UNIVERSIDAD DEL QUINDÍO

UNIVERSIDAD DEL QUINDÍO ACREDITADA DE ALTA CALIDAD

RECTORIA

RESOLUCIÓN No. 6962

24 ENE 2020

POR MEDIO DE LA CUAL SE ADOPTAN EL PLAN ESTRATÉGICO TECNOLOGÍA DE LA INFORMACIÓN (PETI) 2019 – 2022 Y LAS POLÍTICAS DE GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN (TI) DE LA UNIVERSIDAD DEL QUINDÍO.

El Rector de la Universidad del Quindío en uso de sus facultades legales y estatutarias y especialmente las conferidas en los Acuerdos 005 del 28 de febrero de 2005 "Estatuto General" y 020 del 04 de diciembre de 2015 y

CONSIDERANDO

1- Que el proceso de planeación universitario está concebido desde la Constitución Política de Colombia de 1991, donde se estipula la educación superior como un servicio público. Con referencia a la planeación, se trazan lineamientos para que sea participativa y estratégica a fin de garantizar los principios de la función pública.

2- Que la Ley 30 de 1992 a través de la cual se organizó el servicio público de educación superior en su artículo 83 establece: "Las universidades estatales u oficiales deberán elaborar planes periódicos de desarrollo institucional, considerando las estrategias de planeación regional y nacional".

3- Que mediante las leyes 1581 de 2012 y 1712 de 2014, se establecen disposiciones generales para la protección de datos personales y se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional respectivamente.

4- Que el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones define los lineamientos, instrumentos y plazos de la estrategia de gobierno en línea para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones.

5- Que el Plan Estratégico de las Tecnologías de la Información (PETI) es el documento mediante el cual se define la estrategia bajo la cual se espera que las tecnologías de la información (TI) se integran con la misión, visión y objetivos institucionales.

6- Que conforme al Marco de Referencia del MinTIC, el PETI es parte integral de la estrategia de las instituciones y uno de los principales artefactos para expresarla, conformando su visión, estrategias y direccionando el resultado de un adecuado ejercicio de planeación, realizándose previamente a la definición de portafolios de proyectos y de un proceso de transformación que involucre tecnologías digitales.

RECTORIA

RESOLUCIÓN No. 6962

24 ENE 2020

POR MEDIO DE LA CUAL SE ADOPTAN EL PLAN ESTRATÉGICO TECNOLOGÍA DE LA INFORMACIÓN (PETI) 2019 – 2022 Y LAS POLÍTICAS DE GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN (TI) DE LA UNIVERSIDAD DEL QUINDÍO.

7- Que conforme a los principios de "Prioridad al acceso y uso de las Tecnologías de la Información y las Comunicaciones" y la "Masificación del Gobierno en Línea", ahora Gobierno Digital, consagrados respectivamente en los numerales 1° y 8° del artículo 2 de la Ley 1341 de 2009 , las entidades públicas deberán priorizar el acceso y uso a las Tecnologías de la Información y las Comunicaciones (TIC) en la producción de bienes y servicios, así como adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información (TI) en el desarrollo de sus funciones, con el fin de lograr la prestación de servicios eficientes a los ciudadanos.

8- Que el Decreto Único Reglamentario del Sector de Función Pública, desde el Decreto 1083 de 2015 y su modificación mediante el 1499 de 2017 y el 612 de 2018 del Departamento Administrativo de la Función Pública, establece que los organismos y entidades de los órdenes nacional y territorial de la Rama Ejecutiva del Poder Público deben liderar la gestión estratégica con las TIC mediante la definición, implementación, ejecución, seguimiento y divulgación de un PETI, el cual debe estar alineado a la estrategia y al modelo integrado de gestión de la entidad, teniendo un enfoque en la generación de valor público para habilitar las capacidades y servicios tecnológicos necesarios para impulsar las transformaciones, la eficiencia y la transparencia del Estado.

9- Que el Decreto 612 de 2018 establece los instrumentos para implementar la "Estrategia de Gobierno en Línea", ahora Política de Gobierno Digital, exigiendo la elaboración por parte de cada entidad de un Plan Estratégico de TI, así como de un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y un Plan de Seguridad y Privacidad de la Información que deben ser integrados en el plan de acción, el cual debe ser publicado en el sitio web oficial de la entidad.

10- Que mediante Resolución de Rectoría No.0531 del 23 de mayo de 2012 se modifica la estructura, funcionamiento y se asignan funciones en materia de Gobierno en línea al Comité Antitrámites y de Gobierno en Línea de la Universidad del Quindío, como instancia responsable del liderazgo, planeación e impulso de la Estrategia de Gobierno en Línea de la institución

11- Que mediante Acta No. 003, de sesión del día 19 de noviembre de 2019, el Comité Antitrámites y de Gobierno en Línea, aprobó presentar el proyecto de resolución ante la rectoría para la adopción del Plan Estratégico de Tecnologías de la Información y las Políticas de Gobierno de Tecnologías de

RECTORIA

RESOLUCIÓN No. 6982

24 ENE 2020

POR MEDIO DE LA CUAL SE ADOPTAN EL PLAN ESTRATÉGICO TECNOLOGÍA DE LA INFORMACIÓN (PETI) 2019 – 2022 Y LAS POLÍTICAS DE GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN (TI) DE LA UNIVERSIDAD DEL QUINDÍO.

la Información, por parte del área de Sistemas y Nuevas Tecnologías y el Asesor Tic de rectoría.

Que, sin más consideraciones,

RESUELVE

ARTÍCULO PRIMERO: Adoptar para la Universidad del Quindío el **PLAN ESTRATEGICO TECNOLOGÍAS DE LA INFORMACIÓN (PETI) 2019 – 2022 ANEXO No. 1, Y LAS POLITICAS DE GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN (TI) DE LA UNIVERSIDAD DEL QUINDÍO ANEXO No. 2,** en documentos anexos que forman parte integral de la presente Resolución. (PETI 104 Folios- Políticas de Gobierno TI 26 Folios)

ARTICULO SEGUNDO: El **PLAN ESTRATEGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (PETI) 2019 – 2022 Y LAS POLITICAS DE GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN (TI) DE LA UNIVERSIDAD DEL QUINDÍO** que se adoptan estarán vigentes durante el período 2019 – 2022, alineados con el Plan de Desarrollo Institucional, Plan de Mejoramiento para la Acreditación Institucional y el Plan de Fomento a la Calidad PFC, permitiendo revisiones periódicas y actualizaciones anuales siempre que sea necesario alinear o ajustar sus metas de acuerdo con los resultados de los seguimientos y análisis del contexto estratégico que realice el Macroproceso Gestión Tics, y previa aprobación del Comité Antitrámites y de Gobierno en línea o quien haga sus veces.

ARTICULO TERCERO: Es responsabilidad de la Alta Dirección y del Comité Antitrámites y de Gobierno en Línea o quien haga sus veces, prestar el apoyo necesario para la implementación del **PLAN ESTRATEGICO TECNOLOGÍA DE LA INFORMACIÓN (PETI) 2019 – 2022 Y LAS POLITICAS DE GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN (TI) DE LA UNIVERSIDAD DEL QUINDÍO,** y la verificación de su cumplimiento estará a cargo del líder del Macroproceso Gestión Tics de la Universidad del Quindío.

ARTICULO CUARTO: La divulgación y promoción de el **PLAN ESTRATEGICO TECNOLOGÍA DE LA INFORMACIÓN (PETI) 2019 – 2022 Y LAS POLITICAS DE GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN (TI) DE LA UNIVERSIDAD DEL QUINDÍO**, estará a cargo del Macroproceso Gestión Tics de la Universidad del Quindío, en coordinación con la Oficina Asesora de Comunicaciones; a través de los diferentes canales de divulgación dispuestos por la institución.

UNIVERSIDAD DEL QUINDÍO

UNIVERSIDAD DEL QUINDÍO ACREDITADA DE ALTA CALIDAD

RECTORIA

RESOLUCIÓN No. 6962

24 ENE 2020

POR MEDIO DE LA CUAL SE ADOPTAN EL PLAN ESTRATÉGICO TECNOLOGÍA DE LA INFORMACIÓN (PETI) 2019 – 2022 Y LAS POLÍTICAS DE GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN (TI) DE LA UNIVERSIDAD DEL QUINDÍO.

ARTICULO QUINTO: La presente Resolución rige a partir de la fecha de su expedición.

COMUNIQUESE Y CUMPLASE

Dada en Armenia Quindío a los 24 ENE 2020

JOSE FERNANDO ECHEVERRY MURILLO
Rector

	NOMBRES Y APELLIDOS	FIRMA
PROYECTÓ	Luis Horacio Buitrago Gallego - Porfesional Especializado Área TICS	
	Pedro Nel Herrera Garcias - Asesor TICS - Rectoría	
ELABORÓ	Diana Lorena Pardo Ruiz - Profesional Especializado Oficina Asesora Jurídica	
REVISÓ	Reinaldo Sierra Prieto - Jefe Oficina Asesora de Planeación	
	Estella López de Cadavid - Vicerrectora Administrativa	
APROBÓ	Diana Lorena Pardo Ruiz - Jefe Oficina Asesora Juridica (E)	

Los arriba firmantes declaramos que hemos revisado el presente documento y soportes (de ser el caso) y lo encontramos ajustado en términos técnicos y administrativos; así como a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la correspondiente firma.

Tabla de contenido

Historial de Versiones:

Nº Revisión	Fecha	Páginas modificadas	Elaborado/ Modificado por	Descripción del cambio
1	13/11/2019		Jose Daniel Isaza Hernandez	Creación del documento
2	15/11/2019		Revisión consultora password Liliana Andrea Torres Perez	Revisión de políticas

1. OBJETIVO

Disponer de un instrumento que defina las políticas mediante las cuales la Dirección de sistemas y nuevas tecnologías presta sus servicios a la Institución y definir los parámetros mediante los cuales se atiende las necesidades tecnológicas de la Universidad del Quindío.

2. ALCANCE

Estas políticas aplican a todo estudiante, egresado, empleado, contratista, personal temporal y cualquier persona vinculada a la Universidad del Quindío.

3. DEFINICIONES

- **Activo:** Cualquier cosa que tenga valor para la organización.

- **Acuerdo de Confidencialidad:** Es un documento en los que los funcionarios de la UNIVERSIDAD DEL QUINDÍO o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la institución, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

- **Autenticación:** Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

- **Cifrado:** Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos (2.61) no autorizados. [NTC-ISO/IEC 27000].

- **Control:** Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

- **Disponibilidad:** Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad autorizada. [NTC-ISO/IEC 27000].

- **Escritorio lógico:** Se hace referencia al escritorio del sistema operativo.

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Incidente de Seguridad:** Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada de la UNIVERSIDAD DEL QUINDÍO, bajo el control técnico del área de Sistemas y Nuevas Tecnologías , la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

- **Integridad:** Propiedad de la información relativa a su exactitud y completitud. [ISO/IEC 27000: 2017].

- **Licencia de software:** Es un contrato en donde se especifican las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

- **Medio removible:** Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs, Blu Ray y unidades de almacenamiento USB, entre otras.

- **Operación**: Actividades diarias de infraestructura realizadas para soportar y entregar los servicios de tecnología.

- **Perfiles de usuario:** Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas.

- **Política:** Intenciones y direcciones de una organización como se expresan formalmente por la Alta Dirección. [ISO/IEC 27000].

- **Propiedad intelectual:** Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

- **Propietario de la información:** Es el área o proceso donde se crean los activos de información.

- **Recursos tecnológicos:** Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la UNIVERSIDAD DEL QUINDÍO.

- **Responsable por el activo de información:** Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de información:** Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por el área

de Sistemas y Nuevas Tecnologías o de origen externo ya sea adquirido por la Institución como un producto estándar de mercado o desarrollado para las necesidades de ésta.

- **Software malicioso:** Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

4. COMPROMISO DE LA DIRECCIÓN

El Consejo Superior de la UNIVERSIDAD DEL QUINDÍO aprueban estas Políticas de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la Universidad.

El Consejo Superior de la UNIVERSIDAD DEL QUINDÍO demuestran su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los funcionarios de la Institución.
- La verificación del cumplimiento de las políticas aquí mencionadas.

5. RESPALDO DEL GOBIERNO CORPORATIVO AL GOBIERNO DE TI

La Universidad del Quindío se reserva el derecho a revisar, actualizar y modificar los lineamientos y condiciones descritos por medio de las presentes políticas. Las actualizaciones que se realicen a las presentes políticas están respaldadas por el gobierno corporativo de la institución.

6. CONTROL Y SEGUIMIENTO A LAS POLÍTICAS DE GOBIERNO DE TI

La Dirección de sistemas y nuevas tecnologías, en compañía del área de control interno y/o el comité rectoral tendrán la potestad de realizar revisiones periódicas con el fin verificar el cumplimiento de las presentes políticas y comunicar de manera formal a los responsables para que implemente las acciones de mejora y/o acciones correctivas

pertinentes. Cualquier situación no prevista en las presentes políticas será resuelta por la Dirección de sistemas y nuevas tecnologías de la Universidad de Quindío.

7. POLÍTICAS GOBIERNO DE TI

7.1. Adquisición, implementación y mantenimiento de las aplicaciones software

La Universidad del Quindío por medio del macroproceso de Gestión Tecnológica de Información y Comunicación TIC, es el responsable de la planificación y ejecución de la adquisición, implementación y mantenimiento de los servicios y configuración de las Tecnologías de Información y Comunicación (TIC), requeridas para los procesos de la Universidad, buscando, dentro del marco normativo establecido por Mintic, asegurar la calidad de los servicios entregados y de acuerdo con criterios de innovación, confiabilidad, disponibilidad, integridad, confidencialidad e interoperabilidad, que den soporte a los procesos de la institución.

Requerimientos tecnológicos: El proceso que requiera implementar un software, plataforma tecnológica o sistemas de información, debe seguir un procedimiento de adquisición de tecnología y se asignará una persona responsable del área de sistemas y nuevas tecnologías (ASNT) para liderar la implementación solicitada. En caso de no seguir este prcceso, el área de sistemas y nuevas tecnologías no se hará responsable de la administración y funcionamiento de la solución adquirida o desarrollada.

Para el manejo y administración de los requerimientos tecnológicos (adquisiciones, implementación y mantenimiento), las dependencias dueñas de los procesos de la institución tienen la responsabilidad de hacer las pruebas necesarias.

Adquisición y Desarrollo de aplicaciones:

La institución puede adquirir licencias de uso de aplicaciones a través de proveedores. De igual forma, los desarrollos de las aplicaciones, pueden ser realizados por proveedores, estudiantes, docentes, grupos de investigación y los ingenieros del área de sistemas y nuevas tecnologías de la institución.

El proceso de adquisición y desarrollo de las aplicaciones se deberá estructurar y ordenar, considerando las diferentes etapas del ciclo de vida de las soluciones de software.

Las aplicaciones desarrolladas por los estudiantes, grupos de investigación y docentes para la institución deberán tener la previa aprobación del área de sistemas y nuevas tecnologías, el cual deberá conocer claramente el alcance y los beneficios de las mismas, además, deberán ser construida bajo los lineamientos, estándares y herramientas tecnológicas definidas por el área de sistemas y nuevas tecnologías.

Las aplicaciones deben cumplir con los requerimientos de seguridad establecidos por la institución conforme con la Política de Seguridad de la Información.

Se debe garantizar la existencia y separación de los ambientes de desarrollo, pruebas y producción, independientemente si está en proceso de construcción o en producción.

El proceso de entrega de las aplicaciones adquiridas bajo la modalidad de licencia de uso y las aplicaciones desarrolladas, debe contener la documentación técnica, funcional y transferencia de conocimiento. En el caso de los desarrollos se deberá incluir el código fuente para poder ser administrado por la institución.

La documentación de cada uno de las aplicaciones adquiridas por la institución debe contener la copia del contrato con el proveedor que lo brinda, especificando los Acuerdos de Nivel de Servicio (ANS) establecidos y los procesos para obtener el servicio.

La propiedad Industrial y comercial de las aplicaciones desarrolladas por los proveedores dentro de su trabajo debe ser propiedad de la Universidad del Quindío, salvo acuerdo escrito expresc que diga lo contrario.

La propiedad Industrial y comercial de las aplicaciones desarrolladas por estudiantes, docentes, grupos de investigación, ingenieros del área de sistemas y nuevas tecnologías y cualquier funcionario de la institución se regirá conforme con la Política de Propiedad Intelectual institucional Acuerdo del Consejo Superior 075 del 14 de marzo de 2019.

Los proveedores o terceros que tengan acceso a los sistemas TIC de la entidad, no podrán copiar ni ceder sin autorización las aplicaciones que son propiedad de la Universidad del Quindío ni las aplicaciones o programas de los que esta tenga licencia de uso.

A través de acuerdos de confidencialidad específicos y/o cláusulas en los contratos, se debe establecer que cuando un proveedor usa datos suministrados por la institución, garantizará el uso adecuado de la información y la correcta eliminación de la misma de los diferentes ambientes, una vez cese la relación contractual.

7.2. Operación de la infraestructura de TI

Responsabilidades de la operación: Los procedimientos de operación deben estar documentados con sus respectivas políticas, planeación de la operación, el tratamiento y manipulación de la información, las copias de respaldo, los contactos de apoyo para el caso de dificultades operacionales o técnicas inesperadas, reinicio de los sistemas y procedimientos de recuperación a utilizar en caso de falla del sistema de información, gestión de registros de auditoría y el aseguramiento de plataformas.

Monitoreo, capacidad y disponibilidad: Se debe establecer un proceso de monitoreo para proyectar la capacidad futura y para reducir el riesgo de sobrecarga del sistema. Se debe monitorear el uso de los servicios de red y de los sistemas, con el objetivo de ajustar y planificar la capacidad, de acuerdo con el desempeño y disponibilidad de los servicios requerido para cumplir con los Acuerdos de Niveles de Servicio (ANS) y reducir el riesgo de posibles fallas.

Monitoreo y Uso de las Redes: El Área de Sistemas y Nuevas Tecnologías es responsable de definir las necesidades que tiene la institución con respecto a las redes. Es responsable también de la administración de los anchos de banda necesarios para soportar los servicios TIC. El uso de las redes debe ser monitoreado con el objetivo de ajustar y planificar la capacidad, de acuerdo con el desempeño requerido para cumplir con los Acuerdos de Niveles de Servicio(ANS) y reducir el riesgo de posibles fallas.

7.3. Soporte a los usuarios servicio TIC

El centro de servicio al Usuarios (CSU) debe ser el único canal por medio del cual se reporte cualquier incidente o requerimiento asociado a las TIC, con el fin de garantizar el seguimiento y entrega oportuna del servicio solicitado.

Gestión de requerimientos: La Institución, por medio del proceso de Gestión Tecnológica de Información y Comunicación, debe garantizar la disponibilidad del Centro de Servicio al Usuarios (CSU) como único canal para atender los requerimientos de los usuarios de acuerdo con el catálogo de servicios establecido, para ofrecer una respuesta oportuna y con calidad, con base en los acuerdos de nivel de servicio ofrecidos. Por medio de la herramienta tecnológica de gestión del servicio se debe mantener informado al usuario de la evolución del requerimiento. Todos los actores que participan en la gestión de requerimientos deben poder acceder a dicha herramienta a través de la cual

deben ejercer el rol correspondiente. En el caso de que exista riesgo de incumplimiento del Nivel de Servicio, se debe informar al usuario de este hecho.

Gestión de incidentes: La institución, por medio del proceso de Gestión Tecnológica de Información y Comunicación, debe garantizar la disponibilidad del Centro de Servicio al Usuarios (CSU) como único canal para atender los incidentes de los usuarios, de acuerdo con el catálogo de servicios establecido. Los analistas encargados del tema deben seguir el procedimiento para realizar las actividades de registro, asignación de prioridad, valoración del impacto, clasificación, actualización, escalado, resolución y cierre formal del incidente reportado. La atención de incidentes debe restaurar el servicio tan pronto como sea posible con la aplicación de una solución temporal o definitiva. Por medio de la herramienta tecnológica de Gestión del servicio, se debe mantener informado al usuario de la evolución del incidente. En el caso que exista riesgo de incumplimiento del Acuerdo de Nivel de Servicio (ANS) se debe informar al usuario de este hecho.

7.4. Uso aceptable de activos

El área de Sistemas y Nuevas Tecnologías de la UNIVERSIDAD DEL QUINDÍO como propietario de la información generada, procesada, almacenada y transmitida otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

- El Área de Sistemas y Nuevas Tecnologías es la propietaria de los activos de información almacenados en los servidores, en consecuencia, debe asegurar su apropiada operación y administración.

- El Área de Sistemas y Nuevas Tecnologías en conjunto con el Comité de Control de Cambios, son quienes deben autorizar la instalación, cambio o eliminación de componentes de los aplicativos de la UNIVERSIDAD DEL QUINDÍO.

- El área de sistemas y nuevas tecnologías debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

- El área de sistemas y nuevas tecnologías es responsable de preparar los requerimientos técnicos necesarios, incluyendo necesidades de hardware y software para incorporar a los procesos de compra y contratación de las estaciones de trabajo fijas y/o portátiles de los funcionarios.

- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, entre otros. Estos cambios pueden ser realizados únicamente por el personal asignado del área de sistemas y nuevas tecnologías.

- En caso que algún colaborador requiera para el desempeño de sus funciones realizar instalación de software y/o cambios en la configuración del equipo se debe documentar la autorización caso por caso, indicando la duración de la autorización.

- El área de sistemas y nuevas tecnologías de la UNIVERSIDAD DEL QUINDÍO, recomiendan utilizar alguna de las siguientes alternativas en caso de requerir algún software, para mantener el cumplimiento legal:

    - Usar software de dominio público amparado bajo la licencia pública general GNU.

    - Para aplicaciones de ofimática utilizar Open Office, Libre Office y las herramientas de Google.

    - El instalador debe ser descargado de la página oficial del fabricante.

    - Como sistema operativo usar cualquier versión libre de Linux.

    - Para otros casos se debe realizar el proceso formal de adquisición del software comercial debidamente licenciado.

Los equipos de cómputo de la UNIVERSIDAD DEL QUINDÍO, deben ser bloqueados por el funcionario responsable al momento de retirarse de su puesto de trabajo.

Todo problema mecánico, eléctrico o electrónico sobre los equipos de cómputo de la universidad, debe ser atendido únicamente por el personal del área sistemas y nuevas tecnologías.

Todas las estaciones de trabajo deben apagarse o dejarse en estado de hibernación al finalizar la jornada laboral.

Los equipos de cómputo (CPU y monitor), servidores, teléfonos IP y equipos de comunicaciones, deben conectarse a los puntos de corriente eléctrica identificados como regulados.

Los recursos tecnológicos de la UNIVERSIDAD DEL QUINDÍO, deben ser utilizados de forma ética y en cumplimiento de las Leyes y Reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la institución.

Los funcionarios no deben utilizar software no autorizado o de su propiedad en los equipos entregados por la Universidad para el desempeño de sus funciones.

Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

El sistema de correo debe ser utilizado solamente para propósitos de la institución y evitarse su uso para tratar asuntos personales.

Evitar acceder desde redes inalámbricas públicas, pues estas redes al compartir el canal de Internet con todos los usuarios que simultáneamente se conectan a ellas, son altamente inseguras ante ataques de espionaje.

Es muy importante no abrir correos que provengan de destinatarios desconocidos o que tengan asuntos o archivos adjuntos sospechosos.

Los proveedores de servicios de correo electrónico, cuentan con medidas de seguridad. Específicamente, Gmail, motor del correo institucional, informa cuando se han hecho inicios de sesión desde computadores diferentes a los que el usuario normalmente

utiliza. Este es un buen método para enterarse inmediatamente si se presenta actividad inusual en la cuenta. Ante esta situación, cambie inmediatamente la contraseña y reporte la eventualidad mediante el correo de notificación que llega.

La información contenida en las herramientas y equipos asignados por la Universidad para el cumplimiento de sus responsabilidades académicas, administrativas y de investigación son de propiedad de la Universidad y podrán ser revisadas en el momento en que la institución lo determine.

7.4.1. Asignación de activos de información tipo hardware

El área de sistemas y nuevas tecnologías realiza la entrega oficial del activo de información tipo hardware al personal, de acuerdo con los requerimientos técnicos necesarios incluyendo necesidades de hardware y software de acuerdo con las necesidades del usuario. El área de activos fijos identifica los activos tipo hardware físicamente de acuerdo con los procedimientos utilizados en la Universidad para el etiquetado de estos.

7.4.2. Salida y devolución de activos de información tipo hardware

Si se requiere para el desempeño de sus funciones, que el funcionario se desplace con el activo de información tipo hardware dentro o fuera del campus Universitario, debe diligenciar formato de traslado de equipos del área de activos fijos.

7.4.3. Entrega y disposición segura de los activos de información

Para el caso de cambio de rol, traslado administrativo, ascenso o retiro del funcionario, el custodio del activo de información pertinente al proceso de la Universidad debe solicitar al funcionario los activos de información pura como (Archivos físicos, carpetas).

En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo a su jefe inmediato o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

7.5. Control de acceso

7.5.1. Administración de acceso a usuarios

El área de sistemas y nuevas tecnologías debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la institución, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

El área de sistemas y nuevas tecnologías previa solicitud de los Jefes inmediatos de los solicitantes de las cuentas de usuario y aprobación de los líderes de proceso como responsables funcionales de cada una de las dependencias de la UNIVERSIDAD DEL QUINDÍO, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.

El área de sistemas y nuevas tecnologías debe definir lineamientos para la configuración de contraseñas que aplicaran sobre los servicios de red y aplicaciones de la UNIVERSIDAD DEL QUINDÍO; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

- La contraseña no debe tener una longitud inferior a 8 caracteres. Entre más larga sea, será más segura.
- Al momento de crearla debe intentarse combinar letras mayúsculas y minúsculas, números y caracteres especiales (@, $, &, por ejemplo).
- Debe cambiarse, dependiendo de la criticidad del recurso al que da acceso, cada cierta cantidad de tiempo.
- No debe tenerse la misma contraseña para todo. Es altamente recomendable que varíe de un sistema a otro.
- Se debe evitar crear contraseñas con el nombre del usuario de la cuenta o con información personal obvia como nombre del cónyuge, hijos, fechas de cumpleaños, entre otros. Tampoco debe tener una secuencia previsible de letras o números como abad o 1234, o una simple palabra en cualquier idioma.

El área de sistemas y nuevas tecnologías debe establecer un procedimiento que asegure la eliminación, actualización o bloqueo de los privilegios de acceso otorgados sobre los

recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los líderes de proceso como responsables funcionales de cada una de las dependencias de la UNIVERSIDAD DEL QUINDÍO lo reporten.

Los líderes de proceso como responsables funcionales de cada una de las dependencias de la UNIVERSIDAD DEL QUINDÍO, deben definir los perfiles de usuario y autorizar las solicitudes de acceso a los sistemas de información de acuerdo con los perfiles establecidos.

Los usuarios de los servicios de red y los sistemas de información de la UNIVERSIDAD DEL QUINDÍO, deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

Los usuarios no deben compartir sus cuentas de usuario y contraseñas con otros usuarios. El nombre de usuario y contraseña son intransferibles. Todo lo que se haga con el nombre de usuario y contraseña, es responsabilidad del titular.

Los usuarios que posean acceso a los servicios de red y los sistemas de información alojados en la UNIVERSIDAD DEL QUINDÍO, bajo el control técnico del ÁREA SISTEMAS Y NUEVAS TECNOLOGÍAS deben acogerse a lineamientos para la configuración de contraseñas definidos en este documento.

7.5.2. Acceso a redes y recursos de redes

El área de sistemas y nuevas tecnologías de la UNIVERSIDAD DEL QUINDÍO, como responsables de las redes de datos y los recursos de red, debe disponer que dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

El área de sistemas y nuevas tecnologías debe establecer un procedimiento de autorización y controles para proteger el acceso a las subredes donde se encuentran los sistemas de información institucionales.

El área de sistemas y nuevas tecnologías debe asegurar que las redes cableadas de la institución cuenten con controles que eviten accesos no autorizados.

El área de sistemas y nuevas tecnologías debe autorizar la creación o modificación y cancelación del acceso a la red.

Los líderes de proceso como responsables funcionales de cada una de las dependencias de la UNIVERSIDAD DEL QUINDÍO deben autorizar la creación o modificación y cancelación de los accesos a los recursos de red de la UNIVERSIDAD DEL QUINDÍO.

Los funcionarios, antes de contar con acceso lógico por primera vez a la red de datos de la UNIVERSIDAD DEL QUINDÍO, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.

7.5.3. Uso de altos privilegios y utilitarios de administración

El área de sistemas y nuevas tecnologías de la UNIVERSIDAD DEL QUINDÍO garantizara que los recursos y los servicios de red sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos plataforma y servicios.

El área de sistemas y nuevas tecnologías debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.

El área de sistemas y nuevas tecnologías debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.

El área de sistemas y nuevas tecnologías debe restringir las conexiones remotas a los recursos de la UNIVERSIDAD DEL QUINDÍO, únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.

El área de sistemas y nuevas tecnologías debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos alojadas en la UNIVERSIDAD DEL QUINDÍO sean suspendidos o renombrados y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.

Los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información administrados por el área sistemas y nuevas tecnologías, no deben hacer uso de utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.

El área de sistemas y nuevas tecnologías debe deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.

El área de sistemas y nuevas tecnologías debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la UNIVERSIDAD DEL QUINDÍO.

El área de sistemas y nuevas tecnologías debe validar que las políticas de contraseñas establecidas y los sistemas de información son aplicables a los usuarios administradores; así mismo, debe verificar que el cambio de contraseña de los usuarios administradores acoja el procedimiento definido para tal fin.

La administración de los recursos que no estén bajo el control técnico del área sistemas y nuevas tecnologías, deben acogerse a todas las políticas definidas en este numeral.

7.5.4. Acceso a sistemas y aplicativos

El área de sistemas y nuevas tecnologías velará por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

El área de sistemas y nuevas tecnologías debe garantizar que los sistemas de información y aplicativos, sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

El área de sistemas y nuevas tecnologías debe autorizar los accesos a los sistemas de información y aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso definidos por los líderes de proceso como responsables funcionales de cada una de las dependencias de la UNIVERSIDAD DEL QUINDÍO.

El área de sistemas y nuevas tecnologías debe emitir reportes periódicamente de los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos e informar a los líderes de proceso como responsables funcionales de cada una de las dependencias de la UNIVERSIDAD DEL QUINDÍO.

El área de sistemas y nuevas tecnologías debe establecer un procedimiento para la asignación de accesos a los sistemas de información y aplicativos de la UNIVERSIDAD DEL QUINDÍO.

El área de sistemas y nuevas tecnologías debe establecer ambientes para los sistemas de información y aplicativos, separados a nivel físico y lógico para desarrollo, pruebas y

producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

El área de sistemas y nuevas tecnologías debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes usuarios para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

Los sistemas de información y aplicativos que estén bajo el control técnico del área sistemas y nuevas tecnologías debe implementar medidas visuales que distingan los ambientes de desarrollo, pruebas y producción.

7.6. Respaldo de información

El área de sistemas y nuevas tecnologías debe asegurar que la información definida y contenida en servidores, dispositivos de red, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

Así mismo, garantizara que los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

El área de sistemas y nuevas tecnologías a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

El área de sistemas y nuevas tecnologías debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

El área de sistemas y nuevas tecnologías a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

Se definen las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente, en contratos y/o acuerdos a nivel de servicio, si es el caso.

El área de sistemas y nuevas tecnologías debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información de la UNIVERSIDAD DEL QUINDÍO.

El área de sistemas y nuevas tecnologías debe identificar la información crítica de los sistemas de información y aplicativos, que debe ser respaldada y almacenada de acuerdo con su nivel de clasificación.

7.7. Relación con proveedores

La UNIVERSIDAD DEL QUINDÍO, establecerá mecanismos de control en sus relaciones con proveedores, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean suministradas por las mismas, cumpla con las políticas, normas y procedimientos de seguridad de la información.

Las dependencias de la UNIVERSIDAD DEL QUINDÍO responsables de la realización de contratos o convenios con proveedores se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichos proveedores.

El área de sistemas y nuevas tecnologías con apoyo de la Oficina Jurídica deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

La Oficina Jurídica debe elaborar modelos de Acuerdos de Confidencialidad, con los que deben cumplir proveedores de servicios; dichos modelos, deben ser divulgados a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para el proveedor contratado,

El área de sistemas y nuevas tecnologías, con apoyo de la Oficina Jurídica deben generar un modelo base para Acuerdos de Intercambio de Información con proveedores, con los que deben cumplir dicho proveedor; estos, deben ser divulgados a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

Todo sistema externo utilizado por los proveedores para acceder a la información de la UNIVERSIDAD DEL QUINDÍO, debe ser autorizado por los líderes de proceso como responsables funcionales de cada una de las dependencias de la UNIVERSIDAD DEL QUINDÍO con el apoyo técnico del área de sistemas y nuevas tecnologías.

El área de sistemas y nuevas tecnologías debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los proveedores en la red de datos de la UNIVERSIDAD DEL QUINDÍO.

El área de sistemas y nuevas tecnologías debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los proveedores de servicios.

Los líderes de proceso como responsables funcionales de cada una de las dependencias de la UNIVERSIDAD DEL QUINDÍO deben evaluar y aprobar los accesos a la información de la Universidad requeridos por terceras partes, con el apoyo técnico del área de sistemas y nuevas tecnologías.

Las dependencias de la UNIVERSIDAD DEL QUINDÍO responsables de la realización de contratos o convenios con proveedores, deben identificar y monitorear los riesgos relacionados con estos, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología.

Las dependencias de la UNIVERSIDAD DEL QUINDÍO responsables de la realización de contratos o convenios con proveedores, deben mitigar los riesgos relacionados con dichos proveedores, que tengan acceso a información de la Universidad.

Las dependencias de la UNIVERSIDAD DEL QUINDÍO responsables de la realización de contratos o convenios con proveedores, deben divulgar y asegurar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información a dichos proveedores.

Los Supervisores de contratos con proveedores, deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información.

Los Supervisores de contratos y las dependencias de la UNIVERSIDAD DEL QUINDÍO responsables de la realización de contratos o convenios con proveedores, deben

administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

Cualquier actividad realizada por un proveedor en los sistemas de información y aplicativos debe ser monitoreada por el área sistemas y nuevas tecnologías. En el caso que se identifiquen riesgos de seguridad sobre la información, inmediatamente será revocada su autorización.

8. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

8.1. Uso de controles criptográficos y llaves

El área de sistemas y nuevas tecnologías debe almacenar y/o transmitir la información digital y que este clasificado como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

El área de sistemas y nuevas tecnologías debe verificar que todo el sistema de información y aplicativos que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.

El área de sistemas y nuevas tecnologías debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.

El área de sistemas y nuevas tecnologías debe desarrollar y establecer estándares para la aplicación de controles criptográficos en los sistemas de información.

Los desarrolladores de software deben asegurar que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por el área de sistemas y nuevas tecnologías.

El área de sistemas y nuevas tecnologías debe establecer procesos para la gestión apropiada de las llaves en todas sus etapas: generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción. De este modo se protegen contra modificación, pérdida. uso y divulgación no autorizados.

Los equipos usados para generar, almacenar y archivar las llaves, deben estar protegidos físicamente.

8.2. Escritorio limpio pantalla limpia

Los funcionarios deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida de manera inmediata.

Los funcionarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario o huella dactilar en las estaciones de trabajo que soporten dicho sistema. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

La información clasificada como altamente confidencial no debe ser nunca enviada a una impresora de la red, sin que exista una persona autorizada para cuidarla durante y después de la impresión. La variedad de la información que se envía a las impresoras puede alternar entre información pública e información confidencial, dado que información confidencial no puede ser revelada a personas no autorizadas.

El escritorio lógico debe estar libre de información sensible o confidencial.

8.3. Transferencia de información

Los líderes de proceso como responsables funcionales de cada una de las dependencias de la UNIVERSIDAD DEL QUINDÍO, asegurarán la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerán los controles necesarios para el intercambio de información.

La Universidad establecerá Acuerdos de Confidencialidad o de Intercambio de Información con los funcionarios y proveedores con los que se realice dicho intercambio.

La Universidad firmará acuerdos de confidencialidad con los empleados, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la organización. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

El área de Sistemas y nuevas tecnologías dispondrá de los mecanismos de infraestructura tecnológica necesarios para la conservación de la integridad, disponibilidad

y confidencialidad de los documentos electrónicos acorde con las políticas, procedimientos, tablas de retención documental (TRD) y demás estándares establecidas por dependencia de gestión documental.

El área de sistemas y nuevas tecnologías definirá el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información sobre los sistemas de información y aplicativos.

La oficina jurídica de la UNIVERSIDAD DEL QUINDÍO, debe definir los modelos de Acuerdos de Confidencialidad y de intercambio de información entre la UNIVERSIDAD DEL QUINDÍO y proveedores incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos.

Entre los aspectos a considerar se debe incluir:

- La prohibición de divulgar la información entregada por la UNIVERSIDAD DEL QUINDÍO por parte de los terceros con quienes se establecen estos acuerdos.

- La destrucción de dicha información una vez cumpla su cometido.

La División de contratación de la UNIVERSIDAD DEL QUINDÍO, debe incluir en los contratos que se constituyan con proveedores, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de la UNIVERSIDAD DEL QUINDÍO que les ha sido entregada.

Los líderes de proceso como responsables funcionales de cada una de las dependencias de la UNIVERSIDAD DEL QUINDÍO, deben velar porque el intercambio de información con entidades externas se realice en cumplimiento de este Manual de Políticas de Seguridad, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.

Los funcionarios no deben revelar o intercambiar información confidencial de la UNIVERSIDAD DEL QUINDÍO por ningún medio, sin contar con la debida autorización del jefe inmediato.

Los funcionarios deben evitar enviar información restringida a través de correo electrónico, pero en el caso que sea estrictamente necesario debe cifrar la información enviada por correo con la debida autorización del jefe inmediato.

Se debe proteger la información involucrada en transacciones en línea, para evitar la transmisión incompleta, rutas equivocadas, alteración y divulgación.

La información confidencial y sensible deberá permanecer cuando sea necesario en espacios cerrados con llave, entrega en mano, embalaje con sellos de seguridad, entre otros mecanismos de seguridad requeridos para proteger la información.

8.4. Desarrollo seguro

El área de sistemas y nuevas tecnologías debe garantizar que el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el soporte, actualización y mantenimiento requeridos.

El área de sistemas y nuevas tecnologías debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

El área de sistemas y nuevas tecnologías debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la UNIVERSIDAD DEL QUINDÍO.

El área de sistemas y nuevas tecnologías debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

El área de sistemas y nuevas tecnologías debe usar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

El área de sistemas y nuevas tecnologías a través de sus funcionarios, se debe asegurar que las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

El área de sistemas y nuevas tecnologías debe verificar que las pruebas de seguridad sobre los sistemas de información y aplicativos se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.

El área de sistemas y nuevas tecnologías debe aprobar las migraciones entre los ambientes de desarrollo y pruebas de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

Los líderes de proceso como responsables funcionales de cada una de las dependencias de la UNIVERSIDAD DEL QUINDÍO, deben aprobar las migraciones entre los ambientes de pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

El área de sistemas y nuevas tecnologías debe garantizar que la información entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.

El área de sistemas y nuevas tecnologías debe eliminar la información de los ambientes de pruebas que no estén en constante uso, una vez éstas han concluido.

Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

Los desarrolladores y proveedores de software deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

Los desarrolladores y proveedores de software deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

Los desarrolladores y proveedores de software, deben asegurar que los sistemas de información construidos no puedan cambiar la estructura ni el contenido de la base de datos desde el código fuente de dicha aplicación.

Los desarrolladores y proveedores deben incluir en los sistemas a su cargo opciones de desconexión o cierre de sesión de los aplicativos, que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

Los desarrolladores y proveedores deben incluir en los sistemas a su cargo funcionalidades que terminen la sesión en el sistema de información después de un lapso

de tiempo de máximo 20 min de inactividad, que solo podrá ser aumentado con base en un análisis de riesgos aceptado por el área funcional.

Los desarrolladores y proveedores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida con o sin autenticación, almacenada en cookies, variables del lado del cliente y complementos, entre otros.

Los desarrolladores y proveedores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

Los desarrolladores y proveedores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

Los desarrolladores y proveedores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

Los desarrolladores y proveedores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

Los desarrolladores y proveedores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.

Los desarrolladores y proveedores deben garantizar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.

Los desarrolladores y proveedores deben desarrollar los controles necesarios para la transferencia de archivos desde los sistemas de información, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

Los desarrolladores y proveedores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

Los desarrolladores y proveedores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.