad en general.

Alcance

La directriz de publicación de datos abiertos aplica para todas las unidades organizacionales y proyectos especiales de la Universidad Tecnológica de Pereira que sean consideradas fuentes primarias de información.

Responsabilidad

- **Planeación**: Aprobación de los datos susceptibles a publicarse, conformación del inventario de datos abiertos de la institución, revisión, preparación y cargue de la información en la plataforma.
- **Fuentes de datos:** Identificación de los datos que son susceptibles a ser datos abiertos, suministro de la información según lo estipulado en el "Formato de cargue de datos abiertos" para la preparación y cargue.
- **Gestión de Tecnologías Informáticas y Sistemas de Información:** Prestar apoyo a las fuentes de datos para gestionar la información generada por los sistemas de información institucionales.

- **Control Interno:** Verificar que las directrices aquí contempladas se cumplan, al igual que las regulaciones que sobre datos abiertos expida el Gobierno Nacional.

Principios

- **Primarios**: Obtenerse en la fuente de origen, con el más alto nivel de detalle posible, no en forma agregada ni modificada.
- **Accesibles:** Estar disponibles para el rango más amplio de usuarios y para el rango más amplio de propósitos.
- **Completos:** Reflejar la totalidad del tema y contener el mayor detalle posible, garantizando que la información suministrada sea suficiente y consistente y que no contenga datos nulos.
- **Procesables por máquinas:** Encontrarse en formatos que permitan el procesamiento automático.
- **No propietarios:** Estar disponibles en un formato sobre el cual ninguna entidad tenga control exclusivo.
- **Licenciados de forma abierta:** Los conjuntos de datos publicados deben contar con términos de uso y licenciamiento abierto.
- **No discriminados:** Estar disponibles para cualquiera persona, sin requerir registro o autenticación.
- **Oportunos y actualizados**: Estar disponible tan rápido como sea necesario para garantizar su valor y mantener una frecuencia de actualización que garantice la utilidad del dato.

1. Requisitos para la publicación de datos abiertos

La Universidad Tecnológica de Pereira ha definido que los datos susceptibles para cargarse como datos abiertos deben poseer las siguientes características:

- Deben cumplir los principios que rigen los datos abiertos descritos en esta directriz.
- Los datos a publicar no deben corresponder a datos personales o datos sensibles que afecten la intimidad de las personas, en atención a las directrices que la universidad adopte para la implementación de la Ley 1581 de 2012.
- De acuerdo a la normatividad vigente en especial la Ley 1712 de 2014 y al art. 24 de la Ley 1755 de 2015 no se publicará información pública reservada, ni información pública clasificada.
- El conjunto de datos cargados no debe permitir el efecto mosaico, es decir, la individualización de los registros a través de cruce del conjunto cargado con otros conjuntos de datos.
- El conjunto de datos a cargase debe poseer una "hoja de vida" (metadatos) de acuerdo con el formato que se establezca para dicho fin, con concepto favorable emitido por la unidad organizacional Planeación.

- Las fuentes de información deben suministrar el conjunto de datos a cargarse de acuerdo con los metadatos establecidos para dicho fin.
- El conjunto de datos a cargarse a la plataforma estipulada para dicho fin debe preparase como un formato libre.

2. Ruta de cargue de datos abiertos

El proceso de cargue de datos abiertos de la Universidad Tecnológica de Pereira cuenta con dos momentos descritos a continuación:

- **Primer momento:** está relacionado con la identificación de datos susceptibles de carga, así como la definición de sus metadatos.

- **Segundo momento:** obedece a la recolección, consolidación y preparación de los datos hasta el cargue de los datos a la plataforma de datos abiertos.

  En estos momentos se articulan al procedimiento 113-AIE-04 en la sección "reporte de información a entes externos" de planeación y las actividades detalladas se describen en el instructivo de carga de datos abiertos cargado en el Sistema Integral de Gestión asociado a la unidad organizacional de Planeación.

<u>USO DE LA RED DE DATOS INSTITUCIONAL</u>

Declaración Institucional:
Se aplica para el uso del servicio de internet/intranet institucional.

Objetivo:
Definir las reglas para el acceso al servicio de internet/intranet institucional.

Alcance:
Las disposiciones contenidas en la presente directriz serán aplicables a todos los usuarios del servicio de internet/intranet institucional.

Se entiende por usuario de la red de la Universidad a:

- Servidores públicos (administrativos planta) y trabajadores oficiales de la Universidad.
- Administrativos transitorios.
- Personal ocasional por proyecto.

- Contratistas que usen la red de datos institucional.
- Estudiantes.
- Visitantes.

Responsabilidad

- **Comité del Sistema Integral de Gestión**: revisar y aprobar los cambios que requiera la presente directriz.
- **Grupo Técnico para el Sistema de Gestión de Seguridad de la Información**: recomendar ajustes a la presente directriz.
- **Jefes de proceso o Decanos:** Socializar e implementar la presente directriz en su área.
- **Personal que labora o presta servicios y terceros:** Aplicar la presente directriz.

Directrices

1. Disposiciones generales:

La red de datos de la Universidad Tecnológica de Pereira, se usará para cumplir con la misión institucional, igualmente para realizar las actividades derivadas de las funciones y actividades encomendadas al personal administrativo (planta y transitorios), personal ocasional de proyectos y contratistas.

Los funcionarios de la universidad a través del autocontrol deberán hacer uso adecuado de la red de datos institucional.

El acceso a las redes de tipo social (Facebook, Instagram, Tumblr, Twitter, Snapchat, entre otros) no estará permitido, cada Director, Jefe, Interventor o Supervisor podrá autorizar el acceso o bloqueo de estos servicios al interior de su dependencia, lo cual deberá ser solicitado por los canales institucionales a Administración de Redes y Seguridad de la Información.

2. Se restringe

No se podrá utilizar la red de datos institucional con los siguientes fines:

- Acceder, descargar y transmitir contenido fraudulento, difamatorio, obsceno, ofensivo o de vandalismo, insultante, pornográfico o acosador.

- Interceptar, recopilar o almacenar datos sin la autorización de su titular.

- Escanear o explotar vulnerabilidad de equipos, sistemas o segmentos de red (Estas pruebas podrán ser realizadas de forma controlada en la red institucional por GTI-SI, CRIE o por un tercero que se contrate para tal fin).

- Enviar virus o ataques internos o externos a la red universitaria.

- Obtener acceso no autorizado a equipos, sistemas o programas tanto al interior de la red universitaria como fuera de ella.

- Transmitir, copiar o descargar cualquier material que viole cualquier ley. Esto incluye entre otros: material con derecho de autor, pornografía infantil o material protegido por registro de propiedad intelectual.

- Dañar equipos, sistemas informáticos o redes y perturbar el normal funcionamiento de la red.

- Usar la red con fines de lucro, actividades comerciales o ilegales.

- Acceder a sitios de juegos o apuestas en línea.

- Descargar documentos o archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.

- Interferir intencionalmente con la operación normal de cualquier sitio web o portal en Internet.

3. Red inalámbrica

3.1 Acceso

- Para acceder a la red inalámbrica el usuario deberá contar con correo electrónico institucional y usar la contraseña del portal estudiantil o del sistema de información de la Universidad Tecnológica de Pereira.

- La dependencias académicas o administrativas deberán solicitar un usuario de invitado para sus visitantes, este tendrá una vigencia de un mes y la duración de la conexión estará limitada a 1 hora por día, en el momento de cumplirse el mes la dependencia deberá solicitar un nuevo usuario invitado.

- Para la disponibilidad de la conectividad en los eventos que se realicen en la Universidad Tecnológica de Pereira, se deberá solicitar con una (1) semana de anticipación al Centro de Recursos Informáticos y Educativos, por parte del coordinador del evento la configuración de usuarios invitados para el portal cautivo de la universidad.

3.2 Instalación de un punto de acceso (Access Point - AP)

- La Administración de Redes y Seguridad de la Información de Recursos Informáticos y Educativos (CRIE), es la única área autorizada para definir y aprobar dispositivos de acceso inalámbrico (AP) que se instalen en la Institución, así como la reubicación y desinstalación de estos puntos de accesos en el campus universitario.

- La instalación de un dispositivo AP en la institución, depende de la verificación de los usuarios inalámbricos beneficiados, la viabilidad técnica del punto físico de red datos al que se conectará, la disponibilidad de materiales, mano de obra, dispositivo AP y de la licencia para su activación. Una vez instalado se monitoreará y aquellos dispositivos AP que no cumplan con el impacto esperado serán reubicados en lugares del campus con mayor número de usuarios, se exceptúan los puntos de acceso inalámbrico ubicados en auditorios, salas múltiples y salas de juntas.

- En los sitios donde el número de usuarios que se conectan simultáneamente a la red inalámbrica, supere permanentemente el umbral recomendado por el fabricante, se evaluará la posibilidad de ubicar un nuevo dispositivo AP.

- Las diferentes dependencias de la institución que cuentan con red cableada para el desarrollo de su trabajo, no serán prioridad para instalar AP para dar servicio inalámbrico.

4. Monitoreo:

La Administración de redes y seguridad de la información monitorea el uso del servicio de Internet/Intranet y podrá identificar las páginas visitadas por cualquier usuario, a solicitud de un jefe de dependencia o área.

ORIGINAL
06/04/2022