Universidad Estatal a Distancia (UNED)

Informe Auditoría de Tecnologías de la Información

Carta de Gerencia CG-TI 2022

Informe Final.

San José, 08 de marzo del 2023

Señores
Universidad Estatal a Distancia (UNED)

Estimados señores:

Según nuestro contrato de servicios, efectuamos nuestra visita de auditoría externa del período 2022 a la Universidad Estatal a Distancia (UNED) y con base en el examen efectuado observamos ciertos aspectos referentes al sistema de control interno y procedimientos de Tecnología de Información, basados en las "Normas técnicas para el gobierno y gestión de las tecnologías de la información" del MICITT y los estándares establecidos como buenas prácticas según los Objetivos de Control para Información y Tecnología Relacionada – COBIT®., los cuales sometemos a consideración de ustedes en esta carta de gerencia CG-TI 2022.

Considerando el carácter de pruebas selectivas en que se basa nuestro examen, ustedes pueden apreciar que se debe confiar en métodos adecuados de comprobación y de control interno, como principal protección contra posibles irregularidades que un examen basado en pruebas selectivas puede no revelar, si es que existiesen. Las observaciones no van dirigidas a funcionarios o empleados en particular, sino únicamente tienden a fortalecer el sistema de control interno y los procedimientos relacionados con la tecnología de información.

DESPACHO CARVAJAL & COLEGIADOS
CONTADORES PÚBLICOS AUTORIZADOS

IVAN GUSTAVO BRENES PEREIRA (FIRMA)
Firmado digitalmente por IVAN GUSTAVO BRENES PEREIRA (FIRMA)
Fecha: 2023.04.20 14:51:30 -06'00'

Lic. Iván Brenes Pereira
Contador Público Autorizado número Nº 5173
Póliza de Fidelidad Nº 0116 FIG 0007
Vence el 30 de setiembre del 2023

"Exento de timbre de Ley número 6663 del Colegio de Contadores Públicos de Costa Rica, por disposición de su artículo número 8"

INFORME DE CUMPLIMIENTO Y CONTROL INTERNO DE TECNOLOGÍAS DE INFORMACIÓN

I. INTRODUCCIÓN

ORIGEN DEL ESTUDIO

Como parte de la evaluación a los estados financieros de la Universidad Estatal a Distancia (UNED) evaluamos los controles generales de la gestión de tecnologías de información, con el objetivo de medir el grado de riesgo de la información en lo que respecta a seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica.

La evaluación la realizamos basados en las normas técnicas para el gobierno y gestión de las tecnologías de la información" del MICITT, y nos apoyamos en los Objetivos de Control de Tecnologías de Información (COBIT por sus siglas en inglés) emitidos por la "Information Systems Audit and Control Association" (ISACA por sus siglas en inglés) como marco de mejores prácticas de la industria de tecnología de información.

OBJETIVO DEL ESTUDIO

Con el propósito de cumplir con los requerimientos estipulados en la Norma Internacional de Auditoría 315, Entendiendo de la realidad y su entorno y evaluación de representación errónea de importancia relativa y en la Norma Internacional de Auditoría 330, Procedimientos del auditor en respuesta a los riesgos evaluados, realizamos un diagnóstico a la gestión de las tecnologías de información de la Universidad Estatal a Distancia (UNED).

ALCANCE

En esta visita el trabajo fue enfocado principalmente a las siguientes áreas:

- Planificación estratégica de TI.
- Organización de TI.
- Gestión de la seguridad de la información.
- Gestión de respaldos y restauraciones.
- Gestión de la continuidad.
- Gestión de la capacidad y disponibilidad.
- Gestión de solicitudes, incidentes y problemas de TI.
- Gestión de riesgos.
- Gestión de programas y proyectos de TI.
- Gestión de requisitos y soluciones de TI.
- Gestión de activos de TI.
- Gestión de las telecomunicaciones e infraestructura tecnológica.
- Gestión de proveedores de TI.
- Gestión de los servicios brindador por TI.
- Arquitectura empresarial.

- Gestión de la calidad.
- Aseguramiento.
- Seguimiento a recomendaciones emitidas en periodos anteriores.

PERIODO DEL ESTUDIO

El estudio se realizó durante los meses de febrero y marzo del año 2023 y corresponde a la auditoría del periodo del 2022.

LIMITACIONES DEL ESTUDIO

No se presentaron limitaciones.

METODOLOGÍA

Para llevar a cabo este trabajo utilizamos una modalidad de análisis de la información suministrada por la Dirección de Tecnologías de Información y Comunicaciones (DTIC) de la UNED y de las distintas áreas involucradas en el proceso de auditoría. Además, se formularon preguntas sobre la existencia de controles de las tecnologías de información, en todos los casos necesarios solicitamos a los funcionarios las evidencias en formato digital que respaldaran sus afirmaciones.

II. HALLAZGOS Y RECOMENDACIONES

HALLAZGO 01: AUSENCIA DE UN PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD. RIESGO MEDIO.

CONDICIÓN:

Producto de la revisión efectuada en materia de seguridad de la información se solicitó a la Dirección de Tecnologías de Información y Comunicaciones (DTIC) el plan de tratamiento de riesgos de seguridad de la información y privacidad, así como evidencia del cumplimiento de dicho plan, sin embargo, se indicó lo siguiente: "La UNED cuenta e implementa una gestión de riesgos, pero no incorpora la seguridad de la información", además que "No se tiene conocimiento de un plan de tratamiento de riesgos de seguridad de la información y privacidad".

La ausencia de este plan de tratamiento de riesgos evidencia una vulnerabilidad a nivel de gestión de seguridad de la información y privacidad, pues dicho plan de tratamiento representa un control que contribuye a mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la entidad.

CRITERIO:

La práctica de gestión **"APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad",** presente en el COBIT 2019 (Control Objectives for Information Technologies 2019), menciona lo siguiente: "Mantener un plan de seguridad de la información que describa cómo se debe manejar el riesgo de seguridad de la información y cómo se debe alinear con la estrategia y la arquitectura de la empresa. Asegurar que las recomendaciones para implementar mejoras a la seguridad se basen en casos de negocio aprobados, implementados como una parte integral del desarrollo de servicios y soluciones, y que operen como una parte integral de la operación del negocio".

RECOMENDACIONES:

Al área responsable de la seguridad de la información en la UNED:

1. Contar con un plan de administración de riesgos de seguridad de la información y privacidad que considere los objetivos estratégicos y la arquitectura empresarial.
2. Considerar que en la Política de Seguridad de la Información y Ciberseguridad que actualmente está en construcción, refiera que se cuente con la gestión de riesgos de la seguridad de la información y privacidad.
3. Realizar actividades de formación de concienciación sobre seguridad de la información entre los colaboradores de la institución (incluyendo las áreas que no son de TI).
4. Considerar los recursos asociados a las normas técnicas emitidas por el MICITT, especialmente el portafolio de riesgos básicos.

III. Tomar como referencia la normativa nacional en materia de TI y marcos internacionales como COBIT 2019.

IV. SEGUIMIENTO DE RECOMENDACIONES EMITIDAS EN CARTAS DE GERENCIA ANTERIORES

Carta de Gerencia 2021	
HALLAZGO 01: CUENTAS ACTIVAS EN EL ACTIVE DIRECTORY DE EXFUNCIONARIOS. RIESGO MEDIO.	
RECOMENDACIONES	*Al Departamento de Recursos Humanos o equivalente:* 1. Comunicar activamente a la Dirección de Tecnologías de Información y Comunicaciones (DTIC) los funcionarios que cesan actividades en la institución para que TI proceda con la desactivación de las cuentas respectivas. *A la Dirección de Tecnologías de Información y Comunicaciones (DTIC):* 2. Deshabilitar las cuentas de usuario de colaboradores que cesaron sus labores para la organización según la lista identificada y lo informado por el Departamento de Recursos Humanos o equivalente.
COMENTARIOS DE LA ADMINISTRACIÓN	En el Anexo No. 2 del oficio DTIC-2022-195 se indicó que ya había sido reportada como IMPLEMENTADA.
ESTADO	**CORREGIDO** Se evidencia que dentro de la lista de Usuarios Activos del Active Directory no se encuentran activos los usuarios indicados en el hallazgo.
HALLAZGO 02: AUSENCIA DE UN PLAN PARA LA GESTIÓN DE LA CAPACIDAD, DISPONIBILIDAD Y DESEMPEÑO DE LA PLATAFORMA TECNOLÓGICA. RIESGO BAJO.	
RECOMENDACIONES	*A la Dirección de Tecnologías de Información y Comunicaciones (DTIC):* 1. Elaborar un plan documentado para la gestión de la capacidad, disponibilidad y desempeño de la infraestructura tecnológica, contemplando puntos como los siguientes: a. Los equipos que se deben de monitorear. b. Aspectos que deben monitorearse.

	c. Periodicidad del monitoreo. d. Los umbrales de funcionamiento normal. e. Reportes periódicos (mensuales o según la periodicidad que se defina) de lo siguiente: i. Reportes de disponibilidad. ii. Reportes de capacidad. iii. Reportes de excepciones (situaciones esporádicas que pueden generar una alerta sobre capacidad o disponibilidad). f. Acciones de cómo se gestionarán el seguimiento a los incidentes por un desempeño o capacidad inadecuados. 2. Si los resultados presentados por la herramienta Live Optics aportan para atender lo expuesto en este hallazgo, seguir considerando su uso. 3. Realizar un análisis periódico del comportamiento en el consumo de recursos (por ejemplo; memoria, procesamiento, ancho de banda), con el fin de realizar una proyección de recursos y así determinar cuál va a ser el consumo futuro por parte de la UNED. 4. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	En el Anexo No. 2 del oficio DTIC-2022-195 se indicó que se inicia a partir de enero del 2023, se cuenta con un inventario preliminar de componentes de infraestructura.
ESTADO	**EN PROCESO** De acuerdo con lo indicado por la Administración y a lo proporcionado, las actividades establecidas para atender este hallazgo se realizarán durante el 2023 y 2024.
HALLAZGO 03: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE LA CALIDAD Y SEGUIMIENTO DE LOS	

PROCESOS DE TI. RIESGO BAJO.	
RECOMENDACIONES	1. Definir un proceso formal de revisión periódica de los procesos de TI y la asociación y vigencia de los lineamientos y prácticas formalmente establecido para respaldar las actividades de cada proceso. Estas valoraciones deben quedar registradas en los documentos (aunque no apliquen cambios), por lo que según aplican las buenas prácticas, se debe disponer de un apartado en el que se indique la fecha de creación del documento, versión, acción (revisado, modificado, etc.), responsable de revisión y de aprobación, fecha/período de revisión. Tómese esta recomendación para la elaboración de documentos nuevos con base en la "Guía para el Desarrollo de Documentación". 2. Finalizar con la elaboración de los productos esperados para diciembre del 2022, específicamente: a. Documentar el marco de gestión de la calidad, con detalles de objetivos de calidad del proceso y del producto (software adquirido, software desarrollado y recursos de TI). b. Documentaciones relativas a: ✓ Definición de estándares y métricas para el seguimiento ✓ Definición de estructuras básicas de trabajo, procedimientos y protocolos ✓ Toma de evidencias de la implementación realizada 3. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	Punto 1: CORREGIDO. Mediante oficio DTIC-2022-208 se formaliza el punto 1 de este hallazgo y el director DTIC informa a los Coordinadores para que lo tomen en cuenta. Punto 2: PROCESO. Mediante oficio DTIC-USI-2023-003 se resume las actividades y el gran avance que se ha tenido en relación a los aspectos que involucra este punto 2. A pesar de que el esfuerzo realizado ha sido significativo y se cuenta con avances en: Política y objetivos de calidad, Flujos de valor y los indicadores claves de rendimiento de cada unidad de la DTIC, Documentación (procedimientos y guías técnicas), no se ha logrado concluir, a pesar de que un grupo de 3 personas más un experto le han dedicado al menos medio día de trabajo por semana. Para concluir el proceso a nivel de la Unidad de Sistemas Información se estima NOVIEMBRE 2023.

ESTADO	**EN PROCESO** Si bien, como se indica en el comentario de la administración, aún se encuentran en proceso ciertas actividades (cuya finalización se estima para noviembre del 2023) sí se han realizado acciones para atender las recomendaciones del hallazgo; en la evidencia suministrada fue posible identificar un procedimiento de gestión de la calidad, un documento sobre los flujos de valor e indicadores claves de rendimiento y una guía para aseguramiento de calidad, además, un informe de avance del Sistema de Gestión de la Calidad. Cabe indicar que dicha documentación se presentó en formato WORD y no indica en el campo de fecha la validación por parte del director, en caso de que dicha validación esté pendiente se recomienda proceder al respecto y generar un oficio (o equivalente) que refleje que la documentación está formalmente validada y aprobada.
HALLAZGO 04: AUSENCIA DE UN INVENTARIO ACTUALIZADO DE LICENCIAS INSTALADAS POR EQUIPO. RIESGO BAJO.	
RECOMENDACIONES	*A la Dirección de Tecnologías de Información y Comunicaciones (DTIC):* 1. Una vez concretado el proceso de compra del software ARANDA, determinar la información referente a las licencias instaladas en los equipos de manera que, se genere un reporte (o equivalente) para que el departamento correspondiente (que según se comprende es la Oficina de Contabilidad) pueda generar un inventario detallado de las licencias. *A la Oficina de Contabilidad en colaboración con la Dirección de Tecnologías de Información y Comunicaciones (DTIC):* 2. Con base en el reporte brindado por la DTIC generar un inventario detallado de las licencias. 3. Verificar periódicamente que el total de licencias registradas en el inventario general coincida con el detalle del inventario de licencias instaladas por equipo, registrando documentalmente los resultados de dicha verificación, con el fin de tener una mejor gestión del software instalado y de la distribución de licencias en la institución.

	4. Brindar el trato contable correspondiente a las licencias de Software.
COMENTARIOS DE LA ADMINISTRACIÓN	En abril del 2022 se inició la ejecución con la configuración de los servidores, posteriormente la configuración del módulo ARANDA INVENTORY en algunos equipos de cómputo. A nivel de las Sedes Universitarias se podría indicar que un 90% de los equipos de cómputo ya tienen instalado el módulo ARANDA INVENTORY, con lo cual permite generar un listado del software. Se está realizando a nivel de la Sede Central la instalación del Módulo ARANDA INVENTORY.
ESTADO	**EN PROCESO** Además de lo indicado en el comentario de administración, a través de la *nota 144-2022 Anexo No.2* se amplía indicando que "(…)para una primera fase se está considerando el software ARANDA Inventory que es la base para establecer la estructura que estará proporcionando el inventario de hardware y software a nivel institucional y está en proceso la instalación del agente en cada una de las computadoras", además se tiene una segunda fase, esta "(…) considera la adquisición de otro software que va a permitir el valor que se requiere que es precisamente, poder identificar qué software está instalado en una computadora determinada". Al respecto se tienen identificadas tres actividades para la adquisición: 1. Valoración (prueba de concepto) de otra herramienta. 2. Adquisición de la herramienta (Se supone que se cuenta con el presupuesto a nivel de inversión). 3. Instalación, configuración, implementación. De esta forma se evidencia que se continua con la ejecución de actividades para atender las recomendaciones del hallazgo, por lo tanto, se mantiene en proceso de atención.
HALLAZGO 05: AUSENCIA DE LINEAMIENTOS DOCUMENTADOS PARA LA GESTIÓN DE INFRAESTRUCTURA TECNOLÓGICA. RIESGO BAJO.	

RECOMENDACIONES	*<u>A la Dirección de Tecnologías de Información y Comunicaciones (DTIC):</u>* 1. Analizar los siguientes documentos con el fin de determinar si la información que abarca responde y/o contribuye a las recomendaciones del hallazgo 2018-01 (véanse en *recomendación 2*). a. Manual de Procedimientos del Proceso de Gestión de Tecnologías de Información y Comunicaciones de la Universidad Estatal a Distancia. b. Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones de la Universidad Estatal a Distancia. 2. Incluir en el manual (*UNED-MEGA-PEGTI.03- GESTION EN TI*) los siguientes puntos (aplíquese esta recomendación considerando lo establecido en la "Guía para el Desarrollo de Documentación"): a. Los lineamientos para el mantenimiento de Software e Infraestructura. b. Los servicios de TI Institucionales para la gestión y apoyo de administración. c. El estándar de nombres de Servidores y dispositivos electrónicos. d. La Autorización de funcionarios para las labores de soporte y mantenimiento de los equipos y dispositivos. e. Regulaciones sobre el almacenamiento, transmisión y difusión de la información. f. Custodia de Medios Magnéticos de Respaldo e información de carácter institucional. g. Instalación y configuración de hardware, software y dispositivos de red. h. Implementación y administración del programa de antivirus. 3. Para atender la *recomendación 2*, considerar los resultados del análisis de la *recomendación 1* con el fin de evitar retrabajo en la elaboración de la documentación necesaria. 4. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	Se tiene programada una reunión con el CPPI para marzo del 2023 para iniciar el abordaje de la actualización o migración del documento.

ESTADO	**EN PROCESO** De la evidencia obtenida, se identifica un avance en la realización de un procedimiento para Gestionar la Infraestructura como lo son: • FUNED DTIC-UIT 01.00.01 Bitácora de la DTIC sobre usuarios AS 400. • FUNED DTIC UIT 01.00.02 Control de usuarios de red deshabilitados • FUNED DTIC-UIT 01.02.01 Bitácora de respaldos de AS 400 • FUNED DTIC-UIT 01.02.02 Pruebas de restauración de respaldos • Guía para la gestión de la herramienta OsTicket • Guía de respaldos y restauraciones del centro de datos principal y alterno. La documentación anterior aún está en proceso de aprobación por parte de CONRE.
HALLAZGO 06: DEBILIDADES EN LA GESTIÓN DE PERFILES DE LOS USUARIOS DE LOS SISTEMAS DE INFORMACIÓN DE LA UNED. RIESGO BAJO.	
RECOMENDACIONES	*A la Dirección de Tecnologías de Información y Comunicaciones (DTIC):* 1. Continuar con las acciones definidas para documentar los roles y permisos de los usuarios de los sistemas desarrollados en AS400 siguiendo el estándar establecido. 2. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT. *A los líderes de servicio:* 1. Implementar controles que contribuyan a una mejor gestión de la información y sistemas de los cuales son responsables, de manera que, desde cada área se lleve un mapeo de los roles y permisos asignados a los colaboradores que gestionan. 2. En caso de requerirse asesoría para cumplir con la recomendación 1, coordinar con la DTIC.
COMENTARIOS DE LA	Al respecto sobre este hallazgo se realizó una reunión con el señor Rector Rodrigo Arias Camacho el 08 de noviembre del 2022 para plantear la limitación de implementar este hallazgo mediante la herramienta tecnológica

ADMINISTRACIÓN	que se pretendía utilizar. Debido a esto se analiza las limitaciones y oportunidades y se concluye en realizar una labor en conjunto DTIC con el CPPI y algunos líderes de servicios de los sistemas de AS 400. Se documentarán las acciones para que de forma estandarizada todos los líderes de servicio de los Sistemas AS 400 lo realicen, generando el mismo tipo de documentación, es decir, aplicando el mismo procedimiento y formularios (excel), pero cada líder de servicio conservando la información que le corresponda. No se considera levantamiento de información, es decir, se inicia en "blanco" y una vez con los procedimientos y formularios, los usuarios líderes de servicio empiecen a construir la información con el tiempo. Se espera para julio 2023 contar con el procedimiento generado para posteriormente sea remitido a aprobación por parte del CONRE.
ESTADO	**EN PROCESO** Además de lo indicado en el comentario de administración, a través de la *nota 144-2022 Anexo No.2* se amplía indicando que: Con relación a este hallazgo, a pesar de que en el oficio DTIC-2021-234 que fue remitido a la CETIC se indicó una fecha estimada de diciembre del 2023, al contarse con una herramienta identificada como Gestor de Identidades (que no fue adquirida precisamente para resolver esta necesidad), se visualizó que esta podía ayudar en la implementación, sin embargo, la experiencia a este momento es que los esfuerzos son sumamente altos para poder cumplir con los hallazgos, sin tener la certeza clara de que vaya a cumplir a cabalidad. Sumado al interés institucional por eventualmente adquirir un sistema Financiero Contable que cumpla con las NICSP, así como un sistema de recursos humanos orientado al cumplimiento de la política salarial que se está proponiendo desde el CONARE y al ser ambos sistemas dos de los principales que se encuentran en la plataforma del AS400, no se considera factible la implementación por el esfuerzo que implica y por ser parte de los sistemas involucrados que están propensos a sustituirse. Dado lo anterior, se estará proponiendo a la administración, que la solución a los hallazgos se realice fundamentado en que lo que menciona el documento de Responsabilidades de las Áreas Usuarias de la DTIC con fecha 31 de mayo del 2017, el cual indica que los usuarios líderes de servicio son los responsables de la "definición del rol de cada usuario operativo". Debido a esto, deberían ser dichos usuarios líderes de servicio los responsables de contar con un registro o control actualizado de los permisos de acceso y roles que tramitan para

	los sistemas a su cargo. Según lo anterior, ya se ha discutido cómo dar atención a las recomendaciones del hallazgo y se ha planteado cómo llevar a cabo las actividades, por ende, el hallazgo se considera en proceso de atención.
HALLAZGO 07: DEBILIDADES EN LA DEFINICIÓN Y ADMINISTRACIÓN DE ACUERDOS DE SERVICIO. RIESGO BAJO.	
RECOMENDACIONES	*A la Dirección de Tecnologías de Información y Comunicaciones (DTIC):* 1. Elaborar los OLAs faltantes para los servicios de TI con mayor prioridad. Se recomida que todos los servicios de TI cuenten con un OLA asociado. 2. Cumplir con la fecha establecida (septiembre 2022) para la ejecución de las actividades relacionadas. 3. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT. *A la Oficina de Contratación y Suministros en coordinación con la DTIC* 1. Revisar los SLAs con proveedores de TI y ajustarlos según las necesidades y normativa vigente.
COMENTARIOS DE LA ADMINISTRACIÓN	De momento no se cuenta con evidencias. Se ha iniciado con el abordaje de la concepción de los Servicios de TI para posteriormente abordar los SLA y los OLA's que correspondan.
ESTADO	**EN PROCESO** De la evidencia obtenida sobre los acuerdos de servicio, se observa el avance para la identificación de los diferentes servicios de TI y la elaboración del catálogo de servicios esto mediante el documento Gestión y Catálogo de Servicios de TI y propuesta de servicios de TI.
HALLAZGO 08: CUMPLIMIENTO PARCIAL DEL PLAN DE RESPALDOS DEL CENTRO DE DATOS. RIESGO BAJO.	
RECOMENDACIONES	*A la Dirección de Tecnologías de Información y Comunicaciones (DTIC):*

	1. Cumplir con la fecha de inicio establecida para las revisiones a los instructivos elaborados, con la finalidad de implementarlos lo más pronto posible. 2. Llevar un control de las revisiones y actualizaciones realizadas a los instructivos. 3. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	En el Anexo No. 2 del oficio DTIC-2022-195 se detallaron las acciones realizadas para dar como IMPLEMENTADA.
ESTADO	**EN PROCESO** Según se indica en la *nota 144-2022 Anexo No. 2* Comentarios adicionales por hallazgo: "Al respecto se ha generado el documento "IUNED DTIC-UIT 01.02", en mayo del 2022 fue remitido mediante oficio CPPI-068-2022 al Consejo de Rectoría (CONRE) para su aprobación y el CONRE generó el acuerdo en sesión No. 2221-2022, Artículo IV, inciso 1) celebrada el 30 de mayo del 2022 (REF.: CR-2022-796). **Se está a la espera del espacio que el CONRE brindará al CPPI y la DTIC para la presentación del procedimiento y demás documentos para su aprobación**. Se detallan los documentos relacionados al hallazgo, aunque en el oficio CPPI-068-2022 involucran otros documentos • FUNED DTIC-UIT 01.02.01 Bitácora de respaldos AS 400 IUNED DTIC-UIT 01.02 • FUNED DTIC-UIT 01.02.02 Pruebas de restauración de respaldo IUNED DTIC-UIT 01.02 • IUNED DTIC-UIT 01.02 Guía de respaldos y restauraciones de centro de datos principal y alterno PUNED DTIC-UIT 01 • PUNED DTIC-UIT 01 Gestión de la infraestructura de Tecnologías de Información". Fue posible identificar dentro de la evidencia la documentación indicada, sin embargo tal como indica el comentario, se está la espera de aprobación, por lo tanto el hallazgo se mantiene en proceso.
HALLAZGO 09: DEBILIDADES EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. RIESGO BAJO.	
RECOMENDACIONES	*A la Dirección de Tecnologías de Información y Comunicaciones (DTIC):* 1. Elaborar un plan para llevar a cabo lo siguiente:

	a. Contextualización clara y completa de los requerimientos y mecanismos sobre la seguridad que deben ser atendidos e implementados en el software de aplicación, entre estos, los dirigidos a pistas de auditoría, definidos y valorados tanto por instancia técnica como usuaria. b. La definición, establecimiento y valoración de las reglas, parámetros o requerimientos de calidad que debe cumplir el software de aplicación. c. La valoración periódica de la suficiencia y eficiencia de los controles de acceso implementados en el software de aplicación, desarrollado tanto a nivel interno como externo. d. La atención de incidentes y anomalías en materia de seguridad de las tecnologías de la información, en el cual se plasme el proceder y trámite de los presuntos casos de uso irregular por parte de los usuarios del software de aplicación. Para esta acción debe solicitarse la asesoría de la Oficina Jurídica. 2. Establecer una nueva fecha para llevar a cabo la implementación de las recomendaciones. 3. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	Dentro del procedimiento de desarrollo y mantenimiento de sistemas de información mediante el marco de trabajo ágil SCRUM (que está en etapa de revisión con el CPPI), como parte de los criterios de la definición de Hecho o Terminado del incremento de valor de un producto de software, se estableció el ítem referente a "Cumple con Guía de seguridad para implementaciones de software" en el documento Anexo-Definición de terminado.docx. Dicha guía es la que clasificará todos los requerimientos en materia de seguridad entre los cuales se han identificado los siguientes subtemas: mejores prácticas de OWASP, implementación de pistas de auditoría, manejo de usuarios, roles y contraseñas e instructivo para encriptación de información. En cuanto a controles de calidad se han definido los indicadores claves de rendimiento para dos de los flujos de valor de la unidad de sistemas de información, tomando en cuenta la normativa vigente.
ESTADO	**EN PROCESO**

	Además de lo indicado en el comentario de administración, a través de la *nota 144-2022 Anexo No.2* se amplía indicando que: Para los 4 aspectos detallados en el punto 1 de este hallazgo, gracias a los esfuerzos que se están haciendo por medio del establecimiento del marco de trabajo ágil, el planteamiento del Sistema de Gestión de la Calidad, así como otros documentos que han trabajado en conjunto la Unidad de Seguridad Digital (USD) y la Unidad de Sistemas de Información (USI) de la DTIC, se estima que la fecha de implementación de las recomendaciones de dicho hallazgo es junio 2023 Según lo anterior, ya se han realizado acciones que contribuyen a la atención de las recomendaciones, entre ellas fue posible validar avances sobre el Sistema de Gestión de la Calidad. Dado lo anterior, el estado del hallazgo se establece como en proceso.
HALLAZGO 10: DEBILIDADES EN LA GESTIÓN DE LA CONTINUIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN. RIESGO MEDIO.	
RECOMENDACIONES	*A la Vicerrectoría de Planificación (VP:)* 1. A nivel institucional debe realizarse un análisis detallado de sus procesos críticos, de forma tal que pueda identificarse además de su nivel de dependencia de las tecnologías de información para su operación, las acciones a seguir en caso de no disponer de dichos recursos y mientras estos son restablecidos. Con la información resultante, se debe generar un plan de continuidad de la operativa institucional, al cual se alineará el plan de contingencias y recuperación ante desastres establecido por la DTIC. 2. Seguir la hoja de ruta establecida para subsanar las debilidades encontradas con respecto a la continuidad y establecer una fecha límite para la actualización del plan y elaboración de documentos. 3. En caso de requerir información o participación de otras áreas, programas o vicerrectorías para cumplir con las recomendaciones, coordinar con los lideres de cada una. 4. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.

	A la Dirección de Tecnologías de Información y Comunicaciones (DTIC): 1. Colaborar en las situaciones en que se requiera información, participación o asesoría técnica para cumplir con las recomendaciones y subsanar las debilidades encontradas.
COMENTARIOS DE LA ADMINISTRACIÓN	En el Anexo No. 2 del oficio DTIC-2022-195, se indicó que se ha estado realizando una labor de manera conjunta con la Vicerrectoría de Planificación y es importante que realicen la consulta a la persona que está coordinando esta labor Carlos Montoya Rodríguez <cmontoya@UNED.AC.CR>.
ESTADO	**EN PROCESO** Se obtuvo evidencia del avance en la actualización del nuevo Plan de Continuidad, que incluye la propuesta inicial del BIA junto con un análisis preliminar, además, la propuesta inicial sobre política de continuidad para la UNED la cual fue revisada y discutida entre las partes involucradas como lo son: Coordinador del Equipo Técnico Asesor en GRD (Gestión del Riesgo de Desastres) y Coordinadora del Programa de Control Interno (PROCI) para su respectivo análisis y consolidación de los esfuerzos de tal forma, que la Institución cuente con una única Política de gestión del Riesgo que abarque el ámbito de continuidad y considere además, la política ya existente y aprobada de GRD.
HALLAZGO 11: DEBILIDADES ENCONTRADAS EN ALGUNOS DE LOS SISTEMAS DE INFORMACIÓN DE LA UNED. RIESGO BAJO.	
RECOMENDACIONES	*A las Áreas Dueñas de los Procesos Asociados:* 1. Continuar aplicando las mejoras correspondientes que ayuden a subsanar las debilidades encontradas en el hallazgo expuesto. 2. Cumplir con las fechas establecidas para finalizar la implementación de las mejoras en los sistemas mencionados. *A la Dirección de Tecnologías de Información y Comunicación (DTIC):*

	1. Colaborar en las situaciones en que se requiera su participación en la implementación de las mejores a los sistemas.
COMENTARIOS DE LA ADMINISTRACIÓN	En el Anexo No. 2 del oficio DTIC-2022-195, se indicó respecto a este hallazgo que de momento no hay acciones a realizar por parte de la DTIC, y a la fecha se mantiene, ya que, no existen requerimientos por parte de los usuarios líderes de servicios involucrados.
ESTADO	**EN PROCESO** Además de lo indicado en el comentario de administración, a través de la *nota 144-2022 Anexo No.2* se menciona; "Respecto a este hallazgo, de momento no existen acciones a realizar por parte de la DTIC. Se está a la espera de que los usuarios líderes de servicios involucrados generen los requerimientos que correspondan". Dado lo anterior el hallazgo sigue en proceso mientras las Áreas Dueñas de los Procesos asociados sigan aplicando las mejoras correspondientes y finalicen la implementación de las mejoras en los sistemas.
Otros hallazgos	
CG-TI-UNED-1-2019-DECISIONES SOBRE ASUNTOS ESTRATÉGICOS	
RECOMENDACIONES	2. Actualización del Reglamento de la Comisión Estratégica de TIC, con la inclusión de la periodicidad de sesiones, así como la gestión de documentación, aprobación y resguardo de las actas/minutas de cada sesión.
COMENTARIOS DE LA ADMINISTRACIÓN	Se dio respuesta en oficio DTIC-2022-076 anexo No. 2 Esto no compete a la DTIC. En la Carta de Gerencia CG-TI-2019 indica que el responsable de dicha recomendación es la CETIC. Adicionalmente en la Carta de Gerencia CG-TI-UNED-2020 se detalla como ATENDIDA.
ESTADO	**CORREGIDO**

	Se valida lo expuesto en el comentario de administración, el hallazgo se da por corregido.
CG TI 2015-01 HALLAZGO 20: DEFICIENCIAS EN LOS CONTROLES IMPLEMENTADOS PARA LA GESTIÓN DE LAS CUENTAS DE USUARIOS A NIVEL DE ACTIVE DIRECTORY Y BASES DE DATOS.	
RECOMENDACIONES	2. Revisar las cuentas genéricas activas en el directorio de usuarios y valorar la desactivación de las mismas para los casos en que no se usen o no se necesiten. Para los casos requeridos (son necesarias las cuentas genéricas) se debe de contar con la autorización y documentación correspondiente.
COMENTARIOS DE LA ADMINISTRACIÓN	Se dio respuesta en oficio DTIC-2022-195 anexo No. 2 que en la CG-TI-2021 indica respecto a este Hallazgo CORREGIDO, por lo tanto, no hay más acciones que realizar.
ESTADO	**CORREGIDO** Se valida lo expuesto en el comentario de administración, el hallazgo se da por corregido.
CG1-2021-HALLAZGO 8: LA CUENTA DE DESARROLLO DE SISTEMAS AMI REGISTRA SOFTWARE EN DESARROLLO CON UNA ANTIGUEDAD IMPORTANTE Y SIN MOVIMIENTO CON RESPECTO AL PERIODO ANTERIOR. **CG2-2021-HALLAZGO 9: LA CUENTA DE DESARROLLO DE SISTEMAS AMI REGISTRA SOFTWARE EN DESARROLLO CON UNA ANTIGÜEDAD IMPORTANTE Y SIN MOVIMIENTO CON RESPECTO AL PERIODO ANTERIOR.**	
RECOMENDACIONES	Es necesario realizar un análisis y seguimiento de las partidas existentes registradas en la cuenta de desarrollo de sistemas al 31 de diciembre de 2021 y definir la unidad responsable de brindar ese seguimiento y que remita los informes correspondientes a la Unidad de Contabilidad que permita dar de baja, ajuste por liquidación o la reclasificación como activo en uso.
COMENTARIOS DE LA ADMINISTRACIÓN	De parte de la DTIC se generó el oficio DTIC-2023-009 el 07 de febrero del 2023 con la información detallada y requerida por la Oficina de Contabilidad para lo correspondiente.

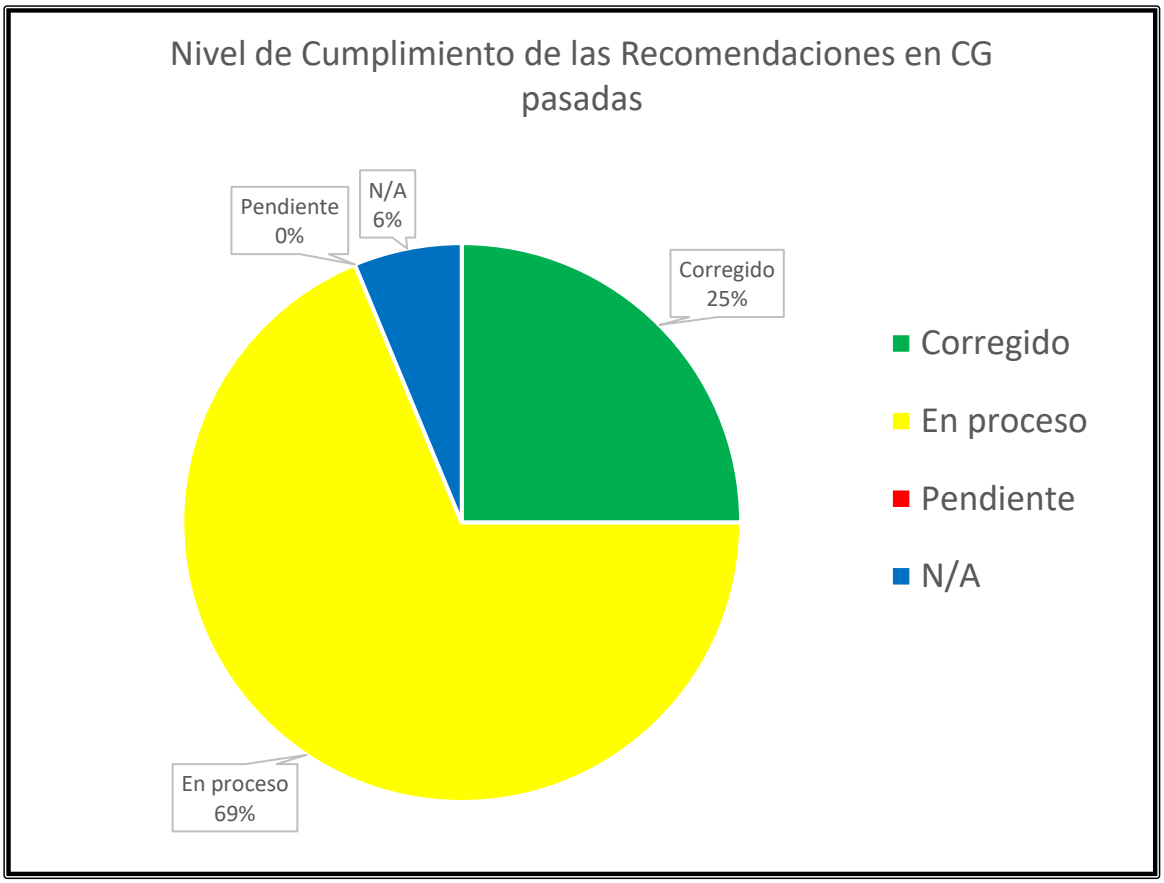
ESTADO	**EN PROCESO** Se adjuntó el DTIC-2023-147 que comunica a la Oficina de Contabilidad General las fechas recibido de Sistemas de Información AMI. El hallazgo queda en proceso hasta que por parte de la Oficina de Contabilidad se comunique oficialmente la atención brindada; dar de baja, ajustar por liquidación o reclasificar como activo en uso.
CG-TI-UNED-1-2019 -INDEPENDENCIA Y RECURSOS HUMANOS DE LA FUNCIÓN DE TI	
RECOMENDACIONES	1. Contar con planes actualizados de capacitación y ejecutarlo en forma oportuna (durante el período de formulación), de forma que los funcionarios puedan actualizar y aplicar sus conocimientos en forma efectiva y oportuna. (El plan de capacitación debe reflejar las necesidades reales y vigentes de actualización para los funcionarios de la DTIC en períodos más cortos (un año máximo) y debe procurarse en el presupuesto las partidas que permitan su ejecución oportuna.)
COMENTARIOS DE LA ADMINISTRACIÓN	Se dio respuesta en oficio DTIC-2022-195 anexo No. 2. Reportado en la CG-TI-UNED-1-2020 como ATENDIDA.
ESTADO	**CORREGIDO** Se valida lo expuesto en el comentario de administración, el hallazgo se da por corregido.
CG 2010-01-OPORTUNIDAD DE MEJORA 6: MEJORAR LAS POLÍTICAS DE SEGURIDAD DE INFORMÁTICA EN LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (DTIC) DE LA UNED.	
RECOMENDACIONES	Definir, implantar y documentar las políticas necesarias para la seguridad de la información, tomando en cuenta tópicas como calidad, seguridad, confidencialidad, controles internos. Además, se deben de definir responsables para la administración de las políticas, se debe de definir la frecuencia de revisión y actualización de las políticas e indicadores de cumplimiento, entre las políticas que se recomiendan definir están: - Política para el tratamiento de los riesgos de seguridad. (Este punto ya fue ejecutado con la Estructura de

	Riesgos) - Política para la organización de la seguridad de la información. - Política para clasificación de la información. - Política para el intercambio de información. - Política para el reporte de eventos en la seguridad de la información. - Política para la administración de medios removibles. - Política para la administración de la seguridad física. - Para la elaboración de esta tarea se recomienda utilizar como referencia la norma ISO 27002 de seguridad de la información.
COMENTARIOS DE LA ADMINISTRACIÓN	Tal y como se indica en el Oficio DTIC-2022-195, esta OPORTUNIDAD no se refleja en la Carta de Gerencia TI del periodo 2021. Es importante al respecto que se defina las acciones.
ESTADO	**NO APLICA** Para el periodo auditado del 2021 este hallazgo no fue identificado dentro de la evidencia en su momento proporcionada para realizar el seguimiento a hallazgos de periodos anteriores, por ende, no se refleja en el Carta de Gerencia TI 2021, sin embargo, para el actual periodo auditado (2022) desde Control Interno hicieron llegar a esta auditoría externa un registro de hallazgos pendientes y en proceso de atención, dentro de los cuales se encuentra este hallazgo, y se procedió a darle seguimiento. Dado lo anterior se validó el hallazgo en cuestión, obteniéndose lo siguiente: A nivel de seguridad de la información se cuenta con un Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones, un reglamento para uso de equipos de cómputo e internet, normas sobre el uso del correo electrónico en la UNED y la Política de seguridad aprobada según acuerdo del Consejo de Rectoría Sesión No. 1160-2000. Actualmente se está trabajando en la Política de Seguridad de la Información y Ciberseguridad, sin embargo, la misma no ha sido aprobada por las autoridades universitarias, como evidencia se adjuntó el borrador “Política de Seguridad de la Información y Ciberseguridad V1.0.docx”, dicha política considera un apartado de políticas de seguridad a la información sobre las siguientes áreas: • Aspectos organizativos de la seguridad de la información

	• Gestión de activos • Gestión de accesos • Uso de criptografía • Seguridad física y ambiental • Seguridad operativa • Seguridad en las telecomunicaciones • Desarrollo y mantenimiento seguro • Relaciones con los proveedores • Gestión de incidentes de ciberseguridad y seguridad de la información • Gestión de la continuidad de negocio Lo anterior evidencia que la DTIC sí cuenta con lineamientos para gestionar la seguridad de la información, y en el caso de la política borrador en la que se está trabajando, esta abarca más temáticas que las recomendadas en este hallazgo. Cabe indicar que durante la revisión de la evidencia asociada a la seguridad de la información se indicó que "La UNED cuenta e implementa una gestión de riesgos, **pero no incorpora la seguridad de la información**", pero para este caso se emite un nuevo hallazgo el cual no solo considera recomendaciones asociadas a la gestión de riesgos en materia de seguridad, sino que también expone otras recomendaciones que ayuden a fortalecer la Política de Seguridad de la Información y Ciberseguridad en la que se está trabajando (véase en la sección HALLAZGOS Y RECOMENDACIONES). Considerando lo anterior y la fecha del hallazgo en cuestión (la cual tiene más de 10 años), este hallazgo queda como no aplicable ya que se incorpora uno nuevo para el periodo auditado.

A continuación, se resume el estado sobre el cumplimiento de las recomendaciones emitidas en informes de auditorías anteriores de manera gráfica:

ESTADO	2010	2015	2019	2021	TOTAL
CORREGIDO	0	1	2	1	**4**
PROCESO	0	0	0	11	**11**
PENDIENTE	0	0	0	0	**0**
N/A	1	0	0	0	**1**
TOTAL	**1**	**1**	**2**	**11**	**16**



IV. APÉNDICES

Apéndice 01: Análisis de Riesgos en la gestión de T.I.

Dirección de Tecnologías de Información y Comunicaciones UNED

Periodo 2022

Tipos de Riesgo	
ALTO	A
MEDIO	M
BAJO	B

Alto ☑	Requiere una atención inmediata por su impacto en seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. No se han establecido controles en este nivel de riesgo.
Medio ☑	Requiere una atención intermedia ya que su impacto representaría riesgos sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles insuficientes en este nivel de riesgo.
Bajo ☑	Requiere una atención no prioritaria ya que su impacto no es directamente sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles adecuados en este nivel de riesgo.

PLANIFICACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

A. PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
A.1.	Se tiene definido un plan estratégico de TI formalmente aprobado y alineado a los objetivos organizacionales.		✓	Se cumple con la condición.	B
A.2.	Se le da seguimiento al PETI por parte del Comité de TI.		✓	Se cumple con la condición.	B
A.3.	Se define anual un plan anual operativo de TI con los proyectos y actividades que realiza el área de TI y se encuentra alineado a las iniciativas y objetivos del PETI.		✓	Se cumple con la condición.	B
A.4.	Se le da seguimiento periódico al cumplimiento del PAO.		✓	Se cumple con la condición.	B

B. GESTIÓN DE LA ARQUITECTURA DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
B.1.	Se cuenta con un modelo de arquitectura de información formalmente establecido y aprobado.		✓	Se cumple con la condición.	B
B.2.	Se le realizan revisiones anuales al modelo de arquitectura para garantizar su actualización de acuerdo con los cambios generados a nivel organizacional.		✓	Se cumple con la condición.	B

C. GESTIÓN DEL RECURSO HUMANO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
C.1.	Se cuenta con un plan de capacitaciones formalmente establecido.		✓	Se cumple con la condición.	B
C.2.	Las capacitaciones se encuentran justificadas (proyectos de TI, evaluaciones del desempeño).		✓	Se cumple con la condición.	B

D. GESTIÓN DE PROVEEDORES DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
D.1.	Se establecen contratos formales para los servicios que son brindados por terceros.		✓	Se cumple con la condición.	B
D.2.	Se realiza un seguimiento al cumplimiento contractual de las responsabilidades de los proveedores.		✓	Se cumple con la condición.	B

E. GESTIÓN DE LA CALIDAD DE LOS SERVICIOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
E.1.	Se cuenta con una política, metodología o procedimiento para la gestión de la calidad de los servicios de TI.	✗		Existe, pero aún no se indica que está validada por el director.	B
E.2.	La normativa y demás documentación de TI es revisada y actualizada periódicamente.		✓	Se cumple con la condición	B

F. GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
F.1.	Se tiene una metodología formalmente establecida y aprobada para la gestión de riesgos de TI.		✓	Se cumple con la condición	B
F.2.	La evaluación de riesgos de TI es periódica y se encuentra revisada y aprobada por la administración (de acuerdo con el nivel de tolerancia al riesgo organizacional).		✓	Se cumple con la condición	B

G. GESTIÓN DE ACUERDOS DE NIVEL DE SERVICIO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
G.1.	Se cuenta con un catálogo de servicios de TI actualizado y aprobado por el Comité de TI.		✓	Se cumple con la condición	B
G.2.	Se cuenta con una política o procedimiento para la gestión de los acuerdos de nivel de servicio (SLAs) de TI.	✗		Actualmente se encuentra en proceso de desarrollo.	M
G.3.	Se tiene definido acuerdos de nivel de servicio para cada uno de los servicios activos que se encuentran definidos en el catálogo.	✗		Actualmente no disponen de SLAs pero están en proceso de desarrollo.	M
G.4.	Cada uno de los SLAs tiene establecido las responsabilidades de las partes, indicadores (disponibilidad, capacidad, confiabilidad, etc.) y requerimientos de soporte.	✗			M
G.5.	Se verifica el cumplimiento, validez y actualización de los SLAs establecidos con las áreas usuarias de manera periódica.	✗			M

IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

H. GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
H.1.	Se cuenta con una metodología para la gestión de proyectos de TI formalmente establecida.		✓	Se cumple con la condición.	B
H.2.	Se documenta cada una de las fases del ciclo de vida del proyecto para cada uno de los proyectos ejecutados por el área de TI (constitución, estimación de recursos, responsabilidades, cronograma, desempeño, riesgos, calidad, cambios y cierre del proyecto.)		✓	Se cumple con la condición.	B

I. GESTIÓN DE DESARROLLOS DE SOFTWARE.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
I.1.	Se cuenta con una metodología para el desarrollo e implementación del software.		✓	Si se cuenta con una metodología para el desarrollo e implementación del software. Actualmente está vigente el MANUAL DE GESTIÓN DE TI que es el que está aprobado y que utiliza un conjunto de plantillas. Adicionalmente está en construcción el nuevo procedimiento de la Unidad de Sistemas de Información PUNEDDTIC-USI 01ProcedimientoDesyMante-sistemasinformación (003) - febrero2023.docx, labor que se está realizando con conjunto con el CPPI y que estaría reemplazando parte del MANUAL DE GESTIÓN DE TI (Una vez que todas las unidades cuenten con sus procedimientos, el MANUAL DE GESTIÓN DE TI es derogado).	B

J. GESTIÓN DE LA CAPACIDAD Y DISPONIBILIDAD.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
J.1.	Se cuenta con una política para la gestión de la capacidad y disponibilidad de la plataforma tecnológica.	✗		No disponen de una política o plan para gestionar la capacidad y disponibilidad, este será abordado en el 2023.	M
J.2.	El equipo de TI es monitoreado periódicamente.		✓	Se cumple con la condición.	B

K. GESTIÓN DE ACTIVOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
K.1.	Se mantienen controles para el ingreso y salida de equipo tecnológico a la organización.		✓	Si se aplica un control para ingreso y salida de equipo tecnológico a la organización, no se hace distinción como tal que sea tecnológico, ya que, se debe realizar para todo activo que salga de la Institución.	B
K.2.	Se mantiene un inventario actualizado de las licencias de software, así como un catálogo de software permitido en la organización.	✗		Se adjuntaron formularios del periodo 2022 donde se otorgó el criterio técnico de la DTIC para lo que corresponde a software (programas) especializados, es algo nuevo que se está incorporando. El procedimiento como tal está en el CONRE en espera de aprobación.	M

SOPORTE Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN.

L. GESTIÓN DE INCIDENTES.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
L.1.	Se cuenta con un procedimiento para la gestión de incidentes de TI.		✓	Se cumple con la condición.	B
L.2.	La gestión de incidentes se mantiene centralizada (mesa de servicios).		✓	Se cumple con la condición.	B

M. GESTIÓN DE PROBLEMAS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
M.1.	Se cuenta con un procedimiento para la gestión de problemas de TI.		✓	Se cumple con la condición.	B
M.2.	Se identifica, clasifica y analiza la causa raíz de los problemas de TI.		✓	Se cumple con la condición.	B

O. GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
O.1.	Se cuenta con un plan de continuidad del negocio (con el componente de TI), formalmente establecido y aprobado por la administración o el Comité de TI.		✓	Se cumple con la condición.	B
O.2.	Se realizan pruebas y capacitaciones sobre el plan de continuidad del negocio.	✗		Actualmente el plan de continuidad se encuentra en proceso de actualización, por lo cual no han realizado pruebas ni capacitaciones sobre este.	M

O.3.	Se cuenta con una política y/o procedimiento para la realización de respaldos de información.		✓		B
O.4.	Se realizan pruebas a los respaldos de información.		✓		B
O.5.	Se tienen medidas de seguridad para los respaldos de información (acceso restringido, traslado de respaldos a un sitio externo).		✓		B
O.6.	Se cuenta con redundancia de equipos que soportan los servicios críticos (servidores, equipo de comunicación, enlaces a redes externas).		✓		B

P. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
P.1.	Se cuenta con una política de seguridad de la información formalmente aprobado por la administración y divulgado a nivel organizacional.	✗		Se cuenta con la Política de Seguridad de la Información y Ciberseguridad V1.0 (PUNED DTIC-USD 01), sin embargo, no ha sido aprobada por las autoridades universitarias.	M
P.2.	Se cuenta con una política de uso de recursos de TI (correo electrónico, equipos, red).	✗			M
P.3.	Se cuenta con una política y/o procedimiento para la gestión de cuentas de usuario.	✗			M
P.4.	Se inhabilitan las cuentas de los usuarios que cesan funciones en la organización (despidos, renuncias, jubilaciones, vacaciones, permisos, etc.).		✓	Se cumple con la condición.	B

EVALUACIÓN DE TECNOLOGÍAS DE INFORMACIÓN.

Q. VALORAR EL CONTROL INTERNO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
Q.1.	Se han establecido normas para la evaluación del control interno de TI.		✓	Se cumple con la condición.	B
Q.2.	Se realizan autoevaluaciones periódicas para que TI identifique de manera proactiva las debilidades de control.		✓	Se cumple con la condición.	B
Q.3.	Se ejecutan estudios de auditoría periódicos (internos o externos) para identificar debilidades en el cumplimiento de obligaciones con normativas relativas a TI.		✓	Se cumple con la condición.	B

--Fin del documento--