UNIVERSIDAD DEL QUINDÍO
Res.MEN 014915 - 02 AGO 2022
RENOVACIÓN ACREDITACIÓN

CONSEJO SUPERIOR
ACUERDO No. 171
22 FEB 2024

"POR MEDIO DEL CUAL SE APRUEBA Y SE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL QUINDÍO Y SE DICTAN OTRAS DISPOSICIONES"

El Consejo Superior, en ejercicio de sus facultades legales y estatutarias, especialmente las conferidas por la Ley 30 de 1992, y el Acuerdo del Consejo Superior Número 005 del 28 de febrero de 2005 "Estatuto General", artículo 1° y,

CONSIDERANDO:

A. Que la constitución Política de Colombia en el artículo 69 señala: "se garantiza la autonomía universitaria. Las Universidades podrán darse sus directivas y regirse por sus propios estatutos, de acuerdo con la ley".

B. Que la autonomía universitaria es una facultad reconocida mediante la Constitución Política, que se traduce en el reconocimiento que el Constituyente hizo de la libertad jurídica que tienen las instituciones de Educación Superior reconocidas como Universidades para autogobernarse y auto determinarse en el marco de las limitaciones que el mismo ordenamiento superior y la Ley les señalen.

C. Que, en armonía con lo anterior, el numeral 1º del artículo 28 del Acuerdo del Consejo Superior No. 005 de 2005 "Estatuto General", señala entre las facultades del Consejo Superior: "Formular y evaluar periódicamente las políticas y objetivos de la institución en el campo académico, administrativo y de planeación, teniendo en cuenta las políticas y programas del Ministerio de Educación Nacional".

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

E. Que la Constitución Política de Colombia en el artículo 15, consagra que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer; actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

F. Que el artículo 69 de la Constitución Política de Colombia establece el principio de autonomía universitaria, por medio del cual las universidades podrán darse sus directivas, regirse por sus propios estatutos y reglamentos, en materia contractual, presupuestal, administrativa y académica.

G. Que tal como lo establece el artículo 74 de la Constitución Política de Colombia, todas las personas tienen derecho a acceder a los documentos públicos, salvo los casos que establezca la ley.

H. Que así mismo, en su artículo 209 establece que la administración pública, en todos sus órdenes, tendrá un control interno, el cual se ejercerá en los términos que señale la ley. Asimismo, en el artículo 269 ordena a las autoridades de las entidades públicas la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno.

CONSEJO SUPERIOR
ACUERDO No. 00.171

22 FEB 2024

"POR MEDIO DEL CUAL SE APRUEBA Y SE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL QUINDÍO Y SE DICTAN OTRAS DISPOSICIONES"

I. 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".

J. Que el numeral 8 del artículo 2 de la Ley 1341 de 2009, establece que el Gobierno Nacional fijará los mecanismos y condiciones para garantizar la masificación del Gobierno en Línea, con el fin de lograr la prestación de servicios eficientes a los ciudadanos, así mismo, la citada Ley determinó que es función del Estado intervenir en el sector de las TIC, con el fin de promover condiciones de seguridad del servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes para el desarrollo de dicho sector; así como reglamentar las condiciones en que se garantizará el acceso a la información en línea, de manera abierta, ininterrumpida y actualizada.

K. Que el artículo 17 de la Ley Estatutaria 1581 de 2012, *"Régimen General de Protección de Datos Personales", y el artículo 2.2.2.25.3.1 del Decreto 1074 de 2015, "Decreto Único Reglamentario del Sector Comercio industria y Turismo",* consagraron la necesidad de garantizar de forma integral la protección y el ejercicio del derecho fundamental de Habeas Data y estableció dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para este derecho.

L. Que la Ley 1712 de 2014, sobre Transparencia y derecho de acceso a la información pública nacional, adiciona nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho; y en su artículo 20, establece la obligación de mantener un índice actualizado de los actos, documentos e informaciones calificados como clasificados o reservados, donde se debe incluir sus denominaciones, la motivación y la individualización del acto en que conste tal calificación; en el mismo sentido, el Decreto 1080 de 2015, "por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura", establece los instrumentos de la gestión de información pública (1) Registro de Activos de Información; (2) índice de Información Clasificada y Reservada; (3) Esquema de Publicación de Información; (4) Programa de Gestión Documental.

M. De otra parte, la Ley 527 de 1999 en artículo 2 literal c), define la firma digital "*como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación*".

N. El artículo 1 del Decreto 2364 de 2012 por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, define la firma electrónica como: métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

CONSEJO SUPERIOR
ACUERDO No. 171
22 FEB 2024

"POR MEDIO DEL CUAL SE APRUEBA Y SE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL QUINDÍO Y SE DICTAN OTRAS DISPOSICIONES"

O. Que el artículo 16 del Decreto 2106 de 2019, "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública" señala en su parágrafo que las autoridades deberán disponer de una estrategia de seguridad digital, para la gestión documental electrónica y preservación de la información, siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

P. Que el artículo 2.2.9.1.1.1 del Decreto 1008 de 2018, establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

Q. Que el artículo 2.2.9.1.1.3 del Decreto 1078 de 2015, subrogado por el Decreto 1008 de 2018, establece que la política de Gobierno Digital se desarrollará con fundamento en varios principios, entre ellos, el de seguridad de la información que "... busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano"

R. Que el anterior Decreto en su artículo 2.2.9.1.1.3. Principios, indica que la política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos consagrados en los artículos 209 de la Constitución Política, 3º de la Ley 489 de 1998, 3º de la Ley 1437 de 2011, 2 y 3 de la Ley 1712 de 2014, así como los que orientan el sector TIC establecidos en el artículo 2 de la Ley 1341 de 2009 y en particular el principio de Seguridad de la Información. Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

S. Que el artículo 2.2.22.3.1 del Decreto número 1499 de 2017 que integra los sistemas de gestión, adoptó la versión actualizada del Modelo Integrado de Planeación y Gestión-MIPG, marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión pública hacia el cumplimiento de los planes de desarrollo, y la resolución de necesidades y problemáticas de la ciudadanía, y fortaleció el componente de evaluación del riesgo a través de la Dimensión 7 de Control Interno y del sistema de Líneas de Defensa que operan con el Modelo Estándar de Control Interno-MECI, para brindar soporte y potenciar la herramienta gerencial hacia la efectividad en el manejo y seguimiento de los riesgos de gestión, corrupción y seguridad digital.

T. Que mediante Resolución No. 00500 del 10 de marzo de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital.

CONSEJO SUPERIOR
ACUERDO No. 00 - 171
22 FEB 2024

"POR MEDIO DEL CUAL SE APRUEBA Y SE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL QUINDÍO Y SE DICTAN OTRAS DISPOSICIONES"

U. Que mediante la Resolución 4156 del 07 de marzo de 2018, la Universidad del Quindío formula y se adopta la política de tratamiento de datos personales.

V. Que, mediante Resolución de Rectoría No. 8193 del 3 de agosto de 2021 "Por medio de la cual se adopta el Modelo integrado de Planeación y Gestión – MIPG, como marco de referencia de buenas prácticas, se ajusta el diseño del sistema integrado de gestión de la Universidad – SIG, y se crea el comité institucional de gestión y desempeño", se ajustó el sistema para facilitar la implementación de buenas prácticas los parámetros y estándares que prevé el MIPG a través de sus dimensiones y políticas.

W. Que, en la mencionada Resolución, se creó el Comité Institucional de Gestión y Desempeño, que establece entre sus funciones la de "Orientar, evaluar y hacer seguimiento a las estrategias, políticas y/o directrices para la planeación, implementación y mantenimiento de la Estrategia de Gobierno Digital".

X. Que la Información que se produce en la Universidad en el ejercicio de sus funciones y en cumplimiento de su misión, constituye un patrimonio con valor económico y estratégico como activos de información, por lo tanto, se hace necesario garantizar las condiciones para su preservación y accesibilidad.

Y. Que, en tal sentido, el Comité Institucional de Gestión y Desempeño, mediante Acta No. 005 del 13 de diciembre del año 2023, otorgó concepto favorable al "Proyecto de Acuerdo por medio del cual se aprueba y se adopta la Política de Seguridad y Privacidad de la Información de la Universidad del Quindío y se dictan otras disposiciones**",** y recomendó ser adoptada por el Consejo Superior.

Z. Que, la Dirección Financiera, expidió certificación con fecha del 12 de febrero del año 2024, en la que indica lo siguiente:

> *"El Consejo Superior de la Universidad del Quindío, mediante Acuerdo No. 0169 del 14 de diciembre de 2023 expidió el Presupuesto de Rentas y Recursos de Capital y el Acuerdo de Apropiaciones de la Universidad del Quindío para la vigencia fiscal del 1 de enero al 31 de diciembre de 2024.*
>
> *En su estructura presupuestal orientada a la inversión, se contempla el Rubro Presupuestal 2.3.2.02.02.008.01.02005 "Gestión de Políticas de Estado en la Institución", rubro que se encuentra enmarcado en el Plan de Desarrollo Institucional "Por una Universidad Pertinente Creativa Innovadora", Pilar 4 "Gestión Creativa" Meta 2 "Desarrollar un diagnóstico para el fortalecimiento del sistema interno de aseguramiento de calidad, que promueva la certificación o acreditación internacional a nivel institucional".*
>
> *Adicionalmente, que en cada vigencia se apropia con cargo al rubro presupuestal mencionado, el recurso requerido para dar cabal cumplimiento a las Políticas de Estado que aplican a las Instituciones Educativas de Educación Superior enmarcadas en las metas del PDI, por tanto, cabe señalar que para la vigencia 2024 se asignaron los recursos planeados para financiar el Sistema de Gestión de Seguridad y Privacidad de la Información para la Universidad del Quindío"*

CONSEJO SUPERIOR
ACUERDO No. 171
22 FEB 2024

"POR MEDIO DEL CUAL SE APRUEBA Y SE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL QUINDÍO Y SE DICTAN OTRAS DISPOSICIONES"

AA. Que, en sesión del 22 de febrero del año 2024, el Consejo Superior se reunió y aprobó el Acuerdo "por medio de la cual se aprueba y se adopta la política de seguridad y privacidad de la información de la universidad del Quindío y se dictan otras disposiciones".

BB. Que, por lo anteriormente expuesto, el Consejo Superior de la institución en pleno uso de sus facultades,

RESUELVE:

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO PRIMERO. Objeto. El presente Acuerdo, tiene como objeto aprobar y adoptar la Política de Seguridad y Privacidad de la Información de la Universidad del Quindío, así como definir los roles y responsabilidades frente al establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI; con el fin de establecer una cultura de seguridad de la información en la institución y en cumplimiento de las políticas de Gobierno Digital y Seguridad Digital, establecidas por el Gobierno Nacional.

ARTÍCULO SEGUNDO. Ámbito de aplicación. La presente política aplica para todos los funcionarios, contratistas, proveedores y demás partes interesadas (Estudiantes, docentes y demás personas vinculadas a la institución que no sean servidores públicos), que en cumplimiento de sus funciones y/o actividades, de acuerdo a lo pactado con la Universidad del Quindío, usen, recolecten, almacenen, procesen, transfieran o consulten la información de la institución. Al igual que, para todos los procesos de la Universidad (estratégicos, misionales, apoyo y de seguimiento y evaluación) de acuerdo con el mapa de procesos y a los diferentes sistemas o modelos de gestión implementados en la institución que componen el Sistema Integrado de Gestión.

De igual manera, aplica para todos los activos de información que soporten dichos servicios, procesos, sistemas o modelos de gestión que hacen parte del Sistema Integrado de Gestión.

ARTÍCULO TERCERO. Política General de Seguridad y Privacidad de la Información. La Universidad del Quindío, consciente del valor de una apropiada gestión de la información y considerándola un factor esencial para el desarrollo de servicios digitales de confianza y calidad, procesos digitales seguros y eficientes, y con el fin de contar con datos e información veraz para la toma de decisiones; se compromete con el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, mediante la adopción del Modelo de Privacidad y Seguridad de la Información - MSPI, en concordancia con la misión y visión institucional y el estricto cumplimiento de la normatividad legal vigente; buscando establecer un marco de

confianza en el ejercicio de sus deberes con el Estado, la comunidad universitaria y los ciudadanos.

Para la Universidad del Quindío, el Modelo de Privacidad y Seguridad de la Información - MSPI permite preservar, gestionar y proteger la confidencialidad, integridad y disponibilidad de la información, así como su autenticidad y no repudio; mediante la gestión integral de los riesgos, activos e incidentes de seguridad de la información, propendiendo por la continuidad de la operación de los servicios, el acceso a sus servicios, el uso efectivo y la apropiación de las TIC (Tecnologías de la Información y las Comunicaciones); acorde con las necesidades y expectativas de las diferentes partes interesadas.

Fomentará entre su comunidad universitaria y terceros que laboren o tengan relación con la institución, una cultura de seguridad de la información, el cumplimiento de los controles, políticas, procedimientos y demás directrices del Modelo de Privacidad y Seguridad de la Información-MPSI

ARTÍCULO CUARTO. Objetivos de la Política de Seguridad y Privacidad de la Información. La Política General de Seguridad y Privacidad de la Información, tendrá los siguientes objetivos:

1. Administrar los activos de información de la Universidad del Quindío, identificando aquellos de mayor criticidad; con el fin de prevenir la pérdida de confidencialidad, integridad y disponibilidad de los mismos.
2. Gestionar los riesgos de seguridad de la información de acuerdo a la metodología y plan de tratamiento utilizados para mantenerlos en niveles aceptables.
3. Gestionar los incidentes de seguridad y privacidad de la información, donde se genere, documente y apliquen las lecciones aprendidas, con el fin de reducir la posibilidad de ocurrencia o el impacto de incidentes futuros.
4. Monitorear el cumplimiento de los requisitos de seguridad y privacidad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y auditorías planificadas a intervalos regulares.
5. Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, de tal forma que se contribuya a la mejora continua del mismo.
6. Fomentar la cultura de seguridad y privacidad de la información, entre la comunidad universitaria y terceros que laboren o tengan relación con la institución, mediante la sensibilización y formación en temas relacionados con seguridad de la información física y digital, con el fin de prevenir los riesgos relacionados con el incumplimiento de las políticas, procedimientos y demás lineamientos establecidos por la universidad.
7. Reducir el impacto de los incidentes de seguridad de la información que comprometan la continuidad del servicio en la Universidad del Quindío o de los servicios definidos en el alcance del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI; mediante la implementación de controles oportunos y pertinentes.

CONSEJO SUPERIOR
ACUERDO No. 22 FEB 2024 ...UC - 171

"POR MEDIO DEL CUAL SE APRUEBA Y SE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL QUINDÍO Y SE DICTAN OTRAS DISPOSICIONES"

CAPÍTULO II

POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ARTÍCULO QUINTO. Políticas Específicas de Seguridad de la Información. La Política General de Seguridad y Privacidad de la Información se encuentra relacionada con las políticas de:

1. **Política para dispositivos móviles.** La Universidad del Quindío adoptará una política y las medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

2. **Política para teletrabajo.** La Universidad del Quindío implementará una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza el teletrabajo, trabajo remoto o cualquier modalidad de trabajo fuera de las instalaciones de la organización.

3. **Política de control de acceso.** La Universidad del Quindío establecerá, documentará y revisará una política de control de acceso con base en funciones, privilegios e información que se utilizará y de acuerdo a los controles previamente establecidos, frente a seguridad de la información.

4. **Política sobre el uso de controles criptográficos.** La Universidad del Quindío desarrollará e implementará una política sobre el uso de controles criptográficos para la protección de la información.

5. **Política de gestión de llaves criptográficas.** La Universidad del Quindío desarrollará e implementará una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.

6. **Política de escritorio limpio y pantalla limpia.** La Universidad del Quindío adoptará una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.

7. **Política de Respaldo de Información**. La Universidad del Quindío desarrollará e implementará una política de respaldo de la información, del software e imágenes de los sistemas, y las copias de respaldo deberán ponerse a prueba regularmente.

8. **Políticas de transferencia de información.** La Universidad del Quindío contará con políticas y controles de transferencia de información para proteger dicho activo, cuando se utiliza cualquier tipo de instalaciones de comunicación.

9. **Política de desarrollo seguro.** La Universidad del Quindío establecerá y aplicará reglas para el desarrollo de software y de sistemas de información, tanto internos

como aquellos que son desarrollados por proveedores.

10. **Política de seguridad de la información para las relaciones con proveedores**. La Universidad del Quindío desarrollará e implementará una política, procedimientos y controles requeridos para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización.

11. **Política de no repudio.** La Universidad del Quindío desarrollará e implementará una política para evitar el no repudio y que las partes interesadas con acceso a la información asuman la responsabilidad de las acciones realizadas en y con los activos de información.

12. **Política de gestión de incidentes de seguridad de la información.** La Universidad del Quindío documentará una política de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Esta deberá ir dirigida a todas las partes interesadas que tienen un acceso autorizado a cualquier sistema de información o activo de la institución.

13. **Política de gestión de activos de información**. La Universidad del Quindío desarrollará e implementará una política que asegure la identificación, clasificación, etiquetado, tratamiento o uso aceptable, devolución, y eliminación segura de los activos de información de cada proceso de la organización.

14. **Política de Sensibilización y Capacitación en Seguridad de la Información:** La Universidad del Quindío definirá e implementará una política que permita la formación y concienciación de la comunidad universitaria y terceros que laboren o tengan relación con la institución, en temas relacionados con la seguridad de la información.

ARTÍCULO SEXTO. Lineamientos de las Políticas Específicas de Seguridad y Privacidad de la Información. La totalidad de políticas enunciadas en este acuerdo, se deben desarrollar de manera clara y detallada en el Manual de Políticas de Seguridad y Privacidad de la Información; e identificar en la Declaración de Aplicabilidad del Sistema de Gestión de Seguridad y Privacidad de la Información. En tal sentido, se adopta el documento denominado "*Manual de Políticas de Seguridad y Privacidad de la Información*", que consta en 44 folios y hace parte integral del presente acuerdo. Asimismo, con el fin de ser actualizadas, se faculta al rector de la institución para que previo concepto del Comité institucional de gestión y Desempeño, expida los actos administrativos a que haya lugar para adoptarlas y/o actualizarlas.

CONSEJO SUPERIOR
ACUERDO No. 171
22 FEB 2024

"POR MEDIO DEL CUAL SE APRUEBA Y SE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL QUINDÍO Y SE DICTAN OTRAS DISPOSICIONES"

CAPÍTULO III

ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ARTÍCULO SÉPTIMO. Separación de deberes. Los deberes y las áreas de responsabilidad frente a la seguridad y privacidad de la información, se deben separar para reducir la probabilidad de la modificación no autorizada o no intencional, el uso no autorizado, indebido o accidental de los activos de información de la Universidad del Quindío, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite, use y coordine, cada uno de los activos que componen el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI.

1. **Alta Dirección (Rector):** Responsable por el direccionamiento estratégico e impulso del Sistema Gestión de Seguridad y Privacidad de la Información - SGSPI.

   Como parte de la gestión de la Alta Dirección para seguridad de la información, se encuentran las siguientes responsabilidades:

   - Asegurar que se definan y asignen las responsabilidades de seguridad y privacidad de la información.
   - Asegurar que se definan la política general, objetivos, políticas específicas de seguridad y privacidad de información y que estos sean compatibles con la planeación estratégica de la universidad, así como la revisión y actualización periódica de esta política.
   - Asegurar la integración y adopción de los requisitos del Modelo de Seguridad y Privacidad de la Información-MSPI en los procesos de la organización.
   - Asignar los recursos necesarios para el Sistema de Gestión de Seguridad y Privacidad de la Información de acuerdo al plan de trabajo presentado en cada vigencia.
   - Revisar el Sistema de Gestión de Seguridad y Privacidad de la Información de la universidad, para asegurarse de su conveniencia, adecuación, eficacia y mejora continua.
   - Dirigir y apoyar a los funcionarios y/o contratistas para contribuir a la eficacia, mejora continua y logro de los resultados previstos dentro del Modelo de Seguridad y Privacidad de la Información-MSPI.
   - Apoyar otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

2. **Comité Institucional de Gestión y Desempeño.** El Comité Institucional de Gestión y Desempeño, debe cumplir con las siguientes responsabilidades frente a la seguridad y privacidad de la información y/o el Sistema de Seguridad y Privacidad de la Información establecido por la Universidad del Quindío:

   - Orientar, evaluar y hacer seguimiento a las estrategias, políticas y/o directrices para la planeación, implementación y mantenimiento de la Estrategia de Gobierno

Digital, conforme se establece en el Modelo Integrado de Planeación y gestión-PIPG, como marco de referencia de buenas prácticas, adoptado por la Universidad del Quindío.

3. **Dirección de Planeación Institucional (Líder del Sistema de Seguridad y Privacidad de la Información)**

- Liderar el desarrollo, implementación, mantenimiento y actualización del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI y presentar los informes al Comité Institucional de Gestión y Desempeño, que correspondan sobre su nivel de implementación en la institución.
- Asegurar la integración y adopción de los requisitos del Modelo de Seguridad y Privacidad de la Información-MSPI en los procesos de la organización.
- Acompañar el desarrollo e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la universidad con base en el alcance definido para el SGSPI.
- Liderar la Implementación de los planes, proyectos, procesos, procedimientos y demás instrumentos de planeación necesarios para el mantenimiento del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI.
- Monitorear los controles y acciones de los riesgos de seguridad y privacidad de la información establecidos por la primera línea de defensa de acuerdo con la información suministrada por los líderes de procesos.
- Verificar la correcta gestión de los riesgos de seguridad y privacidad de la información, y los controles por parte de los procesos.
- Monitorear el estado de las actividades definidas en el Mapa de Ruta de la Estrategia de Gobierno Digital (Habilitador SGSPI), con el fin de determinar su nivel de implementación y cumplimiento.
- Revisar el Sistema de Gestión de Seguridad y Privacidad de la Información de la universidad, para asegurarse de su conveniencia, adecuación, eficacia y mejora continua.

4. **Oficial o Responsable de Seguridad y Privacidad de Información o quien haga sus veces:**

- Identificar la brecha entre el Modelo de Seguridad y Privacidad de la Información-MSPI y la situación de la Universidad del Quindío a través de la herramienta establecida por MinTic.
- Operacionalizar la implementación y mantenimiento del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI velando por el cumplimiento de las políticas de seguridad establecidas, normatividad aplicable y su alineación con estrategias de MinTic o del estado colombiano.
- Velar por el cumplimiento de los objetivos y planes del Sistema de Gestión de Seguridad y Privacidad de la Información- SGSPI de forma que se encuentren alineados con los requerimientos de normas y leyes vigentes.

CONSEJO SUPERIOR
ACUERDO No. 171
22 FEB 2024

"POR MEDIO DEL CUAL SE APRUEBA Y SE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL QUINDÍO Y SE DICTAN OTRAS DISPOSICIONES"

- Realizar actualizaciones documentales a las metodologías, lineamientos y políticas de Seguridad y Privacidad de la Información, a intervalos planificados o cuando sea necesario.
- Administrar, monitorear y coordinar diariamente la Seguridad y Privacidad de la Información en la Universidad del Quindío.
- Apoyar la definición de los controles o acciones a implementar en los planes de tratamiento de riesgos de Seguridad y Privacidad de la Información para cada proceso.
- Apoyar la definición de métodos que permitan identificar las vulnerabilidades en la infraestructura tecnológica de la universidad.
- Atender las auditorías internas, externas y revisiones de entes de control, proporcionando la información correspondiente a Seguridad y Privacidad de la Información.
- Asegurar la adecuada gestión de los incidentes de seguridad de la información en la Universidad del Quindío.
- Divulgar las responsabilidades de seguridad de la información en la Universidad del Quindío con base en los lineamientos del Modelo de Seguridad y Privacidad de la Información-MSPI.
- Realizar periódicamente seguimiento, medición, análisis y evaluación del desempeño de la Seguridad y Privacidad de la Información y eficacia del Modelo de Seguridad y Privacidad de la Información - MSPI.
- Diseñar estrategias para la apropiación de las políticas, procedimientos, manuales, guías e instructivos derivados del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI.
- Participar en las actividades y reuniones con el Comité Institucional de Gestión y Desempeño, cuando sea requerido.
- Asegurarse que el Sistema de Gestión de Seguridad y Privacidad de la Información sea conforme a los requisitos de la norma NTC-ISO-IEC 27001 y sus diferentes actualizaciones.
- Informar anualmente a la Alta Dirección, a través del Líder del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI o su designado, sobre el desempeño del mismo.
- Asegurar la inclusión de la continuidad de seguridad de la información en el plan de continuidad del negocio.
- Las demás responsabilidades asignadas en los procedimientos, instructivos, guías y demás documentación del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI.

5. **Responsables de procesos:** Vicerrectores, Decanos, Directores de Programas Académicos, Directores Técnicos, Directores Técnicos Administrativos, Director Financiero, Directores de Centro, Secretaría General, Jefes de Oficina, o líderes de procesos, quienes deberán asumir y ejecutar las siguientes responsabilidades:

CONSEJO SUPERIOR
ACUERDO No. 171
22 FEB 2024

"POR MEDIO DEL CUAL SE APRUEBA Y SE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL QUINDÍO Y SE DICTAN OTRAS DISPOSICIONES"

- Implantar los controles de seguridad de la información, que sean identificados para su proceso en el marco de la adopción del Modelo de Seguridad y Privacidad de la Información - MSPI.
- Implementar los planes, proyectos, procesos, procedimientos y demás instrumentos necesarios para el mantenimiento del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI.
- Difundir las políticas, procesos, procedimientos, documentos y logros relacionados con el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI en su respectivo proceso.
- Promover la vinculación y compromiso de los funcionarios y contratistas de su proceso, con el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI.
- Liderar y apoyar continuamente la implementación y mantenimiento del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, al interior de su proceso.
- Asegurar la disponibilidad de los funcionarios y contratistas de su proceso, para la asistencia a actividades de formación y sensibilización para el fortalecimiento de la cultura en Seguridad de la Información.
- Asegurar la gestión de activos de información para su proceso de acuerdo al procedimiento establecido por la universidad.
- Asegurar la gestión de los riesgos de Seguridad y Privacidad de la Información, de acuerdo a la metodología establecida por la universidad.
- Definir, aprobar, hacer seguimiento y velar por el cumplimiento del plan de tratamiento de riesgos.
- Aceptar los riesgos residuales de Seguridad y Privacidad de la Información.
- Revisar a intervalos planificados el cumplimiento de las políticas y procedimientos de Seguridad y Privacidad de la Información dentro de su proceso a cargo.
- Atender los requerimientos y solicitudes presentados por el Oficial o responsable de Seguridad y Privacidad de la Información.
- Participar en la definición y/o actualización de las políticas específicas de Seguridad y Privacidad de la Información.
- Implantar los planes, procesos, procedimientos y demás documentación necesaria para el mantenimiento del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI acorde a su proceso.
- Las demás responsabilidades asignadas en los procedimientos, instructivos, guías y demás documentación del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI.

6. Dirección de Tecnologías de la Información - TI

- Implementar, mantener y mejorar controles técnicos de seguridad informática para prevenir riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información de la Universidad del Quindío.

CONSEJO SUPERIOR
ACUERDO No. 171
22 FEB 2024

"POR MEDIO DEL CUAL SE APRUEBA Y SE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL QUINDÍO Y SE DICTAN OTRAS DISPOSICIONES"

- Liderar la formulación, actualización e implementación de controles, políticas, lineamientos y directrices de seguridad y privacidad de la información, referentes a infraestructura tecnológica, servicios de red y demás aspectos relacionados con la seguridad digital, en la Universidad del Quindío.
- Establecer lineamientos y controles de seguridad de la información dentro del ciclo de vida de desarrollo de software, tanto para desarrollos internos como para aquellos que se contraten externamente.
- Gestionar los recursos necesarios para la implementación de controles técnicos y mantenimiento del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI de acuerdo a las necesidades reportadas por los procesos y lo requerido al interior de su proceso.

7. **Dirección de Gestión Humana y Oficina de Asuntos Administrativos y Adquisiciones:** Su responsabilidad principal, frente a la seguridad y privacidad de la información, es la implementación de controles relacionados con los procesos de selección y administración del talento humano (bajo cualquier forma de vinculación con la universidad), de acuerdo con el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, en las siguientes fases:

   - Antes de la vinculación de los servidores públicos / o con la Universidad
   - Antes de la vinculación de contratos de trabajo con la Universidad del Quindío.
   - Durante la vinculación de los servidores públicos / o con la Universidad
   - Terminación y cambio de vinculación de los servidores públicos /o con la Universidad
   - Asegurar que los servidores públicos y contratistas comprendan sus responsabilidades y sean idóneos en los roles para los que se consideran, de tal forma que cumplan con los requerimientos de la universidad de acuerdo con la clasificación de la información a la que se accederá y los riesgos de seguridad y privacidad de la información identificados para cada proceso.
   - Verificar detalladamente para el cargo de Oficial o Responsable de Seguridad y Privacidad de la Información o aquellos cargos donde se desarrollen funciones críticas para la universidad (Acceso a Instalaciones de procesamiento de información crítica, infraestructura tecnológica, manejo de información financiera, manejo de información pública reservada y pública clasificada, entre otros), se tengan las competencias requeridas para desarrollar dichos roles.
   - Establecer los acuerdos de confidencialidad y no divulgación al momento de tomar posesión del empleo y/o firmar el contrato, así como las cláusulas de cumplimiento y las responsabilidades frente a las políticas, procedimientos y controles de seguridad de la información establecidas por la Universidad del Quindío.
   - Asegurar el cumplimiento de las políticas específicas de Seguridad y Privacidad de la Información, tratamiento de datos personales y cumplimiento de controles en las áreas o recintos seguros o restringidos, identificados en la Dirección de Gestión Humana.
   - Informar a los servidores públicos y contratistas sobre el proceso disciplinario y las acciones legales que se tomaran por parte de la Universidad del Quindío, frente al

incumplimiento de alguno de los procedimientos, controles y políticas de seguridad y privacidad de la información, establecidos por la institución.

- Prevenir el incumplimiento de las obligaciones legales, estatutarias de reglamentación o contractuales relacionadas con la Seguridad de la Información.
- Incorporar en el Programa de Inducción, Reinducción y el Plan de Capacitaciones, la formación y/o sensibilización en temas relacionados con el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI.
- Informar al personal que finaliza o cambia su relación laboral con la universidad, sobre las obligaciones y responsabilidades que siguen vigentes después del cambio o terminación del empleo.

8. **Dirección Jurídica:** Con el fin de evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad, en el marco de la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI de la Universidad del Quindío, la Dirección Jurídica, tendrá las siguientes responsabilidades:

   - Apoyar a los líderes de los procesos y/o demás áreas involucradas, cuando se requiera asesoría frente a los requisitos estatutarios, legales, reglamentarios o contractuales para el diseño, mantenimiento, operación y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI de la Universidad del Quindío, entre ellos, la clasificación de activos tipo información en relación a los niveles de confidencialidad, integridad y disponibilidad y la protección de datos personales en el marco de Ley 1712 de 2014 de transparencia y acceso a la información pública y la Ley 1581 de 2012 marco general de la protección de los datos personales en Colombia, o las normas que las modifiquen o sustituyan.
   - Definir los modelos de acuerdos de confidencialidad y no divulgación, para el tratamiento o intercambio de información entre la Universidad del Quindío y los funcionarios, contratistas y terceros vinculados a la institución, incluyendo los compromisos adquiridos y las implicaciones legales por el incumplimiento de dichos acuerdos.
   - Revisar que los contratos, así como las Ordenes de Prestación de Servicios cuenten con los documentos o controles y requisitos de seguridad y privacidad de la información establecidos por la Universidad del Quindío (Acuerdos de confidencialidad y no divulgación, cláusulas de cumplimiento y las responsabilidades frente a las políticas, procedimientos y controles de acuerdo a la información o infraestructura tecnológica a la que se tendrá acceso, entre otras).

9. **Dirección de Gestión y Aseguramiento de la Calidad**

   - Controlar los componentes documentales que consolidan el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI en el marco del Modelo de Seguridad y Privacidad de la información – MSPI y el Sistema Integrado de Gestión - SIG.
   - Realizar acompañamiento en la armonización de los componentes del Sistema de Gestión de Seguridad y Privacidad de la Información- SGSPI con el Sistema

Integrado de Gestión- SIG y las buenas prácticas que se implementen en la Universidad.

- Incluir en las auditorías periódicas la verificación del cumplimiento de los requisitos del Modelo de Seguridad de la Información – MSPI en la Universidad del Quindío.

10. Servidores Públicos, Contratistas y/o terceros vinculados a la Institución (Estudiantes, docentes, consultores, proveedores y demás figuras de vinculación con la universidad que no sean servidores públicos):

- Apoyar la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, de acuerdo con las políticas, metodologías, procesos, procedimientos y los demás lineamientos establecidos para tal fin.
- Aceptar y dar cumplimiento a las políticas de seguridad y privacidad de la información.
- Reportar eventos y/o incidentes de seguridad de la información de acuerdo al procedimiento establecido por la universidad.
- Clasificar, etiquetar y manejar la información de acuerdo con los niveles de seguridad y privacidad procedimientos, lineamientos y políticas establecidas por la Universidad del Quindío y la reglamentación legal vigente.
- Dar uso adecuado a los activos de información asignados por la Universidad del Quindío, de acuerdo a las políticas, controles de seguridad y privacidad y lineamientos establecidos para tal fin.
- Participar activamente en las actividades de sensibilización, formación y toma de conciencia desarrolladas por la Universidad del Quindío.

11. Oficina de Control Interno

- Realizar seguimiento y evaluar el cumplimiento a la normatividad legal vigente nacional y de manera interna, respecto a la de seguridad y privacidad de la información.
- Verificar la ejecución de las auditorías de seguridad y privacidad de la información.
- Recomendar acciones de mejora frente a las debilidades encontradas en las auditorías e informarlas al Comité Institucional de Gestión y Desempeño.

12. Oficina de Control Interno Disciplinario

- Implementar los procesos disciplinarios definidos en la universidad, donde se identifique que los funcionarios y/o contratistas han incurrido en incumplimiento de políticas, controles y lineamientos que hayan producido incidentes de seguridad de la información; por lo que deben ser registrados e investigados con el fin de determinar sus causas y responsables. Es decir, aquellos servidores públicos que hayan sido relacionados con incidentes de seguridad de la información o violaciones a las políticas de seguridad y privacidad de la información establecidas en la entidad, serán citados a descargos y se iniciará el respectivo proceso disciplinario.
- Manejar los procesos disciplinarios derivados de los reportes y del análisis de los incidentes de seguridad de la información de acuerdo a la gravedad y el nivel de

responsabilidad identificadas, con base en la Ley 1273 de 2009 o las normas que las modifiquen o sustituyan.

13. Dirección de Comunicaciones Estratégicas

- Apoyar a las direcciones, oficinas o áreas en el diseño de las piezas gráficas, convocatorias, comunicados, videos de sensibilización y demás componentes que hagan parte del SGSPI, en concordancia con el Manual de Identidad de la universidad.
- Dar a conocer a la comunidad universitaria y demás partes interesadas, de manera oportuna, la información relacionada con los comunicados emitidos por la Dirección de Tecnologías de la Información y/o la Dirección de Planeación Institucional, en virtud de la implementación de los procedimientos de gestión de incidentes de seguridad de la información, gestión de cambios, gestión de la capacidad y demás instrumentos que hacen parte del SGSPI.

14. Oficina de Gestión Documental

- Actualizar los activos de información documentales y el índice de información clasificada y reservada, a partir de la Tablas de Retención Documental vigente. Asimismo, consolidar y publicar de acuerdo a los lineamientos emitidos por el gobierno nacional.
- Comunicar la actualización de los activos de información documentales y el índice de información clasificada y reservada a los lideres de los procesos institucionales del alcance del SGSPI.
- Comunicar oportunamente al Oficial o Responsable de Seguridad y Privacidad de Información o quien haga sus veces, cuando se presenten cambios en las Políticas, procedimientos y formatos del Sistema de Gestión Documental, que afecten los componentes, instrumentos o lineamientos relacionados con el SGSPI de la universidad.

CAPÍTULO IV

DISPOSICIONES FINALES

ARTÍCULO OCTAVO. Revisión, actualización y seguimiento. La Política de Seguridad y Privacidad de la Información debe ser revisada a intervalos planificados, o si ocurren cambios significativos de carácter legal, estatutario o reglamentario, para asegurar su conveniencia, adecuación y eficacia continúas, y se debe hacer seguimiento al cumplimiento de las disposiciones aquí contenidas. Para el efecto, se faculta al rector de la Institución para que actualice la Política de Seguridad y Privacidad de la información, previa recomendación del Comité Institucional de Gestión y Desempeño.

ARTÍCULO NOVENO. Publicidad y comunicación. La presente disposición debe ser publicada, comunicada y/o socializada a todas las partes interesadas, identificadas en el contexto organizacional; y estar disponible como información documentada.

CONSEJO SUPERIOR
ACUERDO No. 171
22 FEB 2024

"POR MEDIO DEL CUAL SE APRUEBA Y SE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL QUINDÍO Y SE DICTAN OTRAS DISPOSICIONES"

ARTÍCULO DÉCIMO. Cumplimiento. Toda la comunidad educativa y en general, para todas las partes interesadas identificadas en el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI de la Universidad del Quindío, deberán dar cumplimiento al 100% de la política.

Parágrafo 1. El incumplimiento de la presente política y las disposiciones aquí contenidas pueden conducir a acciones disciplinarias y/o acciones de índole legal, de acuerdo a los procedimientos internos de la Universidad del Quindío y demás lineamientos aplicables a la Institución.

ARTÍCULO DÉCIMO PRIMERO: Vigencia y derogatoria. El presente acuerdo rige a partir de la fecha de publicación y deroga todas las disposiciones que le sean contrarias.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dado en Armenia, Quindío 22 FEB 2024

AMANDA TANGARIFE CORREA
Presidente Delegada

CLAUDIA PATRICIA BERNAL RODRÍGUEZ
Secretaria General

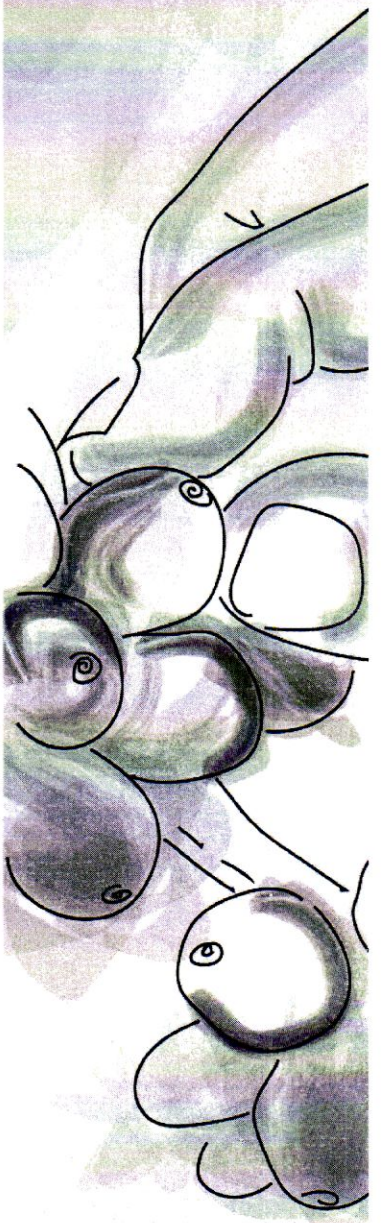
	NOMBRES Y APELLIDOS	FIRMA
PROYECTÓ Y ELABORÓ	Harby Gil Arteaga Profesional Especializado- Dirección de TI Marietta Velásquez Rodríguez-Profesional Especializado de la Dirección de Planeación	MARIETTA VELÁSQUEZ R.
REVISÓ	Nathalie Gallego Arturo – Profesional de la Dirección Jurídica	
	Víctor Alfonso Vélez Muñoz – Director Jurídico	
	Estella López de Cadavid- Presidente del Comité Institucional de Gestión y Desempeño	
APROBÓ	Luis Fernando Polanía Obando-Rector	

Los arriba firmantes declaramos que hemos revisado el presente documento y soportes, encontrándolo 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 firma del Consejo Superior de la institución.

UNIVERSIDAD
DEL QUINDÍO
Res.MEN 014915 - 02 AGO 2022
RENOVACIÓN ACREDITACIÓN

MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGUIRIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dirección de Planeación Institucional



UNIQUINDÍO
en conexión territorial
www.uniquindio.edu.co

HISTORIAL DE VERSIONES DEL DOCUMENTO

VERSIÓN DEL DOCUMENTO	RIGE A PARTIR DE	DESCRIPCIÓN DEL CAMBIO

CONTENIDO

INTRODUCCIÓN

La UNIVERSIDAD DEL QUINDÍO considera la información como un activo fundamental para la entidad, razón por la cual, es necesario establecer un marco para asegurar que la información es protegida independientemente del medio de conservación (físico o digital) y la forma en la que ésta es manejada, procesada, transportada o almacenada.

Las políticas contenidas en este documento constituyen la parte fundamental del Sistema de Gestión de Seguridad y Privacidad de la Información y se consideran la base para la implantación de los controles, procedimientos y estándares definidos por este.

Asimismo, es responsabilidad de todos los funcionarios, contratistas, proveedores, visitantes y todos aquellos con acceso a información de la Universidad del Quindío, dar cumplimiento a las políticas aquí contenidas.

1. OBJETIVO

Establecer los lineamientos en seguridad y privacidad de la información que debe seguir todo el personal (funcionarios, comunidad académica, contratistas, terceros, practicantes, proveedores, ciudadanía y demás personas vinculadas con la Universidad del Quindío), con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información y de sus activos relacionados.

2. ALCANCE DEL DOCUMENTO

Este documento aplica a toda la comunidad universitaria y terceros que laboren o tengan relación con la institución, por lo que es de obligatorio cumplimiento.

Se podrán impartir excepciones para la implementación total de las políticas y controles de seguridad, para la Alta Dirección Institucional, otros cargos directivos e investigadores; siempre y cuando se evidencien asuntos de fuerza mayor o su necesidad para el cumplimiento de los objetivos de la institución.

La excepción a la que haya lugar, será documentada, discutida, autorizada y evidenciada, además deberá contener la respectiva justificación; a su vez, será comunicada y avalada por la Dirección de Tecnologías de la Información, quienes determinarán los controles adicionales a que haya lugar, para que la misma, continúe garantizando la confidencialidad, integridad y disponibilidad de la información, y la minimización de los riesgos identificados y gestionados para el proceso donde se determine dicha excepción.

3. DEFINICIONES

Las políticas apoyan el cumplimiento de la misión de la Institución, teniendo en cuenta las siguientes definiciones, basadas en la norma ISO/IEC 27000.

- **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

- **Activo crítico:** Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectarán el cumplimiento de los objetivos estratégicos de la Universidad.

- **Acuerdos de confidencialidad:** Pacto entre dos o más partes, cuyo objeto es garantizar que se guarde secreto o no se revele determinada información que comparten y que la usen únicamente para el fin acordado.

- **Acuerdos de Niveles de Servicio-ANS**: son parámetros, tiempos y requisitos establecidos para la entrega de productos o servicios de un proceso a los usuarios internos y externos, con los cuales se medirá la oportunidad del mismo.

- **Aplicaciones críticas:** Sistemas donde la menor "amenaza" puede tener consecuencias muy graves a la vez sobre las funciones misionales.

- **Autenticación secreta:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema para llegar a activos valiosos. Por lo general, incluye contraseñas y claves de cifrado, por lo que debe controlarse mediante un proceso de gestión formal y debe ser mantenida en forma confidencial para el usuario.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

- **Cifrado**: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

- **Código malicioso:** Es cualquier software corrupto, dañino, nocivo o no autorizado diseñado para infiltrarse y dañar la información y sus sistemas de procesamiento, entre estos: Virus informáticos, troyanos o "trojan horses", Keyloggers, Virus de macros, entre otros.

- **Confiabilidad**: Propiedad que determina que la información no se haga disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Confidencialidad:** propiedad que determina que la información no se haga disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Control criptográfico:** Se refiere a la protección de la información en el caso de que un intruso pueda tener acceso físico a la información, para lo cual se establece un sistema de cifrado (conjunto de valores matemáticos) de la misma para dificultar la violación de su confidencialidad o su integridad.

- **Control de acceso**: El proceso que limita y controla el acceso a los recursos de un sistema computarizado; un control físico o lógico diseñado para proteger contra usos o entradas no autorizadas. El control de acceso puede ser definido por el sistema (mandatory access control – MAC), o definido por el usuario propietario del objeto (discretionary access control – DAC).

- **Correo electrónico**: El correo electrónico (email, electronic mail) es el intercambio de mensajes almacenados en computadora por medio de las telecomunicaciones. Los mensajes de correo electrónico se codifican por lo general en formato de texto ASCII (American Standard Code for Information Interchange). Sin embargo, se pueden también enviar archivos en otros formatos, tales como imágenes gráficas y archivos de sonidos, los cuales son transferidos como archivos anexos en formato binario.

- **Disponibilidad**: Propiedad de ser accesible y utilizable sobre demanda por una entidad autorizada.

- **Cifrado** (Encriptación, codificación): La encriptación es el proceso para volver ilegible información considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

  Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros.

Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.

- **Evaluación de Riesgos**: Proceso global de identificación, análisis y estimación de riesgos en la operación La UNIVERSIDAD DEL QUINDÍO.

- **Estimación de riesgos**: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

- **Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo (identificación, análisis, valoración y tratamiento).
- **Impacto**: El costo para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros p.ej., pérdida de reputación, implicaciones legales, etc.

- **Incidente de Seguridad**: Evento único o serie de eventos de seguridad de la información inesperada o no deseado que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Integridad:** Propiedad de exactitud y completitud de la información.

- **Internet**: Es un sistema mundial de redes de computadoras, integrado por las diferentes redes de cada país del mundo, por medio del cual un usuario en cualquier computadora puede, en caso de contar con los permisos apropiados, obtener información, efectuar transacciones, comunicarse y participar en toda gama de procesos públicos y privados puesto en dicha red.

- **Intranet**: Red de una organización que utiliza tecnologías y protocolos de Internet, pero que sólo está disponible para determinadas personas, por ejemplo, para los empleados de una compañía. Una Intranet también recibe el nombre de red privada.

- **No repudio**: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La UNIVERSIDAD DEL QUINDÍO, dentro del marco de su misión institucional y los lineamientos de Gobierno Digital, adopta la política para el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI):

La Universidad del Quindío, consciente del valor de una apropiada gestión de la información y considerándola un factor esencial para el desarrollo de servicios digitales de confianza y calidad, procesos digitales seguros y eficientes, y con el fin de contar con datos e información veraz para la toma de decisiones; se compromete con el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información, mediante la adopción del Modelo de Privacidad y Seguridad de la Información - MSPI, en concordancia con la misión y visión institucional y el estricto cumplimiento de la normatividad legal vigente; buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado, la comunidad universitaria y los ciudadanos.

Para la Universidad del Quindío, el Modelo de Privacidad y Seguridad de la Información - MSPI permite preservar, gestionar y proteger la confidencialidad, integridad y disponibilidad de la información, así como su autenticidad y no repudio; mediante la gestión integral de los riesgos, activos e incidentes de seguridad de la información, propendiendo por la continuidad de la operación de los servicios, el acceso a sus servicios, el uso efectivo y la apropiación de las TIC (Tecnologías de la Información y las Comunicaciones); acorde con las necesidades y expectativas de las diferentes partes interesadas.

Fomentará entre su comunidad universitaria y terceros que laboren o tengan relación con la institución, una cultura de seguridad de la información, el cumplimiento de los controles, políticas, procedimientos y demás directrices del Modelo de Privacidad y Seguridad de la Información-MPSI

5. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Administrar los activos de información de la Universidad del Quindío, identificando aquellos de mayor criticidad; con el fin de prevenir la pérdida de confidencialidad, integridad y disponibilidad de los mismos.

- Gestionar los riesgos de seguridad de la información de acuerdo a la metodología y plan de tratamiento utilizados para mantenerlos en niveles aceptables.
- Gestionar los incidentes de seguridad de la información, donde se genere, documente y aplique las lecciones aprendidas, con el fin de reducir la posibilidad de ocurrencia o el impacto de incidentes futuros.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y auditorías planificadas a intervalos regulares.
- Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad y Privacidad de la Información, de tal forma que se contribuya a la mejora continua del mismo.
- Promover la cultura de seguridad de la información, entre su comunidad universitaria y terceros que laboren o tengan relación con la institución, mediante la sensibilización y formación en temas relacionados con seguridad de la información física y digital, con el fin de minimizar los riesgos relacionados con el incumplimiento de las políticas, procedimientos y demás lineamientos establecidos por la universidad.
- Reducir el impacto de los incidentes de seguridad de la información que comprometan la continuidad de la Universidad del Quindío o los servicios definidos en el alcance del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI; mediante la implementación de controles oportunos y pertinentes.

6. NORMATIVA

La Universidad del Quindío cuenta con un Normograma, el cual recopila en forma general todos los elementos normativos que tienen relación con los requisitos legales, reglamentarios, contractuales y técnicos relacionados o que soportan el SGSPI de la institución. Dicho documento, hace parte integral del presente Manual de Políticas. *Ver Anexo No. 2 UNIVERSIDAD DEL QUINDÍO - Normograma MSPI.*

7. CONSIDERACIONES GENERALES DEL SGSPI

7.1 REVISIÓN DE LA POLÍTICA GENERAL Y EL MANUAL DE POLÍTICAS

La política general y el manual de políticas de seguridad de la información deben ser revisados y actualizados al menos una vez al año o cuando haya cambios relevantes en el contexto estratégico de la UNIVERSIDAD DEL QUINDÍO, con el fin de asegurar que sigan siendo adecuados a la estrategia y necesidades de la entidad.

Estos documentos deben ser revisados por la Alta Dirección con el apoyo del Comité Institucional de Gestión y Desempeño, y aprobados por los mismos de acuerdo a la competencia de cada uno.

7.2 ORGANIZACIÓN DE LA SEGURIDAD

- Todo aquel que tenga acceso a la información de la UNIVERSIDAD DEL QUINDÍO, es responsable de velar por la seguridad de la información a la que tiene acceso y de cumplir las políticas descritas en este documento.

- El Oficial o responsable del SGSPI, es el garante de la implementación y mantenimiento del Sistema de Gestión de Seguridad y Privacidad de la Información.

- El Oficial o responsable del SGSPI debe verificar el seguimiento al cumplimiento de las políticas, y en caso de requerirse, prestar asesoría a todo aquel que maneje información de la entidad, coordinar las actividades de gestión de riesgos de la seguridad de la información, apoyar la identificación de controles y reportar el estado de la implementación y seguimiento del mismo, a la Alta Dirección.

- Todo aquel que tenga acceso a la información de la UNIVERSIDAD DEL QUINDÍO, debe tener claramente definidas sus funciones, con el fin de reducir el uso no autorizado, indebido o accidental de los activos de información.

- Todos los sistemas de información de la entidad, deben implementar reglas de acceso, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre las personas o grupo de personas que otorgan los privilegios y aquellos que los utilizan.

- La Dirección de Tecnologías de la Información dispondrá de un directorio actualizado de autoridades y organismos de control, para acceder a alertas tempranas en seguridad de la información, implementar los controles respectivos y solicitar apoyo ante incidentes.

- La Dirección de Tecnologías de la Información en conjunto con el Oficial o Responsable del SGSPI mantiene contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información. Lo anterior con el fin de estar al día con la información relacionada con la seguridad de la información y recibir advertencias de actualizaciones, ataques, y vulnerabilidades del software y firmware utilizado en la UNIVERSIDAD DEL QUINDÍO

7.3 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

La seguridad de la información se debe integrar a la gestión de proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de los proyectos. Lo anterior aplica a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los Directores, Jefes de Dependencia/Área asegurar que se sigan las siguientes directrices:

- Incluir objetivos de seguridad de la información en los objetivos del proyecto.

- Realizar valoración de los riesgos de seguridad de la información en la fase de estudios previos del proyecto, para identificar los controles necesarios.

- Hacer seguimiento a los riesgos y controles aplicados durante todas las fases del proyecto.

8. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

8.1 DISPOSITIVOS MÓVILES

La Dirección de Tecnologías de la Información establecerá medidas de protección a través de mecanismos de seguridad perimetral para la conexión de dispositivos móviles. Se dispondrá de puntos de acceso inalámbrico para la conexión de estos equipos, de acuerdo con las directrices establecidas y las categorías de acceso para los grupos identificados.

Los usuarios deberán estar registrados en un repositorio institucional, y la cantidad de dispositivos móviles conectados por usuario será limitada, de acuerdo a los lineamientos de la Dirección de Tecnologías de la Información, con el fin de efectuar una adecuada gestión sobre la infraestructura y conectividad inalámbrica institucional.

Se tendrá un segmento de red para la conexión temporal de dispositivos móviles de terceros, no haga parte permanente de la comunidad universitaria, es decir, cuando se realicen eventos, simposios, reuniones, entre otros. El líder de dependencia responsable de dicho evento, deberá solicitar permisos de acceso y reportar el tiempo que requieren de conexión. Dichos accesos serán revocados al terminar los eventos o al finalizar el día.

Cualquier dispositivo inalámbrico que represente una amenaza o viole las políticas aquí contenidas o cualquier control de seguridad establecido por la universidad, podrá ser desconectado y desactivado de los servicios de Intranet, Extranet e Internet

La información que se gestione en los dispositivos móviles deberá contar con copia de respaldo en la nube institucional, de acuerdo a las directrices de la Dirección de Tecnologías de la Información.

Se deberá contar con un listado de equipos portátiles personales de los funcionarios y contratistas que gestionan información pública reservada o pública clasificada de la Universidad del Quindío. Dichos equipos tendrán medidas de protección, como mínimo una contraseña y cifrado de disco. Las estaciones de trabajo y equipos portátiles que son propiedad de la UNIVERSIDAD DEL QUINDÍO contarán con software licenciado, cifrado de disco y protección contra código malicioso.

El funcionario, contratista o tercero que gestione información pública reservada o pública clasificada en su equipo personal y se retire de la universidad o cambie de cargo, deberá permitir el borrado seguro de los datos institucionales que contenga en su dispositivo, de acuerdo a las directrices establecidas por la Dirección de Tecnologías de la Información y el esquema de clasificación de la información definido por la Oficina de Gestión Documental.

El contratista que utilice equipos de cómputo de su propiedad para el desarrollo del objeto del contrato deberá:

- Tener y usar solo software legal instalado en su equipo o como mínimo contar con un antivirus activado y reconocido.

- Para el caso de los proveedores que tengan contratos activos de soporte o desarrollo de software deberán comunicar a la Dirección de Tecnologías de la Información el listado de equipos, dirección MAC de sus interfaces, aplicaciones utilizadas o software que van a utilizar con la institución, el tipo de contrato de soporte y licenciamiento por las posibles causales de terceros a la institución. La conexión sobre la aplicación institucional deberá efectuarse como mínimo sobre una solución VPN – Client o cifrada.

- La evidencia de las licencias correspondientes (tanto para el sistema operativo como para las aplicaciones), deberá indicar el nombre del software, fabricante, versión licenciada y fecha de caducidad de la licencia. Esta información debe remitirse a la Dirección de Tecnologías de la Información previo a la conexión de dichos dispositivos a la red de la entidad.

Los dispositivos móviles no se deberán conectar a redes públicas inseguras o lugares públicos son bajos niveles de cifrado.

La protección contra códigos maliciosos se deberá instalar y realizar un análisis frecuente, esta tarea puede ser apoyada por la Dirección de Tecnologías de la Información.

El funcionario o contratista deberá velar por mantener el equipo en lugares seguros y con las protecciones de seguridad como teléfono bloqueado con clave o biometría.

Cuando se utiliza el dispositivo móvil en lugares públicos, el funcionario, contratista o tercero que gestione información pública reservada o pública clasificada, deberá

tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.

La UNIVERSIDAD DEL QUINDÍO se reserva el derecho de monitorear y revisar cuando se requiera, el software instalado en equipos de cómputo, los dispositivos móviles y los servidores conectados a la red de la entidad.

Todo activo tipo información, desarrollo o código fuente, tratamiento de datos y/o bases de datos que se gestione en los dispositivos móviles de la comunidad universitaria y terceros que laboren o tengan relación con la institución, será propiedad de la Universidad del Quindío.

En caso de pérdida de un dispositivo móvil el funcionario, contratista o tercero que labore o tenga relación con la institución y que sea propiedad de la universidad, deberá reportar el evento, de acuerdo al Procedimiento Gestión de Incidentes de Seguridad de la Información y realizar la respectiva denuncia, la cual deberá remitir al área de activos fijos.

8.2 POLÍTICA PARA TELETRABAJO

La modalidad de teletrabajo, trabajo en casa o trabajo remoto, estas dos últimas teniendo en cuenta, las situaciones atípicas o extraordinarias (Desastres naturales, situaciones de salud pública, vandalismo, calamidad del funcionario) que ameriten acogerse a dicha actividad, se deberán tener en cuenta las siguientes condiciones:

- Realizar una solicitud mediante el CSU, previa aprobación del líder del proceso al que pertenece, indicando lo siguiente para la configuración de VPN (Redes Privadas Virtuales):
    - Tiempo por el cual se requiere la conexión.
    - Aplicaciones, dispositivos, sistemas de información y servicios a los cuales se requiere acceder.

- En ningún momento se deberá dejar el equipo desatendido y con pantalla desbloqueada; o en lugares donde pueda ser víctima de hurto o exista la posibilidad de daño físico de la máquina por corrosión, polvo o humedad.

- El usuario que se encuentre fuera de la institución y haga uso de activos propiedad de la Universidad del Quindío, deberá proteger los activos y cumplir con los controles de seguridad establecidos por la institución.

- La responsabilidad de implementar controles de seguridad para los equipos que se encuentren en trabajo remoto o trabajo en casa, que sean propiedad de los funcionarios o contratistas, será exclusiva de los mismos, como es el caso de las actualizaciones a los sistemas, mantenimientos físicos y lógicos, instalación de software de protección, entre otros.

El acceso a los sistemas de información y servicios de TI estará disponible a toda la comunidad universitaria y terceros que laboren o tengan relación con la institución. La Dirección de Tecnologías de la Información implementará los controles de seguridad pertinentes.

La universidad cuenta con un dispositivo de seguridad perimetral para el control de todas las conexiones, y se efectuará un proceso de verificación sobre la versión del sistema operativo y aplicación antimalware, en aras de salvaguardar los activos de información de propiedad de la universidad.

La Dirección de Tecnologías de la Información podrá tomar las medidas necesarias para asegurar el cumplimiento del SGSPI y cualquier otro reglamento que aplique para preservar la confidencialidad, integridad y disponibilidad de los activos de información.

Los funcionarios y contratistas de la UNIVERSIDAD DEL QUINDÍO que se encuentren en modalidad de teletrabajo, trabajo en casa o trabajo remoto, serán los responsables de dar cumplimiento a las políticas de seguridad establecidas en el presente manual.

8.3 POLÍTICA DE CONTROL DE ACCESO

8.3.1 Lineamientos generales de Control de Acceso

La Dirección de Tecnologías de la Información controlará el acceso mediante el enfoque basado en roles, aplicando los siguientes principios:

- Lo que necesita conocer: solamente se concede acceso a la información que la persona necesita para la realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita saber y, en consecuencia, diferentes perfiles de acceso).

- Lo que necesita usar: solamente se concede acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos, recintos) que la persona necesita para la realización de su tarea/trabajo/rol.

8.3.2 Acceso a Redes y a Servicios en Red

- Los puntos de red de acceso físicos que no estén en uso, deben ser deshabilitados, con el fin de evitar conexiones no autorizadas a la red de la UNIVERSIDAD DEL QUINDÍO Adicionalmente, los puntos de red activos se controlan mediante dispositivos de seguridad perimetral.

- La Dirección de Tecnologías de la Información asigna los roles, permisos y controla el acceso de usuarios a cada sistema de información de acuerdo con la solicitud de los jefes de dependencia/área.

    - El acceso de terceros a información institucional debe ser autorizado exclusivamente por el propietario del activo. Esto bajo las condiciones de seguridad, confidencialidad, disponibilidad, control y auditoría.

    - Ningún servidor público o contratista puede acceder al usuario administrador para tomar el control del equipo o su dominio. Esta labor es exclusiva del personal de la Dirección de Tecnologías de la Información y los Administradores Funcionales de las dependencias, cuando estén realizando soporte o actualización de los equipos y aplicaciones, previa autorización del encargado de la Dirección de Tecnologías de la Información.

    - Bimensualmente se cambiará la contraseña de acceso a los equipos y la red de La UNIVERSIDAD DEL QUINDÍO. La Dirección de Tecnologías de la Información es el único autorizado para realizar la programación de estas reglas, para que de manera automática se dé cumplimiento a este control.

- Ningún servidor público o contratista podrá compartir o transferir archivos o carpetas de un equipo de cómputo, que corresponda a información pública clasificada o pública reservada, a otro, sin la respectiva autorización del líder del proceso.

- El acceso a redes Wi-Fi se controla con autenticación por contraseña, cada red tiene configurados privilegios y perfiles de navegación; el acceso a las aplicaciones se controla mediante portal cautivo.

- La Dirección de Tecnologías de la Información administra un servicio de conectividad a todos los funcionarios y contratistas de la institución para la navegación.

- La conexión remota a la red de área local de la universidad, debe ser realizada a través de una conexión VPN segura suministrada por la Dirección de Tecnologías de la Información, previa autorización del jefe de dependencia/área, quien es el encargado de realizar la solicitud formal mediante el CSU al proceso de Gestión TICS.

8.3.3 Gestión de Acceso de Usuarios

- El registro y cancelación de usuarios; el suministro de acceso a usuarios, la gestión de derechos de acceso privilegiado, la gestión de información de autenticación secreta, y la revisión, retiro o ajuste de los derechos de acceso se realizan de acuerdo con el procedimiento Gestión de Usuarios.

- La Dirección de Tecnologías de la Información revisa trimestralmente el listado de usuarios con acceso a sistemas de información de la universidad, y lo confronta con el listado de funcionarios suministrado por Dirección de Gestión Humana y el listado de contratistas suministrado por la Oficina de Asuntos Administrativos y Adquisiciones.

- La solicitud de bloqueo o suspensión del acceso a los sistemas de información de la institución, por vacaciones, permisos temporales, licencias, incapacidades, entre otras situaciones administrativas, es responsabilidad de los supervisores de contrato, para el caso de los contratistas; en lo que respecta a los funcionarios, el responsable será el Director Administrativa de

la Dirección de Gestión Humana. Estas solicitudes deben ser remitidas a la Dirección de Tecnologías de la Información.

8.3.4 Uso de Información de Autenticación Secreta (Responsabilidades de los Usuarios)

- Cada usuario es responsable de salvaguardar la contraseña de ingreso al equipo y a los sistemas de información.

- No está permitido guardar o escribir las contraseñas en papeles físicos ni documentos de texto como bloc de notas, Word o notas de Windows. Para el almacenamiento de las contraseñas se deben acatar las directrices de la Dirección de Tecnologías de la Información.

- La contraseña escogida para el acceso a cada uno de los sistemas de información debe:

    - Ser diferente para cada aplicación o sistema de información con excepción de aquellos sistemas que se autentiquen contra el directorio activo o SSO.

    - No deberá contener datos personales o de familiares tales como nombres, apellidos, fechas de cumpleaños o alguna otra fecha importante.

    - Las contraseñas se deben establecer teniendo en cuenta los siguientes parámetros: Deben contener mayúsculas, minúsculas, números, caracteres especiales y mínimo ocho (08) caracteres.

- Las contraseñas:

    - Deben ser cambiadas de manera bimensual. Para ello, las aplicaciones controladas mediante el directorio activo exigen el cambio automático de contraseñas.

    - Está prohibido facilitar o proporcionar acceso a las aplicaciones e información a usuarios o a terceros no autorizados.

- Para desbloquear la contraseña de acceso a los diferentes sistemas de información, el usuario debe realizar la solicitud ante el Centro de Servicios Universitarios – CSU. En caso tal de que tenga bloqueados los accesos, la solicitud puede ser realizada por formulario externo del CSU, adjuntando copia del documento de identidad en la solicitud realizada.

8.3.5 Control de Acceso a Sistemas y Aplicaciones

- El control de acceso a sistemas y aplicaciones se rige por la política de control de acceso y el procedimiento Gestión de Usuarios

- Las aplicaciones críticas deberán contar con certificado de seguridad SSL, que permita el acceso bajo protocolo de comunicación seguro y cifrado.

- Las aplicaciones críticas deberán implementar mecanismos de protección contra intentos de ingreso mediante fuerza bruta, tales como *recaptcha* y/o bloqueo de cuentas por un tiempo determinado después de múltiples intentos y/o un segundo factor de autenticación.

- Con el fin de controlar el acceso no autorizado a sistemas y aplicaciones, las contraseñas de cuentas de administración genéricas (root, SYS, SYSADMIN, cuenta de administrador de Windows, entre otras) deberán ser cambiadas manualmente o sustituidas por otro identificador de usuario, cada vez que expire el tiempo de acceso concedido a un funcionario o contratista, o cuando se dé una terminación de empleo, igualmente, se debe activar la política de desconexión automática del usuario después de un tiempo de inactividad .

- La Dirección de Tecnologías de la Información debe cambiar las contraseñas por defecto (y donde sea posible, los usuarios por defecto) de las aplicaciones y servicios utilizados por la universidad.

- El uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones, no está permitido para fines diferentes a las actividades propias de la Dirección de Tecnologías de la Información; y se analizará solicitud bajo ticket al Centro de Servicios Universitarios - CSU.

8.3.6. Uso de altos privilegios y utilitarios de administración

La Dirección de Tecnologías de la Información deberá:

- Garantizar que los recursos y los servicios de red sean operados y administrados en condiciones de seguridad digital, que permitan un monitoreo posterior de la actividad de los usuarios administradores, quienes tienen los privilegios sobre dichas plataformas y servicios.
- Otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información a los funcionarios designados para dichas funciones.
- Establecer cuentas personalizadas con privilegios totales para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.
- Restringir las conexiones remotas a los recursos de la institución, únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.
- Asegurar 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, sean suspendidos o renombrados y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.
- 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.
- Generar y mantener actualizado un listado de las cuentas administrativas de los sistemas de información, infraestructura y servicios.

Los usuarios finales de los recursos tecnológicos, servicios de red y sistemas de información administrados por la Dirección de Tecnologías de la Información, no deberán hacer uso de utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.

Se validarán las políticas de contraseñas establecidas en el presente manual, para determinar que se da el cumplimiento de las mismas en todos los sistemas de información y que estas, son aplicables a los usuarios administradores; así mismo, se verificará que el cambio de contraseña de los usuarios administradores acoja el procedimiento y/o controles definidos para tal fin.

La administración de los recursos que no estén bajo el control técnico de la Dirección de Tecnologías de la Información, se acogerá a todas las políticas definidas en este numeral.

8.4. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

La Dirección de Tecnologías de la Información deberá:

- Determinar los algoritmos criptográficos y protocolos autorizados para su uso en la entidad y configurar los sistemas para permitir únicamente aquellos algoritmos autorizados, teniendo en cuenta la información de los grupos de interés, con el fin de descartar: algoritmos de cifrado débiles tales como DES, 3DES, RC3, RC4; algoritmos de hashing débiles tales como MD5 y SHA1; y protocolos débiles tales como SSLv2 y SSLv3.

- Considerar en su lugar, el uso de algoritmos tales como AES (cifrado simétrico), RSA (cifrado asimétrico) y los protocolos SSL/TLS 1.1, 1.2 o posterior. Adicionalmente, los tamaños de llaves de cifrados recomendados son: 168 o 256 bits (cifrado simétrico) y 2048 bits (cifrado asimétrico) como mínimo.

- Identificar el nivel de protección necesario, teniendo en cuenta el tipo, la fortaleza y la calidad del algoritmo de cifrado requerido; tomando como base la evaluación de los riesgos y el tipo de información que va a ser transferida.

- 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 uso de controles criptográficos únicamente será válido cuando sea el resultado de un análisis de riesgos y su implementación sea autorizada por el propietario de la información correspondiente.

Todos los usuarios harán uso de técnicas de cifrado, autorizadas para proteger la confidencialidad e integridad de la información clasificada como pública reservada y pública clasificada y/o datos personales sensibles.

La Universidad del Quindío tendrá en cuenta la reglamentación y restricciones nacionales que puedan resultar aplicables al uso de técnicas criptográficas.

8.5. POLÍTICA DE GESTIÓN DE LLAVES CRIPTOGRÁFICAS

- La solicitud de activación de llaves criptográficas deberá realizarse formalmente a través del Centro de Servicios Universitarios - CSU, con la respectiva justificación y firma del líder del proceso.

- Las llaves criptográficas deberán ser cambiadas anualmente o cada vez que se sospeche que han perdido su confidencialidad. En el caso de los certificados SSL la periodicidad será de un año.

- La administración de llaves criptográficas y certificados digitales estará a cargo de la Dirección de Tecnologías de la Información; Sin embargo, la administración de tokens bancarios y firmas digitales, estará a cargo de la Dirección Financiera.

- El almacenamiento de los tokens, cuando estos no estén en uso, será: bajo llave, caja fuerte u otros mecanismos definidos por la universidad, para prevenir su acceso no autorizado, pérdida o corrupción del dispositivo.

- Las llaves criptográficas digitales se almacenarán en forma cifrada, cumpliendo con la Política de Control Acceso.

- Los equipos usados para generar, almacenar y archivar las llaves criptográficas, deberán estar protegidos físicamente, con controles adicionales a los implementados para usuarios finales.

- El propietario de la llave criptográfica será el funcionario o contratista al que se le asigne este activo de información y por ningún motivo, puede compartir o delegar su uso, a menos que sea por caso fortuito o fuerza mayor, ante lo cual, se solicitará por escrito con la respectiva justificación al líder del proceso.

8.6. POLÍTICA ESCRITORIO LIMPIO Y PANTALLA LIMPIA

Todos los funcionarios, contratistas y terceros que laboren o tengan relación con la institución, deberán:

- Mantener la información sensible (información pública clasificada e información pública reservada), en sus diferentes medios de soporte, bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horarios no laborales.

- Recoger de manera inmediata la información sensible que se envía a las impresoras. De igual forma, se establece un control tecnológico adicional de solicitud de contraseña de impresión o integración con el directorio activo.

- Bloquear la sesión de su estación de trabajo cuando se retiren del mismo, que solo pueda ser desbloqueado con la contraseña de usuario o huella dactilar. Al finalizar las actividades, se deberán cerrar todas las aplicaciones y dejar los equipos apagados o en hibernación.

- Conservar su espacio de trabajo libre de información pública clasificada y pública reservada, que pueda ser alcanzada, copiada o utilizada por terceros o personal sin autorización.

- Mantener el escritorio lógico libre de información pública clasificada e información pública reservada en todo momento.

- Reducir el daño causado en equipos de cómputo por acciones inadecuadas (consumo de alimentos y/o bebidas, obstrucción de ventilación, ubicación inadecuada, entre otros). En caso de presentarse algún daño, será responsabilidad del custodio.

Los equipos de cómputo exhibirán por defecto el fondo de pantalla institucional configurado mediante las políticas del directorio activo de la institución, por la Dirección de Tecnologías de la Información, el cual no puede ser modificado y deberá permanecer activo.

Todos los equipos de cómputo deberán tener configurado el bloqueo automático de sesión por inactividad de cinco (05) minutos.

Se prohíbe el almacenamiento de información personal en los computadores propiedad de la universidad.

8.7. POLÍTICA DE RESPALDO DE INFORMACIÓN

La Dirección de Tecnologías de la Información deberá:

- Asegurar que la información definida y contenida en servidores, dispositivos de red, estaciones de trabajo, archivos de configuración y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, para evitar la pérdida o corrupción de las copias de respaldo o cualquier adición, supresión, modificación, utilización u ocultación no autorizadas.
- Garantizar que los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente. El sitio externo donde se resguarden las copias de respaldo deberá contar con los controles de seguridad física y medioambiental apropiados.
- 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.
- 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.
- Ejecutar los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para comprobar su integridad y posibilidad de uso en caso de ser necesario.
- Proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos información.
- Identificar la información crítica de los sistemas de información y aplicativos, que debe ser respaldada y almacenada de acuerdo con su nivel de clasificación.

Se definirán 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.

Las copias de respaldo de las estaciones de trabajo de los usuarios finales, deberá ser única y exclusivamente de la información institucional y de acuerdo a los procedimientos establecidos por la Dirección de Tecnologías de la Información.

8.8. POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

Se deberá asegurar la protección de la información que se transfiere o intercambia con otras entidades y los líderes de proceso establecerán los controles necesarios.

La Dirección Jurídica, deberá definir los modelos de Acuerdos de Confidencialidad y de intercambio de información entre la universidad y los proveedores incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Incluyendo:

- La prohibición de divulgar información pública reservada o pública clasificada.
- La destrucción de la información que se compartió con el tercero, una vez cumpla su función.

Se firmarán acuerdos de confidencialidad o de Intercambio de Información con los funcionarios, contratistas y terceros que laboren o tengan relación con la institución y que por diferentes razones requieran conocer o intercambiar información pública reservada o pública clasificada. Estos acuerdos se firmarán antes de permitir el acceso o uso de dicha información.

La Dirección de Tecnologías de la Información dispondrá de 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 establecidos por la Oficina de Gestión Documental.

La Dirección de Tecnologías de la Información 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 de Asuntos Administrativos y Adquisiciones deberá incluir en los contratos suscritos, los Acuerdos de Confidencialidad o Acuerdos de intercambio de información conforme los modelos establecidos por la Dirección Jurídica.

El intercambio de información con entidades externas, se realizará cumpliendo el Manual de Políticas de Seguridad, los Acuerdos de Intercambio de Información y el procedimiento definido para tal fin. Los líderes de proceso verificarán el cumplimiento de este control.

Los funcionarios no deberán revelar o intercambiar información pública reservada o pública clasificada por ningún medio, sin contar con la debida autorización del líder del proceso.

Los funcionarios deberán evitar enviar información pública reservada o pública clasificada 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 líder del proceso.

Se deberá proteger la información involucrada en transacciones en línea, por medio de una comunicación cifrada, para evitar la transmisión incompleta, rutas equivocadas, alteración y divulgación.

La información pública reservada o pública clasificada y/o sensible, deberá permanecer en espacios cerrados bajo llave, cuando sea necesaria su transferencia, deberá ser entregada en mano, embalaje con sellos de seguridad, entre otros mecanismos de seguridad requeridos para proteger la información.

8.9. POLÍTICA DE DESARROLLO SEGURO

La Dirección de Tecnologías de la Información deberá:

- Garantizar que el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad establecidos, las buenas prácticas para desarrollo seguro de aplicativos, metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado.
- Asegurar que todo software desarrollado o adquirido, interna o externamente cuenta con el soporte, actualización y mantenimiento requeridos.
- Implantar los controles necesarios para asegurar las migraciones entre los ambientes de desarrollo, pruebas y producción.

- Disponer con sistemas de control de versiones para administrar los cambios de los sistemas de información y aprobarlos de acuerdo con el procedimiento establecido para tal fin.
- Asegurar que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento, donde se especificarán las condiciones de uso del software y los derechos de propiedad intelectual.
- 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.
- Asegurar que las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones recomendadas (estables) y que estén ejecutando la última versión aprobada del sistema.
- 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.
- Aprobar las migraciones entre los ambientes de desarrollo y pruebas de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.
- Garantizar que la información entregada a los desarrolladores para sus pruebas sea anonimizada y no revele información confidencial de los ambientes de producción.
- Eliminar la información de los ambientes de pruebas innecesarios y una vez estos hayan concluido.

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

Para la adquisición, desarrollo o actualización de módulos de cualquier sistema de información, se deberá contar con la autorización de la Dirección de Tecnologías de la Información, de acuerdo al Procedimiento de Gestión de Cambios.

Los desarrolladores de los sistemas de información y proveedores de software deberán:

- 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.
- Construir los aplicativos 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- Remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Prevenir la revelación de la estructura de directorios de los sistemas de información construidos como su código fuente bajo técnicas de ofuscación.

- Remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- 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.
- Garantizar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- 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 sólo tengan privilegios de lectura.
- Proteger el código fuente de los aplicativos desarrollados o adquiridos, evitando su descarga y modificación por los usuarios.
- Asegurar que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo del usuario.

8.10. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON PROVEEDORES

Se establecerán mecanismos de control en las relaciones con proveedores, con el objetivo de asegurar que la información a la que tengan acceso o servicios, sean suministrados por los mismos, cumpla con las políticas, normas y procedimientos de seguridad de la información.

Las dependencias 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.

La Dirección de Tecnologías de la Información con apoyo de la Dirección Jurídica deberán generar modelos de Acuerdos de Niveles de Servicio – ANS, Acuerdos de Confidencialidad e Intercambio de Información y requisitos de Seguridad de la Información, con los que deben cumplir proveedores de servicios. Estos serán divulgados a todas las áreas que adquieran o supervisen recursos y/o servicios

tecnológicos. Los acuerdos contendrán una responsabilidad tanto civil, como penal para el proveedor contratado.

Todo sistema externo utilizado por los proveedores para acceder a la información de la institución, deberá ser autorizado por los líderes de proceso como responsables funcionales de cada una de las dependencias.

La Dirección de Tecnologías de la Información en conjunto con el líder del proceso, deberá 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.

La Dirección de Tecnologías de la Información deberá 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 deberán evaluar y aprobar los accesos a la información de la Universidad requeridos por terceras partes, con el apoyo técnico de la Dirección de Tecnologías de la Información.

Las dependencias responsables de la realización de contratos o convenios y los supervisores de éstos, deberán:

- Identificar y monitorear los riesgos de seguridad de la información relacionados con estos, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología.
- Establecer planes de mitigación de riesgos de seguridad de la información, relacionados con el acceso a información de la Universidad.
- Divulgar y asegurar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información a dichos proveedores.
- Monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio - ANS, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información.
- 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 a los sistemas de información y aplicativos de la universidad, deberá ser monitoreada por la Dirección de Tecnologías de la Información. En el caso que se identifiquen riesgos de seguridad sobre la información, inmediatamente será revocada su autorización.

8.11. POLÍTICA DE NO REPUDIO

La Universidad del Quindío, con el fin de garantizar el no repudio frente a las comunicaciones que se emitan y que sean consideradas críticas o de alto valor legal o reputacional para los procesos, establecerá los siguientes controles:

- Se deberán implementar mecanismos en los que no exista la posibilidad de desafiar la validez de una acción por parte de quien la generó, en especial para los procesos que se consideren críticos para la corporación.
- Se deberá contar un tercero en quien todos confíen para que permita avalar la integridad y el origen de los datos, frente a algunos mecanismos a implementar, en caso de ser necesario.
- Se deberán implementar registros que permitan evidenciar la trazabilidad de las acciones de creación, origen, recepción, entrega de información y otros, lo cual sirve para evidencia y garantizar el no repudio, en una comunicación.
- Los anteriores registros se deberán proteger contra pérdida o modificación de tal manera que se garantice su disponibilidad e integridad.
- Se deberán realizar auditorías continuas a los mecanismos de control y a los procesos, para tener evidencia cuando las partes implicadas posiblemente nieguen haber realizado una acción específica.
- Los servicios de intercambio electrónico de información deben incorporar mecanismos que sean garantía de no repudio.
- Cuando la Dirección de TI, evidencie algún tipo de evento o incidente relacionado a la ejecución de acciones que eviten dejar trazabilidad de lo realizado, deben informarlo de manera oportuna al administrador o propietario del activo de información para que se tomen las medidas pertinentes.

8.11.1 Política de firmas electrónicas o digitales

La Universidad del Quindío en cumplimiento de la normatividad legal vigente y dentro de su proceso de transformación digital, contribuyendo al impulso del comercio electrónico, la promoción de la digitalización y automatización masiva de trámites, a través de la implementación e integración de los Servicios Ciudadanos Digitales, implementará el uso de firmas electrónicas o firmas digitales bajo las siguientes premisas:

- La Alta Dirección Institucional y la Dirección de Tecnologías de la Información, establecerán el grado de confianza requerido (Autenticación: Muy alto, alto, medio y bajo) para los procesos y servicios donde se implementará el uso de las firmas electrónicas o digitales, en concordancia con lo señalado en las leyes, decretos reglamentarios y lineamientos dados por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. Así como la clasificación de la información de la institución y el tipo de documento a remitir.

  En virtud a lo anterior, la universidad deberá documentar qué procesos, servicios, tipos de documentos y personas estarán autorizadas para el uso de las firmas electrónicas o digitales; así como el nivel de confianza requerido y el tipo de mecanismo a utilizar.

- Las firmas electrónicas o digitales implementadas en la universidad, deberán garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

- Al realizarse acuerdos con terceros para el uso de la firma electrónica, se deberá suscribir un documento de acuerdo, en el cual definirán las reglas, parámetros de validez y autenticación que regirán las comunicaciones electrónicas confiables entre el tercero y la universidad.

- Independiente de la herramienta o mecanismo autorizado por la Dirección de Tecnologías de la Información, para la firma de documentos electrónicos, éstos deberán permitir:

  - Firmar los documentos electrónicos con los parámetros establecidos por la universidad.

- Al incluir diferentes firmas, el contenido del documento debe permanecer inalterable.
- Enviar los documentos a la dirección de correo electrónico de terceros, garantizando la integridad de los datos y el no repudio de la información.

- Las firmas electrónicas o digitales que se implementen en virtud de la presente política, tendrán la misma validez, efectos y eficacia jurídica o legal que la firma autógrafa.
- Se deberá solicitar revocación de la firma digital al evidenciarse incidentes de seguridad de la información como corrupción, pérdida de confidencialidad, suplantación, entre otros; en cumplimiento de la política de uso de controles criptográficos y gestión de llaves criptográficas.
- Será responsabilidad del funcionario o contratista cumplir con las políticas de seguridad de la información y las medidas de seguridad y protección del mecanismo, cuando la firma digital haya sido expedida por un ente certificador.
- Al utilizar el uso de firmas digitales con un nivel de confianza "Muy alto" o "alto", se deberá determinar:
  - Los niveles de inalterabilidad, integridad, seguridad, autenticidad, perdurabilidad y confiabilidad.
  - El uso de estampas cronológicas, que aseguren la exactitud, completitud o integridad, indicando que el documento no ha sufrido modificación desde el momento de su firma.
  - La emisión de una firma digital por una entidad externa o tercero de confianza que garantice la asignación a la persona que corresponde, utilizando mecanismos de verificación de identidad.
  - Métodos o algoritmos que garanticen la validez de la firma a largo plazo o su conservación en el tiempo, cuando esta haya expirado.
  - Verificación de la autenticidad de la firma digital, por medio de un aplicativo.

- Las firmas digitales utilizadas deberán garantizar prueba de identidad, Integridad del documento, estampado cronológico y conformidad de las dos partes

- Está prohibido el uso de las firmas electrónicas o digitales para fines contrarios a la legislación vigente o contrarios a las disposiciones, obligaciones y requisitos establecidos por la Universidad del Quindío.

- Los documentos firmados electrónica o digitalmente, tendrán los mismos atributos de registro, custodia, archivo y conservación, establecidos por el Sistema de Gestión Documental de la universidad y directrices del Archivo General de la Nación.

8.12. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Se definen las siguientes directrices:

- Promoverá entre la comunidad usuaria de recursos informáticos y sistemas de información el reporte de los incidentes relacionados con la información y sus medios de procesamiento.

- Se deberán habilitar sistemas de monitoreo que permitan: detectar incumplimientos de la Política de Control de Acceso, registrar eventos que proporcionen evidencia en caso de ocurrir incidentes de seguridad y verificar el uso adecuado de los recursos informáticos y los sistemas de información.

- Sin excepción, los funcionarios y contratistas de la Universidad, deberán informar acerca de cualquier evento o problema de seguridad de la información detectado, a la mayor brevedad, mediante el Centro de Servicios Universitarios – CSU y de acuerdo a lo estipulado en el Procedimiento de Gestión de Incidentes de Seguridad de la Información.

- Los incidentes de seguridad de la información que estén relacionados con requerimientos legales o regulatorios, serán reportados a autoridades competentes por el personal autorizado de la Universidad.

- Se asignarán responsables y responsabilidades para el tratamiento de los incidentes de seguridad de la información en la Universidad del Quindío, a fin de dar tratamiento y/o solucionar de la manera eficaz de acuerdo con la criticidad de los mismos; tomando las medidas necesarias, haciendo un análisis de causas y documentando todas las fases desde la ocurrencia del mismo hasta las lecciones aprendidas, a fin de prevenir su re-ocurrencia, mitigar el impacto o mejorar los tiempos de recuperación en caso de que se vuelva a presentar.
- Se llevará un registro de todos los incidentes de seguridad de la información con su respectiva evidencia de solución, de tal forma, que permita facilitar su consulta, revisión y análisis, para implementar estrategias, gestionar los riesgos y contribuir a la mejora continua de los procedimientos.

8.13. POLÍTICA DE GESTIÓN DE ACTIVOS

Será responsabilidad de las direcciones, dependencias/áreas asegurar el cumplimiento de los controles de seguridad establecidos sobre sus activos de información, y monitorear el uso adecuado de los mismos, de acuerdo a las directrices aquí contenidas.

La Dirección de Tecnologías de la Información deberá:

- Definir las reglas para el uso adecuado de los activos de la institución.
- Asegurar la apropiada administración de la información almacenada en los servidores, y por lo tanto la adecuada operación de estos.
- Autorizar la instalación, cambio o eliminación de componentes de los aplicativos de universidad, conforme a lo establecido en el Procedimiento de Gestión de Cambios.
- 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.

- Elaborar los requerimientos técnicos obligatorios, incluyendo necesidades de hardware y software para incorporar a los procesos de compra y contratación, relacionados con infraestructura tecnológica y/o comunicación.

El personal asignado la Dirección de Tecnologías de la Información serán los únicos autorizados para realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, conexiones de red, gestión de usuarios locales de la máquina, instalación de software, traslado de equipos y la aplicación de las políticas contenidas en el presente manual y los procedimientos establecidos para tal fin.

En caso que algún funcionario, contratista y terceros que laboren o tengan relación con la institución, requiera para el desempeño de sus funciones realizar instalación de software y/o cambios en la configuración del equipo, se deberá realizar la solicitud mediante el Centro de Servicios Universitarios - CSU, indicando los motivos de estos cambios.

La Dirección de Tecnologías de la Información, recomienda utilizar alguna de las siguientes alternativas en caso de requerir algún software, que no cuente con licencia adquirida para la universidad, a fin de 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 Proveedor del correo electrónico.
- El instalador debe ser descargado de la página oficial del fabricante.
- Como sistema operativo usar cualquier versión libre de Linux.

Para otros casos, se deberá realizar el proceso formal de adquisición del software comercial debidamente licenciado conforme los procedimientos establecidos para tal fin.

Los funcionarios, contratistas y terceros que laboren o tengan relación con la institución deberán:

- Bloquear sus equipos al momento de retirarse de su puesto de trabajo.
- Reportar a la Dirección de Tecnologías de la Información, todo problema mecánico, eléctrico o electrónico sobre los equipos de cómputo propiedad de la universidad.
- Apagar o dejar en estado de hibernación las estaciones de trabajo, al finalizar las actividades.
- Conectar los equipos de cómputo (CPU y monitor), servidores, teléfonos IP y equipos de comunicaciones, a los puntos de corriente eléctrica identificados como regulados.
- Utilizar de forma ética y en cumplimiento de las Leyes y Reglamentos vigentes, los recursos tecnológicos de la universidad, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la institución.
- Utilizar el sistema de correo electrónico solo para propósitos institucionales.
- Evitar el acceso a los sistemas de información institucionales desde redes inalámbricas públicas, este tipo de servicios son altamente inseguros ante ataques de espionaje o robo de información.
- Eliminar o ignorar correos que provengan de destinatarios desconocidos o que tengan asuntos o archivos adjuntos sospechosos.

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

La información contenida en las herramientas y equipos asignados por la Universidad para el cumplimiento de las responsabilidades académicas,

administrativas y de investigación son propiedad de la Universidad y podrán ser revisadas en el momento en que la institución lo determine.

8.13.1. Asignación de activos de información tipo hardware

La Dirección de Tecnologías de la Información realizará la entrega oficial del activo de información tipo hardware a los funcionarios, contratista y terceros que laboren o tengan relación con la institución, de acuerdo con los requerimientos técnicos necesarios incluyendo necesidades de hardware y software que se determinen para el usuario y el procedimiento de Procedimiento inventarios - activos fijos.

El área de activos fijos identifica los activos tipo hardware de acuerdo con los procedimientos utilizados en la Universidad para el etiquetado de estos.

8.13.2. Salida y devolución de activos de información tipo hardware

Si se requiere para el desempeño de sus funciones, que el funcionario o contratista se desplace con el activo de información fuera del campus Universitario, se deberá dejar el registro en la herramienta definida por el área de activos fijos, indicando su ubicación final.

Para el caso de la devolución de los equipos, se deberá seguir los procedimientos, controles o lineamientos definidos por el área de activos fijos.

8.13.3. Entrega y disposición segura de los activos de información

Cuando haya cambio de rol, traslado administrativo, ascenso o retiro del funcionario, el líder del proceso, como propietario de los activos de información, deberá solicitar al funcionario la entrega de los activos de información y se deberá seguir los procedimientos, políticas y controles de seguridad de la información, establecidos en el marco del SGSPI.

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

8.13.4. Uso adecuado de documentos electrónicos

Los productores documentales responsables del manejo y custodia de los archivos físicos y electrónicos institucionales, seguirán los lineamientos establecidos en el "Reglamento interno de archivo" y definidos por el Oficina de Gestión Documental, para la organización de documentos.

Se deberán documentar e implementar procedimientos de seguridad y control durante todas las etapas del ciclo de vida del documento para evitar la pérdida o corrupción de los documentos de archivo o cualquier adición, supresión, modificación, utilización u ocultación no autorizadas, así como la protección de los medios de almacenamiento y su infraestructura tecnológica.

8.13.5. Uso adecuado de correo electrónico

La política busca promover una comunicación más adecuada y efectiva, además de proporcionar a los usuarios una guía que describa sus responsabilidades, relacionadas con la confidencialidad, privacidad, uso racional y correcto de este servicio. Los lineamientos establecidos, aplican a todos los usuarios que conforman la comunidad Universitaria (estudiantes, docentes, administrativos y trabajadores oficiales) y terceros que laboren o tengan relación con la institución, que usan los servicios de correo electrónico en la institución para la ejecución de sus actividades.

El correo electrónico institucional hace parte de los canales oficiales de comunicación y permite el intercambio de información oficial entre las dependencias de la institución, de esta con otras entidades públicas y organismos de control, y de la institución con los usuarios o ciudadanía en general.

Las personas que requieran actuar en nombre de la institución, mediante una cuenta de correo institucional, como contratistas en sus diferentes modalidades podrán contar con el servicio de correo electrónico; donde el líder del área indica que su trabajo o rol así lo requiere.

Una vez finalizada su vinculación contractual con la institución los funcionarios, docentes y contratistas deberán realizar la entrega de su correo institucional al superior inmediato.

El cumplimiento de estos lineamientos plasmados complementará las políticas de seguridad, privacidad y uso del correo establecidas por el Proveedor del correo electrónico.

Está prohibido utilizar las cuentas de correo institucional para propósitos personales, o para guardar o archivos de respaldo de información personal. La Universidad no se hace responsable de la información de este tipo que los usuarios almacenen o gestionen en las cuentas creadas por la institución.

El correo electrónico es parte de los registros de la entidad y es un activo de información que se facilita para el desarrollo de las funciones.

Los mensajes de correo electrónico tienen igual carácter probatorio que los documentos físicos (Ley 527 de 1999), por lo que se deberá tener especial cuidado con la información que se almacene, transmita o recepcione en las cuentas institucionales.

La institución hará:

- Monitoreo y seguimiento al servicio de correo electrónico para brindar un mejor servicio o por solicitudes de la autoridad competente, en caso de identificar incidentes o eventos de seguridad de la información relacionados con este activo o donde actúe como prueba dentro de un proceso.

- Trasladar a la autoridad competente cualquier conducta irregular y que se considere un delito informático según la Ley 1273 de 2009.

- Verificar el contenido de estas cuentas en el momento que se considere necesario, así como la reasignación a través de la modificación de la contraseña.

Los correos electrónicos son uno de los mecanismos utilizados para disminuir el uso de papel. Por tanto, los únicos que podrán imprimirse, serán los que hacen parte de expedientes o procesos judiciales.

Las solicitudes relacionadas con la gestión del correo electrónico institucional, deberán remitirse a través del Centro de Servicios Universitarios - CSU.

Las solicitudes, entrega, desactivación y creación de correo, siguen las directrices del procedimiento *"Administración cuentas de correo institucional personal administrativo, docente y estudiantes matriculados"*.

8.13.5.1 Tipos de cuentas de cuentas de correo en la Universidad del Quindío

La institución cuenta con un servicio de correo electrónico con un proveedor externo bajo una categoría *"Education Standard"*. A través del dominio @uniquindio.edu.co se asignan cuatro tipos de cuentas: laborales personales, por dependencia, temporales; para estudiantes y graduados el dominio asignado @uqvirtual.edu.co.

La Dirección de Tecnologías de la Información deberá identificar el tipo de cuenta a crear, el propósito, la vigencia de las mismas y las observaciones que considere pertinentes, de acuerdo a la solicitud recibida, a fin de estandarizar y controlar las categorías, privilegios y permisos para transmisión de la información institucional.

Se tendrán cuentas y dependencias específicas autorizadas para el envío de correos masivos desde y fuera de los dominios, antes mencionados de la universidad, las cuales serán consideradas por la rectoría y validadas por la Dirección de Tecnologías de la Información.

Se deberá incluir el siguiente mensaje en pie de página de los correos referidos anteriormente, para la comunicación del ciudadano con la entidad:

> *"No responda este email, es un mensaje informativo y no se encuentra habilitado para recibir mensajes. Cualquier inquietud, duda o aclaración, favor enviar su requerimiento mediante un ticket al CSU o al correo electrónico de contactenos@uniquindio.edu.co"*

La Oficina de Gestión Documental definirá los lineamientos para la gestión de correos electrónicos institucionales, con base en directrices establecidas por el Archivo General de la Nación y la Ley de Transparencia y Acceso a la Información Pública.

8.13.5.2 Responsabilidades específicas de los usuarios

Con la gestión del buzón de correo

Los usuarios serán los responsables de todas las actividades realizadas a través de la cuenta de correo institucional asignado; serán los encargados de hacer uso adecuado, prudente y pertinente del correo electrónico, para el cumplimiento de sus funciones.

Deberán gestionar adecuadamente su buzón de correo electrónico, con el fin de proyectar el almacenamiento asignado; de acuerdo a las directrices emitidas por la Dirección de Tecnologías de la Información.

El correo electrónico institucional podrá registrarse en Blogs, Redes Sociales, siempre y cuando sean concernientes a temas asignados por la institución dentro de sus funciones y autorizado por el Líder de departamento, dependencia o área.

Con la seguridad de la cuenta de correo

La cuenta de correo de la Universidad es personal e intransferible, por tanto, será responsabilidad del usuario salvaguardar la clave y no revelarla bajo ninguna circunstancia.

Deberán cambiar la contraseña periódicamente y ante cualquier sospecha de afectación de la seguridad de la cuenta, según los lineamientos descritos en la Política de Control de Acceso.

Deberán cerrar la sesión la cuenta de correo, en caso de ausentarse del puesto de trabajo durante la jornada laboral, de acuerdo a los lineamientos definidos en la Política de Escritorio Limpio y Pantalla Limpia.

Los archivos adjuntos de correos electrónicos con remitentes desconocidos o de contenido sospechoso, no se deberán descargar, ni acceder a los enlaces o URLs incluidos en los mensajes. De igual forma, no responder a remitentes desconocidos.

En caso de recibir un e-mail de este tipo, deberán:

- Hacer caso omiso a los links que vengan agregados en el cuerpo del correo de cuentas externas.

- Marcar el correo sospechoso como Spam o denunciar suplantación de identidad, si es el caso.

- Digitar directamente la página que deseen consultar en el navegador del equipo.

- Eliminar o ignorar correos de procedencia desconocida, correo basura, SPAM, correo no deseado o sospechoso, con el fin de evitar posibles infecciones por código malicioso o virus.

- Reportar a través del CSU, como un incidente de seguridad de la información, este tipo de correos y cualquier fallo que se evidencie en su cuenta de correo, incluyendo su uso no autorizado, pérdida o corrupción de la contraseña, entre otros.

Los funcionarios, contratista y terceros que tengan acceso a la información clasificada como pública reservada y pública clasificada, deberán cumplir con los controles de seguridad de la información, establecidos por el líder del proceso y evitar la remisión de la misma a menos que esté autorizado para hacerlo. En caso que deba enviarse se deberá hacer uso de controles criptográficos y verificar la autenticidad del destinatario, en cumplimiento de las políticas y procedimientos diseñados para tal fin.

En caso que deba enviarse: se etiquetará en el asunto conforme las directrices emanadas por la Oficina de Gestión Documental.

Restricciones del uso del correo institucional

Los funcionarios, contratistas y terceros que tengan asignado un correo institucional tendrán prohibido:

- Enviar de correos con mensajes que contravengan normas legales, la moral, el orden público, la intimidad o el buen nombre de las personas, que contengan contenido irrespetuoso, ofensivo, amenazante, difamatorio, racista, religioso, discriminatorio, de acoso o intimidación; tratamiento de datos relativos a la salud, vida sexual o la orientación sexual de una persona, así como imágenes o videos con contenidos ilegales, ofensivo, extorsivo, indecente o con material sexual.

- Violar los derechos de cualquier persona o institución, incluso aquellos que se encuentren protegidos por derechos de autor, propiedad industrial, patentes o cualquier otra forma de propiedad intelectual.

- Usar el correo electrónico institucional para el envío de propaganda comercial, político, religioso, negocios personales, avisos publicitarios o cualquier información ajena a las labores propias del cargo que de una u otra manera se comprometa su credibilidad e institucionalidad de la Universidad.

- Compartir contactos o listas de distribución de la Universidad con personal externo, con el objetivo de propiciar el envío de propagandas, ofertas, negocios personales, avisos publicitarios, o información de otro tipo, ajena a las labores propias del cargo.

- Emplear cuentas de correo para el envío de información personal.

- Copiar ilegalmente o reenviar mensajes sin tener la autorización del remitente original para hacerlo.

- Usar seudónimos y enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.

- Ocultar o suplantar la identidad del emisor de correo.

- Intentar modificar los parámetros de la seguridad de los sistemas informáticos de la Institución.

- Enviar archivos que contengan algún tipo de amenaza tecnológica o que atenten contra la infraestructura o información de los sistemas informáticos de la institución y el público en general.

Causas para inactivar cuentas de correo electrónico

Se inactivarán las cuentas de correo electrónico, cuando se presenten las siguientes situaciones:

- Los funcionarios, contratistas y terceros que tengan asignado un correo institucional y pierdan la vinculación con la universidad del Quindío en un tiempo de sesenta (60) días calendario.

- Se presente uso inadecuado del servicio o se incurra en el incumplimiento de la presente política, la Universidad se reserva el derecho de deshabilitar el servicio de correo institucional.

- Por solicitud de las autoridades competentes ya sean internas o externas.

- Se presente deserción de los estudiantes en cualquier semestre. Dichas cuentas, se desactivarán en un tiempo mínimo de 60 días.

- Por Incumplimiento de las políticas del proveedor del correo electrónico.

8.14. POLÍTICA DE SENSIBILIZACIÓN Y CAPACITACIÓN EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8.14.1 Sensibilización y comunicación

La universidad, definirá un "***Plan de Comunicación en Seguridad y Privacidad de la Información"*** a través de la Dirección de Comunicaciones Estratégicas, donde se planificará anualmente la manera en que se comunicarán las recomendaciones o tips de seguridad de la información por diferentes medios a todos los funcionarios y contratistas, con el fin de socializar las políticas institucionales de seguridad de la información o las buenas prácticas en seguridad que desean socializar para aumentar las capacidades de las dependencias y generar la cultura de seguridad requerida por la institución. La creación de los contenidos, se hará con el apoyo de la Dirección de Tecnologías de la Información y el Oficial o Responsable de SGSPI.

8.14.2 Capacitación

La Universidad del Quindío a través del Proceso de Gestión Humana, incluirá en sus inducciones, reinducciones y capacitaciones las temáticas de seguridad de la información, para que cualquier funcionario y/o contratista que se vincule a la institución, tenga pleno conocimiento de las políticas de seguridad de la información. La Dirección de Tecnologías de la Información y el Oficial o Responsable de SGSPI apoyarán las inducciones, reinducciones y el diseño de planes de capacitación en estos temas.

9. CONTROLES ADICIONALES

La Universidad cuenta con controles y políticas adicionales que contribuyen a la seguridad de la información, entre las cuales están:

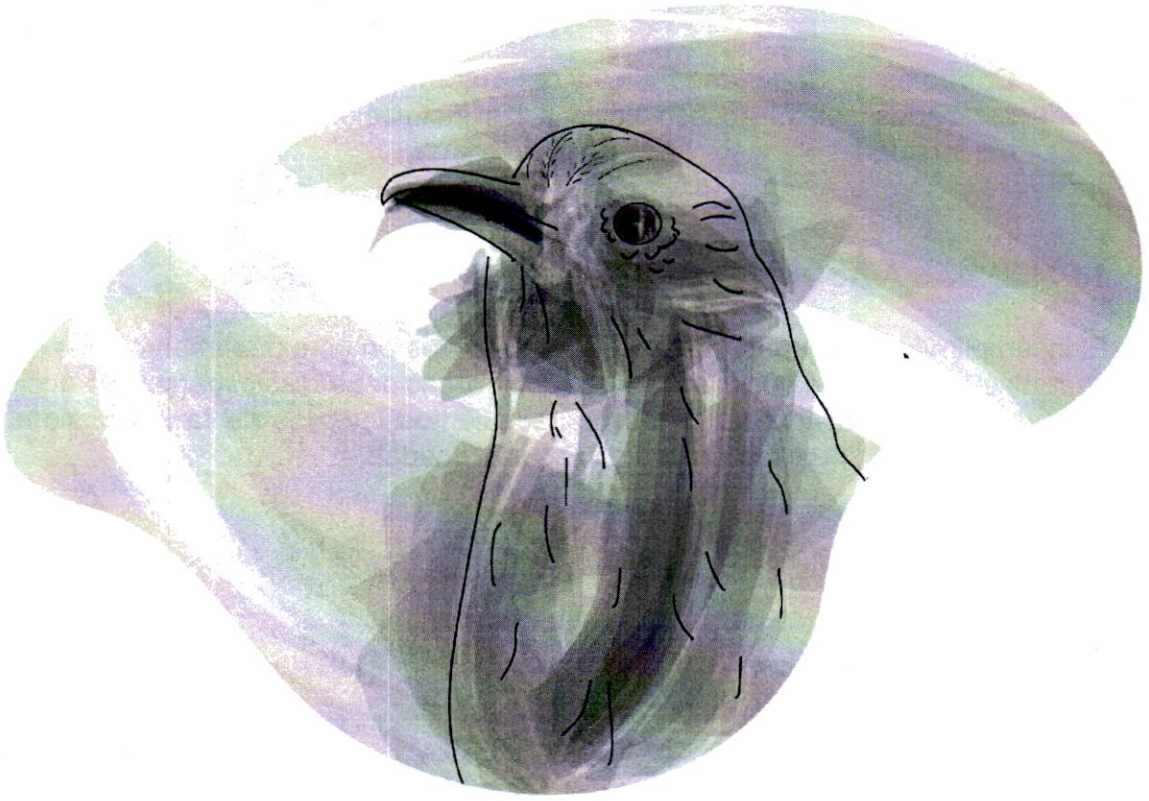
- La Política de Propiedad Intelectual – Acuerdo No. 075 del 14 de marzo de 2019
- La Política de Tratamiento de Datos Personales – Resolución No. 4156 del 07 de marzo de 2018
- Política del Talento Humano – Resolución No. 3955 del 22 de diciembre de 2017
- Política de Gestión Documental – Acuerdo No. 07 del 22 de diciembre de 2009
- Política de Administración de Riesgos – Resolución No. 7322 del 27 de julio de 2020

- Controles de Seguridad Física y del Entorno, con el fin de mitigar los riesgos asociados con el acceso físico a las instalaciones y áreas seguras de la universidad.

10. MEDIDAS A ADOPTAR EN CASO DE INCUMPLIMIENTO

El incumplimiento de una o más políticas descritas en este documento y los demás controles aquí contenidos, pueden conducir a acciones disciplinarias y/o acciones de índole legal, de acuerdo a los procedimientos internos de la Universidad del Quindío y demás lineamientos aplicables a la entidad.

Elaboró:	Revisó	Aprobó
Diana Amortegui Barbosa Consultora Password Consulting Services SAS Oficial de Seguridad de la Información	Marietta Velásquez Rodríguez Profesional Especializado Dirección de Planeación Institucional Harby Gil Arteaga Profesional Especializado Dirección de TI Julián Fernando Restrepo Granada Técnico Operativo Dirección de TI	Consejo Superior Acuerdo No. del 22/02/2024
01/03/2022	07/04/2022	22/02/2024



DIRECCIÓN DE PLANEACIÓN INSTITUCIONAL

Tel: (57) 6 735 9300 Ext 326
Carrera 15 Calle 12 Norte
Armenia, Quindío – Colombia
sgsi@uniquindio.edu.co

UNIQUINDÍO, en conexión territorial

Carrera 15 Calle 12 Norte Tel: (606) 7 35 93 00 Armenia - Quindío - Colombia

www.uniquindio.edu.co