Crowe Horwath CR, S.A.

Universidad Estatal a Distancia (UNED)

Informe sobre sistemas de tecnología de información

Al 31 diciembre de 2023

Universidad Estatal a Distancia (UNED)

Sistema de tecnología de información

Índice

Página

Crowe Horwath CR, S.A.
2442 Avenida 2
Apdo. 7108-1000
San José, Costa Rica
Tel + (506) 2221 4657
Fax + (506) 2233 8072
www.crowe.cr

19 de julio de 2024

Señores
Consejo Universitario
Universidad Estatal a Distancia (UNED)
Atención: Rodrigo Arias Camacho
Rector y presidente

ASUNTO: INFORME DE CONTROLES DE TECNOLOGIA DE INFORMACION

Al revisar los Sistemas de Información de Universidad Estatal a Distancia (UNED), como parte de la auditoría de los estados financieros al 31 de diciembre de 2023, observamos asuntos relacionados con los sistemas de información y procesos de TI, sobre los cuales preparamos las conclusiones en el informe con fecha de corte al 31 de diciembre de 2023. Este informe se estructura como resultado del cumplimiento de las NIA 315 y 330; no es ni debe interpretarse como una auditoría externa de la Dirección de Tecnología de Información de forma específica.

Al planear y ejecutar la revisión evaluamos la estructura de control interno existente y aplicamos pruebas selectivas de cumplimiento, con el fin de determinar el alcance de los procedimientos de auditoría para expresar opinión sobre los estados financieros al 31 de diciembre de 2023, y no para opinar sobre la estructura de control interno o los sistemas de información en su conjunto.

Es necesario señalar que nuestra evaluación es limitada para efectos de una revisión de controles generales, por lo que una revisión más detallada de controles de aplicación podría revelar más oportunidades de mejora de las que incluye este informe.

En este informe se incluyen comentarios de la Administración que no modifican las revelaciones ni el criterio expresado y no son parte integral de los hallazgos.

Los temas tratados no se refieren a empleados en particular y tienen por objeto plantear medidas para fortalecer los controles internos sobre los sistemas de información.

Nuestra responsabilidad sobre el informe de sistemas de tecnología de información al 31 de diciembre de 2023 se extiende hasta el 19 de julio de 2024. La fecha del informe de auditoría indica al usuario de éste, que el auditor ha considerado el efecto de los hechos y de las transacciones de los que ha tenido conocimiento y que han ocurrido hasta dicha fecha; en consecuencia, no se amplía por la referencia de la fecha en que se firme digitalmente.

Atentamente,

FABIAN ZAMORA AZOFEIFA (FIRMA)
Firmado digitalmente por FABIAN ZAMORA AZOFEIFA (FIRMA)
Fecha: 2024.07.24 12:03:59 -06'00'

Fabián Zamora Azofeifa
Socio

Nombre del CPA: FABIAN ZAMORA AZOFEIFA
Carné: 2186
Cédula: 302870450
Nombre del Cliente: Universidad Estatal a Distancia
Identificación del cliente: 4000042151
Dirigido a: Universidad Estatal a Distancia
Fecha: 24-07-2024 10:27:34 AM
Tipo de trabajo: Sistemas de tecnología de información
Timbre de ¢25 de la Ley 6663 adherido y cancelado en el original.

FABIAN ZAMORA AZOFEIFA
Contador Público Autorizado No. 2186
COSTA RICA

COSTA RICA TIMBRE
25 COLONES 25

Código de Timbre: CPA-25-340670

c.c. Comité de Tecnología de Información

Universidad Estatal a Distancia (UNED)

Sistema de tecnología de información

I. Resumen ejecutivo

Como parte del trabajo de la auditoría de estados financieros al 31 de diciembre de 2023 se llevó a cabo la evaluación de controles generales a los Sistemas de Información de la Universidad Estatal a Distancia (UNED), se basó en el cumplimiento de la Norma Internacional de Auditoría 315, "Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y su entorno", la Norma Internacional de Auditoría 330 "Procedimientos del auditor en respuesta a los riesgos evaluados", marco normativo para TI y no es ni debe interpretarse como una auditoría de los sistemas de información, ni de la Dirección de Tecnologías de Información de la UNED.

En la Carta de Gerencia relacionada con la auditoría financiera y ejecución presupuestaria del periodo se han comunicado riesgos y recomendaciones que son vinculantes y deben ser revisados de forma integral con los resultados de este informe.

El Marco de Gobierno y Gestión de TI se encuentra aprobado, declarado y divulgado tomando como referencia diferentes marcos de la industria como COBIT 2019, ITIL, las Normas Técnicas del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) para la gestión y control de las Tecnologías de la Información, así como las mejores prácticas de la industria. El propósito de este marco es preservar la autonomía institucional.

En el periodo de evaluación, se realiza la revisión para los siguientes módulos de los sistemas de información Contable y de Recursos Humanos:

Sistema Financiero-Contable:

- ✓ Activos Fijos
- ✓ Adelanto y Liquidación de Viáticos
- ✓ Contabilidad General
- ✓ Control de presupuesto
- ✓ Cuentas por cobrar
- ✓ Cuentas por pagar
- ✓ Devoluciones a estudiantes
- ✓ Fondos de trabajo y Caja Chica
- ✓ Ingresos
- ✓ Movimientos bancarios
- ✓ Presupuesto
- ✓ Relación de puestos
- ✓ Sistema de Facturación
- ✓ Sistema de Facturación de Librería
- ✓ Sistema de Inventarios

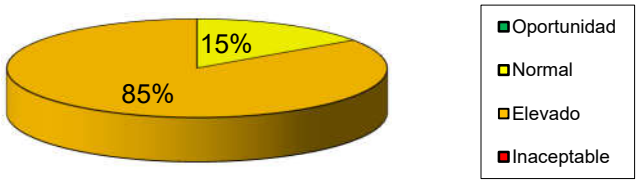
Recursos humanos

- ✓ Pago de Liquidaciones (AS-400)
- ✓ Sistema de Honorarios (AS-400)
- ✓ Sistema de planillas (AS-400)
- ✓ Sistema de pago de salarios

Entre las pruebas de auditorías se realizaron entrevistas con los usuarios y lideres de los sistemas mencionados, en donde se identifican observaciones que se detallan en la sección "D. Gestión de sistemas de información" de este informe y adicionalmente se ejecutó una encuesta con 8 preguntas para cada módulo de los sistemas Financiero- Contable y de Recursos humanos, estos resultados se visualizan en el Anexo #1 de este documento.

En la evaluación del área de TI se comunican trece observaciones del periodo 2023, de acuerdo con la naturaleza del riesgo representan 15% de riesgo normal y 85% de riesgo elevado. Se mantienen 7 observaciones de seguimiento de la carta anterior en proceso de atención[1].

Oportunidades de mejora UNED



En la sección de conclusiones de este informe se indican las observaciones identificadas.

II. Objetivo

Evaluar el cumplimiento de requerimientos de seguridad y control en Tecnología de Información (TI) en Universidad Estatal a Distancia (UNED) de acuerdo con las Normas Internacionales de Auditoría 315 y 330, el marco normativo interno y las buenas prácticas de control para gobierno y control de TI.

III. Alcance

El alcance incluyó aspectos relacionados con la gestión de control y sistemas de información de la UNED respecto a la elaboración de procedimientos y aplicación de controles que fortalezcan la seguridad, integridad, funcionalidad y precisión de los procesos de gestión del área de TI, gestión de la seguridad de la información, gestión de riesgos de TI, gestión de los sistemas de información, gestión de la continuidad y seguimiento de observaciones anteriores; el informe no es ni debe tomarse como una auditoría de los sistemas de información.

[1] No se encuentran incluidas las observaciones de seguimiento en la gráfica.

IV. Periodo de la evaluación

La evaluación se realizó durante los meses de marzo, abril y mayo de 2024.

V. Procedimientos

A partir del alcance se elaboraron y utilizaron instrumentos para recopilar la información referente al alcance indicado; entre estos, entrevistas, cuestionarios, revisión documental, inspección física, levantamiento de minutas, selección de muestras y verificación de la funcionalidad de los sistemas.

Entre los temas evaluados en cada área se indican las observaciones encontradas.

VI. Criterios de evaluación

De acuerdo con la evaluación de control interno del área de TI y con base en el riesgo que representan para los recursos de TI (aplicaciones, información, infraestructura y personas), se presenta el mapa de riesgos que resume la relación entre el impacto para la organización y la posibilidad de materialización del riesgo que garanticen la alineación con los criterios de información (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad).

Los niveles de cumplimiento se describen a continuación:

Cumple	La entidad muestra desempeño adecuado respecto al factor evaluado.
Cumplimiento parcial alto	La entidad muestra algunas deficiencias, pero en general el desempeño respecto al factor evaluado es satisfactorio.
Cumplimiento parcial bajo	La entidad muestra débil desempeño respecto al factor evaluado.
No cumple	La entidad muestra desempeño crítico respecto al factor evaluado, por lo que no es aceptable clasificarlo en ninguno de los tres niveles anteriores.

Las categorías de riesgos se describen a continuación[2]:

Nivel de riesgo	Descripción
Inaceptable	Se estima que este nivel de riesgo es mucho más allá de su riesgo tolerable; cualquier riesgo que se encuentre en esta clasificación puede desencadenar una respuesta inmediata al riesgo.
Elevado	Riesgo elevado, por encima del riesgo tolerable; la entidad puede, como política interna, mitigar el riesgo u otra respuesta adecuada definida dentro de un tiempo límite.
Normal	Nivel aceptable de riesgo, por lo general sin realizar una acción en especial excepto para el mantenimiento de los actuales controles u otras respuestas.
Oportunidad	Nivel de riesgo muy bajo, en el cual las oportunidades de ahorro de costos pueden ser disminuir el grado de control o determinar en cuáles oportunidades pueden asumirse mayores riesgos.

El formato de este informe fue estructurado para proporcionar dos referencias específicas; Cumplimiento y Nivel de riesgo.

En la práctica el "apetito de riesgo" puede ser definido en términos de una combinación de frecuencia y magnitud de un riesgo descritos en bandas de significancia del riesgo. Hemos establecido niveles de riesgo en las bandas descritas anteriormente basándonos en la frecuencia y magnitud de los riesgos.

La frecuencia y magnitud de los riesgos no necesariamente están directamente relacionados con niveles de cumplimiento de la normativa, debido a que, aunque haya incumplimiento, el impacto que puede ocasionar y la frecuencia de veces que puede ocurrir pueden tener efecto poco significativo en el proceso de administración integral de riesgos y en las operaciones.

VII. Determinación del cumplimiento y nivel de exposición al riesgo

Para obtener el nivel de exposición al riesgo nos hemos basado en la aplicación de una matriz de 25 cuadrantes (5 verticales y 5 horizontales), en la cual el riesgo de los factores es determinado por su ocurrencia e impacto.

Para cada acción evaluada que presenta incumplimiento hemos determinado el nivel de impacto y ocurrencia y obtuvimos el nivel de exposición al riesgo basados en la matriz indicada anteriormente.

[2] Datos tomados del Manual CRISC (*Certified in Risk and Information Systems Control*), emitido por el ISACA.

La frecuencia (cuadrantes horizontales) se basa en la verificación de las siguientes categorías:

Muy baja	La probabilidad de ocurrencia es insignificante, puede ocurrir solo en circunstancias excepcionales.
Baja	Tiene poca probabilidad de ocurrencia; no se espera que ocurra en cierto periodo de tiempo.
Frecuente	El evento ocurrirá más de una ocasión en un determinado lapso.
Alta	Se espera que suceda en muchas ocasiones en un periodo de tiempo dado, en circunstancias definidas.
Muy alta	Se materializa de forma continua y ocurrirá bajo muchas circunstancias.

El impacto (cuadrantes verticales) se basa en las siguientes categorías:

Insignificante	El costo no afecta la entidad. No es necesario tomar medidas al respecto.
Mínimo	La materialización podría traer un costo para la entidad, sin embargo, no es de importancia para los resultados de la entidad. Debe valorarse los motivos de la materialización del riesgo.
Moderado	Su materialización conlleva un costo para la entidad que puede incluir pérdidas. Deben establecerse medidas de prevención para posibles eventos.
Serio	Representa un costo elevado. Las medidas que deben tomarse son correctivas y preventivas.
Crítico	El costo asumido no es tolerable y es necesario tomar medidas correctivas inmediatas.

A continuación, presentamos la matriz de 5 x 5 cuadrantes

		Frecuencia				
		Muy baja	**Baja**	**Frecuente**	**Alta**	**Muy alta**
Impacto	**Crítico**	5	10	15	20	25
	Serio	4	8	12	16	20
	Moderado	3	6	9	12	15
	Mínimo	2	4	6	8	10
	Insignificante	1	2	3	4	5

Calificaciones

Basado en los resultados de los análisis por acción se determina el nivel de exposición al riesgo de acuerdo con los siguientes rangos:

De 1 a 2: El nivel de riesgo es de oportunidad.
De 3 a 9: El nivel de riesgo es normal.
De 10 a 12: El nivel de riesgo es elevado.
De 15 a 25: El nivel de riesgo es inaceptable.

VIII. Conclusiones generales del año 2023

En cumplimiento con la NIA 260, "Comunicaciones de asuntos de auditoría con los encargados del gobierno corporativo", el auditor tiene la responsabilidad de comunicar en una auditoría de estados financieros los hechos observados relacionados con los riesgos de TI y negocio que gestiona actualmente la Administración y que son significativos y relevantes en relación con la responsabilidad de supervisión del proceso de información financiera.

Los riesgos y recomendaciones informadas en la Carta de Gerencia podrían ser vinculantes y deben ser revisados de forma integral con los resultados indicados en este informe.

Observaciones del periodo 2023

Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
A.1	Oficial de seguridad de la información	Cumplimiento parcial bajo	Moderado	Alta	Elevado
A.2	Implementar el marco de gestión de TI	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
A.3	Marco normativo para el uso de inteligencia artificial	Cumplimiento parcial alto	Moderado	Baja	Normal
B.1	Aplicación de pruebas de vulnerabilidades	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
B.2	Implementación del Sistema de Seguridad de la Información	Cumplimiento parcial bajo	Moderado	Alta	Elevado
B.3	Informe de revisión de roles y perfiles de usuario	Cumplimiento parcial bajo	Moderado	Alta	Elevado
D.1	Manuales a los sistemas sin actualizar o se carecen de los mismos	Cumplimiento parcial alto	Moderado	Alta	Elevado
D.2	Informes sobre evaluaciones a los sistemas de información	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
D.3	Sistemas sin aplicación de pruebas de continuidad	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
E.1	Plan de continuidad de negocio	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
E.2	Plan de capacitación sobre la continuidad de operaciones	Cumplimiento parcial alto	Moderado	Baja	Normal
E.3	Pruebas sobre restauración de respaldo	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
E.4	Pruebas de continuidad de negocio	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

Seguimiento de observaciones de periodos anteriores

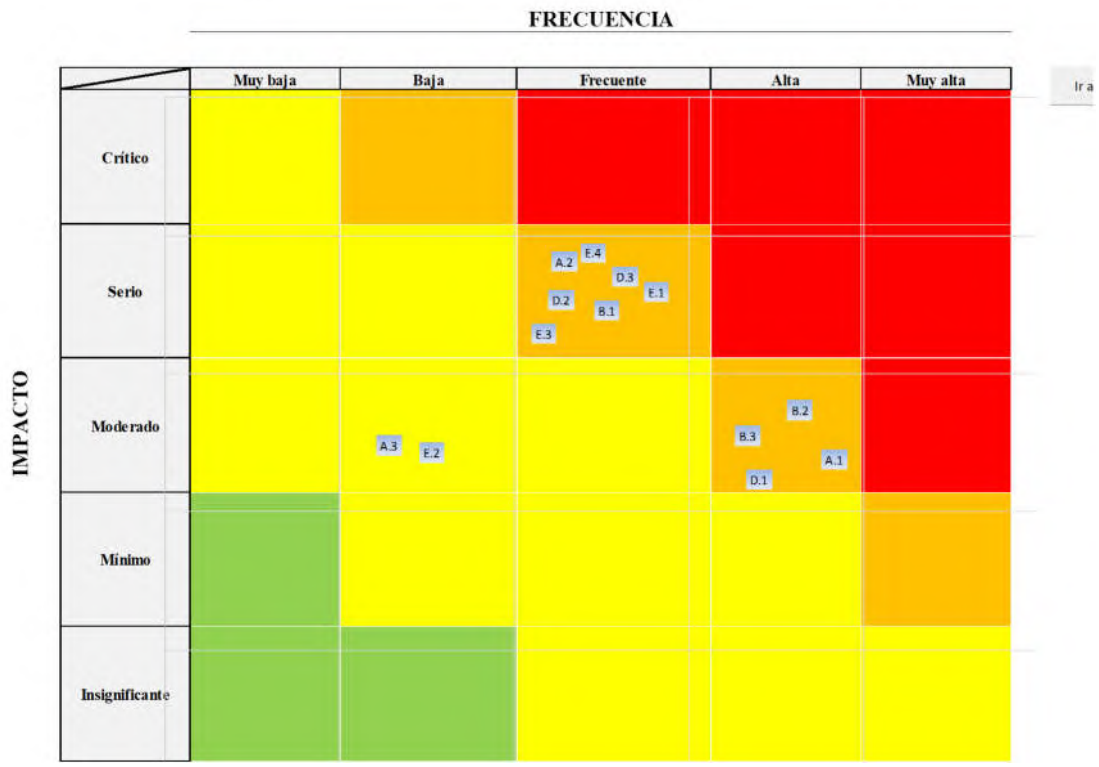
De las observaciones de periodos anteriores[3] 4 se encuentra atendida según se indica en el "*Seguimiento plan remedial auditoria 2022*" y las siguientes observaciones se encuentran en proceso:

Ref.	Oportunidades de mejora
F.1	Ausencia de un plan de tratamiento de riesgos de seguridad de la información y privacidad. (2022).
F.2	Ausencia de un plan para la gestión de la capacidad, disponibilidad y desempeño de la plataforma tecnológica (2021).
F.4	Ausencia de un inventario actualizado de licencias instaladas por equipo (2021).
F.5	Ausencia de lineamientos documentados para la gestión de infraestructura tecnológico (2021).
F.7	Debilidades en la definición y administración de acuerdos de servicio (2021).
F.9	Debilidades en la gestión de la seguridad de la información (2021).
F.10	Debilidades en la gestión de la continuidad de las tecnologías de información (2021).

[3] Realizadas por otras firmas de auditores

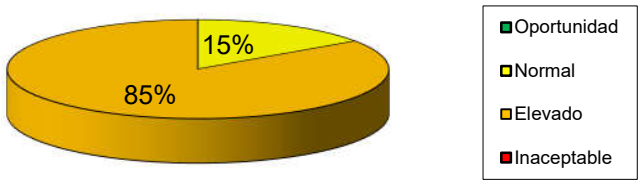
IX. Mapa de calor de los riesgos evidenciados en las observaciones de seguimiento

De acuerdo con nuestra revisión y a la metodología de calificación del nivel de exposición al riesgo, presentamos a continuación la matriz de 25 cuadrantes donde se resume de manera gráfica, las observaciones que incluimos en nuestro informe y su nivel de riesgo.



Mapa de riesgos identificado para los hallazgos de sistemas de información de la UNED.

Oportunidades de mejora UNED



Como resultado de la revisión se comunican 13 observaciones que son clasificadas en dos categorías de riesgo ubicadas en las áreas revisadas en la siguiente forma:

- 2 de riesgo normal
- 11 de riesgo elevado

X. Actividades evaluadas

A. Gestión de Tecnologías de Información

En la revisión de estas actividades se verificó lo siguiente:

1. Plan operativo de TI.
2. Informes de labores de TI del periodo auditado.
3. Matriz o informe sobre las recomendaciones en proceso o pendientes de atender internas, externas y regulatorias.
4. Marco de Gobierno y Gestión de TI – UNED.
5. Informes sobre mejoras, cambios o implementación de los procesos.
6. Portafolio con sus programas de proyectos TI e institucional.
7. Revisiones de la auditoría interna de TI.
8. Metodología de riesgos de TI.
9. Gestión de proveedores.
10. Evaluaciones de riesgos de TI a los procesos o servicios.

Se comunican las siguientes oportunidades de mejora:

A.1 Oficial de seguridad de la información

Elevado
✔

Se cuenta con un marco normativo para implementar un Sistema de Seguridad de la Información, que no cuenta con perfil para Director de la Seguridad de la Información, que le permita a un alto nivel ser el responsable de alinear las iniciativas de seguridad con los planes operativos y los objetivos institucionales, con el objetivo de garantizar que los bienes y tecnologías de la información están protegidos.

Al ser la información uno de los activos más importantes, los sistemas y procesos que manejan esta información se han vuelto críticos en todas las instituciones de negocio y gubernamentales. Es relevante la definición del puesto de trabajo del CISO (Chief Information Security Officer).

Criterio

El Marco de Gobierno y Gestión de TI de la UNED, indica en el *Objetivo de gestión-Seguridad de la información de TI:*

"Debe cubrir los controles para establecer que la información custodiada, almacenada, transferida, procesada e incluso eliminada cumpla los requerimientos de confidencialidad, integridad, disponibilidad y autenticidad establecida en la normativa de seguridad de la información institucional.

Así mismo, se debe elaborar e implementar un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de estas y la ejecución de sus respectivos procesos de concienciación y capacitación del personal de la institución sobre la seguridad de la información de TI".

Se indica que el rol a cargo de las practicas es el "Gestor de seguridad" *El gestor de la seguridad de TI se ocupa de salvaguardar la confidencialidad, integridad y disponibilidad de los activos, información, datos y servicios de TI de una organización.*

Causa

Se carece del perfil profesional que puedan implementar un SGSI por sus competencias y experiencia profesional.

Efectos

Sin un SGSI, la institución es más vulnerable a ataques cibernéticos, accesos no autorizados, pérdida de datos y otras amenazas de seguridad. Esto puede resultar en la interrupción de operaciones, pérdida de información crítica y daños a la infraestructura tecnológica.

Pérdida de Confidencialidad, Integridad y Disponibilidad de la Información: Sin un enfoque estructurado para proteger la información, es más probable que se produzcan brechas de seguridad que comprometan la confidencialidad (acceso no autorizado a la información), integridad (modificación no autorizada de la información) y disponibilidad (acceso no disponible cuando sea necesario).

Recomendaciones

A.1.1 Analizar la contratación de un Oficial o Director de la Seguridad de la Información con el objetivo de centralizar las decisiones de seguridad de TI, el cumplimiento regulatorio y de la continuidad del negocio, responsable por las decisiones de seguridad institucional (física, lógica e investigaciones), la planificación, desarrollo, control y gestión de las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información con los pilares fundamentales de confidencialidad, integridad y disponibilidad.

A.1.2 Realizar evaluaciones periódicas de riesgos para identificar y priorizar las amenazas más críticas para la información de la institución. Analizar las vulnerabilidades y el impacto potencial de los diferentes tipos de ataques.

A.1.3 Proporcionar capacitación regular a las personas funcionarias sobre prácticas de seguridad de la información. Fomentar una cultura de seguridad donde todos los empleados comprendan su papel en la protección de la información dentro de la institución.

A.1.4 Implementar herramientas y prácticas de monitoreo para detectar actividades sospechosas y responder rápidamente a incidentes de seguridad. Establecer un proceso claro para manejar y reportar incidentes de seguridad.

A.2 Implementar el Marco de Gestión de TI

Elevado
✔

El diseño de un marco de gestión que contenga los procesos que gestiona la institución es fundamental para proporcionar la agilidad necesaria para detectar y responder ante las necesidades de las partes interesadas, actualmente el marco se encuentra diseñado y aprobado, pero aún no ha sido implementado, por lo que se cuenta con procedimientos internos que requieren ser reforzados y que se encuentren alineados a buenas prácticas de gestión de TI.

Criterio

El principio de cumplimiento de las normas del MICITT, indica:

"Normativo de Gobierno y Gestión de las Tecnologías de Información orienta a la institución en la implementación de buenas prácticas que permiten la adecuada gestión de los procesos requeridos para brindar de forma oportuna y efectiva los servicios brindados a través del uso y administración de los recursos tecnológicos de forma tal que garanticen la continuidad de las operaciones institucionales, la salvaguarda de la información gestionada, la entrega de valor y el cumplimiento normativo. Para el proceso de implementación es necesario tener conocimiento sobre la gestión institucional, naturaleza, tamaño y complejidad, volumen de operaciones y cómo esta se apoya en su operativa con el uso de los recursos tecnológicos y su nivel de dependencia. Este proceso puede ser progresivo, debidamente planificado, de acuerdo con las prioridades institucionales, criticidad de los procesos y riesgos asociados al uso de recursos tecnológicos y los servicios requeridos que se brindan a través de la gestión de TI".

Causa

La implementación del marco de gestión aprobado no se ha completado porque es un proyecto que está formulado en el Plan Táctico de Tecnologías de Información y Comunicaciones 2023-2027 de la UNED.

Efecto

Podría incrementar la vulnerabilidad a amenazas de seguridad y el incumplimiento al no estar implementado todo el Marco de Gobierno y Gestión de la UNED.

Recomendaciones

A.2.1 Implementar el Marco de Gestión de TI de acuerdo con los procesos y servicios de la institución, con el objetivo de orientar y alinear las estrategias internas con los lideres de servicios bajo la aplicación de buenas prácticas de TI.

A.2.2 Confeccionar un perfil de proceso para asegurar una adecuada implementación de cada proceso que soporta la gestión de tecnologías de información, se podría considerar las siguientes actividades para cada proceso:

1. Debe estar formalmente definido a través de la disposición de un objetivo claro y metas específicas, que sean ejecutables, reales, orientadas a resultados y medibles.

2. La propiedad del proceso debe estar claramente establecida, sobre el diseño, interacción con otros procesos, rendición de cuentas de los resultados finales, medición del desempeño e identificación de mejora.

3. Debe estar claramente establecida la secuencia de actividades de forma lógica, consecuente, flexible, y escalable de forma tal que produzca los resultados esperados, considerando el manejo de excepciones y emergencias.

4. Los roles y responsabilidades deben estar exactamente asignados para la ejecución efectiva de las actividades clave y su documentación, además de la rendición de cuentas sobre los entregables finales asociados.

5. Debe disponer de lineamientos y planes debidamente formalizados, revisados, actualizados, aprobados, almacenados, comunicados, publicados y utilizados en forma consecuente, que establezcan las directrices y acciones requeridas. Los lineamientos deben estar accesibles y asegurar el claro entendimiento por parte de los responsables de su aplicación, así como de las partes interesadas. Los lineamientos se constituyen por:

   - ✓ Planes de gestión, de trabajo y de acción, que permitan establecer las actividades y tareas para un período específico y el logro de resultados

   - ✓ Políticas y directrices que brinden la información necesaria en el más amplio nivel de detalle sobre las normas y mecanismos que se deben cumplir

   - ✓ Normas que definan los propósitos generales dentro de un marco o política regulatoria, indicando lo que debe hacerse para su cumplimiento de acuerdo con el entorno de gestión y alcances establecidos por la organización.

   - ✓ Procedimientos, para tareas específicas de tipo operativo-administrativo, indicando el cómo se lleva a cabo una actividad o un proceso describiendo con alto grado de detalle el modo de realizar las actividades principales y la parametrización de los componentes e integrantes del proceso que describen.

   - ✓ Estándar Técnico, desarrollado como guía para la configuración de valores, reglas, condiciones o características en productos de hardware y software que integran la arquitectura de procesos alcanzados por los requerimientos normativos, regulatorios y legales relacionados con las actividades institucionales.

- ✓ Instructivos, listas de chequeo y formularios, documentación anexa a los procedimientos y que sirven como guía de paso a paso, documento de control y/o registros que presentan resultados obtenidos o proporcionan evidencia de actividades realizadas.

6. Deben contar con indicadores de desempeño, de tal forma que permitan identificar el nivel de logro de las metas. Deben establecerse las formas de recopilación de datos asociados y la presentación de los resultados y acciones para tratar las desviaciones según aplique.

A.3 Marco normativo para el uso de inteligencia artificial

Normal
✔

Se identificó la ausencia de un marco normativo específico que aborde de manera integral las diversas facetas y desafíos que presenta la Inteligencia Artificial (en adelante IA), incluyendo la ética, la privacidad y la seguridad de la información.

Criterio

La IA requiere ser regulada en las instituciones, sin embargo, este rápido avance ha superado la capacidad de los marcos regulatorios existentes para adaptarse y ofrecer un control adecuado sobre el uso de tecnologías emergentes, actualmente ofrecen ventajas y desventajas, entre algunas se detallan:

Ventajas

Automatización de procesos

Permite que las máquinas hagan de forma automática tareas que para los humanos resultan repetitivas y tediosas.

Reduce el error humano

Al reducir la intervención de los humanos en ciertos procesos, acaba con las posibilidades de que estos puedan cometer errores. Por ejemplo, una errata al introducir un dato en la contabilidad de un negocio.

Potencia la creatividad

Al liberar a los trabajadores de tareas repetitivas y poco motivadoras, la mente de estos es mucho más libre para dedicarse al proceso creativo.

Aporta precisión

Al ser capaz de tomar decisiones por sí misma, la inteligencia artificial da lugar a procesos productivos mucho más eficientes y con una menor tasa de error.

Agiliza la toma de decisiones

La inteligencia artificial es capaz de analizar miles de datos en apenas minutos y además tener en cuenta posibles actualizaciones de estos. La información bien sintetizada y actualizada ayuda a los profesionales a tomar decisiones estratégicas.

Desventajas

Dificultad de acceso a los datos

Para que una inteligencia artificial funcione de forma adecuada debe tener datos actualizados y fiables, pero esto nos siempre es así. Por eso, uno de los principales retos a abordar es garantizar que estos sistemas puedan acceder a los datos que necesitan en cada momento.

Falta de profesionales cualificados

Uno de los inconvenientes de esta tecnología es que su desarrollo no está siendo tan rápido como debería porque faltan profesionales bien cualificados que puedan implementar los ajustes necesarios.

Su desarrollo es costoso

Aunque las inteligencias artificiales aplicadas al ámbito de la medicina, la producción, la dirección de empresas, etc. pueden ser muy útiles, el desarrollo de estas tiene todavía un coste muy elevado, lo que hace que no sean accesibles para todo el mundo.

Los modelos actuales de inteligencia artificial son generativos tomando como punto de partida la información suministrada a lo largo de muchos años por todos nosotros, en la dinámica actual es importante acotar que en Costa Rica no existe ninguna regulación particular con relación al uso de este tipo de tecnologías, pero no con esto se puede dejar por alto lo relacionado con la privacidad, confidencialidad y seguridad de la información ya que al utilizar estos servicios según sus términos y condiciones estamos ayudando al entrenamiento de los mismos, por lo tanto estamos cediendo o compartiendo información que en algunos casos podría ser sensible.

Causa

Esta falta de regulación específica para la IA plantea riesgos significativos para la privacidad y seguridad de la información personal y corporativa. La falta de un marco normativo adecuado sitúa a la organización en una posición donde no existe una guía clara sobre cómo implementar y utilizar la IA de manera responsable y sin la exposición de los datos empresariales.

Efecto

Puede llevar a que se incrementa el riesgo de violaciones de privacidad y seguridad de la información, tanto personal como corporativa, debido a la falta de directrices claras sobre la gestión y protección de datos. La falta de regulación puede dar lugar a un uso irresponsable o éticamente cuestionable de la IA, afectando la reputación de la institución y generando desconfianza entre los clientes y el público en general.

Recomendación

A.3.1 Valorar y considerar la confección de normativa relacionada a este tipo de tecnologías emergentes con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información. La normativa debería contemplar elementos clave como:

- ✓ Establecer principios éticos claros

  Definir normas sobre la transparencia y el respeto por la privacidad y la dignidad humana en el desarrollo y aplicación de la IA.

- ✓ Garantizar la seguridad y privacidad de los datos

  Implementar estándares para la protección de datos, asegurando la confidencialidad, integridad, y disponibilidad de la información.

- ✓ Fomentar la responsabilidad y la rendición de cuentas

  Crear mecanismos específicos que permita a la entidad ser responsable de los impactos derivados del uso de la IA, estableciendo procedimientos claros y detallados para la evaluación y mitigación de riesgos, asegurando que las aplicaciones de inteligencia artificial se alineen con principios éticos y legales establecidos.

B. Gestión de las prácticas de seguridad de la información

En la revisión de estas actividades se verificó lo siguiente:

1. Políticas y procedimientos para la administración de la seguridad.
2. Evaluaciones de seguridad de la red, infraestructura, sitio web internos.
3. Informes sobre las pruebas de vulnerabilidad y pent test.
4. Plan de acción de las recomendaciones en proceso y pendientes de atender sobre las evaluaciones de vulnerabilidad.
5. Informe de revisión de roles y perfiles de usuario 2023.
6. Plan de trabajo de la seguridad informática y seguridad de la información.
7. Gestión de roles y perfiles de acceso.
8. Gestión en la atención de incidentes.

Se comunican las siguientes oportunidades de mejora:

B.1 Aplicación de pruebas de vulnerabilidades

Elevado
✔

No se evidencia la aplicación de pruebas ni análisis de vulnerabilidades externas durante el periodo 2023, es importante tomar medidas para fortalecer la seguridad de los sistemas, red, infraestructura y otros.

Las pruebas de vulnerabilidades deben llevarse a cabo de manera ética y con el consentimiento de la institución, se requiere de profesionales en seguridad informática o empresas especializadas en pruebas de seguridad para realizar estas evaluaciones de manera efectiva y minimizar el riesgo de interrupción de los sistemas o la violación de la privacidad de los datos.

Entre algunas posibles pruebas se detallan:

Escaneo de vulnerabilidades: Se utiliza un software especializado para identificar posibles vulnerabilidades en la red, como puertos abiertos, servicios expuestos, configuraciones débiles, entre otros.

Evaluación de aplicaciones web: Se analizan las aplicaciones web de la institución en busca de vulnerabilidades como inyecciones de código, cross-site scripting (XSS), secuencias de comandos entre sitios (CSRF), entre otros.

Evaluación de seguridad de redes inalámbricas: Se verifica la seguridad de las redes inalámbricas utilizadas por la institución, buscando posibles puntos de acceso no autorizados, configuraciones débiles o cifrado inadecuado.

Análisis de seguridad de la infraestructura: Se evalúa la seguridad de los servidores, routers, switches y otros dispositivos de red utilizados por la institución para detectar posibles vulnerabilidades y configuraciones inseguras.

Pruebas de ingeniería social: Se intenta engañar o manipular a los empleados de la institución para obtener información confidencial o acceso no autorizado a los sistemas. Esto ayuda a evaluar la conciencia de seguridad de los empleados y la efectividad de las políticas de seguridad.

Criterio

El Marco de Gobierno y Gestión de TI de la UNED, indica en el *Objetivo de gestión-Seguridad de la información de TI:*

En la práctica siguiente se identifica la detección de vulnerabilidad:

"Practica #2. Gestionar riesgos ante amenazas: Debe enfocarse en varios temas, como identificación de riesgos de seguridad de TI y la protección de la información en tránsito y almacenada, educación y compromiso del personal institucional con la seguridad de la información, implementación de controles y detección de vulnerabilidades".

Causa

No se ha implementado las herramientas indicadas en el Marco de Gobierno y Gestión de TI sobre la aplicación de pruebas de vulnerabilidad.

Efectos

Al no evaluar regularmente la seguridad de los sistemas y redes, la institución se expone a posibles ataques cibernéticos. Los ciberdelincuentes pueden aprovechar las vulnerabilidades no detectadas para acceder de manera no autorizada a la información confidencial, robar datos, interrumpir los servicios o incluso comprometer la integridad de los sistemas.

Pérdida de datos sensibles de la institución estén en riesgo. Los ataques exitosos pueden resultar en la pérdida de información confidencial, como datos personales de los ciudadanos, registros financieros, secretos comerciales o información estratégica.

Las vulnerabilidades no detectadas pueden ser aprovechadas para interrumpir los servicios de la institución. Los atacantes pueden realizar ataques de denegación de servicio (DDoS) o desplegar malware que afecte la disponibilidad de los sistemas y la infraestructura, lo que podría tener un impacto negativo en la prestación de servicios públicos esenciales.

Los incidentes de seguridad pueden resultar en costos significativos para la institución, incluyendo el costo de recuperación de datos, mitigación de ataques, reparación de sistemas dañados, notificación a los afectados, posibles demandas legales y la implementación de medidas de seguridad adicionales.

Recomendaciones

B.1.1 Fortalecer la aplicación de pruebas de vulnerabilidades con regularidad y anualmente, con el objetivo de optimizar controles y minimizar la exposición de ser vulnerables a terceros.

B.1.2 Establecer un programa regular de pruebas, por ejemplo, anuales o semestrales, para garantizar que los sistemas se evalúen continuamente en busca de nuevas vulnerabilidades que puedan surgir debido a actualizaciones de software, cambios en la configuración o nuevas amenazas.

B.1.3 Tomar las medidas necesarias para cerrar las brechas de seguridad identificadas en las pruebas de vulnerabilidad y pent test. Esto puede incluir la aplicación de parches, actualizaciones de software, reconfiguración de sistemas o la implementación de controles adicionales.

B.1.4 Brindar capacitación regular sobre seguridad informática a todo el personal de la institución para fomentar una cultura de seguridad y concientización. Esto ayudará a prevenir errores humanos y a mantener los sistemas protegidos.

B.2 Implementación del Sistema de Seguridad de la Información

Elevado
✔

Se identifican procedimientos y controles de seguridad de la información, sin embargo, se requiere la implementación de la estrategia de seguridad de TI de acuerdo con el Marco de Gobierno y Gestión de TI.

Se identifica una política de seguridad de la información que requiere la oficialización de esta.

Criterio

El Marco de Gobierno y Gestión de TI de la UNED, indica en el *Objetivo de gestión-Seguridad de la información de TI*:

En la práctica siguiente se identifica la detección de un marco de seguridad de la información:

"Practica #1. Implementar un marco de seguridad de la información: Establecer un marco metodológico que incluya la clasificación de los activos de TI, según su criticidad."

Causa

No se ha implementado las actividades que se estaría ejecutando para el sistema de Gestión de Seguridad de la UNED.

Efectos

La información sensible puede perderse debido a ataques cibernéticos, errores humanos, o fallos técnicos. La pérdida de datos críticos puede afectar gravemente las operaciones de una organización.

La falta de seguridad puede resultar en la exposición de información personal de empleados, clientes o socios comerciales, lo cual puede llevar a problemas legales y pérdida de confianza.

Vulnerabilidad a los ataques cibernéticos como el ransomware, que pueden paralizar las operaciones y exigir grandes sumas de dinero para recuperar el acceso a los datos.

Los incidentes de seguridad pueden interrumpir las operaciones normales de una organización, causando ineficiencias y pérdida de productividad.

Recomendaciones

B.2.1 Implementar las actividades que han sido diseñadas para el cumplimiento del objetivo de Gestionar la Seguridad de la Información, tal y como se detallan de seguido:

"Alinear la estrategia de seguridad de la información de TI con la estrategia institucional de TI.

Establecer la base para un plan de acción que logre los objetivos de seguridad de la información y permitan avanzar al nivel de madurez o capacidad esperada.

Generar estrategias para el uso de las tecnologías digitales, fomentando principios de respeto a los derechos humanos, privacidad y coordinación con entes internos y externos.

Monitorear el cumplimiento y los resultados de la aplicación de la estrategia y plan de seguridad para reforzar los criterios de integridad, confidencialidad y disponibilidad de la información, la infraestructura tecnológica para minimizar el impacto de vulnerabilidades e incidentes de seguridad".

B.2.2 Aprobar la política de seguridad de la información con las respectivas firmas.

B.3 Informe de revisión de roles y perfiles de usuario

Elevado
✔

Se evidenció la utilización de sistema AS400 que incluye una sección Financiera- Contable y de Recursos Humanos, sin embargo, no se posee una opción que permita realizar un levantamiento automatizado de inventario a nivel de usuarios, perfiles, menús, programas y objetos en el AS400, por lo que no se ejecutan informes de revisión de roles y perfiles de usuario.

Criterio

El Marco de Gobierno y Gestión de TI de la UNED, indica en el propósito del *Objetivo de gestión-Organización TI*, practica #2 Establecer roles y responsabilidades de TI, actividad 4:

"Determinar la correcta aplicación de roles y responsabilidades de TI por medio de mecanismos de control adecuados".

Además, la descripción de esta actividad indica:

"Por medio de un mecanismo de control claro y documentado, que permita el seguimiento de aplicación de roles y responsabilidades asignadas a los funcionarios".

Basado en estos criterios, la elaboración periódica de informes de revisión de roles y perfiles de usuario constituye un control adecuado para garantizar que los roles y responsabilidades se apliquen correctamente en los sistemas.

Causa

Hay un procedimiento para Gestión de usuarios y accesos en el AS400 que no se evidencia su aplicación periódica, en el cual se establece que es responsabilidad del líder de servicio, llevar un registro de todas las solicitudes de acceso tramitadas de los sistemas a su cargo. No se ha establecido la confección de informes sobre perfiles.

Efecto

La falta de informes sobre las cuentas usuario aumenta la probabilidad de que funcionarios no autorizados puedan obtener acceso a datos críticos y módulos no autorizados, lo que podría resultar en el conocimiento y divulgación de la información.

Recomendaciones

B.3.1 Actualizar y aplicar el procedimiento de revisión de accesos, que se integre al proceso de Incluir la revisión de roles y cuentas de usuario a los sistemas de información que se gestionan, con el objetivo de eliminar asignaciones de accesos a los colaboradores que no son de su necesidad actual laboral, de ahí la importancia de tener ese levantamiento de roles y perfiles de usuario con los colaboradores actuales y así fortalecer la seguridad e integridad de la data.

B.3.2 Confeccionar al menos una vez al año el informe sobre roles y accesos de los colaboradores a los sistemas, aplicativos y herramientas de trabajo.

B.3.3 Revisar y actualizar en caso requerido el marco normativo para la revisión de cuentas de usuario y perfiles de acceso.

C. Gestión de riesgos de TI

En la revisión de estas actividades se verificó lo siguiente:

1. Metodología de riesgos de TI
2. Evaluaciones de riesgos de TI a los procesos o servicios
3. Plan de acción para mitigar los riesgos
4. Mapa o lista de riesgos de TI
5. Informes de riesgos comunicados a los Órganos de Dirección

De acuerdo con el resultado de las pruebas realizadas no evidenciamos situaciones que nos hagan creer que no se cumple con los requerimientos de seguridad y control en la Gestión de riesgos de TI al 31 de diciembre de 2023.

D. Gestión de sistemas de información

En la revisión de estas actividades se verificó lo siguiente:

1. Diagrama de la integración de los sistemas de información.
2. Inventario de los activos (software, hardware, aplicaciones) gestionados por TI.
3. Lista de cambios realizados a los sistemas y aplicativos del periodo.
4. Inventarios de activos de información.
5. Verificación del mantenimiento y desempeño de las bases de datos de AS400.
6. Manuales de los sistemas de información.
7. Aplicación de políticas y metodologías para el desarrollo del ciclo de vida de sistemas.
8. Informes sobre las evaluaciones a los sistemas.
9. Aplicación de pruebas de continuidad a los sistemas financieros y de recursos humanos.

Se comunican las siguientes oportunidades de mejora:

D.1 Manuales de los sistemas sin actualizar o se carecen de los mismos

Elevado
✔

Se cuenta con un procedimiento llamado “PUNED DTIC-USI 01 Desarrollo y mantenimiento de sistemas de información” el cual contempla las tareas de documentar el manual técnico y de usuario para nuevos desarrollos, en donde la creación de los manuales queda en el equipo de desarrollo utilizando herramientas y plantillas; sin embargo, se identifican sistemas sin manuales y otros desactualizados.

Se identifican los siguientes sistemas de información sin manuales de usuario a los sistemas:

a. Sistema Facturación de librería.
b. Fondos de trabajo y caja chica.

Se identifican los siguientes sistemas de información con manuales desactualizados:

a. Sistema de presupuesto.
b. Sistema de ingresos.
c. Sistema de liquidaciones.
d. Sistema de honorarios.
e. Sistema de planillas
f. Sistema de Pago de salarios.

Criterio

El Marco de Gobierno y Gestión de TI de la UNED, indica en el *Objetivo de Gestión-Construcción de servicios:*

"Garantizar la disponibilidad de los componentes de servicio, como hardware, software, información, personal capacitado, documentación relevante, entre otros, cuándo y dónde se necesite, mejorando las capacidades antes de poner en producción los servicios nuevos y modificados, con esto se asegura que el servicio satisfaga los requisitos dados en las especificaciones para su implementación.".

En la práctica siguiente se identifica el uso de manuales de herramientas:

"Practica #5. Desplegar servicios: Coordinar y asegurar la transición exitosa al ambiente de producción de los servicios nuevos o actualizados, esto incluye el retiro de servicios."

Causas

La actualización de manuales no es vista como una prioridad en comparación con otras tareas operativas más urgentes. La gestión de incidentes y la implementación de nuevos proyectos suelen recibir más atención.

Los responsables de la actualización de los manuales pueden no ser plenamente conscientes de la importancia de mantener la documentación al día. Esto puede deberse a una falta de formación o a una subestimación de los riesgos asociados con manuales desactualizados.

No está definido con claridad quién es el responsable de actualizar los manuales. Sin una designación clara de responsabilidades, esta tarea puede pasar desapercibida o ser ignorada.

Efectos

Sin manuales actualizados, los procedimientos y prácticas pueden variar entre los diferentes miembros del equipo, lo que lleva a inconsistencias en la gestión de los sistemas. Esto puede resultar en errores y configuraciones incorrectas que comprometan la seguridad y el rendimiento del sistema.

Los manuales proporcionan instrucciones claras y detalladas para la operación y mantenimiento de los sistemas. Sin ellos, los empleados pueden cometer errores que podrían ser fácilmente evitables, afectando negativamente la estabilidad y seguridad del sistema.

Los manuales son herramientas esenciales para la capacitación de nuevos empleados. Sin documentación actualizada, la curva de aprendizaje se vuelve más empinada y los nuevos empleados pueden tener dificultades para comprender y realizar sus tareas de manera eficiente.

En caso de problemas o incidentes, los manuales actualizados son cruciales para una resolución rápida y efectiva. La falta de esta documentación puede llevar a demoras en la identificación y solución de problemas, aumentando el tiempo de inactividad y afectando la continuidad del negocio.

La documentación actúa como un repositorio de conocimiento institucional. Sin manuales actualizados, el conocimiento crítico sobre la gestión de los sistemas puede perderse, especialmente si empleados clave dejan la organización.

Recomendaciones

D.1.1 Confeccionar y actualizar los manuales para los sistemas que se indican en la observación que están desactualizados y los que se deben de confeccionar utilizando la metodología del procedimiento "PUNED DTIC-USI 01 Desarrollo y mantenimiento de sistemas de información" que indica el uso de herramientas y plantillas.

D.1.2 Proporcionar capacitación sobre la importancia de la documentación y cómo mantenerla actualizada. Crear conciencia sobre los riesgos asociados con manuales desactualizados.

D.1.3 Implementar un proceso de revisión periódica de los manuales para asegurar que se mantengan actualizados.

D.2 Informes sobre evaluaciones a los sistemas de información

Elevado
✔

Con base en la evidencia aportada no se identifican informes de auditoría, evaluaciones de vulnerabilidades y revisiones de bases de datos para los sistemas de información dentro del alcance de auditoría.

Criterio

El Marco de Gobierno y Gestión de TI de la UNED, indica en el *Objetivo de gestión-Control interno:*

"Supervisar, evaluar y ajustar las medidas que permitan mantener un apropiado control de los procesos soportados por la gestión de TI que apoyan el cumplimiento de los objetivos de la institución."

En la práctica siguiente se identifica el uso de manuales de herramientas:

"Practica #1. Dar seguimiento a las actividades de control: Revisar, comprobar y mejorar continuamente el entorno de control de TI, de tal forma que mitigue riesgos que impidan alcanzar los objetivos de la institución, verificando que las excepciones de control se comuniquen y se apliquen las acciones correctivas correspondientes".

Causas

Recursos limitados: La realización de auditorías y evaluaciones de vulnerabilidades requiere tiempo, personal calificado y recursos financieros.

Falta de personal especializado: Las auditorías de seguridad y las evaluaciones de vulnerabilidades requieren conocimientos especializados. La falta de personal con las habilidades necesarias puede ser una barrera para la realización de estas evaluaciones.

Dependencia de sistemas heredados: El utilizar sistemas heredados pueden enfrentar desafíos adicionales en la realización de auditorías y evaluaciones de vulnerabilidades debido a la complejidad y la antigüedad de estos sistemas.

Efectos

Aumento de Riesgos de Seguridad: Exposición a vulnerabilidades: Sin evaluaciones regulares de vulnerabilidades, las debilidades de seguridad no identificadas pueden ser explotadas por atacantes, lo que puede llevar a brechas de seguridad y accesos no autorizados.

Falta de detección de amenazas: La ausencia de auditorías y evaluaciones significa que las amenazas potenciales pueden no ser detectadas a tiempo, dejando los sistemas expuestos durante períodos prolongados.

Impacto en la Confidencialidad, Integridad y Disponibilidad de los Datos:

Pérdida de datos: La falta de evaluaciones puede resultar en la pérdida de datos críticos debido a ataques, errores o fallos del sistema.

Alteración de datos: Sin auditorías, los cambios no autorizados en los datos pueden pasar desapercibidos, comprometiendo la integridad de la información.

Interrupciones del servicio: Las vulnerabilidades no identificadas pueden ser explotadas para causar interrupciones en el servicio, afectando la disponibilidad de los datos y sistemas.

Consecuencias Financieras: Costos de recuperación: La resolución de incidentes de seguridad puede ser costosa, incluyendo la recuperación de datos, la reparación de sistemas y las sanciones por incumplimiento de normativas.

Pérdida de ingresos: Las interrupciones del servicio y la pérdida de confianza de los clientes pueden llevar a una disminución de los ingresos.

Ineficiencia Operativa: Procesos no optimizados: Las auditorías internas ayudan a identificar ineficiencias y áreas de mejora en los procesos operativos.

Desorganización y Caos: La falta de evaluaciones puede llevar a una falta de claridad y organización en la gestión de sistemas y datos, resultando en caos y desorden.

Recomendaciones

D.2.1 Realizar evaluaciones periódicas de vulnerabilidades, auditorías internas y revisiones de bases de datos para identificar y mitigar riesgos de seguridad.

D.2.2 Asignar los recursos necesarios, incluyendo personal capacitado y herramientas adecuadas, para llevar a cabo estas evaluaciones de manera efectiva.

D.2.3 Establecer políticas y procedimientos para la realización de auditorías y evaluaciones, y asegurarse de que se sigan de manera consistente.

D.2.4 Proporcionar capacitación continua al personal sobre las mejores prácticas de seguridad y la importancia de las auditorías y evaluaciones.

D.2.5 Implementar herramientas de gestión de vulnerabilidades, análisis de bases de datos y auditorías para facilitar el proceso de evaluación.

D.2.6 Utilizar los resultados de las auditorías y evaluaciones para mejorar continuamente las prácticas de seguridad y gestión de la información.

D.3 Sistemas sin aplicación de pruebas de continuidad

Elevado
✔

No se evidencia durante el periodo 2023 la ejecución de pruebas de continuidad para los sistemas enmarcados en el alcance de la auditoría.

Criterio

El Marco de Gobierno y Gestión de TI de la UNED, indica en el *Objetivo de gestión-Seguridad de la información de TI:*

En la práctica siguiente se identifica implementar el plan de continuidad de TI para servicios críticos.:

"Practica #4. Implementación de la gestión de proyectos de la seguridad de TI: Esta práctica incluye la gestión de incidentes de seguridad, gestión de la continuidad de servicios de TI y la comunicación y activación de planes de emergencia.".

Causas

La alta dirección y los responsables de TI pueden no ser plenamente conscientes de la importancia de tener informes y protocolos de continuidad, lo que lleva a que estas tareas no se prioricen adecuadamente.

La falta de tiempo, personal y presupuesto puede impedir que se desarrolle y mantenga informes y protocolos de continuidad, enfocándose en actividades operativas inmediatas en lugar de en la planificación a largo plazo.

Falta de políticas y procedimientos establecidos que definan la necesidad y la frecuencia de los informes de continuidad y los protocolos, estas tareas pueden pasarse por alto debido a la ausencia de un marco normativo interno que impulse su desarrollo y mantenimiento.

Efectos

La ausencia de protocolos de continuidad y recuperación ante desastres puede resultar en una incapacidad para responder de manera rápida y efectiva a incidentes inesperados, como fallos del sistema, desastres naturales o ataques cibernéticos. Esto puede llevar a interrupciones prolongadas de las operaciones comerciales, afectando la capacidad de mantener sus servicios y productos disponibles para los clientes.

Sin informes y evaluaciones regulares, las estrategias de respaldo y recuperación de datos pueden ser insuficientes o estar desactualizadas. Esto puede resultar en la pérdida irreparable de datos críticos y en procesos de recuperación ineficientes, dificultando la restauración de operaciones normales y causando retrasos significativos en la reanudación de actividades comerciales.

La falta de una gestión efectiva de la continuidad del negocio puede generar costos financieros significativos debido a la interrupción de operaciones, pérdida de ingresos y posibles sanciones por incumplimiento de normativas. Además, la incapacidad para mantener la continuidad del negocio puede dañar la reputación, disminuyendo la confianza de los clientes y socios de negocios, lo que puede llevar a la pérdida de oportunidades comerciales y clientes a largo plazo.

Recomendaciones

D.3.1 Verificar que en el plan de pruebas se incluyan los sistemas que son identificados como críticos y valorar protocolos de recuperación para los sistemas que no se identifican como críticos, pero son de importancia para la gestión financiera contable.

D.3.2 Implementar un programa de auditorías internas para revisar periódicamente los sistemas y procesos de continuidad del negocio. Utilizar los hallazgos de las auditorías para mejorar continuamente las prácticas y protocolos.

D.3.3 Realizar simulacros regulares de los planes de continuidad del negocio y recuperación ante desastres para asegurar que el personal esté familiarizado con los procedimientos y para identificar áreas de mejora.

D.3.4 Probar periódicamente los procedimientos de recuperación de datos para asegurar que los respaldos sean efectivos y que los datos críticos puedan restaurarse rápidamente.

E. Gestión de la continuidad de negocio

En la revisión de estas actividades se verificó lo siguiente:

1. Plan de Continuidad de Negocio.
2. Existencia del plan de continuidad de TI.
3. Análisis de Impacto de Negocio (BIA).
4. Capacitación a los colaboradores en continuidad de negocio.
5. Pruebas de validación a los respaldos.
6. Sitio alterno para el procesamiento de los datos.

Se comunican las siguientes oportunidades de mejora:

E.1 Plan de continuidad de negocio

Elevado
✔

En la revisión efectuada se identifica que UNED cuenta con un Plan de Continuidad de Negocio con fecha de 25 de enero de 2016, el cual requiere de una actualización y alineación con buenas practicas y el marco regulatorio.

Criterio

La norma del MICITT en el apartado XIII, Continuidad y disponibilidad operativa de los servicios tecnológicos menciona:

"La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas.

La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.

Causa

No se ha llevado a cabo la actualización del plan de continuidad.

Efecto

Podrían no aplicarse procedimientos en tiempo para responder, recuperar, reanudar y restaurar a un nivel de operación aceptable predefinido luego de un evento de continuidad.

Recomendaciones

E.1.1 Actualizar el plan de continuidad de negocio con el objetivo de preparar a la institución ante interrupción de su negocio, por medio de la documentación de procedimientos, estrategias de recuperación, análisis del impacto, manejo de crisis durante la contingencia y sus diversos planes relacionados a la continuidad.

E.1.2 Establecer el marco de trabajo tomando en cuenta la estructura institucional para administrar la continuidad, la cobertura de roles, las tareas y responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI.

E.2 Plan de capacitación sobre la continuidad de operaciones

Normal
✔

No se evidencia un plan o programa de capacitación institucional sobre continuidad aprobado sobre las acciones de entrenamiento y formación del personal, en donde la transferencia de conocimiento consta de actividades teóricas o prácticas, aunque los objetivos de un plan de capacitación varían según las necesidades, en general buscan:

1. Integrar a los funcionarios en los procesos de la institución.
2. Promover la adquisición y las habilidades técnicas y conductuales.
3. Entrenar a las personas para desempeñar de forma satisfactoria las funciones específicas de un cargo y en cumplimiento del marco normativo interno.

Criterio

El Marco de Gobierno y Gestión de TI de la UNED, indica en el *Objetivo de gestión-Organización TI:*

En la práctica siguiente se identifica implementar el plan de continuidad de TI para servicios críticos.:

"Practica #4. Mantener actualizadas las habilidades y competencias. Definir y administrar las habilidades y competencias que necesita el personal de TI. Generar oportunidades de capacitaciones afines al desempeño de las actividades que realizan, con el fin de promover la actualización de conocimientos y fomentar el aprendizaje continuo para desarrollar nuevas habilidades y competencias y, así, alcanzar las metas establecidas en los planes de trabajo y ejecución de proyectos institucionales.".

Causa

La ausencia de un plan o programa de capacitación institucional sobre continuidad se debe a una falta de priorización y asignación de recursos para el desarrollo y aprobación de un esquema formal de entrenamiento y formación del personal.

Efectos

Puede generar una respuesta descoordinada y menos efectiva ante eventos adversos, aumentando el riesgo de tiempos de inactividad prolongados, pérdida de datos, y afectaciones a la continuidad operativa.

La ausencia de capacitación adecuada puede disminuir la capacidad de la organización para mitigar riesgos, mantener la resiliencia y cumplir con los estándares de seguridad y continuidad establecidos.

Recomendación

E.2.1 Aplicar un programa de formación sobre la continuidad a los colaboradores, con el objetivo que el recurso humano que se encuentra en la primera línea de defensa contra las amenazas, que le permita desarrollar las habilidades y conocimientos necesarios para asumir con una adecuada preparación, los eventos inesperados a los que la institución se pueda enfrentar.

E.3 Pruebas sobre restauración de respaldos

Elevado
✔

No evidenciamos la aplicación de pruebas documentadas para la restauración de respaldos internamente en la UNED, con el objetivo de minimizar la probabilidad y el impacto de interrupciones en los servicios de TI, sobre funciones, servicios y procesos claves del negocio con regularidad.

Criterio

El Marco de Gobierno y Gestión de TI de la UNED, indica en el *Objetivo de gestión-Continuidad de los servicios de TI:*

En la práctica siguiente se identifica la implementar el plan de continuidad de TI para servicios críticos.:

"Practica #3. Evaluar y realizar las mejoras para favorecer la continuidad de los servicios de TI. Establece la necesidad de una revisión y seguimiento para mejorar su operación, tomando acciones correctivas y preventivas, con base en los resultados de la revisión por la dirección para lograr la mejora continua de los servicios de continuidad."

Causa

El tiempo de duración al no poder activar los sistemas de información antes eventos disruptivos de acuerdo con el Análisis de Impacto definido, se debe concientizar a todos los niveles de la organización sobre la importancia de las pruebas de restauración y asegurar que se asignen los recursos y el tiempo necesarios para realizarlas de manera regular y efectiva.

Efecto

Aumenta el riesgo de pérdida de datos, afecta la continuidad operativa y puede tener un impacto negativo en la confianza de los usuarios y la reputación de la institución.

Recomendaciones

E.3.1 Confeccionar y aplicar como parte de la continuidad de negocio pruebas sobre restauración de respaldos no por demanda, sino como práctica de control para asegurar que los servicios y sistemas estén disponibles cuando se requieran y asegurar un impacto mínimo a la organización en eventos de interrupciones mayores.

E.3.2 Confeccionar y definir los requerimientos de recuperación para los sistemas y procesos de la UNED a los cuales han sido definidos como críticos y requieren la ejecución de pruebas de restauración de respaldo.

E.4 Pruebas de continuidad de negocio

Elevado
✔

No evidenciamos pruebas integrales o unitarias de continuidad de negocio.

Es necesario establecer un plan de pruebas de continuidad de negocio y recuperación, con el objetivo de minimizar la probabilidad y el impacto de interrupciones en los servicios de TI, sistemas y procesos claves del negocio con alguna regularidad.

Criterio

El Marco de Gobierno y Gestión de TI de la UNED, indica en el Objetivo de gestión-Continuidad de los servicios de TI:

En la práctica siguiente se identifica la detección de un marco de seguridad de la información:

“Practica #2. *Diseñar y ejecutar los mecanismos y procedimientos de continuidad de los servicios de TI adecuados y medibles Implementar y operar la política, controles, procesos y procedimientos de continuidad, incluye la ejecución de los planes de recuperación y continuidad, así como verificar las medidas de reducción de riesgo, alineados con los objetivos de continuidad.”*

Causa

La falta de preparación puede llevar a pruebas de continuidad lentas, costosa obteniendo a tener respuestas improvisas y desorganizadas ante incidentes.

Efecto

Sin un plan de pruebas de continuidad y recuperación, la institución enfrenta una mayor probabilidad de tiempos de inactividad prolongados, pérdida de datos críticos y fallos en la recuperación de operaciones.

Recomendaciones

E.4.1 Activar la ejecución de pruebas para identificar la capacidad de respuestas en tiempo y efectividad ante el restablecimiento de servicios y obtener una razonabilidad de la continuidad del negocio.

E.4.2 Revisar y evaluar la estrategia de continuidad actual con el objetivo de obtener opciones viables y efectivas en costos en donde se pueda asegurar la continuidad y recuperación frente a los incidentes, evento mayor o disrupción de los servicios.

E.4.3 Revisar y considerar en el plan de pruebas de Continuidad, entre algunas pruebas las siguientes:

a. Pruebas de escritorio: un método para el ejercicio de los planes en los que los participantes revisan y discuten las acciones que se toman sin tener que realizar las acciones.

b. Prueba de componente: estas pruebas se realizan con el objetivo de probar, encontrar, reparar fallas, verificar la efectividad del protocolo de recuperación y documentar las mejoras del comportamiento de los módulos independientes.

c. Prueba integral: prueba en la cual se incluyen como parte del alcance de esta, toda la plataforma tecnológica que soporta un Sistema crítico de TI.

d. Prueba de punta a punta: prueba en la cual se evalúan todos los componentes de todos los servicios críticos de la institución, considerando desde un sitio principal hasta un Segundo sitio.

E.4.4 Incorporar las mejoras requeridas al plan de continuidad en base a los resultados de la aplicación de pruebas.

F. Seguimiento a recomendaciones del periodo anterior

Se presenta a continuación la matriz de seguimiento de recomendaciones[4] que se han incorporado en informes sobre tecnología de información anteriores y se encuentran en proceso de atención.

La matriz incluye el año de corte del informe, el nombre del hallazgo y el nivel de riesgo indicado en el año del informe, el estado actual de cumplimiento, la descripción de la observación, la(s) recomendación (es) y comentario de la administración.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
F.1	31/12/2022	**Ausencia de un plan de tratamiento de riesgos de seguridad de la información y privacidad.** **Riesgo Medio**	☐	☒	☐

Recomendación

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

Comentario de la administración

La DTIC había remitido a PROCI el oficio DTIC-2023-100 en agosto 2023 donde se explica que de momento no es posible proporcionar una fecha.

Además, la DTIC remitió a Recursos Humanos el oficio DTIC-2023-122 para solicitud de creación de plaza CISO.

El Consejo de Rectoría, toma el acuerdo sesión No. 2293-2023, Artículo I, inciso 4), celebrada el 30 de octubre del 2023 (REF.: CR-2023-2111), donde se indica que a más tardar para el 15 de diciembre del 2023 se debe entregar el detalle de las acciones realizadas en torno a este hallazgo.

[4] Observaciones realizadas por otras firmas de auditores

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.2	31/12/2021	**Ausencia de un plan para la gestión de la capacidad, disponibilidad y desempeño de la plataforma tecnológica.** **Riesgo Bajo**	☐	☒	☐

Recomendación

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).

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.

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.

Comentario de la administración

Este hallazgo va en ejecución, se ha finalizado con la actividad del inventario, el cual no se adjunta por contener información sensible. La actualización del inventario es una actividad permanente.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.3	30/11/2021	**Ausencia de un procedimiento para la gestión de la calidad y seguimiento de los Procesos de TI.** **Riesgo Bajo**	☒	☐	☐

Recomendación

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.

Comentario de la administración

1. 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.

2. Punto 2: CORREGIDO. 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.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.4	31/12/2021	**Ausencia de un inventario actualizado de licencias instaladas por equipo** **Riesgo Bajo**	☐	☒	☐

Recomendación

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.

Comentario de la administración

Se adjunta como evidencia un correo que detalla las acciones realizadas.
RE-SEGUIMIENTO CG-TI 2021 Auditoría Externa Hallazgo 04 INVENTARIO ACTUALIZADO DE LICENCIAS INSTALADAS POR EQUIPO
Dada la nueva Ley de Contratación, el proceso de compra ha tenido mucho retraso y por ende su proceso de implementación.

Se adjunta como evidencia acciones que se han realizado para considerar la instalación del AGENTE ARANDA en las computadoras: Remisión Oficio DTIC-2023-088 Formalización DTIC UST D01 Condiciones mínimas generales del equipo de cómputo.
Además, es importante mencionar que este hallazgo, forma parte de la ejecución o implementación del MGGTI-UNED. Al respecto también se está a la espera de que se concrete una consultoría que colabore con el abordaje de los productos. Han existido varios atrasos en el proceso de contratación, dada la nueva Ley de contratación.

Se adjunta como evidencia los oficios Ref. 005-2023 MGGTI y Oficio Ref. 006-2023 MGGTI remitidos a la CETIC y los cuales ya fueron vistos, únicamente se está a la espera de los respectivos acuerdos y de que el proceso en la OCS avance.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.5	31/12/2021	**Ausencia de lineamientos documentados para la gestión de infraestructura tecnológico** **Riesgo Bajo**	☐	☒	☐

Recomendación

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.

Comentario de la administración

Sobre este hallazgo, no se ha podido avanzar, ya que, la DTIC primeramente se ha enfocado a destinar esfuerzos por generar la actualización de los diferentes procedimientos primarios de todas las unidades y se está pronto a remitir a aprobación el procedimiento de la Unidad de Seguridad Digital que es el que falta, sin embargo, con la demanda de cumplimiento de las Normas Técnicas SINPE dadas por el Banco Central, esta labor se tendrá que retrasar un año y medio más, para que los diferentes responsables de la actualización de los contenidos del documento, puedan realizar una revisión detallada.

Se solicita que esto sea programado para noviembre 2025, dado que también requiere apoyo del CPPI y aprobación por parte del CONRE en algunos productos.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.6	31/12/2021	**Debilidades en la gestión de perfiles de los usuarios de los sistemas de información de la UNED.** **Riesgo Bajo**	☒	☐	☐

Recomendación

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.

Comentario de la administración

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 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.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.7	31/12/2021	**Debilidades en la definición y administración de acuerdos de servicio** **Riesgo Normal**	☐	☒	☐

Recomendación

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.

Comentario de la administración

Sobre este hallazgo, forma parte de la ejecución o implementación del MGGTI-UNED. Al respecto también se está a la espera de que se concrete una consultoría que colabore con el abordaje de los productos. Han existido varios atrasos en el proceso de contratación, dada la nueva Ley de contratación.

Se adjunta como evidencia los oficios Ref. 005-2023 MGGTI y Oficio Ref. 006-2023 MGGTI remitidos a la CETIC y los cuales ya fueron vistos, únicamente se está a la espera de los respectivos acuerdos y de que el proceso en la OCS avance.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.8	31/12/2021	**Cumplimiento parcial del plan de respaldos del centro de datos** **Riesgo Bajo**	☒	☐	☐

Recomendación

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.

Comentario de la administración

Aprobado mediante acuerdo tomado por el Consejo de Rectoría, sesión extraordinaria No. 2318-2024, Artículo VI, inciso 2) celebrada el 27 de mayo del 2024 (REF.: CR-2024-935) UIT Procedimiento PUNED DTIC-UIT 01Gestión de la infraestructura de Tecnologías de Información y documentos DUNED DTIC-UIT 01.01, DUNED DTIC UIT 01.02; DUNED DTIC-UIT 01.03, DUNED DTIC-USI 00.01, FUNED DTIC-UIT 01.00.01, FUNEDDTICUIT01.00.02, FUNED DTIC-UIT 01.02.01, FUNED DTIC-UIT 01.02.02, IUNED DTIC-UIT 01.02.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
F.9	31/12/2021	**Debilidades en la gestión de la seguridad de la información** **Riesgo Bajo**	☐	☒	☐

Recomendación

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.

Comentario 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.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
F.10	31/12/2021	**Debilidades en la gestión de la continuidad de las tecnologías de información** **Riesgo Medio**	☐	☒	☐

Recomendación

1. Colaborar en las situaciones en que se requiera información, participación o asesoría técnica para cumplir con las recomendaciones y subsanar las debilidades encontradas.

Comentario de la administración

Es importante mencionar que en tema de Continuidad un equipo de trabajo estaba siendo convocado y coordinado por el señor Carlos Montoya de la Vicerrectoría de Planificación en su momento, sin embargo, el equipo de trabajo no se volvió a convocar y es necesario que se designen las responsabilidades para continuar con el curso que se llevaba y retomar los productos que estaban siendo elaborados.

	Carta	Asunto	Estado		
			Atendido	En proceso	N/A
F.11	31/12/2021	**Debilidades encontradas en algunos de los sistemas de información de la UNED** **Riesgo Bajo**	☐	☐	☒

Recomendación

1. Colaborar en las situaciones en que se requiera su participación en la implementación de las mejores a los sistemas.

Comentario de la administración

Se adjunta correo de evidencia que demuestra que no existen requerimientos por atender.RE Seguimiento HALLAZGO 11 CG-TI-202.

Anexo No. 1

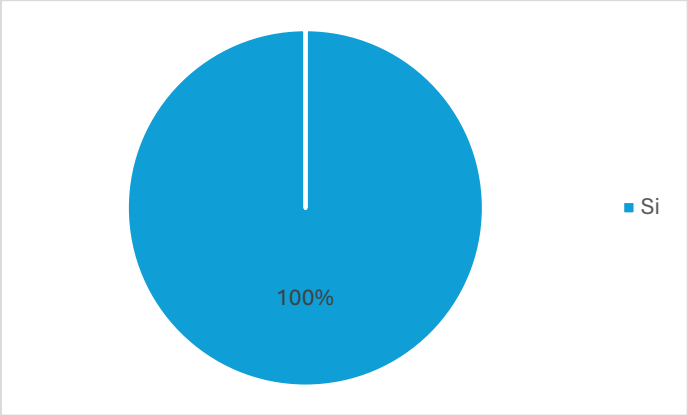
Se describen las actividades de cómo fueron ejecutadas las encuestas para los sistemas indicados en el alcance de la auditoria.

1. Se hace coordinación de agendas para explicar el objetivo y el completado de la encuesta con los colabores responsables.
2. Se reciben las respuestas completadas.
3. Se analizan y tabulan los resultados, los mismos se identifican por medio de gráficos para cada una de las preguntas solicitadas.

Pregunta No.1

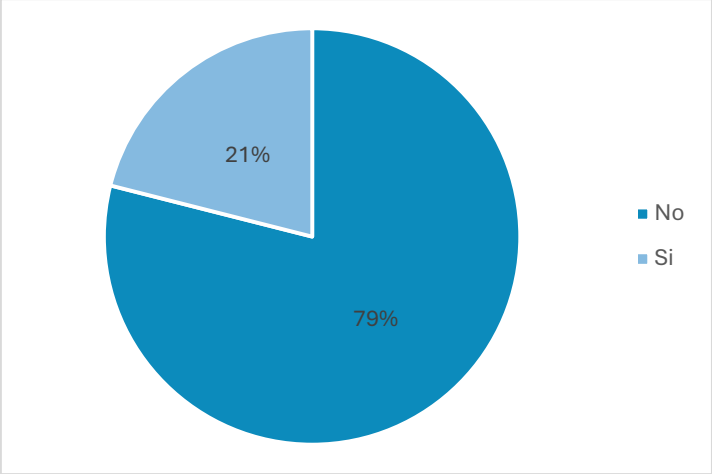
¿Se recibió capacitación para conocer el uso y funcionalidad del sistema?

Si	19
Total general	**19**



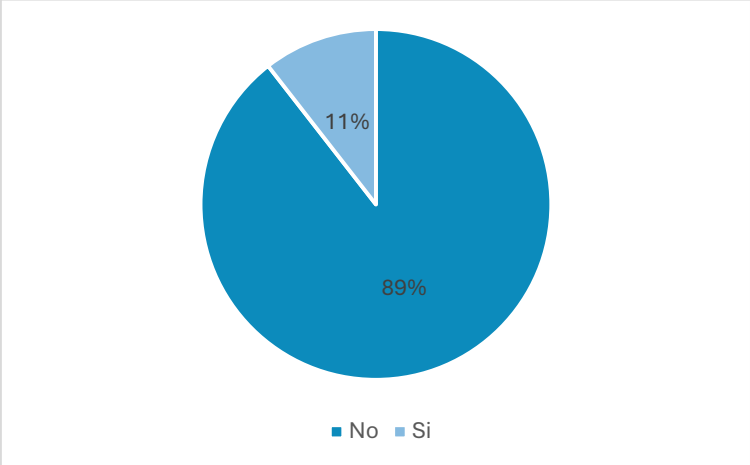
Pregunta No.2

¿Existen manuales de usuario para el sistema actualizados?	
No	15
Si	4
Total general	**19**



Pregunta No.3

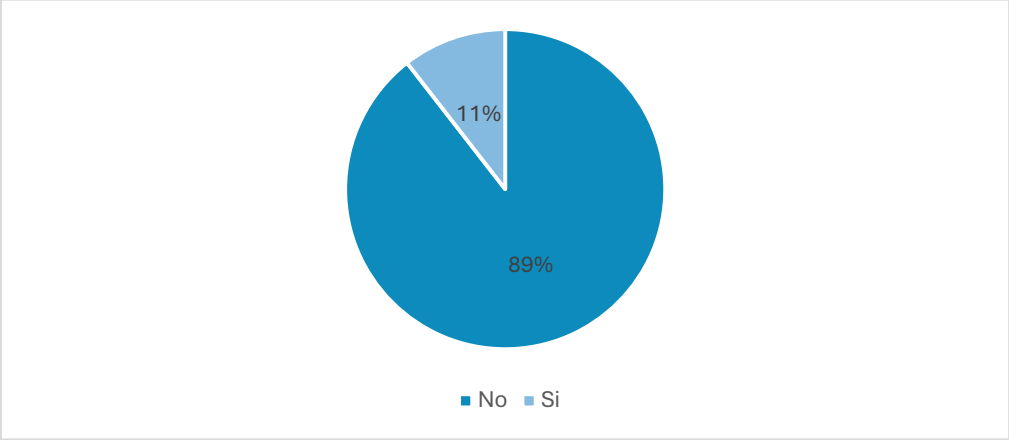
¿El sistema tiene recomendaciones de auditoría en proceso de atención?	
No	17
Si	2
Total general	**19**



Pregunta No.4

¿Ha participado en pruebas de continuidad de negocio planificadas, para identificar el tiempo o inconvenientes de volver a reanudar el uso del sistema ante un evento disruptivo?

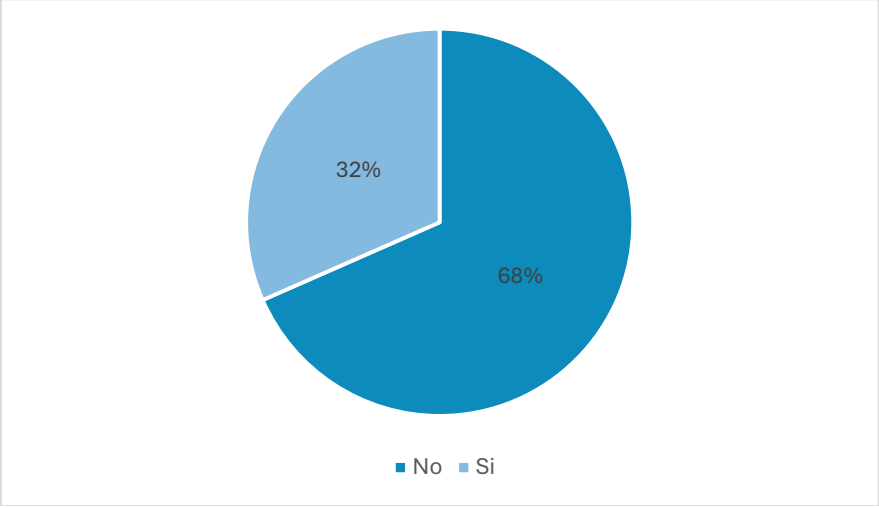
No	17
Si	2
Total general	**19**



Pregunta No.5

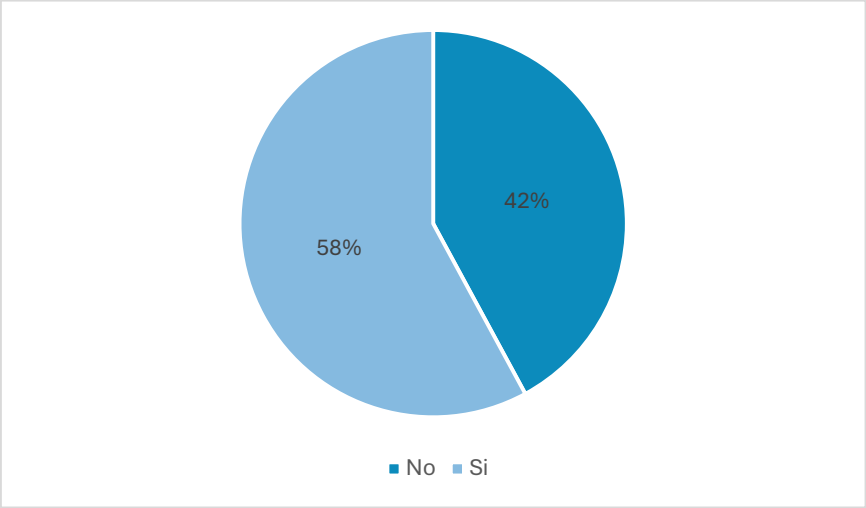
¿El sistema ha dejado de operar en los últimos 18 meses? ¿Cuánto tiempo estimado a estado fuera de servicio el sistema?

No	13
Si	6
Total general	**19**



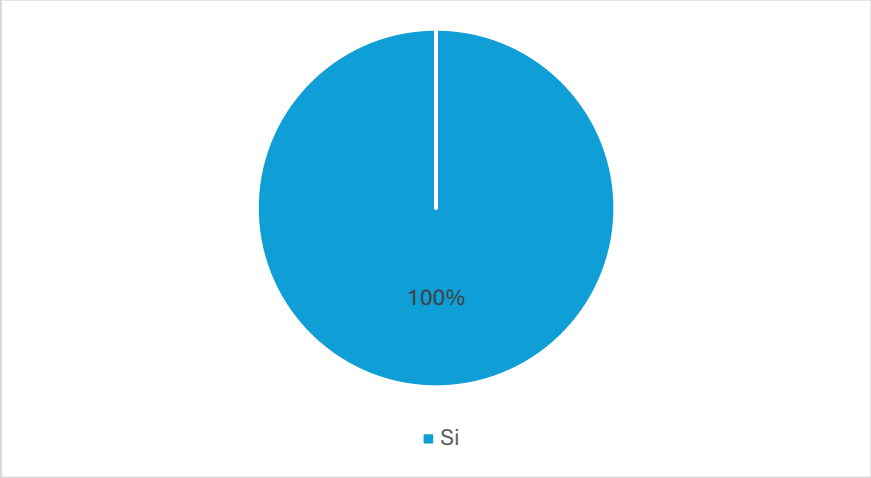
Pregunta No.6

¿Conoce como se hacen o ejecutan las interfases entre los sistemas vinculantes del AS400?	
No	8
Si	11
Total general	**19**



Pregunta No.7

¿El sistema tiene la capacidad de generar reportes de forma automática? ¿Los encuentra útiles para sus funciones?	
Si	19
Total general	**19**



Pregunta No.8

¿Se han considerado requerimientos para automatizar actividades o mejorar aspectos del sistema?

Si	19
Total general	**19**