

INFORME DE AUDITORÍA INTERNA PROCESO DE GESTIÓN TIC

OFICINA ASESORA DE CONTROL INTERNO
“Gestión para resultados con Valores”
Mayo de 2021

PERTINENTE CREATIVA INTEGRADORA

 @uniquindio  universidaddelquindio  uniquindioconectada

www.uniquindio.edu.co

1. INTRODUCCIÓN

La Ley 87 de 1993 “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones”, señala en su artículo 12, frente a las funciones de los auditores internos:

“(…) d) Verificar que los controles asociados con todas y cada una de las actividades de la organización estén adecuadamente definidos, sean apropiados y se mejoren permanentemente, de acuerdo con la evolución de la entidad; (…)”

En el mismo sentido, el Consejo Superior de la Universidad del Quindío en el Acuerdo 040 del 27 de mayo de 1994, “Por el cual se establece el Sistema de Control Interno en la Universidad del Quindío y se reestructura la Oficina de Auditoría interna”, menciona en su artículo 3°, que dentro de los objetivos del Sistema de Control Interno se encuentran los siguientes:

“a. Proteger los recursos de la Organización, buscando su adecuada administración ante posibles riesgos que la afecten.

b. Garantizar la eficacia, la eficiencia y economía en todas las operaciones, promoviendo y facilitando la correcta ejecución de las funciones y actividades definidas para el logro de la misión institucional. (…)”

“(…) d. Garantizar la correcta evaluación y seguimiento de la gestión organizacional. (…)

“(…) f. Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos. (…)”

Asimismo, la Resolución de Rectoría N° 4275 del 11 de abril del 2018 “por medio de la cual se ajusta el manual de funciones y de competencias laborales para los cargos de los niveles directivos, asesor, profesional, técnico y asistencial establecidos en la planta global de personal administrativo de la Universidad del Quindío”, señala que el Jefe de Control Interno, entre otras funciones tiene la de **“prestar asesoría a la alta dirección y responsables de áreas o grupos de trabajo en la institución, a través de mejores prácticas para el logro de los objetivos institucionales”**.

Es así como el comité de coordinación de Control Interno de la Universidad del Quindío, en sesión del 23 de febrero de 2021, aprobó el Plan de Auditoría para la vigencia 2021 y en el cual quedo seleccionado el proceso de Gestión TIC.

2. OBJETIVO

Evaluar la Gestión y la efectividad de los controles aplicados en el proceso de Gestión TIC, con el propósito de identificar oportunidades de mejora que contribuyan al cumplimiento de los objetivos de la Universidad del Quindío.

3. ALCANCE

El periodo a auditar se encuentra comprendido entre el 01 de enero y el 30 de diciembre de 2020 y el primer trimestre de la vigencia 2021, y se hará énfasis en los siguientes aspectos:

- Seguimiento al Plan Estratégico de Tecnologías de la Información (PETI).
- Evaluación de la seguridad y privacidad de la información.
- Evaluación al Sistema de información (SEVEN ERP).
- Gestión de riesgos.
- Seguimiento al Plan Anual de Gestión.
- Gestión documental.

4. CRITERIOS

- Decreto 1008 del 2018: Implementación de la política de Gobierno digital.
- Resolución 6962 del 24 de enero 2020: Adopción PETI 2019 - 2022 y política de Gobierno TI.
- Resolución 1519 del 24 de agosto del 2020: Por el cual se definen los estándares y directrices para publicar la información señalada en la ley 1772 del 2014.
- ACS 020 del 2015: Estructura organizacional de la Universidad del Quindío.
- Resolución 4275 del 2018: Manual de funciones y competencias laborales de la Universidad del Quindío.
- Norma ISO 27000 del 2013 Sistema de Gestión de Seguridad de la Información.

5. METODOLOGÍA

Aplicación del procedimiento de auditoría interna SE.CI-01 y utilización de la guía de Auditoría Interna para entidades públicas versión 4, emitida por el Departamento Administrativo de la Función Pública.

- Planeación del Seguimiento.
- Solicitud de información.
- Análisis de información.
- Observación directa.
- Elaboración de informe con conclusiones y recomendaciones.
- Reunión de cierre del seguimiento.
- Entrega informe final.
- Plan de mejoramiento.

6. RESULTADOS Y ANÁLISIS DE LA AUDITORIA INTERNA

6.1 Información de contexto

De acuerdo con la Resolución de Rectoría 6962 del 24 de enero del 2020, “Por medio de la cual se adoptan el Plan Estratégico Tecnología de la Información - PETI (2019-2022) y las Políticas de Gobierno de Tecnologías de la Información (TI) de la Universidad del Quindío”, el PETI es:

“(…) el documento mediante el cual se define la estrategia bajo la cual se espera que las tecnologías de la información (TI) se integran con la misión, visión y objetivos institucionales”.

Es así como, entre la información contenida en dicho documento se encuentra la estructura organizacional del Área de Sistemas y Nuevas tecnologías, la cual se encuentra al frente del Proceso de Gestión TIC y se muestra en la imagen 1.

Imagen 1. Estructura organizacional del área de sistemas y nuevas tecnologías



Fuente: Plan estratégico tecnología de información (PETI) – 2019 - 2022

Entre las funciones de la Oficina de Sistemas y nuevas tecnologías se encuentra la de “Apoyar los demás procesos y unidades organizacionales en el desarrollo y óptimo funcionamiento de los sistemas de información y comunicación”¹, así mismo, para el desarrollo de la Auditoría, se tuvo en cuenta el Manual de Funciones, el cual fue ajustado mediante Resolución de Rectoría 4275 de 2018 donde se establece los siguientes cargos para el área de Gestión TIC:

Tabla No 1. Cargos de Sistemas y Nuevas Tecnologías

NIVEL	DENOMINACION DEL EMPLEO	REQUISITOS
Profesional	Profesional Especializado Grado 18	Título Profesional universitario en las áreas de Ingeniería y afines, específicamente Ingeniería de sistemas o cómputo, Ingeniería de Software o Ingeniería de redes, Ingeniería Electrónica, título de posgrado en la modalidad de especialización en áreas afines a las funciones del cargo (Decreto 1785 de 2014)
Profesional	Profesional Especializado Grado 13	Título Profesional Ingeniería de sistemas, Ingeniería de Software o Ingeniería telemática, Ingeniería Electrónica, título de posgrado en la modalidad de especialización.
Técnico	Técnico Operativo Grado 18(2)	Título de formación tecnológica con especialización, o terminación y aprobación del pensum académico de educación superior en la modalidad de formación profesional (Decreto 1785 del 18 de septiembre de 2014)
Técnico	Técnico Operativo Grado 16	Título de formación tecnológica o aprobación de tres (3) años de educación superior en la modalidad de formación profesional o universitaria (Decreto 1785 del 18 de septiembre de 2014)
Asistencial	Auxiliar Administrativo Grado 21	Aprobación de un (1) año de educación superior de pregrado.

Fuente: Resolución de Rectoría 4275 de 2018

En la revisión realizada por el equipo auditor se encontró que los cargos del área se encuentran operando, sin embargo, se evidencia la necesidad de una actualización del Manual de Funciones, puesto que en el cargo de técnico Operativo Grado 18, hay asignados dos personas, pero en el momento solo está ocupado un cargo en el área TIC, adicionalmente, hay funciones que se encuentran desactualizadas frente a los retos actuales de la oficina en relación con el cumplimiento del Plan Estratégico de Tecnologías de la Información.

¹ Acuerdo N°20 Consejo Superior diciembre 18 año 2015.

6.2 Fortalezas del Macroproceso TIC

- Disposición del Director y Jefe del área al recibir el proceso auditor, el cual busca agregar valor y minimizar riesgos asociados a la gestión.
- Amplia experiencia y formación del Talento humano en las actividades relacionadas con las tecnologías de la información y comunicación.
- Se evidencia división de funciones en todos los procesos procurando el cumplimiento de las obligaciones respectivas.
- Se evidencia interés, compromiso y disposición de la Alta Dirección en la ejecución del PETI, teniendo en cuenta la asignación de recursos que ha permitido la ejecución de la mayor parte de proyectos planeados.
- Se refleja una robusta y renovada infraestructura tecnológica de la Universidad del Quindío, la cual ayuda a mejorar los servicios de toda la comunidad institucional, soportada con licenciamientos de sistemas de información, además, de fortalecimiento y modernización de las plataformas tecnológicas para facilitar la virtualización.

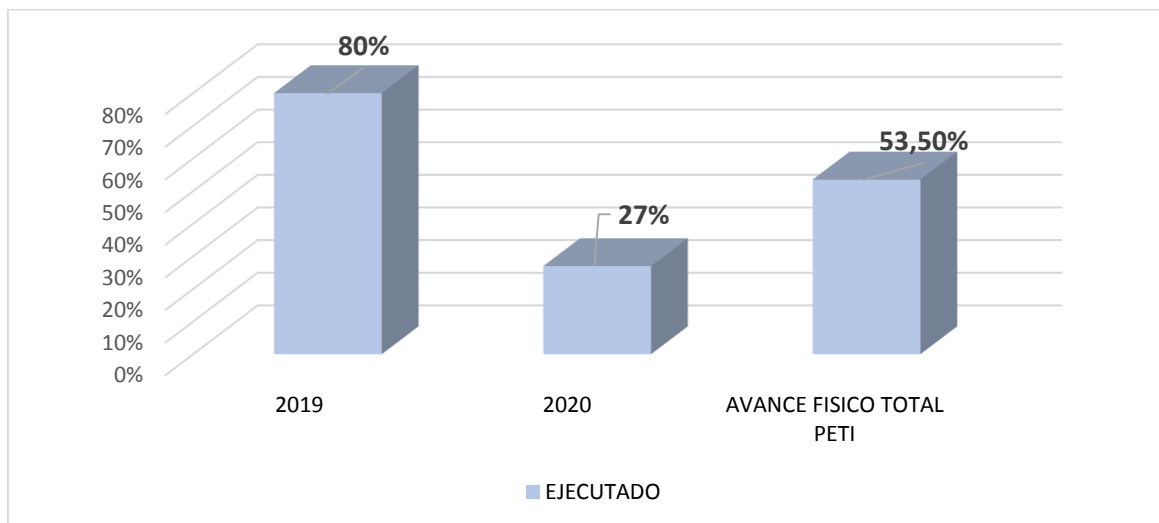
6.3 Observaciones de la Auditoría

1. SEGUIMIENTO AL PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACIÓN (PETI)

El Plan Estratégico de Tecnologías de la Información – PETI, tiene como objetivo definir las estrategias, las acciones, los procesos, los proyectos y las iniciativas de las tecnologías de información que contribuirán al logro de los objetivos y metas de la Universidad del Quindío alineados con el Sector, para el periodo del 2019 al 2022.

Para conseguir los objetivos del PETI, se planeó la ejecución de 32 proyectos durante los 4 años de la vigencia del Plan, de los cuales, en esta auditoría se hizo seguimiento a 11 proyectos de la vigencia 2019 y 15 proyectos de la vigencia 2020, obteniendo un avance físico promedio de 53.5% de dichos proyectos, como se muestra en el siguiente gráfico:

Gráfico No 1. Avance físico de proyectos planeados en el PETI de las vigencias 2019 y 2020.



Fuente: Información suministrada por el área de sistemas.

Se evidencia un porcentaje bajo de ejecución física para la vigencia 2020 (27%), el cual es explicado porque no hubo asignación presupuestal en los siguientes proyectos: Diseñar e implementar el plan de continuidad de los servicios de TI y el DRP (Disaster Recovery plan) cuyo presupuesto es de \$470.000.000 y mejorar las condiciones de alimentación eléctrica y climatización del Centro de Datos de la Institución de \$300.000.000, entre otros.

Sin embargo, al realizar la verificación de la información reportada por parte el Área de Sistemas y Nuevas Tecnologías se observó que existen diferencias en los datos del valor total de los proyectos y el valor total contratado, por ejemplo, en el proyecto OBJ3-P04.

Imagen 2. Revisión de información presupuestal del Proyecto OBJ3-P04

OBJ3 -P04	MATRIZ	SIA OBSERVA	DIFERENCIA
CONT-026 = \$98.778.948 (28 PC).	\$ 98.778.948	\$ 98.778.948	\$ -
CONT-0035=\$176.628.200 (58 PC).	\$ 176.628.200	\$ 176.628.200	\$ -
OC-706=\$21.245.070 (SW ANTIPLAGIO).	\$ 21.245.070	\$ 21.245.070	\$ -
OC-245=\$22.116.150 (SW ARTICULATE).	\$ 22.116.150	\$ 22.116.150	\$ -
OC-162=\$49.921.200 (10 PC).	\$ 49.921.200	\$ 55.785.830	-\$ 5.864.630
OC-250=\$4.609.557 (1 PC).	\$ 4.609.557	\$ 5.033.700	-\$ 424.143
OC-316=\$14.667.000 (5 PC).	\$ 14.667.000	\$ 15.416.700	-\$ 749.700
OC-363=\$62.986.000 (22 PC).	\$ 62.986.000	\$ 62.986.000	\$ -
OC-250=\$1.428.000 (1 TABLE).	\$ 1.428.000	\$ 1.428.000	\$ -
CONT-017=\$18.775.000 (350 TABLES).	\$ 187.775.000	\$ 187.775.000	\$ -
OC-338=\$2.408.000 (4 TABLES).	\$ 2.408.000	\$ 2.408.000	\$ -
OC-351=\$80.627.736 (24 VIDEOBEAMS).	\$ 80.627.736	\$ 88.132.757	-\$ 7.505.021
OC-29=\$5.766.740 (SW CONCEPT DROW OFFICE)	\$ 5.766.740	\$ 5.766.740	\$ -
OC-455=\$88.000.000 (. SW MAP LAB)	\$ 88.000.000	\$ 88.000.000	\$ -
	\$ 816.957.601	\$ 831.501.095	-\$ 14.543.494

Fuente: área de Sistemas

Con relación a la Imagen 2, se realizó la verificación de la información y se observó en el reporte de la matriz enviada por el área de sistemas en el OBJ3-P04 una diferencia total de \$ 14.543.494 que equivale al 1,78% alterando los reportes financieros de la ejecución de los proyectos (**Ver Anexo 3 – IM7743**).

De acuerdo con lo anterior se evidencian debilidades en el sistema de control sobre la ejecución presupuestal de los proyectos, reflejándose inconsistencias en los reportes presentados por el área de sistemas.

Ahora bien, respecto al avance financiero en las vigencias 2019 y 2020, esto es, ejecutado versus presupuestado, se alcanzó un 97,8%, y el avance financiero global del Plan a los 4 años es del 45,8%, como se muestra en la siguiente tabla:

Tabla No 2. Avance Financiero Proyectos – PETI

FINANCIERO	2019	2020	TOTAL PRESUPUESTO	TOTAL PRESUPUESTO PETI
PLANEADO	\$ 867.000.000	\$ 1.912.000.000	\$ 2.779.000.000	\$ 5.929.000.000,00
EJECUTADO	\$ 1.732.808.672	\$ 985.020.411	\$ 2.717.829.083	
%	199,9%	51,5%	97,8%	45,8%

Fuente: Información suministrada por el área de sistemas.

De acuerdo con el modelo de planeación implementado en el PETI se describen los siguientes objetivos estratégicos que permiten operar las acciones de la gestión de TI:

Objetivo Estratégico OBJ1: Posicionar el área de TI como un actor estratégico de la institución mediante la adopción de los requerimientos establecidos por la política de gobierno digital del Ministerio de las TIC.

Objetivo Estratégico OBJ2: Habilitar nuevos servicios de información automatizados y fortalecer los servicios actuales para dar cobertura a las necesidades y lograr la mejora de los procesos de la institución, ofreciendo información útil, confiable y oportuna.

Objetivo Estratégico OBJ3: Modernizar y mantener la capacidad de los recursos de infraestructura de TIC que requiere la institución mejorando los indicadores de disponibilidad de los servicios

Objetivo Estratégico OBJ4: Contribuir al fortalecimiento de la institución mediante el asesoramiento y apoyo en la ejecución del plan de desarrollo institucional implementando estrategias de TIC que facilite el logro de los objetivos institucionales.

En la siguiente tabla se observa la ejecución presupuestal del PETI dividido en cada uno de los objetivos estratégicos, así:

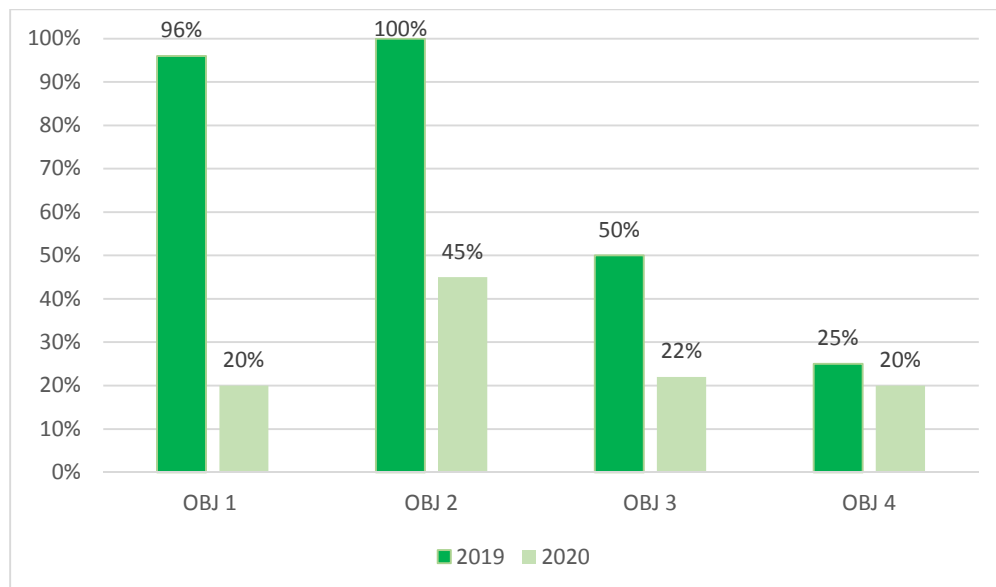
Tabla No 3. Relación Porcentaje presupuestal por Objetivos 2019-2020 PETI

PROYECTOS	VALOR TOTAL PRESUPUESTADO EN EL PETI	COMPROMISOS	OBLIGACIONES	% CUMPLIMIENTO POR OBJETIVOS
OBJ 1	\$505.000.000	\$366.251.457	\$366.251.457	72,5%
OBJ 2	\$924.000.000	\$524.894.464	\$524.894.464	56,8%
OBJ 3	\$2.920.000.000	\$1.590.820.412	\$1.590.820.412	54,5%
OBJ 4	\$750.000.000	\$235.862.750	\$235.862.750	31,4%
TOTAL	\$5.099.000.000	\$2.717.829.083	\$2.717.829.083	53,3%

Fuente: Información suministrada por el área de sistemas.

Para el Objetivo 1, su ejecución presupuestal acumulada fue del 72.5%, reflejándose en la construcción y aprobación del PETI, elaboración del dominio de gobierno de TI, diseño del documento con dominio del modelo Uso y apropiación e implementación de 32 trámites y servicios en línea. Así mismo, se evidenciaron avances que se han realizado con profesionales del área de sistemas.

Gráfico No 2. Avance Físico proyectos 2019-2020



Fuente: área de Sistemas

Respecto al Objetivo 2, se refleja un avance presupuestal del 56,8%, evidenciándose en los sistemas instalados en los servidores de la institución, capacitación a usuarios, módulo de seguridad, gestión de prácticas y de pasantías y en el contrato con la firma NEXSURA en el rediseño e implementación del portal institucional, además de lo anterior se adquirieron los servicios de XERTIFY para la implementación de la firma digital con el fin de expedir diplomas y actas de grado.

Adicional a lo anterior, es importante anotar que para la vigencia 2019 las actividades planeadas del objetivo 2 se ejecutaron en un 100%, sin embargo, la ejecución para la vigencia 2020 fue del 45%, esto se debió a que algunos proyectos no presentan compromisos, como: la implementación del Plan institucional de Archivo-PINAR, dado que sus actividades se han realizado con profesionales del área y el proyecto de solución tecnológica para la gestión de inventarios de laboratorios, el cual no refleja ningún avance.

Con respecto al Objetivo 3, se evidencia una ejecución financiera del 54,5%, reflejándose en el fortalecimiento y modernización de la infraestructura de conectividad, seguridad en la red, renovación y ampliación de la red wifi e internet para la institución.

Finalmente, respecto al Objetivo 4, se observa un avance inferior, teniendo en cuenta que algunas actividades no cuentan con compromisos ni obligaciones, como son: diseñar e implementar un BALANCED SCORE CARD utilizando plataformas tecnológicas, diseño e implementación de un plan de gestión del cambio e implementar una solución de software que facilite el control y seguimiento de planes de acción de mejoramiento institucional. **Ver anexo 2. (Matriz de avance de PETI).**

OBSERVACIÓN 1: En relación a la ejecución y seguimiento del Plan Estratégico de Tecnologías de la Información (PETI), para las vigencias 2019 – 2020, se pudo establecer, que no se tiene implementado un esquema de seguimiento con indicadores que permita medir la ejecución y realizar una precisa evaluación de su efectividad, además de presentar imprecisiones en la información suministrada de la ejecución presupuestal y lo reportado en SIA OBSERVA, incumpliendo lo establecido en la Política de Gobierno Digital, en el Capítulo 4. MEDIR LA POLÍTICA específicamente en el punto 4.1 Seguimiento y evaluación por parte de la Entidad², lo cual podría generar riesgos de incumplimiento de los objetivos para los cuales fue creado dicho Plan.

² Implementación de la Política de Gobierno Digital Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1

1.1 Revisión de ejecución contractual del PETI

Frente a la evaluación del cumplimiento del PETI, esta auditoría tomó como muestra los siguientes proyectos:

- a. *OBJ 3-P03: Fortalecer y modernizar la infraestructura de conectividad y seguridad en la Red.*

Se evaluaron los siguientes contratos en el marco de este proyecto:

Tabla No 4. Relación de Contratos OBJ3 – P03

CONTRATO N°:	CT12
TIPO DE CONTRATO:	APOYO A LA GESTION
OBJETO:	PRESTACION DEL SERVICIO DURANTE UN TERMINO DE 12 MESES, DE SAAS COLLABORATION FLEX PLAN FOR EDUCATION CISCO CLOUD ADVANCED MEETING, CON UN TERMINO DE DURACION DE 12 MESES PARA EL CUMPLIMIENTO DE LOS OBJETIVOS MISIONALES ACADEMICOS Y EL DESARROLLO DE LAS ACTIVIDADES DE GESTION CREATIVA Y UNIVERSIDAD INTEGRADORA, SEGUN LA NECESIDAD
CONTRATISTA:	OPEN GROUP S.A.S
PLAZO DE EJECUCION:	362 DIAS
VALOR EJECUTADO:	\$ 80.992.131
FECHA DE INICIO:	04/05/2020
FECHA DE TERMINACION:	30/04/2021

CONTRATO N°:	OC47
TIPO DE CONTRATO:	PRESTACION DE SERVICIOS
OBJETO:	LICENCIAMIENTO Y GARANTIA DE SOFTWARE
CONTRATISTA:	BRITO MEJIA IVAN MAURICIO
PLAZO DE EJECUCION:	22 DIAS
VALOR EJECUTADO:	\$ 119.742.082
FECHA DE INICIO:	15/02/2019
FECHA DE TERMINACION:	08/03/2019

CONTRATO N°:	CT31
TIPO DE CONTRATO:	COMPRAVENTA
OBJETO:	EJECUTAR LA VENTA, ENTREGA Y CONFIGURACION DE UN DISPOSITIVO CPE PARA OPTIMIZAR Y MODERNIZAR EL SERVICIO DE INTERNET CONTRATADO POR LA INSTITUCION.
CONTRATISTA:	OPEN GROUP SAS
PLAZO DE EJECUCION:	31 DIAS
VALOR EJECUTADO:	\$ 62.662.148
FECHA DE INICIO:	25/11/2019
FECHA DE TERMINACION:	25/12/2019

CONTRATO N°:	CT22
TIPO DE CONTRATO:	PRESTACION DE SERVICIOS
OBJETO:	SERVICIO ESPECIALIZADO DE MONITOREO Y SEGUIMIENTO DE SEGURIDAD INFORMATICA PARA LA DETECCION Y MONITOREO CONTINUO DE AMENAZAS Y VULNERABILIDADES.
CONTRATISTA:	PASSWORD CONSULTING SERVICES S.A.S
PLAZO DE EJECUCION:	59 DIAS
VALOR EJECUTADO:	\$ 263.095.000
FECHA DE INICIO:	02/11/2020
FECHA DE TERMINACION:	30/12/2020

Fuente: Elaboración propia con base en datos suministrados por la oficina de Compras

De acuerdo a lo anterior, se confirmaron los contratos con la oficina de contratación y en el SIA OBSERVA evidenciándose la exactitud de la información en los contratos relacionados, para un total en los contratos adquiridos de \$ **526.470.361. ver anexo 3 (SIA OBSERVA).**

b. OBJ 1-P09: Implementar un modelo de Seguridad Informática para el área de TI, basado en la norma iso-27001.

Se verificó la documentación enviada por la oficina de sistemas y nuevas tecnologías, evidenciándose un avance del 80% en el alcance físico del proyecto; No obstante, la fase de implementación y puesta en operación del modelo, corresponde a ese 20% para cumplir con lo establecido en la norma ISO 270001 que *“Especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar los sistemas de gestión de seguridad de la información (SGSI) formalizado dentro del contexto de los riesgos globales de negocio de la organización. Especifica los requisitos para la aplicación de los controles de 1ª seguridad de la información adaptados a las necesidades de las organizaciones o partes de las mismas. (International Organization for Standardization/International Electrotechnical Commission, 2014)”*.

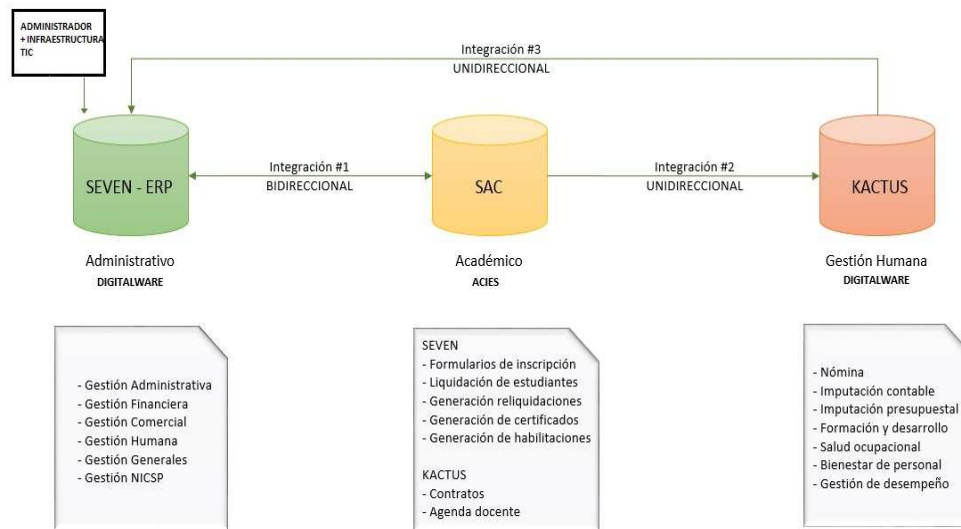
Lo anterior, según los líderes de la oficina, debido a la falta de talento humano especializado para liderar la implementación y puesta en operación del proyecto.

2. EVALUACIÓN DE LA APLICACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Uno de los aspectos a evaluar en esta auditoría interna es la aplicación de controles en el marco del Sistema de Seguridad y Privacidad de la Información que deben implementar las instituciones públicas, de acuerdo con esto, se decidió tomar como muestra de auditoría, dentro de la variedad de sistemas de información que se tienen en la Universidad, el sistema SEVEN-ERP.

El sistema SEVEN-ERP es el software utilizado por la Universidad del Quindío para la gestión administrativa y financiera, el cual cuenta con integraciones de diferentes softwares, permitiendo la ampliación de sus funcionalidades necesarias en diferentes procesos administrativos de la universidad, en el siguiente gráfico se observa la estructura de integración del mismo.

Grafico No 3. Diagrama Plataforma SEVEN-ERP



Fuente: Información suministrada por el área TIC

De acuerdo a la información suministrada por el área encargada, la valoración de **SEVEN ERP**, se realizó a través de una prueba de campo, coordinada con la administradora del software y el jefe de infraestructura TIC, donde se identificó el estado actual del sistema a través de unas preguntas seleccionadas bajo los criterios que se muestran en la imagen 3.

Imagen 3. Criterios de seguridad de la información

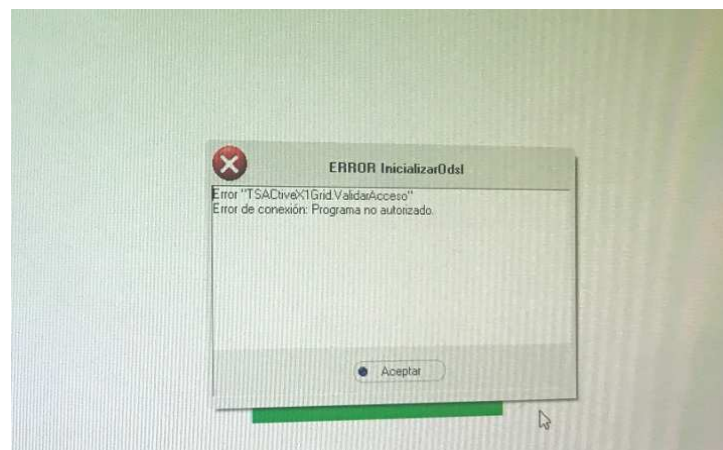


Fuente: Elaborado por las autoras del documento

De acuerdo con lo anterior, se analizaron los controles establecidos por los usuarios y administradores de la plataforma, así:

Integridad: El sistema SEVEN ERP está cubierto por controles que permiten garantizar la exactitud y completitud de los datos, toda vez que el usuario cuenta inicialmente con conexión segura VPN, instalación de permisos en el directorio activo usando la dirección IP y el nombre del equipo autorizado, así como también se asignan grupos de usuarios con funciones específicas y accesos limitados por módulos evitando que los datos sean modificados como se observa en la siguiente imagen:

Imagen No 4. Evidencia acceso limitado



Fuente: Información suministrada por el contador de la Universidad

Confidencialidad: se identifican controles donde ningún individuo, entidad o proceso no autorizado dispone de la información del sistema SEVEN-ERP, a cada usuario se le asigna una clave individual, la cual debe modificar en el primer ingreso y de forma periódica, por otra parte, cada usuario se le asigna un perfil de acuerdo al cargo que ejerce a solicitud y conocimiento del Jefe del área completando así el esquema de accesos y roles.

Disponibilidad: desde el punto de vista de Infraestructura, el sistema cuenta con un porcentaje importante de accesibilidad para la operatividad diaria del 97%, reflejando el buen manejo de los controles establecidos, además se realizan actualizaciones y mantenimiento a este sistema en días festivos y horas nocturnas, evitando así la interrupción del servicio. De la misma forma, se dispone de un servidor con características similares, con el fin de respaldar la operación en caso de daño.

Privacidad: se cuenta con un antivirus centralizado, el cual identifica que determinados programas infecciosos no afecten el sistema. Igualmente, se observó que cada módulo cuenta con un líder responsable, el cual se encarga de asignar usuarios, accesos y roles en coordinación con el administrador del sistema como se encuentra documentado en la política de TI “*Gestión de acceso a los servicios de TI*”.

Auditabilidad: cada líder del proceso se encarga de verificar la pertinencia, coherencia y exactitud de los datos registrados en cada módulo, no obstante, en el momento en que se identifique un dato erróneo, el líder se encarga con la administradora del sistema de realizar la trazabilidad. De igual manera, es importante garantizar que todo el personal vinculado a la entidad, y que maneje sistemas de información conozca y aplique la Política de Protección de Datos Personales.

En resumen, esta auditoría encontró la aplicación de los siguientes controles:

Tabla No 5. Controles de Seguridad en la Plataforma SEVEN ERP

ID	DESCRIPCION DE CONTROL	TIPO DE CONTROL	RESPONSABLE	PERIODICIDAD	DOCUMENTADO	CONTROL EFICAZ
A	BACKUPS	DETECTIVO	TIC	2 VECES AL DIA	NO	SI
B	ACTUALIZACIONES	DETECTIVO	PROVEEDOR + ADMINISTRADOR	PROMEDIO CADA 4 MESES	CONTRATO	SI
C	CONTRASEÑAS DE INGRESO	PREVENTIVO	ADMINISTRADOR	CAMBIO OBLIGATORIO CADA 3 MESES	POLITICA TI	SI
D	ROLES Y ACCESOS	PREVENTIVO	LIDER DE PROCESO + ADMINISTRADOR	JEFE DEL AREA INDICA Y SOLICITA LA ASIGNACION DE PERMISOS	POLITICA TI	SI
E	LICENCIA	PREVENTIVO	PROVEEDOR	VITALICIA	CONTRATO	SI
F	CORTAFUEGOS Y ANTIVIRUS	PREVENTIVO	TIC	AVAST CENTRALIZADA	CONTRATO	SI

Fuente: Elaborado por las autoras del documento

OBSERVACIÓN 2: En relación a la administración de la plataforma SEVEN- ERP, para los seis módulos adquiridos por la Universidad del Quindío, se evidencia un Recurso Humano altamente calificado para el soporte de toda la operatividad del Sistema, sin embargo, no se cuenta con un técnico suplente que tenga la capacitación necesaria para reemplazar en cualquier contingencia al administrador actual, incumpliendo lo establecido en la Política de TI, **ítem 3.8 Contingencia de Recurso Humano**, lo cual puede representar un riesgo en la disponibilidad del sistema en caso de eventuales ausencias del administrador.

3. SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

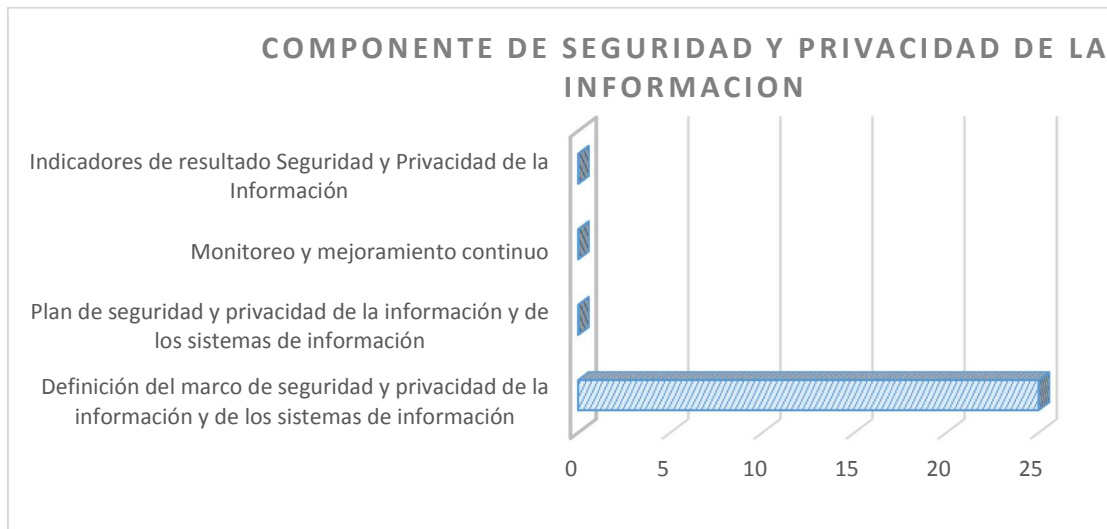
La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de “TIC para la Gestión”, al aportar en el uso estratégico de las tecnologías de la información la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad³.

Es así como la planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales, el tamaño y estructura de la Entidad.

Para el desarrollo del componente de Seguridad y Privacidad de la Información, se tomó como base el resultado obtenido de las preguntas asociadas al Modelo Integrado de Planeación y Gestión-MIPG, empleando la herramienta dispuesta en el sitio web (DAFP,2018) “2019-03-20_autodiagnostico_gobierno_digital.xls”, con el fin de analizar la implementación desde la perspectiva de cumplimiento en cuanto a los indicadores de proceso logro e indicadores de resultado del componente 4.

³ articles-5482_Modelo_de_Seguridad_Privacidad

Grafico No 4. Categorías del Componente 4: Seguridad y Privacidad de la Información.



Fuente: Autodiagnóstico Gobierno Digital - MIPG

Como se observa en las categorías del grafico 4, el componente Definición del marco de seguridad y privacidad de la Información y de los sistemas de información presentó un avance de 25 puntos sobre 100, evidenciándose un desarrollo incipiente, ya que si bien la entidad generó un documento de diagnóstico del plan de transición de protocolo IPV4 a IPV6 y construyó la metodología de la Gestión de Activos, no estableció la política de seguridad y privacidad de la Información que contenga los objetivos, el alcance y el nivel de cumplimiento; así como tampoco el manual de políticas que garantice el adecuado uso de los activos de la información, definiendo responsabilidad generales y específicas para la gestión de la seguridad de la información.

En el mismo sentido, no se tiene establecido un acto administrativo donde se vean reflejados las modificaciones o creación de funciones en el comité institucional de desarrollo administrativo, donde se incluyan los temas de Seguridad y privacidad de la información ni tampoco se evidencia un plan de sensibilización, comunicación y capacitación que incluya la estrategia para que la seguridad de la información, se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad⁴.

⁴ https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

Continuando con el componente 2; Plan de Seguridad y Privacidad de la Información y de los sistemas de Información, se identificó que no tuvo ningún avance, reflejándose un puntaje de 0 en la ausencia de planificación e implementación del tratamiento de riesgos, y en los indicadores de gestión del modelo que permitieran medir la efectividad, eficiencia y eficacia de las acciones implementadas.

Así mismo se observa un puntaje de 0 en el componente 3 Monitoreo y mejoramiento continuo, debido a que no se han desarrollado las actividades de las anteriores fases del modelo como son la planificación e implementación como lo señala la guía No- 16 Evaluación del desempeño⁵.

Finalmente, se evidencia el mismo puntaje para el componente 4 en relación a los indicadores de resultado y a la valoración de activos de infraestructura crítica donde no se miden ni se gestionan los incidentes de seguridad.

Se recomienda tener en cuenta la resolución N°00500 de marzo 10 de 2021 Por la cual 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, en su ARTÍCULO 5 “**La estrategia de seguridad Digital**” la Universidad debe contemplar lo siguiente para avanzar en el proceso de implementación:

1. *“Ser aprobada a través de un acto administrativo de carácter general.*
2. *Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos.*
3. *Establecer los roles y responsabilidades al interior de la entidad asociados a la seguridad digital.*
4. *Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones PIC, o el que haga sus veces.*
5. *La estrategia debe incluir todas las tecnologías de la información y las comunicaciones que utiliza la organización, incluida la adopción de nuevas tecnologías o tecnologías emergentes*
6. *Aplicar las demás consideraciones que a juicio de la entidad contribuyan a elevar sus estándares de seguridad digital”.*

⁵ Guía No 16 – Evaluación del desempeño: <http://www.mintic.gov.co/gestioniti/615/articles>

4. GESTION DE RIESGOS

Tabla No 5. Relación Riesgos Macroproceso TIC

FECHA DE IDENTIFICACIÓN	RIESGO	EFFECTOS (CONSECUENCIAS POTENCIALES)	TIPO DE IMPACTO	INDICADOR
12/07/2012	Virus informático	Daños en equipos, pérdida de información y daños tecnológicos afectación en la calidad del servicio	Operativo	# equipo afectados / Total de equipos
15/03/2013	Vulnerabilidad en los sistemas de información	Perdidas económicas Parálisis del sistema de información inestabilidad de los procesos mala imagen Institucional	Confidencialidad de la información	# de capacitaciones realizadas
09/11/2015	Interrupción de los servicios de conectividad	Baja productividad en las oficinas Demoras en los tramites Mala imagen institucional Insatisfacción de usuarios internos y externos reprocesos inoperatividad de sistemas de información, Interrupción de los servicios informáticos al interior y exterior de la institución. (Página web, Academusoft, correo electrónico, Aulas virtuales, telefonía, internet, procesos de inscripción y convocatorias) Atraso en el calendario académico, Pérdidas económicas, mala imagen Institucional disgusto en la comunidad en general.	Credibilidad o imagen	Inversión realizada en equipos / Inversión proyectada en equipos Mantenimiento de redes realizados/ total de mantenimiento programados

Fuente: Intraweb unquindio.

Conforme a la Tabla N°5, se logró evidenciar que desde el año 2015 no se actualizan los riesgos en el Sistema Integrado de Gestión⁶ por parte del área de sistemas y nuevas tecnologías, además, algunos indicadores no miden la eficiencia, eficacia y efectividad del control establecido para mitigar el riesgo.

OBSERVACIÓN 3: En la formulación de los indicadores de gestión de riesgos, en el riesgo “vulnerabilidad en los sistemas de información” el indicador es “# de capacitaciones realizadas”, el cual no mide la ocurrencia de incidentes en un periodo de tiempo, lo anterior no permite realizar una evaluación sobre la materialización del riesgo, lo cual va en contravía de la Guía para la Administración del Riesgo y Diseño de controles en entidades públicas del DAFP¹, esto podría ocasionar una materialización del riesgo sin que se tomen las acciones de mejora oportunas.

⁶

https://intraweb.uniquindio.edu.co/index.php?option=com_formasonline&formasonlineform=Documentos_pub

5. PLAN ANUAL DE GESTIÓN

Respecto a los Planes Anuales de Gestión, la Resolución de Rectoría N° 224 del 8 de abril de 2013¹, los define de la siguiente forma:

"ARTÍCULO PRIMERO: PLAN ANUAL DE GESTIÓN (PAG)". *El Plan Anual de Gestión (PAG) es una herramienta que permite ordenar información relevante para llevar a cabo la gestión de un área institucional (macro-proceso) durante un período de un año, en concordancia con la orientación estratégica de la Universidad contenida en el Plan Estratégico. Contempla la interrelación del talento humano, con los recursos financieros, materiales y tecnológicos disponibles para el cumplimiento de los propósitos del área, en concordancia con el acuerdo de gestión o acuerdo de compromisos laborales suscrito por el responsable de la misma y materializa los compromisos de cada unidad organizacional en términos de resultados concretos, medibles, realizables y verificables. (...)"*

De la revisión efectuada, a las acciones estratégicas del Plan anual de Gestión-PAG-2020 del Área de Sistemas y Nuevas tecnologías, se encontró que sus actividades se cumplieron en un 100% de acuerdo a los elementos definidos en el formato código Plan Anual de Gestión E.PE-01.01. F.06 versión 05.

Ahora bien, frente al cumplimiento de estos planes, se tomaron como muestra los siguientes procesos:

- a. Mejoras de las estrategias de la Seguridad Electrónica Institucional.
- b. Adquisición de un servidor especializado en Streaming para el total de cámaras institucionales.

Para dar cumplimiento a lo anterior, se revisó la información suministrada por el Área de Sistemas y Nuevas tecnologías – ASNT, donde se evidenció la correcta ejecución de los contratos de suministro de las cámaras de seguridad y elementos biométricos, como también la adquisición de los equipos Tipo Servidor que reposan en el centro de servidores institucional (Data Center). Anexo 4 fotos.

En el marco de la inspección y verificación de la instalación de las cámaras y equipos biométricos, se evidencio el daño por los desmanes causados en la noche de 24 de mayo en el bloque de Ciencias Básicas de la Universidad, a 10 cámaras, 1 PC y 2 biométricos, cuyo valor aproximado asciende a la suma de \$ 17.251.651, afectando la infraestructura de Seguridad de la Entidad entre otros (Anexo 5).

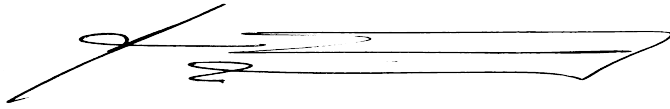
6. CONCLUSIONES

- Se evidencia un avance significativo en los proyectos establecidos en el PETI para la vigencia 2019, lo cual ha permitido un fortalecimiento de la infraestructura tecnológica, los sistemas de información y la automatización de procesos en la institución.
- Se evidencia la aplicación de controles dentro del proceso de Gestión TIC, particularmente se analizaron los controles asociados a la seguridad de la información en el aplicativo SEVEN-ERP, encontrando que en su mayoría se encuentran documentados y son eficaces.
- Frente a las categorías del componente 4: Seguridad y Privacidad de la Información, en el marco del manual de Gobierno Digital, la Universidad del Quindío se encuentra en un desarrollo incipiente de sus actividades.

7. RECOMENDACIONES

- Es importante que el Área de Sistemas y Nuevas Tecnologías – ASNT dando cumplimiento al cronograma de ejecución financiera, gestione los recursos necesarios para dar continuidad y celeridad a los proyectos establecidos para cada vigencia en el PETI, de manera que se evidencie el avance cuantitativo y cualitativo. Así mismo, la oficina de planeación y Desarrollo deberá definir la frecuencia de las revisiones periódicas con el fin de verificar el cumplimiento del avance financiero y físico de los proyectos.
- Se recomienda mejorar los indicadores de la matriz de Riesgos del Macroproceso TIC según la “Guía para la administración del Riesgo y el diseño de controles de Entidades Públicas Versión 5” ya que algunos de estos, no miden el nivel de eficiencia, eficacia y efectividad de los controles existentes.
- Establecer un plan de trabajo en conjunto con la Oficina de Planeación y Desarrollo, que permita la reglamentación y aplicación del Sistema de Seguridad de la Información al interior de la institución, el cual deberá reflejar los controles que hoy se están aplicando en materia informática, pero que también incluyan controles asociados a otros activos de la información estratégicos para las diferentes áreas de la Universidad.
- Se recomienda apoyarse en el Comité Antitrámites o quien haga sus veces, para la implementación del componente de Seguridad y privacidad de la Información en el marco de la política de Gobierno Digital, con el fin de definir aspectos importantes tales como: recurso humano, presupuesto, roles y responsabilidades de los procesos involucrados.

Cordialmente,



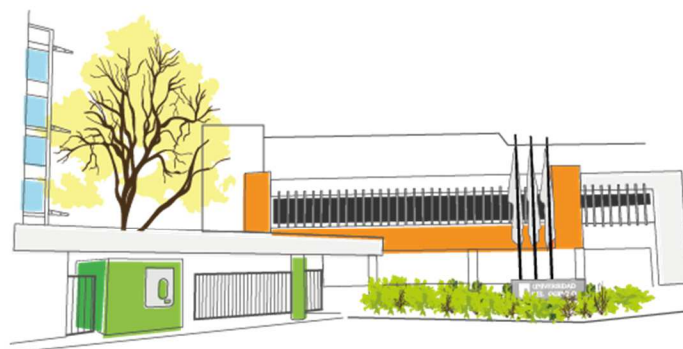
ERWIN FABIÁN ÁLVAREZ ROJAS
Jefe Oficina Asesora de Control Interno

Elaboró:

Yasmid Osorio Pinilla.
Diana Marcela Herrán Ruíz.

LISTA DE ANEXOS

- Anexo 1: Pantallazos SIA OBSERVA Proyecto OBJ3-P03.
- Anexo 2: Matriz de Avance PETI.
- Anexo 3: Pantallazos SIA OBSERVA Proyecto OBJ3-P04.
- Anexo 4: Fotos Evidencia (Gestión del Riesgo).
- Anexo 5: Informe Daños 24 de mayo de 2021.



OFICINA ASESORA DE CONTROL INTERNO

Tel: (57) 6 735 9300 Ext 324
Carrera 15 Calle 12 Norte
Armenia, Quindío – Colombia
control@uniquindio.edu.co

PERTINENTE CREATIVA INTEGRADORA



@uniquindio



universidaddelquindio



uniquindioconectada