TABLA DE CONTENIDO

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, componentes que también son parte esencial del modelo de Seguridad de Información mediante la arquitectura de tecnología informática, un ambiente de administración y control 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 la política 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 del cumplimiento e interiorización de las directrices

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.

TÉRMINOS Y DEFINICIONES

Para este manual se aplican los siguientes términos y 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.
- **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.

- **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.
- **Bloqueo dispositivo móvil:** Método de bloque de los dispositivos móviles (contraseña, biométrico, patrón o reconocimiento de voz.)
- **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 o sistemas no autorizados, deben tener acceso a la información únicamente aquellas personas que cuenten con la debida autorización.
- **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.

- **Datos sensibles:** Información catalogada como reservada o clasificada la cual es de primordial importancia para el funcionamiento de la universidad Tecnológica de Pereira.
- **Dispositivos móviles:** Computadores portátiles, tabletas, teléfonos inteligentes y dispositivos de almacenamiento.
- **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.
- **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.
- **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.

- **Información clasificada:** Información disponible sólo para personas autorizadas y cuyo acceso podrá ser rechazado o denegado.
- **Información pública**: Información que puede ser entregada o publicada por personas autorizadas sin restricciones.
- **Información reservada:** Información disponible sólo para personas autorizadas y el acceso a ella está prohibido por una norma legal o constitucional.
- **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.
- **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, catedra).

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

La Universidad Tecnológica de Pereira está comprometida con la implementación de estrategias de seguridad, 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 proceso o Decanos:** 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, mesa de ayuda 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 contratado a través de la administradora de nómina.
- Contratistas (con previa solicitud por escrito del supervisor o interventor)
- Estudiantes de pregrado y posgrado.
- Egresados.
- Jubilados y pensionados.

Responsabilidad

- **Comité de Sistema Integral de Gestión de Calidad:** 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 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

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

- Esta 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 al correo electrónico será el utilizado para acceder a los diversos sistemas de información de la institución.

- La creación del nombre de usuario, se reglamentará a través de un procedimiento para tal efecto 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, catedra), contratistas y personal vinculado por administradora de nómina 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.

- Se debe excluir de la firma cualquier tipo de información no institucional (logos, frases, emoticones, entre otros).

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

- La información que trasmita 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 debe implementar el uso de la opción con copia oculta “CCO o BCC” cuando se realice envíos a más de cinco cuentas de correo electrónicos.

- Los usuarios que utilicen clientes de correos (Outlook, Thunderbird, otros) para el manejo y uso de las cuentas de correo institucionales deben utilizar los protocolos seguros (imaps, smtps, pops) o solicitar este servicio en el área de Administración de Recursos Informáticos (soporte técnico).

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 virus, programas de uso mal intencionado o introducción de software malicioso en la red o en los servidores.

- Él envió 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 por un periodo de 6 meses cuando se den por terminados los contratos de los usuarios.

- 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.

5. Eliminación del correo Institucional

5.1 Cuentas de correo de personal administrativo (planta y transitorio), personal docente (planta, transitorio, catedra), contratistas y personal vinculado por administradora de nómina.

- Pasados los 6 meses del periodo de suspensión de la cuenta.

- Cuando se retire por jubilación o pensión y solicite a través de su correo electrónico institucional a admred@utp.edu.co la eliminación del mismo.

5.2 Cuentas de correo de estudiantes de pregrado y postgrado.

El correo institucional de los estudiantes se eliminará 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.

6. 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 este determine. 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. También puede usarse como lista de distribución de correos.

- 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, catedra) 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.

CONTROL DE ACCESO.

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 contratado a través de la administradora de nómina.
- Contratistas (con previa solicitud por escrito del supervisor o interventor)
- Estudiantes de pregrado y posgrado.
- Egresados.
- Jubilados y pensionados.

Responsabilidad

- **Comité del Sistema Integral de Gestión de Calidad:** 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 proceso o Decanos**: 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 de creación de cuentas de correo electrónico.

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 proceso, 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 responsabilidad.

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 contratado a través de la administradora de nómina.
- Contratistas (con previa solicitud por escrito del supervisor o interventor)
- Estudiantes de pregrado y posgrado.
- Egresados.
- Jubilados y pensionados.

Responsabilidad

- **Comité de Sistema Integral de Gestión de Calidad:** 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 le asignará un usuario y una clave mediante una 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) que se va a transferir, 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 acciones realizadas 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 contratado a través de la administradora de nómina.
- Contratistas (con previa solicitud por escrito del supervisor o interventor)

- Estudiantes de pregrado y posgrado.
- Egresados.
- Jubilados y pensionados.

Responsabilidad

- **Comité de Sistema Integral de Gestión de Calidad:** Revisar y aprobar los cambios que requiera la presente directriz.
- **Jefes de proceso o Decanos**: 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 contratado a través de la administradora de nómina.
- Contratistas (con previa solicitud por escrito del supervisor o interventor)
- Estudiantes de pregrado y posgrado.
- Egresados.
- Jubilados y pensionados.

Responsabilidad

- **Comité de Sistema Integral de Gestión de Calidad:** 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.
- **Jefes de proceso o Decanos:** 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 equipo 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 de Sistema Integral de Gestión de Calidad:** 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:** 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 cuente 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 a la mesa de ayuda 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 contratado a través de la administradora de nómina.
- Contratistas (con previa solicitud por escrito del supervisor o interventor)
- Estudiantes de pregrado y posgrado.
- Egresados.
- Jubilados y pensionados.

Responsabilidad

- **Comité de Sistema Integral de Gestión de Calidad:** 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.

- **Jefes de proceso o Decanos:** 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 de Sistema Integral de Gestión de Calidad:** 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 adecuaran 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 GTIYSI 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 de Sistema Integral de Gestión de Calidad:** 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 los aplicativos 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.

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 tres ambientes: producción, desarrollo y pruebas.

4. Los datos en los ambientes de desarrollo y pruebas deben ser diferentes a los de producción o usar herramientas de enmascaramiento de datos, garantizando que los desarrolladores o probadores no conozcan datos reales de la institución.

5. Todas las normas definidas deben estar alineadas con las normas ISO o su equivalente con referencia a seguridad de la información y buenas prácticas.

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

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

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

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

10. La interconexión con sistemas internos o externos deberá cumplir con los criterios de confidencialidad, integridad, disponibilidad y no repudio, además de definir los niveles de acuerdo del servicio.

11. Todas las aplicaciones deben pasar por fases de pruebas arquitectónicas, de seguridad, funcionales, no funcionales o las que apliquen en su momento de las cuales se deben dejar registros o evidencias de las mismas.

12. Se debe contar con procesos de gestión de cambios y gestión de entregas y despliegue.

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 terceros o 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 de Sistema Integral de Gestión de Calidad:** 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.
- **Jefes de proceso o Decanos:** 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 manera razonable que se tomaran las medidas que garanticen la protección de la información que está a su disposición, manteniendo los niveles de protección y clasificación establecidos para la misma.

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 acordaran políticas comunes y se formalizaran 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 está autorizada la utilización de equipos de cómputo, portátiles y otros similares en las redes de los sistemas de información y comunicación, que no cumplan con los controles de seguridad especificados por el sistema de gestión de seguridad de la información.

- No está autorizada 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 RIE 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.