UNIVERSIDAD DE CÓRDOBA

ACUERDO N°062

acreditada INSTITUCIONALMENTE

POR MEDIO DEL CUAL SE ESTABLECE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE CÓRDOBA

EL CONSEJO SUPERIOR DE LA UNIVERSIDAD DE CÓRDOBA
En uso de sus facultades legales y estatautarias, y

CONSIDERANDO:

Que el artículo 21 del Acuerdo N°270 de 2017, define las funciones del Consejo Superior Universitario, y en su numeral 1° contempló que: *1) Definir la políticas académicas, las políticas administrativas y la planeación institucional.*

Que el uso de las Tecnologías de Información y Comunicación conlleva riesgos, los cuales deben ser reconocidos y mitigados, de acuerdo a la Política de Riesgos adoptada por la Universidad.

Que la Universidad cuenta con una reglamentación sobre protección de la Información, por medio de la resolución 1650 de 2017, pero no cuenta con una Política de Seguridad de La Información, por lo que es necesario ampliar el alcance, de acuerdo a la normatividad vigente como lo son: La Constitución Política de Colombia, Ley de Comercio Electrónico, Ley de Delitos Informáticos en Colombia, Ley de Protección de Datos, Ley sobre los Derechos de Autor, Guía para la Administración del Riesgo establecido por el Departamento Administrativo de La Función Pública, Guía para la Elaboración de la Política de Seguridad y Privacidad de la información de MINTIC, Decreto 1078 de 2015, PEI (Proyecto Educativo Institucional – PEI), Normatividad Universidad de Córdoba (Estatutos, acuerdos y resoluciones vigentes), Norma ISO 9001 vigente, Sistema Integral de Gestión de Calidad SIGEC.

Que esta política busca definir, implementar, operar y mejorar de forma continua la Seguridad de la Información, soportado en lineamientos claros de acuerdo a las necesidades de la Institución y a los requerimientos regulatorios.

Que es necesario apoyar la innovación tecnológica y proteger los activos tecnológicos de la Universidad, estableciendo políticas, procedimientos e instructivos en materia de seguridad de la información y fortaleciendo la cultura de seguridad de la información en los funcionarios, docentes, estudiantes, terceros, aprendices, practicantes y clientes de la Universidad de Córdoba.

Que, de acuerdo con lo anterior, esta política aplica a la Institución según como se defina en su alcance, a sus funcionarios, docentes, estudiantes, aprendices, practicantes, proveedores, terceros y la ciudadanía en general.

Que en mérito de lo expuesto, se

ACUERDA:

ARTÍCULO 1. Establézcase la Política de Seguridad y Privacidad de la Información de la Universidad de Córdoba, en donde se indican los lineamientos sobre los que se tomarán las decisiones alrededor de la seguridad de la información, y conformar un entorno, que le permita a todos los procesos institucionales contar con herramientas y reglamentaciones referentes a la seguridad informática, los cuales tendrán aplicación sobre los siguientes elementos:

- Personas
- Procesos
- Datos
- Software
- Hardware
- Instalaciones físicas

La Universidad de Córdoba reconoce la información como un activo, así como la importancia de una adecuada gestión de la información y es consciente de que la seguridad y protección de la información genera un marco de confianza y de valor en el ejercicio de sus deberes con sus partes interesadas, enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión.

Para la Universidad de Córdoba, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados, con el propósito de preservar la integridad, disponibilidad y confidencialidad de la información.

ARTÍCULO 2. Objetivos generales y específicos: el objetivo general de La Política de Seguridad y Privacidad de La Información es el de establecer los criterios y medidas básicas que deben aplicarse para proteger, preservar y gestionar la información institucional y la plataforma tecnológica

utilizada para su procesamiento, asegurando la conservación de los atributos de confidencialidad, integridad, disponibilidad y legalidad.

Los Objetivos específicos son los siguientes:

1. Definir los lineamientos para la adecuada valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.
2. Brindar las herramientas para la protección e integridad de la información y de la Infraestructura Tecnológica Institucional.
3. Promover la cultura de seguridad de la información.

ARTÍCULO 3. Alcance y área de aplicación: El ámbito de aplicación de la Política de Seguridad y Privacidad de la Información se establece en todas las dependencias de la Universidad, procesos, contratos o acuerdos con terceros, miembros de la comunidad universitaria cualquiera que sea su rol (funcionario, practicante, contratista, estudiante, docente, visitante) y terceros no vinculados directamente a la Universidad pero que presten su servicio o se encuentren involucrados en la generación, almacenamiento, uso, eliminación y transferencia de la información de la Universidad.

ARTÍCULO 4: Responsable de su aplicabilidad, evaluación y seguimiento: El área responsable de velar por el cumplimiento de la Política de Seguridad y Privacidad de la Información será el Proceso de Gestión del Desarrollo Tecnológico, el cual deberá desarrollar los mecanismos para la aplicación de la misma, teniendo en cuenta que esta, será parte integral de los sistemas de gestión de Planeación de la Universidad y se incorporará al Sistema de Control Interno para la evaluación y control de su cumplimiento.

ARTÍCULO 5. Organización de la Seguridad de la información: Se establecen las siguientes políticas para la Organización de la Seguridad de la Información:

1. La Universidad de Córdoba, por medio de su Comité Institucional de Calidad y de Coordinación del Sistema de Control Interno y la Unidad de Control Interno realizará los seguimientos a la implementación de las actualizaciones y al cumplimiento de la normativa,

y propiciarán el entorno necesario para crear un Sistema de Gestión de Seguridad de La Información.

2. La Universidad establecerá un Comité Técnico de Seguridad TIC, el cual dependerá del Comité Institucional de Calidad y de Coordinación del Sistema de Control Interno, y estará a cargo de las decisiones y seguimiento de los planes y programas establecidos para la gestión de la seguridad de la información. Su constitución y responsabilidades se definirán por medio de una directiva interna, dentro de las cuales como mínimo deberá realizar las siguiente actividades:
   - La formulación y propuestas de actualización de políticas y directrices para la seguridad de la información.
   - El tratamiento de datos personales.
   - Implementar las directrices a seguir en materia de seguridad de la información y al seguimiento periódico de las mismas.
   - Establecer los canales de comunicación que serán usados para tal fin.
   - El mejoramiento continuo.

ARTÍCULO 6. Manejo de la Información: Se establecen las directrices con el fin de proteger la información de la Universidad en lo referente a su uso no autorizado, divulgación o publicación, modificación, daño o pérdida, y al cumplimiento de reglamentaciones y leyes aplicables a la Universidad y acogiendo como parte de esta política la resolución rectoral 1650 de 2017 para la protección de datos personales:

1. **Acuerdos de Confidencialidad**: Los funcionarios y/o contratistas se obligarán mediante cláusulas de confidencialidad a no divulgar a terceras partes, la "Información confidencial", que reciba por parte de la Universidad de Córdoba o de un tercero en el ejercicio de su labor, y en el caso de datos personales, dará estricto cumplimiento a las disposiciones constitucionales y legales sobre la protección del derecho fundamental de habeas data, lo dispuesto en el artículo 15 de la Constitución Política y la ley 1581 de 2012, y en la resolución rectoral 1650 de 2017, y/o las normas que la modifiquen. En caso de incumplimiento parcial o total con las obligaciones establecidas en estas cláusulas, será responsable de los daños y perjuicios que dicho incumplimiento llegase a ocasionar a la Universidad de Córdoba y/o terceros.

2. **Propiedad de la Información**: La información procesada, manipulada o almacenada por el funcionario y/o contratista en el ejercicio de su relación Laboral con la Universidad es propiedad exclusiva de la Universidad de Córdoba.
3. **Derechos de Autor**: El usuario es responsable de respetar la Ley de Derechos de Autor, no abusando de los medios electrónicos para distribuir de forma ilegal licencias de software, libros electrónicos u otros, o reproducir información sin autorización del autor.
4. **Procesamiento de datos**: Los administradores de los sistemas y la infraestructura tecnológica local y central, son los responsables de garantizar los mecanismos para la custodia y confidencialidad de la información almacenada en esos recursos respectivamente, asegurando los roles y los perfiles de los usuarios mediante la asignación de las credenciales que les correspondan.

ARTÍCULO 7. Acceso Remoto: Se contemplan las conexiones y comunicaciones manejadas de forma remota de usuarios autorizados para el acceso a las redes de datos de la Universidad:

1. El acceso remoto a la red de datos de la Universidad deberá estar autorizado por el Proceso de Gestión del Desarrollo Tecnológico.
2. Durante el desarrollo de actividades de trabajo con acceso remoto los funcionarios y/o contratistas deben hacer uso de las herramientas de seguridad dados por la Universidad y teniendo en cuenta las recomendaciones de seguridad que permitan mitigar la posibilidad de fuga o acceso no autorizado o fraudulento de la información.
3. Se deben desarrollar programas de sensibilización para la seguridad y protección de los activos de información durante el desarrollo de actividades de trabajo acordes con las políticas, procedimientos internos y controles definidos por el Proceso de Gestión del Desarrollo Tecnológico.
4. Para el acceso a los recursos de equipos de procesamiento de datos de tipo servidor deberá habilitarse un servicio de conexión de acceso remoto con previa autorización de los administradores de los sistemas y la infraestructura tecnológica local y central.

ARTÍCULO 8. Uso de Recursos Tecnológicos:

1. Uso de los Recursos Tecnológicos: Cada departamento, facultad o proceso, tendrá un responsable por el/los activo/s crítico/s o de mayor importancia para la facultad, departamento y/o la Universidad.

- La persona o entidad responsable de los activos de departamento, facultad o proceso, y/o puesto de trabajo, velará por la salvaguarda de los activos físicos tecnológicos requeridos para la prestación del servicio tecnológico al área (hardware, medios magnéticos, aires acondicionados, mobiliario.), activos de información (bases de datos, archivos, documentación de sistemas, procedimientos operativos, configuraciones), activos de software (aplicaciones, software de sistemas, herramientas y programas de desarrollo).
- El Proceso de Gestión del Desarrollo Tecnológico, deberá adoptar medidas de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles (teléfonos inteligentes, computadores portátiles, entre otros), en la red de datos propiedad de La Universidad, y contar con controles de seguridad para mitigar el acceso no autorizado a la información de la institución.

2. Activos de información: Los activos de información deberán clasificarse de acuerdo con la confidencialidad, integridad y disponibilidad. Estos activos deben contar con un propietario quien tendrá la responsabilidad de velar por la administración correcta de los mismos durante su ciclo de vida.

- Los activos críticos de información deben contar con los controles asociados al riesgo de seguridad.
- Ningún funcionario y/o contratista puede divulgar información valorada como confidencial o de uso interno de la Universidad a personas no autorizadas. Para lo anterior se debe definir y divulgar las sanciones correspondientes, de acuerdo al régimen disciplinario y normatividad legal vigente.
- Todos los usuarios y administradores de la plataforma tecnológica institucional serán instruidos en seguridad de la información, de acuerdo con el área operativa a la que pertenecen y las actividades que desarrollan.

3. Uso de equipos de cómputo: Los equipos asignados a cada uno de los usuarios que son propiedad de la Universidad de Córdoba, el Proceso de Gestión del Desarrollo Tecnológico será quien definirá las aplicaciones que se instalarán en cada equipo de acuerdo al control establecido, rol del usuario y uso, y los procedimientos para la instalación o desinstalación de aplicaciones de software.

4. Instalación, mantenimiento y actualización de equipos de cómputo: Se restringe el uso e instalación sin previa autorización del Proceso de Gestión del Desarrollo Tecnológico, de

programas o utilitarios de comunicación no autorizados en los equipos de la Universidad. Así como la realización de mantenimientos o corrección de problemas a dichos equipos por personal no autorizado por la Universidad.

5. Uso de software y licencias: El Proceso de Gestión del Desarrollo Tecnológico será el encargado de autorizar el software licenciado o libre que se tendrá instalado en los equipos que sean propiedad de la Universidad de Córdoba.

6. Protección contra software malicioso: Todo equipo tecnológico de la Universidad debe estar protegido con una solución de antivirus de gestión centralizada y actualización automática.

7. Software desarrollado en La Universidad: Todo desarrollo, implementación e implantación, de una solución tecnológica de software para la Universidad de Córdoba debe seguir los Procedimientos establecidos por el Proceso de Gestión del Desarrollo Tecnológico.

9. Monitoreo del acceso y uso del sistema: Se realizarán registros y monitoreo de toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la plataforma tecnológica institucional, mediante archivos de Log, Bitácoras de Sistemas y/o herramientas lógicas de monitoreo.

ARTÍCULO 9. Control de Acceso a la Información: Los controles de acceso deben considerar los activos de información físicos para los lugares donde se encuentra alojada la información, así como los controles de acceso lógicos para los sistemas de información y plataformas de servicios.

Al momento de definir los controles de acceso se debe tener en cuenta la clasificación de los activos de información a la que se tendrá acceso, según el rol y la segregación de tareas, teniendo en cuenta que:

1. El acceso a centros de datos y de cableado serán restringidos y controlados.
2. Cualquier petición de acceso a información, servicio o acción proveniente de un determinado usuario o dependencia, se deberá efectuar siguiendo los canales de gestión formalmente establecidos de acuerdo a su competencia y/o rol.
3. Son considerados usuarios de la plataforma tecnológica institucional, los empleados docentes y administrativos, contratistas, estudiantes, y toda aquella persona, que utilice los servicios tecnológicos institucionales de la Universidad de Córdoba.

4. Los diferentes tipos de usuarios tendrán acceso únicamente a los servicios y recursos autorizados de la plataforma tecnológica institucional de acuerdo a su vinculación, rol y quehacer.
5. El acceso a la plataforma tecnológica por parte de usuarios externos o terceros es restrictiva y permisible con la autorización pertinente, y debe definirse como se va a documentar la aceptación de la confidencialidad hacia la institución y la forma como será establecido el compromiso con el uso exclusivo del servicio para el que le será provisto el acceso.
6. Los servicios accedidos por terceros acataran las disposiciones generales de acceso a servicios por el personal interno de la institución, además de los requisitos expuestos en su contrato y/o o acuerdo con la Universidad.
7. Los servicios solicitados por un usuario, departamento o facultad serán proporcionados una vez completados los procedimientos de autorización necesarios para su ejecución de acuerdo al tipo de servicio solicitado.
8. Las áreas o dependencias que gestionan, contratan y/o vinculan personal susceptible de ser usuario de las diferentes plataformas institucionales, en conjunto con el Proceso de Gestión del Desarrollo Tecnológico definirán los mecanismos para notificar el ingreso, traslado o retiro de funcionarios y/o contratistas, con el fin de garantizar la actualización continua de la base de datos de los usuarios y el control de acceso a los Servicios Tecnológicos Institucionales.

ARTÍCULO 10. Responsabilidades de los Usuarios Frente a la Información de Autenticación: Los usuarios de la Universidad de Córdoba tendrán las siguientes responsabilidades en lo referente al acceso a los sistemas de información e infraestructura tecnológica:

1. El usuario es responsable exclusivo de salvaguardar su contraseña de acceso a los servicios tecnológicos institucionales y será responsable del uso que haga de su cuenta de acceso a los sistemas o servicios.
2. El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él, teniendo en cuenta las recomendaciones de seguridad que desde su rol de usuario puede llevar acabo.
3. Cualquier usuario que encuentre una falla de seguridad en los servicios tecnológicos de la institución, está obligado a reportarlo inmediatamente al Proceso de Gestión del Desarrollo Tecnológico.

4. Los usuarios estudiantes y docentes, son responsables de respaldar la información, producto de los trabajos realizados en las salas y/o equipos de trabajo propiedad de la Universidad en el medio que considere.
5. No se permite el uso de los recursos tecnológicos institucionales a personal no autorizado. Es responsabilidad del funcionario y jefe del área o unidad hacer cumplir esta directriz.

ARTÍCULO 11. Uso de Correo Electrónico, Plataformas Colaborativas, de Aplicaciones y de Comunicación:

1. El uso de los servicios de correo electrónico plataformas colaborativas, de aplicaciones y de comunicación, se deben realizar acatando todas las disposiciones de seguridad diseñadas para su utilización.
2. Todo uso indebido de los servicios de correo electrónico, plataformas colaborativas, de aplicaciones y de comunicación, serán motivo de suspensión temporal o definitiva del acceso al servicio. Para la suspensión definitiva, esta será autorizada por El Comité Técnico de Seguridad.
3. El usuario será responsable de la información que sea enviada o generada desde sus cuentas.
4. Las cuentas de las plataformas colaborativas, aplicaciones específicas y de gestión y correo electrónico son personales e intransferibles. El propietario de la cuenta es responsable de la privacidad de la clave de acceso a su cuenta; cualquier acción efectuada desde la misma será atribuida a dicho propietario.
5. La creación de los correos electrónicos institucionales es responsabilidad del Proceso de Gestión del Desarrollo Tecnológico, quien definirá los nemotécnicos, estructura, viabilidad y plataforma que se utilizará.
6. El Proceso de Gestión del Desarrollo Tecnológico, se reservará el derecho de monitorear la plataforma tecnológica institucional y bloqueará y/o reportará aquellos accesos y/o cuentas que presenten un comportamiento sospechoso para la seguridad de la información, funcionamiento y operación de La Plataforma Tecnológica Institucional.
7. Está prohibido a los usuarios de plataformas colaborativas y correo electrónico, realizar las siguientes acciones:

    - El uso de cuentas ajenas, así como la cesión de la cuenta propia a terceros.

- Iniciar o reenviar mensajes encadenados o el envío de correo masivo, exceptuando los autorizados y de carácter institucional.
- Uso de seudónimos y envió de mensajes anónimos.
- Envió de mensajes que atenten contra la dignidad humana y las garantías fundamentales.
- Usar el correo corporativo para fines personales, comerciales, publicitarios, religiosos o políticos.
- Generar o enviar correos electrónicos a nombre de otra persona (suplantación).

ARTÍCULO 12. Respuestas a Incidentes y Anomalías de Seguridad:

1. Los incidentes de seguridad graves deberán ser tratados en el Comité Técnico de Seguridad, y para aquellos que sean considerados como delitos informáticos deberán establecerse los mecanismos a implementar para reportarlos.

2. Se realizarán respaldos de la información de acuerdo con el procedimiento establecido por el Proceso de Gestión del Desarrollo Tecnológico, para los activos de información de mayor importancia o críticos, los cuales deberán ser almacenados en condiciones adecuadas.

3. Cualquier situación anómala y contraria a la seguridad deberá ser documentada, luego de la revisión de los registros o Log de sistemas con el objetivo de verificar la situación y dar una respuesta congruente y acorde al problema, tanto en el ámbito legal como en cualquier situación administrativa.

ARTÍCULO 13. Uso de Controles Criptográficos: Se debe asegurar el uso adecuado y eficaz de cifrado para proteger la confidencialidad, autenticidad y/o integridad de la información para lo cual se definen los casos en los cuales se usarán controles criptográficos:

1. En el almacenamiento de contraseñas de sistemas operativos, gestión de identidad y acceso a bases de datos.

2. En el resguardo de información con clasificación confidencial o en la cual se haya identificado riesgos asociados por los dueños de la información o el grupo asignado para la gestión de la Seguridad de la Información de la Universidad.

ARTÍCULO 14. Seguridad Física y del Entorno:

1. El Proceso de Gestión del Desarrollo Tecnológico definirá el manejo de la infraestructura de la red dependiendo de las necesidades del servicio, con el fin de mantenerla y optimizar los recursos existentes, para lo cual debe cumplir con las normas técnicas y estándares adoptados por el mismo, garantizando la integridad, conservación de la estética y seguridad de la infraestructura física.

2. El Proceso de Gestión del Desarrollo Tecnológico debe establecer los controles y definiciones para asegurar que el acceso físico a los equipos e infraestructura de red sea realizado por el personal idóneo en el ejercicio de sus labores de cuidado y mantenimiento de los mismos.

3. El sistema de control de accesos a áreas seguras o restringidas deberá ser definido por el Proceso de Desarrollo Tecnológico y aprobado por la Unidad de Planeación y Desarrollo; la solución Tecnológica adoptada debe documentarse en procedimientos, manuales y/o guías, establecidos por el Proceso de Gestión de Desarrollo Tecnológico.

Parágrafo 1. Está prohibido a los usuarios de la red e infraestructura tecnológica de la Universidad, realizar las siguientes acciones:

1. Utilizar la infraestructura de tecnología de información y redes de la Universidad para conseguir o trasmitir material con ánimo de lucro excepto cuando se trate de cumplir con fines institucionales.
2. Utilizar la infraestructura de tecnología de información y redes de la Universidad para realizar acosos, difamación, calumnia o cualquier forma de actividad hostil en contra de miembros de la comunidad universitaria y en general de cualquier persona o institución.
3. Ejecutar cualquier herramienta o mecanismo de monitoreo de la red de manera no autorizada.
4. Burlar los mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.

5. Desconectar o manipular los elementos de red tales como swtiches, routers, antenas, racks y demás elementos pertenecientes a la infraestructura de red de la Universidad.
6. Instalar equipos de comunicaciones u otro tipo de dispositivo sin la autorización del Proceso de Gestión del Desarrollo Tecnológico.

ARTÍCULO 15. Vulnerabilidades Técnicas: La información de las vulnerabilidades técnicas que pueden tener los sistemas de información deben ser detectadas de forma preventiva y evaluadas con el fin de que se tomen las medidas necesarias para abordar el riesgo asociado, por lo cual como mínimo deberán realizarse las siguientes acciones:

1. Establecer roles y responsabilidades asociados a la gestión de vulnerabilidades técnicas.

2. Definir procedimientos específicos para la ejecución de escaneos planeados o por demanda según las necesidades identificadas.

3. Como mínimo deben ser tratadas las vulnerabilidades identificadas en los escaneos de los activos de información clasificados como críticos.

4. Debe analizarse la viabilidad de las acciones para remediar las vulnerabilidades frente al riesgo de su implantación.

ARTÍCULO 16. Seguridad en el desarrollo, adquisición y mantenimiento de los sistemas de información:

1. Los activos de información y los riegos asociados de los nuevos proyectos o desarrollos deben ser identificados.

2. La información involucrada en los cambios a los sistemas en el ciclo de vida de desarrollo y a las plataformas de producción debe protegerse mediante procesos formales de control de cambios.

3. Los datos de salida de los aplicativos que manejan activos de información o datos críticos deben contener los datos relevantes requeridos para su uso de acuerdo con el rol y se deberán enviar exclusivamente a los usuarios y/o terminales autorizadas.

4. Los aplicativos deben pasar por un proceso de pruebas y aceptación en un ambiente destinado para tal fin antes de ser puestos en ambientes productivos.

ARTÍCULO 17. Gestión de servidores e Infraestructura central de almacenamiento y conectividad: Los servidores y equipos de comunicación centrales y de borde que soportan los servicios tecnológicos institucionales serán mantenidos en condiciones físicas y ambientales seguras y protegidas con mínimo las siguientes características:

- Controles de acceso y seguridad física.
- Sistemas de detección y extinción de incendio.
- Regulación de temperatura y humedad.
- Sistemas eléctricos regulados y respaldados.
- Otros que se consideren necesarios.

1. La información institucional en formato digital será mantenida en servidores autorizados y dispuestos por el Proceso de Gestión del Desarrollo Tecnológico. No se permite el alojamiento de información en servidores externos sin que exista una justificación aprobada por el Comité Institucional de Calidad y de Coordinación del Sistema de Control Interno.

2. El Proceso de Gestión del Desarrollo Tecnológico establecerá un Plan de mantenimiento preventivo anual a la Infraestructura de Tecnología e Información y Comunicación.

3. Los servidores y equipos centrales de red, deben contar con soluciones y procedimientos de copias seguridad, respaldo y recuperación para casos de desastre. Así como una disposición y conservación adecuada de los medios de resguardo.

4. Los administradores de servidores y servicios son responsables de cumplir y hacer cumplir las políticas de seguridad. El Proceso de Gestión del Desarrollo Tecnológico podrá realizar revisiones periódicas a los mismos con la finalidad de mejorar la seguridad o detectar fallas.

5. El acceso a la configuración del sistema operativo de los servidores, debe ser únicamente permitido al usuario administrador. Así como todo servicio provisto o instalado en los servidores, correrá o será ejecutado bajo cuentas restrictivas. En las situaciones en que se

detecten servicios corriendo con cuentas no administrativas, estos privilegios tendrán que ser eliminados o configurados correctamente.

6. Está prohibido a los usuarios de la tecnología de procesamiento de información y redes de la Universidad de Córdoba lo siguiente:

- Violación de los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier forma de propiedad intelectual.
- Realizar copia, digitalización, distribución de imágenes y fotografías de cualquier origen, música, audio, video, o instalación de software sin licencia, y/o permisos de su autor y sin autorización de la Universidad.
- Extraer o exportar información técnica sin la autorización expresa de la Universidad.

ARTÍCULO 18. Monitoreo, evaluación y seguimiento: Esta política será parte integral del Sistema Integral de Gestión de la Calidad y se incorporará al Sistema de Control Interno para el monitoreo, evaluación y control de su cumplimiento. Los riesgos digitales serán tratados de acuerdo a la Política de Riesgos de la Universidad y El Modelo de Seguridad y Privacidad de La Información (MSPI), establecido por MINTIC.

ARTÍCULO 19. Cumplimiento de la política: Todo incumplimiento por parte de los usuarios a lo establecido en esta política acarreará sanciones de tipo disciplinario y legal, de acuerdo con lo establecido en los Regímenes Disciplinarios y Reglamentos Estudiantil, Docente y de Personal Administrativo de la Universidad de Córdoba.

1. Los funcionarios, contratistas y terceras partes deben velar por el cumplimiento de las políticas de seguridad de la información y deben cumplir con las disposiciones establecidas por la Legislación Colombiana vigente asociados a la de protección de datos personales y seguridad de la información.
2. Todos los requisitos relevantes a nivel legislativo, estatutario, regulatorio y contractual, así como el enfoque de la institución para cumplir con tales requisitos debe estar explícitamente identificado, documentado y actualizado para la Universidad.
3. El Proceso de Gestión de Desarrollo Tecnológico y/o las áreas de gestión regulatoria, como las Unidades de Control Interno, Planeación y Desarrollo y Desarrollo Organizacional

y Gestión de la Calidad, Asuntos Jurídicos, a partir de la identificación de requisitos de seguridad de la información que sean de cumplimiento obligatorio y emitidos por entes gubernamentales o privados y cualquier disposición colombiana vigente, impartirán directrices y harán seguimiento a la implementación de los controles necesarios por parte de las áreas pertinentes de la institución, para dar cumplimiento y proteger los activos de información.

4. Los usuarios cuyas acciones puedan afectar la Seguridad de la información de la Universidad no serán exentos de su responsabilidad disciplinaria y legal sin importar que estas no se encuentren documentadas en esta política y la normatividad legal vigente.

ARTÍCULO 20. Implementación y actualización de la política: La implementación y actualización de esta Política estará a cargo del Proceso de Gestión del Desarrollo Tecnológico, el cual deberá en un término de tres meses presentar el Plan de Implementación a La Unidad de Planeación y Desarrollo, el cual incluirá un Sistema de Gestión de Seguridad de La Información, para la viabilización, formulación de los proyectos asociados para la aprobación en las instancias institucionales.

ARTÍCULO 21. Vigencia. El presente acuerdo rige a partir de su publicación.

COMUNIQUESE, PUBLÍQUESE Y CUMPLASE

Dado en Montería, a los 21 días del mes de julio de 2021.

JOSÉ MAXIMILIANO GÓMEZ TORRES
Presidente

CELY FIGUEROA BANDA
Secretaria