UNIVERSIDAD CES
CONSEJO SUPERIOR
ACTA 794
ACUERDO No 292

POR EL CUAL SE REGLAMENTA LAS POLÍTICAS DE TECNOLOGÍA DE LA INFORMACIÓN DE LA UNIVERSIDAD CES.

El Consejo Superior en el uso de sus atribuciones Estatutarias y en especial las conferidas por el artículo 25, literal b. de los Estatutos, que reza lo siguiente: Son funciones y atribuciones del Consejo Superior: b. Expedir los reglamentos internos.

ACUERDA:

TÍTULO I. DISPOSICIONES GENERALES
CAPÍTULO I. PRINCIPIOS GENERALES

ARTÍCULO 1. NATURALEZA JURÍDICA. La Universidad CES es una Institución de Educación Superior, autónoma, privada, con carácter de fundación, sin ánimo de lucro, autosostenible, no confesional desde el punto de vista religioso o político, que ofrece servicios educativos de pre y postgrado en todas las áreas del conocimiento, con énfasis en salud.

ARTÍCULO 2. AUTONOMÍA. Dentro de los límites del orden jurídico, la Universidad CES es autónoma para desarrollar sus programas académicos y de extensión o servicios, designar su personal, admitir a sus alumnos, arbitrar y disponer de sus recursos y darse su organización y gobierno.

ARTÍCULO 3. RÉGIMEN CONTRACTUAL. Los contratos que suscriba la Universidad CES para el cumplimiento de su misión se rigen por las normas del derecho privado y sus efectos estarán sujetos a las normas civiles, según la naturaleza de los contratos.

ARTÍCULO 4. OBJETIVO. El objetivo de esta política es establecer los principios y las reglas generales que regirán la disposición y uso de las tecnologías de la información de la Universidad CES, con el fin de gestionar los recursos de la Institución de manera responsable, eficiente y sostenible.

CAPITULO II. DEFINICIONES GENERALES

ARTÍCULO 5. DEFINICIONES GENERALES. En la aplicación e interpretación de la presente política, se acudirá a la definición dada a los siguientes conceptos:

www.ces.edu.co Calle 10 A Nº 22-04 A.A. 054 591 Conmutador 444 05 55 Fax 266 60 46 NIT 890.984.002-6 Medellín / Colombia VIGILADA MINEDUCACIÓN

- **Acceso a datos:** Definición y control de quién puede ver y utilizar los datos de la organización.
- **Activo de información**: Recurso de datos valioso para una organización que requiere protección.
- **Activo de información**: Recursos valiosos como datos, software, hardware y sistemas que necesitan protección.
- **Actualizaciones de software**: Procedimientos para mantener el software actualizado con los últimos parches de seguridad y mejoras.
- **Amenaza**: Potencial de un evento o actividad que pueda causar daño a un activo de información.
- **Aplicación:** Es un programa o conjunto de programas diseñados para realizar tareas específicas para el usuario.
- **Auditoría de accesos**: Revisión regular de los accesos a sistemas y datos.
- **Auditoría de cumplimiento**: Revisiones periódicas para asegurar el cumplimiento con todas las políticas de seguridad y regulaciones.
- **Auditoría interna de seguridad**: Revisiones internas periódicas para asegurar el cumplimiento de las políticas de seguridad.
- **Auditorías de seguridad**: Revisión periódica de los sistemas y políticas de seguridad para identificar y corregir vulnerabilidades.
- **Autenticación de usuarios**: Métodos para verificar la identidad de los usuarios antes de conceder acceso a los sistemas de ti.
- **Autorización de software**: Procedimientos para la autorización y el uso de software dentro de la organización.
- **Backup de datos**: Estrategias y métodos para realizar copias de seguridad de los datos críticos de la organización.
- **Backup**: Copia de seguridad de datos para recuperación ante pérdidas.
- **Cableado categoría 6A**: Cableado de red de alta velocidad que soporta hasta 10 gbps y frecuencias de hasta 500 mhz.
- **Capacitación continua**: Programas de formación continua en seguridad para todo el personal.
- **Catálogo de servicios:** Base de datos detallada que enumera y describe los servicios de ti disponibles en una organización, diseñada para satisfacer eficientemente las necesidades de los usuarios.
- **Cifrado de datos**: Uso de técnicas de cifrado para proteger los datos en tránsito y en reposo.
- **Clasificación de datos**: Categorización de datos según su nivel de sensibilidad y riesgo.
- **Componente:** Un componente de software es una parte independiente y modular de un sistema, diseñada para ser reutilizable y actualizable sin afectar negativamente al sistema en su conjunto.
- **Concienciación sobre phishing**: Capacitación para identificar y evitar ataques de phishing.
- **Control de acceso físico**: Medidas para proteger físicamente los sistemas de ti contra accesos no autorizados.

- **Control de acceso**: Procesos y tecnologías para restringir y monitorear el acceso a recursos o áreas.
- **Control de cambios:** Es el proceso de gestionar, documentar y aprobar las modificaciones realizadas en un sistema para asegurar su estabilidad y calidad.
- **Control de dispositivos externos**: Normas para el uso de dispositivos externos como usbs y discos duros externos.
- **Control de medios de almacenamiento**: Normas para el uso y eliminación segura de medios de almacenamiento.
- **Controles de acceso basado en roles**: Asignación de permisos de acceso según las funciones y responsabilidades de los empleados.
- **Controles de red**: Implementación de medidas para proteger la red interna y los datos que circulan en ella.
- **Copia de seguridad de sistemas**: Procedimientos para garantizar que se realicen copias de seguridad regulares de todos los sistemas críticos.
- **Coworking**: Espacio de trabajo compartido que fomenta la colaboración y la flexibilidad laboral.
- **Cuentas de usuario**: Proceso para la creación, gestión y eliminación de cuentas de usuario.
- **Cumplimiento de normativas**: Asegurarse de que todas las prácticas de ti cumplan con las leyes y regulaciones pertinentes.
- **Cumplimiento de políticas de TI**: Mecanismos para asegurar que todos los empleados cumplan con las políticas de ti.
- **Datacenter**: Instalación que alberga servidores y equipos para procesar y almacenar datos.
- **Desarrollo de software seguro**: Prácticas para asegurar que el software desarrollado internamente sea seguro y libre de vulnerabilidades.
- **Destrucción de datos**: Métodos seguros para eliminar datos que ya no son necesarios.
- **Dispositivos móviles**: Políticas para el uso seguro de dispositivos móviles dentro de la organización.
- **Dominio**: Nombre único que identifica un sitio web en internet.
- **Evaluación de riesgos**: Identificación y evaluación regular de riesgos de seguridad.
- **Evaluación de seguridad de aplicaciones**: Revisión y prueba de aplicaciones para detectar vulnerabilidades de seguridad.
- **Firewall**: Configuración y mantenimiento de firewalls para proteger la red interna de amenazas externas.
- **Gestión de accesos de terceros**: Control y monitoreo del acceso de terceros a los sistemas de la organización.
- **Gestión de activos**: Inventario y seguimiento de todos los activos de ti.
- **Gestión de actualizaciones de firmware**: Procedimientos para la actualización segura del firmware de dispositivos.
- **Gestión de cambios**: Procedimientos para la gestión de cambios en la infraestructura de ti.

www.ces.edu.co Calle 10 A Nº 22-04 A.A. 054 591 Conmutador 444 05 55 Fax 266 60 46 NIT 890.984.002-6 Medellín / Colombia VIGILADA MINEDUCACIÓN

- **Gestión de configuraciones de red**: Control y revisión de las configuraciones de la red para asegurar la seguridad.
- **Gestión de contraseñas maestras**: Control y protección de contraseñas maestras utilizadas en la organización.
- **Gestión de derechos digitales**: Control del acceso y uso de información digital.
- **Gestión de identidades y accesos**: Estrategias para gestionar identidades digitales y sus permisos de acceso.
- **Gestión de incidentes**: Procedimientos para la identificación, gestión y resolución de incidentes de seguridad.
- **Gestión de logins y sesiones**: Control y monitoreo de inicios de sesión y sesiones de usuario.
- **Gestión de parcheo de sistemas**: Implementación de parches de seguridad de manera oportuna.
- **Gestión de parches**: Estrategias para la implementación de parches de seguridad en sistemas y aplicaciones.
- **Gestión de proveedores**: Evaluación y gestión de la seguridad de los proveedores y socios externos.
- **Gestión de riesgos de TI**: Identificación, evaluación y mitigación de riesgos relacionados con ti.
- **Gestión de vulnerabilidades**: Identificación y corrección de vulnerabilidades en los sistemas de ti.
- **ID del activo**: Identificador único asignado a cada activo de información para su seguimiento y gestión.
- **Impacto inherente**: Consecuencia potencial de una amenaza si explota una vulnerabilidad, sin tener en cuenta los controles existentes.
- **Impacto**: Consecuencias o efectos de un evento de riesgo sobre los activos de información.
- **Implementación de MFA**: Uso de autenticación multifactor para mejorar la seguridad de accesos.
- **Integridad de datos**: Medidas para asegurar que los datos no sean alterados o manipulados sin autorización.
- **Levantamiento de requisitos:** Es el proceso de recopilar, documentar y analizar las necesidades y expectativas de los usuarios y stakeholders para definir las funcionalidades y características que debe tener un sistema.
- **Malware:** Cualquier código de software o programa informático, escrito intencionadamente para dañar los sistemas informáticos o a sus usuarios.
- **Manejo de contraseñas**: Reglas para la creación, gestión y almacenamiento seguro de contraseñas.
- **Mantenimiento de hardware**: Planificación y ejecución del mantenimiento regular del hardware de ti.
- **Metodologías de desarrollo:** Marco de trabajo que se emplea para organizar, planificar y gestionar el proceso de desarrollo de sistemas de información.
- **Mini split**: Tipo de aire acondicionado que se compone de dos unidades, una interior y otra exterior, para climatizar espacios.

- **Monitoreo de actividades sospechosas**: Vigilancia continua para detectar actividades sospechosas en la red.
- **Monitoreo de red**: Vigilancia continua de la red para detectar y responder a actividades sospechosas.
- **Normas para el uso de aplicaciones web**: Directrices para el uso seguro de aplicaciones web.
- **Normas para el uso de vpn**: Directrices para el uso seguro de redes privadas virtuales (VPN).
- **Opciones de tratamiento**: Estrategias disponibles para gestionar el riesgo, incluyendo la aceptación, mitigación, transferencia o eliminación del riesgo.
- **Política de acceso remoto**: Directrices para asegurar el acceso remoto seguro a los sistemas de la empresa.
- **Política de almacenamiento seguro**: Normas para el almacenamiento seguro de datos y documentos.
- **Política de antivirus**: Uso y actualización regular de software antivirus en todos los dispositivos.
- **Política de conexiones remotas**: Directrices para las conexiones remotas seguras a la red corporativa.
- **Política de contraseñas seguras**: Requisitos mínimos para la creación y uso de contraseñas.
- **Política de responsabilidad de usuarios**: Definición de responsabilidades de los usuarios en relación con la seguridad de ti.
- **Política de seguridad de ti**: Documento integral que recoge todas las políticas y procedimientos de seguridad de ti.
- **Política de uso de redes sociales**: Normas para el uso seguro de redes sociales en el entorno corporativo.
- **Política de WIFI**: Directrices para el uso seguro de redes inalámbricas dentro de la organización.
- **Privacidad de datos**: Garantizar que los datos sensibles sean manejados de acuerdo con las políticas de privacidad.
- **Privilegio**: Derecho especial otorgado a un usuario o programa para realizar acciones específicas en un sistema.
- **Probabilidad de ocurrencia**: Probabilidad de que una amenaza específica ocurra, considerando los controles existentes.
- **Probabilidad inherente**: Probabilidad de que una amenaza explote una vulnerabilidad sin considerar los controles existentes.
- **Procedimientos de respuesta a incidentes**: Estrategias y acciones para responder a incidentes de seguridad.
- **Procedimientos de seguridad para BYOD**: Políticas para la seguridad en el uso de dispositivos personales en el trabajo (Bring Your Own Device).
- **Protección contra amenazas internas**: Medidas para detectar y prevenir amenazas provenientes de empleados internos.
- **Protección contra ataques DDOS**: Medidas para prevenir y mitigar ataques de denegación de servicio distribuido (DDOS).

www.ces.edu.co Calle 10 A Nº 22-04 A.A. 054 591 Conmutador 444 05 55 Fax 266 60 46 NIT 890.984.002-6 Medellín / Colombia VIGILADA MINEDUCACIÓN

- **Protección contra malware**: Políticas para la detección y eliminación de software malicioso.
- **Protección de comunicaciones electrónicas**: Medidas para asegurar la privacidad y seguridad de las comunicaciones electrónicas.
- **Protección de datos personales**: Garantizar la privacidad y seguridad de los datos personales almacenados.
- **Protección de información confidencial**: Medidas para proteger la información confidencial de la organización.
- **Protección de información financiera**: Medidas específicas para proteger la información financiera.
- **Protección de infraestructura crítica**: Medidas específicas para proteger los componentes críticos de la infraestructura de ti.
- **Protección de redes inalámbricas**: Medidas para asegurar la red inalámbrica corporativa.
- **Pruebas de penetración**: Evaluaciones periódicas de seguridad mediante pruebas de penetración.
- **Pruebas de recuperación de desastres**: Ejecución regular de pruebas de recuperación de desastres para asegurar la preparación.
- **Rack**: Estructura metálica diseñada para alojar equipos electrónicos, informáticos y de telecomunicaciones.
- **Recuperación ante desastres**: Planes y procedimientos para recuperar datos y sistemas en caso de un desastre.
- **Registro de actividades**: Mantenimiento de registros detallados de actividades y accesos a sistemas críticos.
- **Requerimiento de software:** Es una descripción detallada de una funcionalidad o característica que un sistema de software debe tener para cumplir con las necesidades y expectativas de los usuarios o stakeholders.
- **Respaldo de configuraciones**: Copias de seguridad regulares de las configuraciones de sistemas críticos.
- **Responsable**: Persona o equipo designado para la gestión y protección de un activo de información.
- **RETIE**: Reglamento técnico de instalaciones eléctricas, normativa colombiana para la seguridad en instalaciones eléctricas.
- **Revisión de configuraciones de seguridad**: Evaluación y ajuste periódico de las configuraciones de seguridad.
- **Riesgo inherente**: Nivel de riesgo antes de la implementación de controles, calculado como la combinación de la probabilidad y el impacto inherentes.
- **Riesgo residual**: Riesgo que permanece después de implementar controles para mitigar el riesgo inherente.
- **Riesgo**: Potencial de pérdida o daño debido a vulnerabilidades o amenazas.
- **Seguridad de bases de datos**: Protección de las bases de datos contra accesos no autorizados y otras amenazas.
- **Seguridad de dispositivos personales**: Normas para el uso de dispositivos personales en el trabajo.

- **Seguridad de servidores**: Protección de servidores contra accesos no autorizados y otras amenazas.
- **Seguridad en aplicaciones web**: Prácticas para proteger las aplicaciones web contra ataques.
- **Seguridad en el almacenamiento en la nube**: Normas para la protección de datos almacenados en servicios de la nube.
- **Seguridad en el ciclo de vida del software**: Prácticas de seguridad integradas en todo el ciclo de vida del desarrollo del software.
- **Seguridad en el correo electrónico**: Políticas para proteger el correo electrónico contra spam, phishing y otras amenazas.
- **Seguridad en el desarrollo ágil**: Incorporar prácticas de seguridad en el desarrollo ágil de software.
- **Seguridad en la gestión de proyectos**: Incorporar prácticas de seguridad en la gestión de proyectos de ti.
- **Seguridad en la infraestructura**: Protección de la infraestructura de ti contra amenazas físicas y cibernéticas.
- **Seguridad en la nube**: Políticas para el uso seguro de servicios y almacenamiento en la nube.
- **Seguridad en proyectos de TI**: Incorporar consideraciones de seguridad en todas las fases de los proyectos de ti.
- **Seguridad en transacciones electrónicas**: Políticas para asegurar la integridad y confidencialidad de las transacciones electrónicas.
- **Seguridad física de TI**: Medidas para proteger los equipos de ti contra daños físicos y robos.
- **Sensibilización del usuario**: Programas de capacitación para educar a los empleados sobre las mejores prácticas de seguridad.
- **Software libre:** Software que permite su uso, copia, estudio, modificación y distribución.
- **Software SAAS:** Es un modelo de distribución de software donde las aplicaciones se alojan en servidores de un proveedor y los usuarios acceden a ellas a través de internet, generalmente mediante una suscripción.
- **Software**: Programas y sistemas operativos utilizados por computadoras.
- **Teletrabajo seguro**: Políticas para garantizar la seguridad de los empleados que trabajan de forma remota.
- **Ti:** Tecnologías de la información
- **Transparencia de seguridad**: Comunicación clara de políticas y procedimientos de seguridad a todos los empleados.
- **UPS**: Sistema de alimentación ininterrumpida que proporciona energía eléctrica sin cortes a dispositivos críticos.
- **URL**: Dirección específica que localiza un recurso en la web.
- **Uso de software de terceros**: Normas para la evaluación y utilización de software de terceros.
- **Virtual Private Network (VPN):** Conexión segura y cifrada a través de internet para acceder a una red privada.

www.ces.edu.co Calle 10 A Nº 22-04 A.A. 054 591 Conmutador 444 05 55 Fax 266 60 46 NIT 890.984.002-6 Medellín / Colombia VIGILADA MINEDUCACIÓN

- **Virus:** Es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo.
- **Vulnerabilidad**: Debilidad o fallo en un sistema que puede ser explotado por una amenaza para causar daño.
- **WIFI**: Tecnología que permite la conexión inalámbrica a internet o entre dispositivos.

TÍTULO II. INFRAESTRUCTURA FÍSICA Y TELECOMUNICACIONES
CAPÍTULO I. CUARTOS TÉCNICOS

ARTÍCULO 6. CONDICIONES DE CUARTOS TÉCNICOS

- Los cuartos técnicos están distribuidos en todos los bloques de la Universidad y centros de servicio, estos están destinados para el alojamiento de los equipos de telecomunicaciones y de carácter tecnológico los cuales por cuestiones técnicas no puedan ser alojados en los data centers, estos cuartos deben de tener un espacio mínimo de catorce metros cuadrados (14 Mts^2).
- Estos deben de contar con polo a tierra según normativa RETIE vigente.
- Deben de tener suministro de energía eléctrica regulada.
- Deben de contar con UPS de respaldo.
- Deben de contar con aire acondicionado tipo mini split.
- Se deben de tener rutas de acceso para el cableado de datos o fibra óptica debidamente organizado y señalizado.
- Debe de contar con sistema antiincendios debidamente señalizada según la normativa de seguridad y salud en el trabajo institucional.
- Los cuartos técnicos deben de estar en zonas libres de humedad, donde se tenga riesgo ambiental.
- Cualquier equipo que deba ser alojado en los cuartos técnicos deberá contar con la revisión y aprobación del área de TI y debe de cumplir con requerimientos mínimos:
    - Debe de ser un equipo de rack.
    - Debe de soportar 120 Voltios de energía corriente alterna (AC).
    - Los equipos deben de contar con polo a tierra.

ARTÍCULO 7. RESTRICCIONES DE CUARTOS TÉCNICOS

- Está prohibido usar los cuartos técnicos con fines ajenos a temas tecnológicos.
- Está prohibido usar los cuartos técnicos como bodegas.
- En los cuartos técnicos no se deben de instalar tableros eléctricos, los temas eléctricos deben de tener un espacio diferente.
- El acceso a los cuartos técnicos solo estará permitido por el área de TI.
- Las llaves de los cuartos técnicos deben de ser custodiadas por el área de TI.
- Para la manipulación de los equipos y cableado alojado en los cuartos técnicos deben de estar presente personal de TI.
- Está prohibido la manipulación los equipos de telecomunicaciones por personal ajeno al área de TI.

- Está prohibido el acceso a los cuartos técnicos por usuarios particulares.

CAPÍTULO II. DATACENTERS

ARTÍCULO 8. CONDICIONES DE DATACENTERS

- Los datacenters son espacios los cuales están destinados para alojar equipos tecnológicos que requieran unas condiciones muy específicas para la prestación de su función, estos sitios están ubicados de manera centralizada en la Universidad y sus centros de servicios.
- Estos deben de contar con polo a tierra.
- Deben de tener suministro de energía eléctrica regulada.
- Deben de contar con UPS y planta eléctrica de respaldo.
- Deben de contar con ingreso mediante control de acceso enlazado a la central de monitoreo de la Universidad.
- Deben de contar con aire acondicionado de precisión.
- Se deben de tener rutas de acceso para el cableado de datos o fibra óptica debidamente organizado y señalizado.
- Debe de contar con sistema antiincendios debidamente señalizada según la normativa de seguridad y salud en el trabajo institucional.
- Los cuartos técnicos deben de estar en zonas libres de humedad, o donde se tenga riesgo ambiental.
- Cualquier equipo que deba ser alojado en los cuartos técnicos deberá contar con la revisión y aprobación del área de TI y debe de cumplir con requerimientos mínimos:
- Debe de ser un equipo de rack.
- Debe de soportar 120 Voltios de energía corriente alterna (AC).
- Los equipos deben de contar con polo a tierra.

ARTÍCULO 9. CONDICIONES DE DATACENTERS

- Está prohibido el uso de los datacenters con fines ajenos a temas tecnológicos.
- No está permitido su uso como bodegas.
- Los datacenters deben de estar libres de objetos que pongan en riesgo la integridad de los equipos.
- En los cuartos técnicos no se deben de instalar tableros eléctricos, los temas eléctricos deben de tener un espacio diferente.
- El acceso a los datacenters solo está permitido bajo autorización del personal de Infraestructura de TI.
- Para la manipulación de los equipos y cableado alojado en los cuartos técnicos deben de estar presente personal de Infraestructura de TI.
- Está prohibida la manipulación de los equipos de telecomunicaciones a personal ajeno de Infraestructura de TI.
- Está prohibido el acceso a los cuartos técnicos por usuarios particulares.

www.ces.edu.co Calle 10 A Nº 22-04 A.A. 054 591 Conmutador 444 05 55 Fax 266 60 46 NIT 890.984.002-6 Medellín / Colombia VIGILADA MINEDUCACIÓN

CAPÍTULO III. PUNTOS DE DATOS

ARTÍCULO 10. CONDICIONES DE PUNTOS DE DATOS

- Los puntos de datos para trabajo están destinados para las áreas que no son de coworking y que debido a las funciones del empleado requiera una conexión estable y continua.
- Los puntos de datos están reservados solo para personal administrativo y de docencia.
- Para la solicitud del punto de datos debe de haber previa aprobación por parte de seguridad y salud en el trabajo avalando que cumpla con las condiciones mínimas para la utilización del espacio como lugar de trabajo.
- Para la instalación del punto de datos debe cumplir los requisitos mínimos los cuales se relacionan a continuación:
- No debe superar los 90 metros de distancia del cuarto técnico más cercano.
- El punto debe de tener aval técnico por parte del área de TI.
- Los puntos de datos se instalarán mínimamente en cableado categoría 6A según la norma internacional y según el tipo de uso para el cual se requiera.

ARTÍCULO 11. RESTRICCIONES DE PUNTOS DE DATOS

- No está permitido el uso de puntos de datos por personal externo de la Universidad y sus centros de servicios o proyectos institucionales.
- No se permite la conexión de equipos como switches o enrutadores a los puntos de red de la Universidad ni sus centros de servicios para ampliar la capacidad de puntos.
- Solo se permite la conexión de quipos de cómputo institucionales o teléfonos físicos los cuales se deberán suministrar por el área de TI.
- Queda prohibida la manipulación de los tomas de puntos de datos por personal externo ni administrativo sin el acompañamiento del área de TI.

CAPÍTULO IV. WIFI

ARTÍCULO 12. DEFINICIONES DE WIFI.

- La Universidad CES dispone del servicio WIFI en todos sus bloques, zonas comunes y aulas de clase, al igual que a sus centros de servicios.
- Para usuarios administrativos se cuenta con una red WIFI dedicada para su uso diario la cual le permitirá la movilidad, para el acceso a esta deberá de acceder mediante un usuario y contraseña previamente suministrado por el área de TI.
- Para usuarios estudiantes la Universidad provee una red WIFI con la cual podrán conectar sus equipos y dispositivos personales con el usuario y contraseña previamente informado por el área de TI.
- Para los puntos de ventas (Concesionarios) la Universidad CES le proporcionará una red exclusiva para la prestación del servicio pactado con la Universidad, para la asignación de un acceso, estos deberán de tener aval de la Coordinación Administrativa.

- Para los invitados y usuarios externos, la Universidad CES proveerá una red con la cual se podrá acceder a los servicios de internet.
- Para los proyectos que se encuentren en ejecución, el área de TI proveerá un usuario sobre la red de empleados para su acceso a los servicios de internet.
- Para solicitar cobertura WIFI se deberá de informar al área de TI quienes revisaran en sitio la solicitud y viabilidad financiera y técnica.

ARTÍCULO 13. RESTRICCIONES DE WIFI

- Las credenciales de acceso a la red wifi son personales e intransferibles.
- La cobertura WIFI, está sujeta a disponibilidad y factibilidad técnica.

CAPÍTULO V. SERVICIOS DE VOZ

ARTÍCULO 14. DEFINICIONES DE SERVICIOS DE VOZ

- La Universidad CES y centros de servicio dispone para sus colaboradores líneas telefónicas para la comunicación con personal interno y externo.
- Las solicitudes de líneas telefónicas deberán de contar con el aval del jefe del área.
- Todas las extensiones telefónicas sin excepción deberán estar debidamente identificadas con el nombre de la persona responsable de la línea, en caso de ser un centro o área de servicio, deberá contener el nombre que identifica.
- El área de TI deberá de validar el tipo de acceso que se debe de instalar, teléfono físico u otra solución, la determinación del tipo de acceso se basará única y exclusivamente en aspectos técnicos.
- Para solicitar llamadas nacionales y celular deberá de contar con el aval del jefe del área.
- Para solicitar salidas internacionales deberá contar con aprobación del jefe del área.
- Se dispone de teléfonos físicos en zonas comunes para uso de la comunidad universitaria para comunicación con las diferentes áreas.

ARTÍCULO 15. RESTRICCIONES DE SERVICIOS DE VOZ

- No se instalarán líneas telefónicas a personal externo o de proyectos ajenos a la Universidad.
- Es responsabilidad de la persona que se le asigna la línea telefónica el correcto uso de esta.
- No está permitido el uso de los teléfonos ubicados en zonas comunes para llamadas externas, líneas celulares, nacionales o internacionales.

CAPÍTULO VI. SERVICIOS DE TELECOMUNICACIONES PARA PROYECTOS

ARTÍCULO 16. DEFINICIONES DE SERVICIOS DE TELECOMUNICACIONES PARA PROYECTOS

- El área de TI apoyará en los proyectos con los aspectos tecnológicos, según la necesidad de cada proyecto se evaluará y se propondrán las opciones más costo-beneficiosas.

www.ces.edu.co Calle 10 A Nº 22-04 A.A. 054 591 Conmutador 444 05 55 Fax 266 60 46 NIT 890.984.002-6 Medellín / Colombia VIGILADA MINEDUCACIÓN

- Toda solicitud de servicios de telecomunicaciones debe de estar avalada por el jefe del área a la que corresponde el proyecto y deberá contar con presupuesto para su implementación.

ARTÍCULO 17. RESTRICCIONES DE SERVICIOS DE TELECOMUNICACIONES PARA PROYECTOS

- No se atenderán solicitudes sin el aval del jefe del área.
- El área de TI actuará como sugerente de buenas prácticas y de medios tecnológicos en nombre de la Universidad, no será responsable ni administrador de los recursos económicos del proyecto.

TÍTULO III. SISTEMAS DE INFORMACIÓN
CAPÍTILO I. CORREO INSTITUCIONAL

ARTÍCULO 18. DEFINICIONES DE CORREO INSTITUCIONAL

- Cada empleado que requiera acceso a correo, el área de TI le proveerá una cuenta institucional.
- El jefe del área deberá realizar la solicitud mediante el catálogo de servicios.
- Las cuentas de correo genéricas deberán contar con aprobación del jefe del área y del jefe de comunicaciones, estas se deberán solicitar por medio del catálogo de servicios.
- Cada usuario es responsable del contenido enviado y recibido en el correo electrónico.
- El usuario asignado es único e intransferible.
- Cada estudiante matriculado deberá contar con correo institucional asignado por el are de TI, estos correos deberán de llevar el siguiente estándar: apellido.nombre@uces.edu.co y será la herramienta de comunicación institucional tanto interna como externa, cada usuario es responsable por el envío de información desde estas cuentas.
- Las cuentas de usuario y contraseñas utilizados para acceder a los sistemas de información deben tratarse como información confidencial de la Universidad. Por lo tanto, las contraseñas son de uso personal e intransferible.
- Las cuentas de correo bajo los dominios CES y UCES deben tener activada aplicaciones de validación de identidad.
- La firma de correo electrónico deberá de manejarse según el estándar indicado por el área de comunicaciones institucionales.
- Solo las áreas autorizadas por comunicaciones institucionales podrán enviar correos masivos.
- En caso de requerir conservar la información del correo electrónico de un usuario al momento de retirarse de la organización, el jefe del área deberá solicitar en un plazo menor a 30 días calendario el respaldo de la información, luego de este tiempo, TI no se hará responsable por la pérdida de la misma.
- Los usuarios deberán reportar a TI cualquier comportamiento sospechoso como intentos de suplantación de identidad o uso indebido de las cuentas institucionales.

- Las cuentas de correo que lleven más de 365 días inactivas serán eliminadas, esto aplica para cuentas administrativas, genéricas, de estudiantes y de

ARTÍCULO 19. RESTRICCIÓN EN CUENTAS INSTITUCIONALES

- No se permite el uso de las cuentas institucionales para fines personales.
- Las cuentas institucionales solo se asignan a personal con contrato o matrícula en la Universidad, no se realiza asignación de correos institucionales a personal externo.
- No se permite desactivar verificaciones de acceso a las cuentas institucionales.

CAPITULO II. SOFTWARE Y LICENCIAMIENTO

ARTÍCULO 20. CONDICIONES DE ADQUISICIÓN SOFTWARE

- Todas las solicitudes de adquisición de software a la medida o licencia deben tener autorización del ordenador del gasto y tener presupuesto asignado.
- El área de TI apoyará en los proyectos con los temas tecnológicos, según la necesidad de cada proyecto se evaluará y se propondrán las opciones más costo-beneficiosas y así dar viabilidad al proyecto.
- Es responsabilidad del área en donde surge la necesidad solicitar el acompañamiento del área de TI, cuando requiera algún tipo de implementación de software.
- Es responsabilidad del área de TI definir el requerimiento y procesos, manteniendo la colaboración y la comunicación entre las diferentes áreas.
- Para realizar selección de proveedor desde el área de TI se debe contemplar la política de adquisición de bienes y servicios. Con el proveedor seleccionado se implementan metodologías de desarrollo, selección adecuada de tecnologías, teniendo en cuenta los requisitos específicos de cada proyecto y las tendencias del mercado, así como la asignación de recursos adecuados y la planificación de tiempos y costos.
- El área de TI implementa mecanismos de seguimiento y control con los proveedores para garantizar que los proyectos de desarrollo se ejecuten según lo planificado y se cumplan los objetivos establecidos.
- Es responsabilidad de TI generar o solicitar documentación completa y comprensible de la solución.

ARTÍCULO 21. RESTRICCIONES DE ADQUISICIÓN DE SOFTWARE

- El área de TI no desarrolla ni implementa soluciones sin la debida autorización del ordenador del gasto.
- No se realizan implementaciones de sistemas construidos con tecnologías obsoletas o que no cumplan con las condiciones de seguridad establecidas en la presente política.

ARTÍCULO 22. DEFINICIONES DE RENOVACIÓN DE SOFTWARE

- Las solicitudes de renovación de licenciamiento de software deben tener autorización del ordenador del gasto y tener presupuesto asignado.

- El área de TI es el área autorizada por la Universidad para realizar renovaciones de licenciamiento de software.
- Es responsabilidad del área de TI realizar todo el proceso de renovación de licenciamiento en conjunto con el proveedor y dar respuesta a las diferentes áreas antes de las fechas de vencimiento establecidas.
- El área de TI estará en la facultad de desactivar las licencias que hayan caducado, ya sea porque finalizó el período de licenciamiento asignado y no fue aprobada su prórroga de uso, o porque sus características no se ajustan a las necesidades o requerimientos de la Universidad, o por cualquier otra situación que impida su uso.
- El área de TI implementa mecanismos de seguimiento y control de los licenciamientos a cargo para garantizar su renovación en los tiempos establecidos en la contratación del servicio y así evitar interrupción que puedan afectar la operación de los procesos.

ARTÍCULO 23. RESTRICCIONES DE RENOVACIÓN DE SOFTWARE

- No se permiten procesos de renovación de licenciamiento de software de terceros sin autorización del área de TI.
- No se realiza procesos de renovación de licenciamiento de software de terceros para fines personales.

ARTÍCULO 24. DEFINICIONES DE CONTROL DE CAMBIOS

- Todas las solicitudes de control de cambios en software deben incluir la autorización del aprobador del gasto y tener presupuesto asignado.
- El área de TI realiza el levantamiento de requisitos, utilizando el procedimiento definido para este proceso.
- El control de cambios será sometido a la aprobación del líder funcional.
- Una vez aprobado el control de cambios, se solicitará al proveedor tecnológico la estimación de costos, horas de desarrollo y tiempo de entrega.
- Desde el área de TI debe ser aprobada la estimación del proveedor.
- El control de cambios debe considerar entregables y cronograma de actividades, según metodología implementada.
- El área de TI acompaña la implementación en conjunto con el proveedor, realizando seguimiento a los entregables.
- Se realizarán pruebas funcionales exhaustivas de los entregables para garantizar su correcto funcionamiento.
- La entrega de los cambios implementados se coordinará con el área funcional correspondiente.

ARTÍCULO 25. RESTRICCIONES DE CONTROL DE CAMBIOS

- No se realizan controles de cambio en software si no cumplen con los estándares o normativas legales.
- No se emplean recursos, ni funcionalidades que posean propiedad intelectual o derechos de autor de terceros sin la previa autorización correspondiente.
- No se implementan cambios que comprometan o afecten la integridad de la infraestructura o seguridad de la aplicación.

- No se implementan cambios o mejoras en software si no garantiza la protección de datos.

ARTÍCULO 26. DEFINCIONES DE MANTENIMIENTO Y SOPORTE DE SOFTWARE

- El área de TI, realiza mantenimiento y soporte a las aplicaciones corporativas a través de los proveedores tecnológicos.
- Los jefes inmediatos realizan la solicitud al área de TI a través de los canales establecidos, de la creación de los usuarios en las aplicaciones requeridas de acuerdo con el rol y perfil requerido.
- El área de TI desactiva las cuentas de usuario en las aplicaciones una vez los usuarios finalizan su vínculo laboral.
- El área de TI gestiona el mantenimiento a las aplicaciones, así como control de versiones y actualización de componentes.
- Una vez la aplicación esté en funcionamiento, se incluye en la política de backup para respaldar la base de datos de la aplicación.
- El área de TI acordará con una de las áreas cuando se realizarán actividades de soporte y manteniendo preventivo.

ARTÍCULO 27. RESTRICCIONES MANTENIMIENTO Y SOPORTE DE SOFTWARE

- A través del catálogo de servicios no se reciben solicitudes de proyectos de software e infraestructura.
- Sólo se brindará soporte y mantenimiento sobre los aplicativos que estén dentro de los servicios contratados y gestionados por el área de TI.

ARTÍCULO 28. DEFINICIONES DE SOFTWARE LIBRE

- El uso de software libre o de código abierto debe ser autorizado por el área de TI, proporcionando una justificación fundamentada sobre su necesidad y utilidad, junto con una evaluación de los posibles riesgos de seguridad.
- Se realizarán pruebas de seguridad y verificación de compatibilidad antes de autorizar la instalación de cualquier software de código abierto en los sistemas institucionales.
- En caso de aprobación, el software libre será instalado y configurado por personal autorizado del área de TI.
- El área de TI realizará de manera regular auditorías para garantizar el cumplimiento de las políticas y procedimientos relacionados con la instalación de software libre.

ARTÍCULO 29. RESTRICCIONES DE SOFTWARE LIBRE

- Solo el personal designado por el área de TI estará autorizado para realizar la instalación, actualización y configuración del software.

CAPÍTULO III. OTRAS HERRAMIENTAS

ARTÍCULO 30. DEFINICIONES DE TRABAJO COLABORATIVO Y ESPACIOS EN NUBES

- La Universidad CES proveerá a las áreas, facultades y proyectos según la necesidad de herramientas ofimáticas con las cuales se puedan realizar trabajos de manera colaborativa.
- El área de TI proveerá sitios en los servidores institucionales y en nube según necesidad, los usuarios podrán solicitar recuperación de la información en un plazo menor a 30 días calendario.
- Para solicitud de herramientas y aplicaciones de terceros alojadas en internet, se deberá contar con el visto bueno del ordenador del gasto, contar los formatos del área de contabilidad debidamente diligenciados y el trámite de adquisición se deberá realizar en compañía del área de TI.
- En caso de requerir adquisición de software de un proveedor especifico, se deberá justificar el motivo y TI deberá evaluar la viabilidad de la adquisición, se deberá contar con los formatos del área de contabilidad debidamente diligenciados y el trámite de adquisición se deberá realizar en compañía del área de TI.
- Para la instalación de herramientas o software gratuito, el área de TI evaluará los riesgos e implicaciones que tenga la herramienta, esta deberá cumplir los lineamientos indicados en la presente política y solo se podrá instalar con previa aprobación de TI.
- La Universidad dispone de espacios en servidores y nube para almacenamiento de información de manera segura, cada área o proyecto deberá solicitarlo a TI

ARTÍCULO 31. RESTRICCIONES TRABAJO COLABORATIVO Y ESPACIOS EN NUBES

- Queda prohibido almacenar información personal en los espacios de trabajo colaborativo y nubes de la Universidad, la información almacenada en los servidores y nubes deberá ser única y exclusivamente utilizada para información relacionada a los proyectos, áreas y facultades de la Universidad.
- No se permitirá el uso de software que incumpla alguno de los requerimientos anteriormente descritos.
- No se tramitará software sin las autorizaciones correspondientes.
- No se instalará software que sea requerido con fines personales.
- TI no se hace responsable por la pérdida de información superior a 30 días calendario.

TÍTULO IV. SEGURIDAD DE LA INFORMACIÓN
CAPÍTULO I. VPN

ARTÍCULO 32. DEFINICIONES DE VPN PARA USUARIOS INSTITUCIONALES

- Los usuarios institucionales que según sus funciones requieran acceso mediante la VPN institucional, deben solicitarla al área de TI mediante el catálogo de servicios con la respectiva autorización del jefe inmediato.
- Si se tiene indicios de un compromiso de credenciales o cualquier actividad sospechosa relacionada con el acceso remoto, TI está en la potestad de bloquear el acceso.

- El equipo que se emplee para acceder de forma remota debe ser avalado por el área de TI.

ARTÍCULO 33. RESTRICCIONES DE VPN PARA USUARIOS INSTITUCIONALES

- Las credenciales de acceso a la VPN son personales e intransferibles, no se permite compartirlas con terceros bajo cualquier circunstancia.
- El acceso remoto mediante la VPN solo está permitido para llevar realizar actividades relacionadas con las responsabilidades laborales o académicas dentro de la Universidad.

ARTÍCULO 34. DEFINICIONES DE VPN PARA USUARIOS CONTRATISTAS Y EXTERNOS

- Los contratistas y usuarios externos que requieran acceder remotamente a los recursos de red de la Universidad deben solicitar este acceso al área de TI y contar con los respectivos avales del área de seguridad de la información.
- Contratistas o personal externo deberán firmar los acuerdos de confidencialidad y delegación de responsabilidades para la entrega de la VPN.
- Las credenciales de la VPN están diseñadas para ser utilizadas por un único usuario a la vez.
- Todo contratista y personal externo deberá recibir una capacitación impartida por el área de seguridad de la información sobre el manejo de la VPN, como requisito previo a la asignación de acceso.
- El equipo que se emplee para acceder de forma remota debe ser avalado por el área de TI.

ARTÍCULO 35. RESTRICCIONES DE VPN PARA USUARIOS CONTRATISTAS Y EXTERNOS

- El acceso remoto a través de la VPN está limitado a actividades relacionadas únicamente con proyectos o colaboraciones institucionales.
- Las credenciales de acceso a la VPN son personales e intransferibles, no se permite compartirlas con terceros bajo cualquier circunstancia.

CAPÍTULO II. DOMINIOS Y URL'S INSTITUCIONALES

ARTÍCULO 36. DEFINICIONES DE DOMINIOS Y URL'S INSTITUCIONALES

- Toda solicitud de creación de dominios y URL's institucionales debe ser enviada a través del catálogo de servicios. Estas solicitudes deben contar con la previa autorización del área de comunicaciones.
- Todo sitio o dominio publicado en internet deberá ser aprobado y revisado por TI quienes revisarán que cumpla con certificados y estándares para su protección ante amenazas del ciber espacio.
- Los sitios institucionales deberán de estar cobijados bajo el contexto "ces.edu.co", en caso de requerir un dominio diferente por una línea de negocio diferente, este deberá contar con el visto bueno de la rectoría y su gestión y administración será por TI.

ARTÍCULO 37. RESTRICCIONES DE DOMINIOS Y URL'S INSTITUCIONALES

- El área de TI es responsable de registrar, renovar y mantener el control de todos los dominios y sitios web asociados con su marca institucional.
- Se establecerán controles estrictos para evitar registros de dominios similares o falsificados que puedan ser utilizados para engañar a los usuarios y comprometer la seguridad de la comunidad universitaria.
- Toda la información publicada en internet bajo los dominios institucionales y líneas de negocio, deben de cumplir la normativa vigente de propiedad intelectual.

CAPÍTULO III. ACCESO A SISTEMAS DE INFORMACIÓN

ARTÍCULO 38. DEFINICIONES DE ACCESO A SISTEMAS DE INFORMACIÓN

- Cualquier usuario con credenciales de acceso activas puede acceder a los diferentes sistemas de información de acuerdo los permisos establecidos.
- Cada jefe de área deberá notificar al área de TI sobre las fechas de vacaciones, novedades, el TI, realizará bloqueo a los sistemas de información durante el período de ausencia del empleado
- El área de Talento Humano deberá notificar periódicamente a las personas retiradas de la institución y el área de TI se encargará de realizar los bloqueos.
- La suspensión o desactivación de cuentas se realizará únicamente por el personal autorizado del área de TI después de recibir una notificación oficial y verificada.
- La notificación deberá ser realizada de manera oficial y a través de canales seguros de comunicación, evitando cualquier comunicación informal que pueda comprometer la seguridad de la información.
- El área de TI deberá identificar y clasificar los activos tecnológicos esenciales de la Universidad, tales como servidores, bases de datos y URLs.
- El área de TI deberá introducir medidas de seguridad concretas destinadas a salvaguardar estos activos de información, incluyendo rigurosos controles de acceso, supervisión constante y respaldo regular de datos.

ARTÍCULO 39. RESTRICCIONES DE ACCESO A SISTEMAS DE INFORMACIÓN

- No se tramitan solicitados por fuera de los canales oficiales de comunicación.

CAPÍTULO IV. ALMACENAMIENTO DE INFORMACIÓN

ARTÍCULO 40. DEFINICIONES DE ALMACENAMIENTO DE INFORMACIÓN

- El área de TI establecerá procedimientos para el almacenamiento centralizado y seguro de la información, en caso de necesitar restauración o recuperación esta, se podrá hacer en un plazo menor a 30 días calendario, pasado este tiempo TI no será responsable, la medida aplica para archivos guardados en los servidores, SharePoint, Correo Electrónico.
- Se establecerá un proceso regular de respaldo de datos con el objetivo de garantizar la disponibilidad, confidencialidad e integridad de la información en caso de incidentes o desastres.

- Se implementarán herramientas de monitoreo y auditoría para registrar y supervisar todas las actividades relacionadas con el almacenamiento de información.
- El área de TI se reserva el derecho de eliminar archivos maliciosos que contengan virus, malware o que se encuentren corruptos.

ARTÍCULO 41. RESTRICCIONES DE ALMACENAMIENTO DE INFORMACIÓN

- El almacenamiento de información sensible estará restringido a sistemas y plataformas autorizadas por el área de TI, evitando el uso de dispositivos o servicios no aprobados que puedan comprometer la seguridad de los datos.
- La asignación de permisos de acceso estará sujeta a una revisión y aprobación previa por parte de los responsables de seguridad de la información, evitando el acceso no autorizado o indebido a los datos.
- El acceso a los datos de respaldo estará restringido al personal autorizado y solo se utilizará para fines de recuperación de información, evitando su uso indebido o no autorizado.
- No está permitido almacenar información en USB o discos duros externos, los medios de almacenamiento permitidos son SharePoint, Correo, servidor de archivos.

CAPÍTULO V. NAVEGACIÓN EN INTERNET

ARTÍCULO 42. ACCESO A INTERNET

- Las páginas permitidas para navegación y consulta en internet son aquellas que cumplan los siguientes propósitos:
  - **Educativas**: Páginas de institutos, Universidades, colegios e instituciones dedicadas a la educación en general como bibliotecas y contenido educativo en general
  - **Informativas**: Páginas web relacionados con noticias, medios de comunicación, revistas, revistas científicas, sitios de divulgación científica, blogs relacionados con articules especializados.
  - **Servicios de streaming** Páginas que sean utilizadas por la Universidad CES para transmitir eventos institucionales, podcast y contenido educativo
  - **Comercio electrónico:** Sitios relacionados con entidades financieras, servicios de banca, páginas dedicadas a venta de artículos masivos o especializados.
  - **Gobierno y servicios públicos:** Páginas web de ministerios, agencias e instituciones gubernamentales.
  - **Salud y bienestar:** Páginas web dedicados a proporcionar información, recursos, y servicios que promueven la salud física, mental y emocional.
- Los empleados deben solicitar el acceso a URL's previamente bloqueadas por los sistemas de seguridad de la red, proporcionando una justificación para solicitar dicho acceso a la URL bloqueada, y obtener la aprobación del área de TI.
- Es responsabilidad del área de TI realizar campañas para divulgar a los usuarios sobre los riesgos de seguridad asociados con la navegación en línea y proporcionar capacitación regular sobre concienciación en seguridad cibernética.

ARTÍCULO 43. RESTRICCIONES DE NAVEGACIÓN

- El área de TI bloqueará las páginas que sean consideradas como no seguras, en caso de requerir acceso a alguna de estas, deberá solicitar por medio del catálogo de servicios el desbloqueo.
- No se permite navegación en páginas que infrinjan las normativas colombiana ley 1453 de 2011 artículo 8, Ley 679 de 2001, Ley 1581 de 2012, Decreto 1524 de 2002, Ley 1273 de 2009
- Para los puestos de trabajo implicados en recaudo de dinero (Cajas y puntos de pago) solo se está permitida la navegación para páginas de comercio electrónico, gobierno y servicios públicos.
- No se permite la navegación en páginas de redes sociales salvo para áreas donde sea requerido por razones laborales, para ello deberá solicitar según TITULO IV, Capítulo V Artículo 42. ACCESO A INTERNET.

ARTÍCULO 44. INCIDENTES DE SEGURIDAD

- Cualquier usuario que utilice los servicios de información de la Universidad, debe informar cualquier incidente, sospecha de amenazas o debilidad que pueda comprometer la confidencialidad, integridad o disponibilidad de los activos de información. Estos casos deben ser reportados a la Mesa de Ayuda o al correo ciberseguridadces@ces.edu.co para su gestión adecuada.
- Todos los incidentes de seguridad deben ser gestionados buscando su causa raíz, con el objetivo de minimizar su ocurrencia.

ARTÍCULO 45. SEGURIDAD PARA LOS PROVEEDORES

- Los proveedores deben informar al área de TI cualquier incidente que comprometa la confidencialidad, integridad y disponibilidad de los activos de información, poniendo en riesgo la operación de la Universidad.
- Los proveedores vinculados a la Universidad que tengan acceso a información sensible deben firmar un acuerdo de confidencialidad.

ARTÍCULO 46. TRABAJO REMOTO

- Para proteger la información y los sistemas de la Universidad, todas las conexiones entre los equipos de teletrabajo y la red deben realizarse a través de una VPN aprobada por el jefe del Área.
- Todos los equipos utilizados para teletrabajo deben contar con la línea base aplicada antivirus actualizado y avalado por el área de TI, y mantenerse actualizados con los últimos parches de seguridad y actualizaciones de software.
- Los usuarios son responsables de custodiar físicamente sus equipos y reportar cualquier incidente de seguridad.
- Es fundamental que los empleados participen en programas de capacitación continua y promuevan una cultura de seguridad y concienciación sobre las amenazas cibernéticas.

TÍTULO V. SERVICIOS DE MESA DE AYUDA

ARTÍCULO 47. SOPORTE A USUARIOS INSTITUCIONALES Y COMUNIDAD EN GENERAL

- Los canales autorizados para la atención de requerimientos e incidentes son la línea telefónica, el correo electrónico y el catálogo de servicios.
- La mesa de servicios está autorizada solo para revisión de equipos de la Universidad.
- La mesa de servicio podrá atender las solicitudes presencial o virtualmente según corresponda.
- Solo el área de TI por medio de la mesa de ayuda podrá intervenir los equipos de voz, computo, impresión, ninguna otra área o persona está autorizada para estas actividades.
- TI tendrá equipos de cómputo e impresoras para eventos académicos, culturales y de interés general para la comunidad universitaria, dicha solicitud se realizará mediante el catálogo de servicios institucional.
- El solicitante de los equipos de cómputo para los eventos será responsable por la custodia de los equipos una vez sean entregados por la mesa de ayuda.

ARTÍCULO 48. RESTRICCIÓN SOPORTE A USUARIOS INSTITUCIONALES Y COMUNIDAD EN GENERAL

- No está permitida la intervención o mantenimiento técnico de equipos de particulares o ajenos a la Universidad.
- No se hacen prestamos de equipos a personal externo.
- Solo se prestan equipos para eventos dentro de las diferentes sedes de la Universidad.
- Ningún equipo salvo por autorización expresa del área de TI podrá tener privilegios de administrador.
- No se permite el retiro de los equipos para eventos externos de la Universidad o sus sedes.
- No se permite la instalación de software a los equipos para eventos salvo previa autorización de TI, que deberá tramitarse mediante el catálogo de servicios.

ARTÍCULO 49. SOLICITUD DE ASIGNACIÓN DE EQUIPO USUARIOS NUEVOS

- Los jefes de área deben solicitar la asignación de equipos de cómputo para usuarios nuevos mediante el catálogo de servicios, proporcionando los datos del nuevo usuario y el tipo de equipo requerido.
- La solicitud debe realizarse con al menos cinco días hábiles de anticipación a la fecha de inicio del nuevo usuario.
- El área de TI se encargará de preparar y entregar el equipo al nuevo usuario, asegurándose de que cumpla con las políticas de seguridad y configuración establecidas.

ARTÍCULO 50. PAZ Y SALVO POR RETIRO

- En caso de retiro voluntario o renuncia, los usuarios deben entregar todos los equipos y accesos asignados a través del área de TI.
- El paz y salvo incluye la devolución de equipos, la desactivación de credenciales y la transferencia de cualquier información relevante.
- El jefe inmediato debe notificar al área de TI sobre el retiro del usuario a través del catálogo de servicios, para coordinar el proceso de devolución y desactivación.

ARTÍCULO 51. SOLICITUD DE CAMBIO DE EQUIPO DE COMPUTO

- Para solicitar el cambio de equipo de cómputo, los usuarios deben enviar una solicitud a través del catálogo de servicios, detallando las razones para el cambio y el tipo de equipo requerido.
- El área de TI evaluará la solicitud considerando la disponibilidad de equipos y la justificación proporcionada.
- Las solicitudes aprobadas serán atendidas en un plazo acordado con el usuario, garantizando la mínima interrupción de sus actividades.

ARTÍCULO 52. ACOMPAÑAMIENTO DE EXÁMENES ACADÉMICOS

- El área de TI a través de su mesa de ayuda ofrecerá soporte y acompañamiento técnico para la realización de exámenes académicos, según lo solicitado por los profesores o coordinadores académicos.
- Las solicitudes de acompañamiento deben realizarse a través del catálogo de servicios con al menos cinco días hábiles de anticipación.
- El personal de TI por la mesa de ayuda estará disponible en el examen para resolver cualquier incidencia técnica que surja.

ARTÍCULO 53. SOPORTE A EQUIPOS EXTERNOS

- El área de TI evaluará la solicitud y determinará la viabilidad de proporcionar soporte, considerando la compatibilidad y políticas de seguridad.
- Los usuarios externos deben aceptar y cumplir con las políticas de uso de la Universidad CES para recibir soporte técnico.
- La mesa de ayuda no podrá destapar o abrir el equipo de cómputo de personal externo.

TÍTULO VI. GOBIERNO DE TI

ARTÍCULO 54. ESTRUCTURA DE GOBIERNO DE TI

El Gobierno de TI define la priorización y definición de proyectos de acuerdo con los planes estratégicos y operativos. Si mismo, establece un control sobre el uso de los recursos asignados a los proyectos y permite que las diferentes áreas se involucren en la planeación y ejecución de estos.

El Gobierno de TI está compuesto de la siguiente manera:

- Comité ejecutivo de TI
- Comité operativo de TI

ARTÍCULO 55. RESPONSABILIDADES DEL GOBIERNO DE TI

- Comité ejecutivo de TI: Revisión y control en relación con los recursos humanos, financieros y tecnológicos. Alineación de prioridades institucionales en relación con los proyectos de TI en curso, nuevas necesidades, así como la planeación a mediano y largo plazo.
- Comité operativo de TI: Gestión de TI para la alineación y toma de decisiones en relación con los recursos humanos, financieros y tecnológicos de operación y proyectos.

ARTÍCULO 56. MIEMBROS DEL GOBIERNO DE TI

- Comité ejecutivo de TI: Directora administrativa y financiera, comité operativo de TI.
- Comité operativo de TI: Líder de TI, Coordinador de infraestructura de TI, Coordinador de sistemas de información, Coordinador de servicios digitales.

ARTÍCULO 57. FRECUENCIA DE REUNIONES DEL GOBIERNO DE TI

- Comité ejecutivo de TI: trimestral
- Comité operativo de TI: semanal

TÍTULO VII. CONSIDERACIONES FINALES

ARTÍCULO 58. REVISIÓN Y ACTUALIZACIÓN

- La tecnología y las amenazas cibernéticas están en constante evolución. Por lo tanto, la política de TI sea revisada y actualizada periódicamente. Se realizará una revisión anual como mínimo, o más frecuentemente si hay cambios significativos en el entorno tecnológico o normativo. Las revisiones deben involucrar a todas las partes interesadas relevantes, incluyendo el equipo de TI y la alta dirección.

ARTÍCULO 59. CUMPLIMIENTO Y AUDITORÍA

- El cumplimiento de esta política debe ser monitoreado regularmente a través de auditorías internas y externas. Las auditorías ayudarán a identificar cualquier incumplimiento o área de mejora, asegurando que la organización se adhiera a las mejores prácticas y a las normativas legales vigentes. Los resultados de las auditorías deben ser reportados a la alta dirección y se deben implementar acciones correctivas de manera oportuna.

ARTÍCULO 60. EDUCACIÓN Y CAPACITACIÓN

- La concienciación y formación de los empleados son esenciales para la efectividad de la política de TI. Se deben realizar programas regulares para asegurar que todos comprendan sus responsabilidades en relación con la seguridad de la información y la protección de los recursos tecnológicos. La capacitación debe incluir simulaciones de incidentes y actualizaciones sobre nuevas amenazas y mejores prácticas.

ARTÍCULO 61. GESTIÓN DE CAMBIOS

- Cualquier cambio en la infraestructura de TI, incluyendo la introducción de nuevos sistemas, aplicaciones o hardware, debe seguir un proceso de gestión de cambios formal. Este proceso debe incluir la evaluación de riesgos, pruebas y la aprobación de las partes interesadas antes de la implementación. La documentación de todos los cambios debe mantenerse de manera detallada.

ARTÍCULO 62. CONFIDENCIALIDAD Y ÉTICA

- Todos los empleados deben adherirse a las normas de confidencialidad y ética en el manejo de la información de la organización. Cualquier violación de estas normas debe ser tratada con seriedad y puede resultar en acciones disciplinarias, incluyendo la terminación del empleo y posibles acciones legales.

ARTÍCULO 63. DOCUMENTACIÓN Y REGISTRO

- Mantener una documentación precisa y detallada de todas las políticas, procedimientos, incidentes y auditorías de TI. Esta documentación debe estar accesible para las partes autorizadas y debe ser mantenida de manera segura.

ARTÍCULO 64. COMUNICACIÓN

- Mantener una comunicación clara y efectiva sobre la política de TI. Se deben establecer canales de comunicación para reportar problemas, sugerencias y consultas relacionadas con la política de TI. La política de TI y cualquier cambio significativo deben ser comunicados a todos los empleados de manera oportuna.

ARTÍCULO 65. EVALUACIÓN DE RIESGOS

- La evaluación de riesgos debe ser un proceso continuo y dinámico. Se deben identificar, evaluar y mitigar los riesgos de manera proactiva. Los resultados de las evaluaciones de riesgos deben ser utilizados para ajustar la política de TI y mejorar las medidas de seguridad.

ARTÍCULO 66. COMPROMISO DE LA ALTA DIRECCIÓN

- El éxito de la política de TI depende del compromiso y apoyo de la alta dirección. La dirección debe demostrar su compromiso proporcionando los recursos necesarios, promoviendo una cultura de seguridad y cumplimiento.

ARTÍCULO 67. MEJORA CONTINUA

- La política de TI debe estar sujeta a un proceso de mejora continua, basado en el aprendizaje de incidentes pasados, la evolución de las mejores prácticas y los avances tecnológicos. Este enfoque asegurará que la organización esté siempre preparada para enfrentar nuevas amenazas y desafíos.

ARTÍCULO 68. PUBLICACIÓN

El presente acuerdo debe ser publicado mediante medio idóneo para el conocimiento de todos los integrantes de la comunidad educativa.

Comuníquese y cúmplase

Dado en Medellín a los treinta (30) días del mes de octubre de 2024.

JUAN GONZALO ARISTIZÁBAL VÁSQUEZ
Presidente (E)
Consejo Superior

PATRICIA CHEJNE FAYAD
Secretaria
Consejo Superior

www.ces.edu.co **Calle 10 A Nº 22-04** A.A. 054 591 **Conmutador 444 05 55** Fax 266 60 46 **NIT 890.984.002-6** Medellín / Colombia VIGILADA MINEDUCACIÓN