Crowe Horwath CR, S.A.

Universidad Estatal a Distancia, S.A.

Sistema de tecnología de información

Al 31 de diciembre de 2024

Universidad Estatal a Distancia, S.A

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

31 de marzo de 2025

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

ASUNTO: CARTA SOBRE CONTROLES DE TECNOLOGIA DE INFORMACION

Al revisar la gestión de Tecnología de Información de Universidad Estatal a Distancia, S.A., como parte de la auditoría de los estados financieros al 31 de diciembre de 2024, observamos asuntos relacionados con las buenas prácticas de control de TI, sobre los cuales preparamos las conclusiones incluidas en el documento adjunto. Este informe se estructura como resultado del cumplimiento de las NIA 315 y 330; no es ni debe interpretarse como una evaluación 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 2024, y no para opinar sobre la estructura de control interno o los sistemas de información en su conjunto. Este informe no es ni debe interpretarse como una auditoría de los sistemas de información.

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 el sistema de tecnología de información.

Nuestra responsabilidad sobre este informe sobre sistema de tecnología de información al 31 de diciembre de 2024 se extiende hasta el día 31 de marzo de 2025. La fecha de la carta de gerencia indica al usuario, 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: 2025.05.06 15:02:32 -06'00'

Fabian 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: 05-05-2025 04:21:41 PM
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-25-485341

c.c. Comité de Auditoría

Universidad Estatal a Distancia, S.A

Sistema de tecnología de información

I. Resumen ejecutivo

Como parte del trabajo de la auditoría de los estados financieros del periodo 2024 se llevó a cabo la evaluación de controles para el área de Tecnología de Información (TI), de Universidad Estatal a Distancia, S.A (en adelante UNED) la cual 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" y marco normativo para TI y no es ni debe interpretarse como una auditoría de los sistemas de información, ni de la Jefatura de Tecnologías de Información de 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 se realiza la revisión para los siguientes módulos de los sistemas de información Contable y de Recursos Humanos:

<u>Sistema Financiero-Contable:</u>

- ✓ 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

Aunque no se puede eliminar completamente el riesgo inherente de ciberseguridad, se pueden reducir sus impactos mediante una gestión efectiva de riesgos, controles robustos y un monitoreo constante. Esto es esencial para proteger los activos digitales y garantizar la continuidad del negocio. El riesgo inherente en ciberseguridad se refiere a las amenazas y vulnerabilidades propias de los entornos tecnológicos que podrían comprometer la confidencialidad, integridad y disponibilidad de la información, sin considerar las medidas de mitigación o controles existentes.

En la evaluación del área de TI se identificaron 13 observaciones de seguimiento del periodo 2023, que de acuerdo con la naturaleza del riesgo se distribuyen de la siguiente manera: 15% representa un riesgo normal y un 85% representan un riesgo elevado.

Adicionalmente se identifican 5 observaciones del periodo 2021 y 2022 realizadas por otra firma de auditores en proceso de atención.

En la sección de conclusiones de este informe se comunican los resultados.

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 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 recomendaciones anteriores.

IV. Periodo de la evaluación

La evaluación se realizó durante los meses de diciembre 2024, febrero y marzo de 2025.

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, levantamiento de minutas, selección de muestras y verificación de la funcionalidad de los sistemas.

Entre los temas evaluados en cada área se indican los hallazgos evidenciados.

VI. Valoración basada en riesgo

Para determinar el nivel de riesgo al que se expone la entidad derivada del incumplimiento de aspectos normativos y/o deficiencias detectadas en el control interno, se procede a aplicar un análisis de impacto y frecuencia, que da como resultado la ubicación de este en un mapa de calor de 5x5 cuadrantes.

El riesgo puede evaluarse en términos de una combinación de frecuencia y magnitud y de acuerdo con dicha relación se concibe un nivel de exposición al riesgo y la posible medida a tomar en caso de mitigación.

VII. 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 continuación1:

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.

VIII. 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.

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

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

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.

IX. Conclusiones generales del año 2024

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.

Hay observaciones que han sido comunicadas sobre riesgos inherentes, financieros y de mercado en la Carta de Gerencia de la auditoría financiera que deben ser revisados de forma integral con este informe.

El riesgo inherente de ciberseguridad representa una exposición significativa y natural a las amenazas que enfrentan las organizaciones debido a la creciente dependencia de la tecnología y la conectividad digital. Este riesgo, definido por la naturaleza misma de los sistemas tecnológicos, existe independientemente de los controles implementados y afecta directamente la confidencialidad, integridad y disponibilidad de los datos y sistemas, motivo por el cual es inevitable pero gestionable. Requiere un enfoque proactivo y estratégico para proteger los activos tecnológicos y garantizar la resiliencia organizacional frente a las amenazas emergentes.

Seguimiento de observaciones del periodos 2023

Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
F.1	A.1 Oficial de seguridad de la información (2023)	Cumplimiento parcial bajo	Moderado	Alta	Elevado
F.2	A.2 Implementar el marco de gestión de TI (2023)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
F.3	A.3 Marco normativo para el uso de inteligencia artificial (2023)	Cumplimiento parcial bajo	Moderado	Baja	Normal
F.4	B.1 Aplicación de pruebas de vulnerabilidades (2023)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
F.5	B.2 Implementación del Sistema de Seguridad de la Información (2023)	Cumplimiento parcial bajo	Moderado	Alta	Elevado
F.6	B.3 Informe de revisión de roles y perfiles de usuario (2023)	Cumplimiento parcial bajo	Moderado	Alta	Elevado
F.7	D.1 Manuales de los sistemas sin actualizar o se carecen de los mismos (2023)	Cumplimiento parcial bajo	Moderado	Alta	Elevado
F.8	D.2 Informes sobre evaluaciones a los sistemas de información (2023)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
F.9	D.3 Sistemas sin aplicación de pruebas de continuidad (2023)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
F.10	E.1 Plan de continuidad de negocio (2023)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
F.11	E.2 Plan de capacitación sobre la continuidad de operaciones (2023)	Cumplimiento parcial alto	Moderado	Baja	Normal
F.12	E.3 Pruebas sobre restauración de respaldo (2023)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
F.13	E.4 Pruebas de continuidad de negocio (2023)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

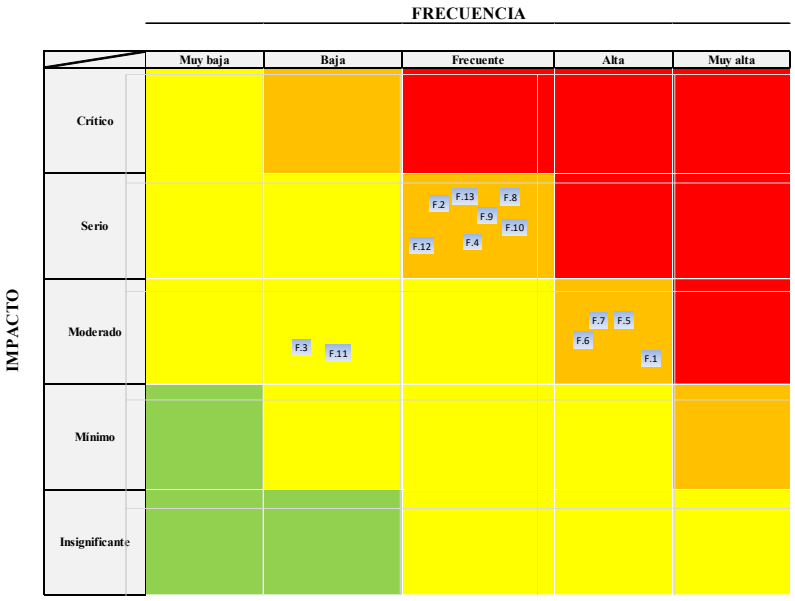
Seguimiento de observación del periodo 2022 y 2021

De las 7 observaciones de periodos anteriores[2] dos se encuentran atendidas según se indica en el "*Seguimiento plan remedial auditoria 2024*" y las siguientes observaciones se encuentran en proceso:

Ref.	Oportunidades de mejora
F.14	Ausencia de un plan de tratamiento de riesgos de seguridad de la información y privacidad. (2022)
F.16	Ausencia de un inventario actualizado de licencias instaladas por equipo (2021).
F.17	Ausencia de lineamientos documentados para la gestión de infraestructura tecnológico (2021).
F.18	Debilidades en la definición y administración de acuerdos de servicio (2021).
F.20	Debilidades en la gestión de la continuidad de las tecnologías de información (2021).

X. Mapa de calor de los riesgos evidenciados

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 las observaciones del 2023 de los controles de TI.

Como resultado de la revisión se comunican 13 observaciones que de acuerdo con la naturaleza del riesgo se distribuyen de la siguiente manera:

[2] Realizadas por otras firmas de auditores

- 2 de riesgo normal
- 11 de riesgo elevado

XI. 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.
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.
11. Actas del Comité de TI.
12. Evaluaciones de los SLA´s con los proveedores actuales de los servicios de TI.
13. Informes de avances sobre la implementación del Marco de Gobierno y TI alineado a las normas de tecnología del MICITT.
14. Cronograma de la implementación del Marco de Gobierno de TI.
15. Reglamento del Comité de TI.
16. Plan de capacitación a los colaboradores del área de TI del periodo y su grado de ejecución.

En la sección F) Seguimiento del periodo anterior de este informe, se incluye una matriz con el seguimiento de las recomendaciones en donde se identifican oportunidades de mejora en proceso de atención sobre la gestión de tecnología de información.

B. Gestión de la 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 2024.
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.

En la sección F) Seguimiento del periodo anterior de este informe, se incluye una matriz con el seguimiento de las recomendaciones en donde se identifican oportunidades de mejora en proceso de atención sobre la gestión de seguridad de la información.

C. Gestión de riesgos de tecnologías de información

En la revisión de estas actividades se verificó lo siguiente:

1. Plan de acción para mitigar los riesgos.
2. Evaluaciones de riesgos de TI a los procesos o servicios.
3. Informes de riesgos comunicados a los Órganos de Dirección.
4. Marco normativo para la gestión de riesgos.

De acuerdo con el resultado de las pruebas realizadas no evidenciamos situaciones que nos hagan creer que no se cumple con los requerimientos de gestión de riesgos de tecnologías de información al 31 de diciembre de 2024.

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.

En la sección F) Seguimiento del periodo anterior de este informe, se incluye una matriz con el seguimiento de las recomendaciones en donde se identifican oportunidades de mejora en proceso de atención sobre la gestión de sistemas de información.

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.

En la sección F) Seguimiento del periodo anterior de este informe, se incluye una matriz con el seguimiento de las recomendaciones en donde se identifican oportunidades de mejora en proceso de atención sobre la gestión de continuidad de negocio.

F. Seguimiento del periodo anterior

Se presenta a continuación la matriz de seguimiento de recomendaciones que se ha incorporado en informes sobre tecnología de información.

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	**31/12/2023**	**A.1 Oficial de seguridad de la información** **Riesgo 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).

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.

Comentario de la administración 2024:

1. *Dar seguimiento mediante oficio y correo electrónico a la solicitud de creación de la Plaza de CISO.*
2. *Una vez que se cuente con el Código de plaza de CISO, se debe buscar el perfil idóneo para el puesto. Proceso que debe ser validado por las Autoridades Universitarias.*
3. *Asignar las funciones respectivas como Oficial de Seguridad de la Información para la UNED.*

A.1.1 *Detalle en anexo No. 2 y 4 del oficio DTIC-2024-137.*

EN PROCESO.

1. Dar seguimiento mediante oficio y correo electrónico a la solicitud de creación de la Plaza de CISO.
2. Una vez que se cuente con el código de plaza de CISO, se debe buscar el perfil idóneo para el puesto. Proceso que debe ser validado por las Autoridades Universitarias.
3. Asignar las funciones respectivas como Oficial de Seguridad de la Información para la UNED.
Evidencia:
Acuerdo CONRE (CR-2024-1155) ORH.2024.648 Sobre estudio técnico creación plaza Analista Informático DTIC (REF.1701-2024)
nota 025-2023 CONRE Solicitud de recurso humano para Seguridad Digital (firmado)

A.1.2 *Detalle en anexo No. 2 y 4 del oficio DTIC-2024-137.*
ATENDIDA.

Se cambia el estado a "Atendida", en el primer semestre del 2024 se ejecutó la valoración de riesgos a los Sistemas de Información general, donde se contemplan los riesgos de seguridad de la información y ciberseguridad.

Evidencia:
PROCI-110-2024 Valoración del riesgo Sistemas de información.
VR_Sistemas de información 2024

A.1.3 *Detalle en anexo No. 2 y 4 del oficio DTIC-2024-137.*
ATENDIDA.

Dar continuidad al Programa Plan de Concienciación de Ciberseguridad ambiente SINPE.
Evidencia:
Programa Plan de Concienciación de Ciberseguridad ambiente SINPE

A.1.4 *Detalle en anexo No. 2 y 4 del oficio DTIC-2024-137.*
EN PROCESO.

1. Continuar con la implementación de herramientas y prácticas de monitoreo para detectar actividades sospechosas, esto como parte del cumplimiento de la Norma de Ciberseguridad de SINPE BCCR y el Marco de Gobierno y Gestión de TI de la UNED, con el apoyo del Servicio de SOC SIEM que cuenta la UNED actualmente.

2. Continuar con el desarrollo e implementación del Plan de Respuesta a Incidentes de la UNED, esto como parte del cumplimiento de la Norma de Ciberseguridad de SINPE BCCR y el Marco de Gobierno y Gestión de TI de la UNED, con el apoyo del Servicio de SOC SIEM que cuenta la UNED actualmente.

3. Planificar y coordinar la Ejecución de ejercicios de respuesta a incidentes producto de la implementación de la Norma de Ciberseguridad de SINPE BCCR.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.2	**31/12/2023**	**A.2 Implementar el Marco de Gestión de TI** **Riesgo 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.

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.

Comentario de la administración 2024:

Esto va alineado con el plazo del PTTI (2023-2027).

Se evidencia oficio remitido a la Auditoría Interna donde describe el avance que se tiene en cuanto a Servicios de TI. Oficio DTIC-2024-136.

A.2.1 *Detalle en anexo No. 2 y 4 del oficio DTIC-2024-137.*
EN PROCESO.

Esto va alineado con el plazo del PTTI (2023-2027)
Se adjunta como evidencia oficio remitido a la Auditoría Interna donde describe el avance que se tiene en cuanto a Servicios de TI. Oficio DTIC-2024-136.

A.2.2
EN PROCESO.

** La Institución cuenta con un estándar para documentar los procesos (Guía para el desarrollo de documentación PUNED CPPI 01 V5), conforme se vaya implementando el MGGTI-UNED y se van identificando los respectivos procesos, se documentarán siguiendo el estándar documental. Este perfil de proceso se satisface cuando los procesos que se han identificado en la implementación del MGGTI-UNED se hayan documentados.*
** Se estará analizando por parte del CPPI la opción de realizar una mejora en la guía de documentación con el fin de incorporar indicadores de desempeño y poder atender el punto 6.*

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.3	**31/12/2023**	**A.3 Marco normativo para el uso de inteligencia artificial** **Riesgo 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.

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.

Comentario de la administración 2024:

A.3.1 En proceso
02/04/2025:

1. *Existe el documento llamado Orientaciones generales de uso de la Inteligencia Artificial en la UNED. Este documento fue aprobado por el Consejo de Rectoría en junio del año pasado. Este documento es el único lineamiento oficial relacionado a la IA.*

2. *A raíz de ese documento, el CU inició la gestión para crear una Política de Inteligencia Artificial de la UNED. Ya el borrador de la política está, se trabajó desde la Comisión de Políticas de Desarrollo Académico y una comisión específica que se nombró para esto y, ahora, y según los acuerdos que adjunto, está a la espera de observaciones por parte de los Vicerrectores de Docencia, Investigación, Vida Estudiantil y Extensión. Según el acuerdo, tenían tiempo de enviar sus observaciones a más tardar el 31 de marzo, por lo que esperaríamos que pronto se esté aprobando una Política de IA en la UNED, y así se pueda marcar como atendido.*

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.4	**31/12/2023**	**B.1 Aplicación de pruebas de vulnerabilidades** **Riesgo 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.

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.

Comentario de la administración 2024:

UNED fortalece implementación de buenas prácticas en ciberseguridad.

Acuerdo CONRE (CR-2024-606). DTIC-2024-046 Declaratoria interés institucional capacitación Track Gestión de la Ciberseguridad (REF.905-2024).

B.1.1
EN PROCESO.
1. Investigar opciones en el mercado para el escaneo de vulnerabilidades de ambientes IBMi.
2. Solicitar presupuesto para la adquisición de la solución.
3. Realizar trámite de compra de la solución.
4. Implementación de la solución.

B.1.2
Sin iniciar.

1. Investigar opciones en el mercado para el escaneo de vulnerabilidades de ambientes IBMi.
2. Solicitar presupuesto para la adquisición de la solución.
3. Realizar trámite de compra de la solución.
4. Implementación de la solución.
5. Desarrollar el programa de pruebas de vulnerabilidades de ambientes IBMi.

B.1.3
ESTADO: PROCESO

COMENTARIO: Se realizaron pruebas de vulnerabilidades y pent test y se están tomando medidas para cerrar las brechas.

B.1.4
ESTADO: ATENDIDA
COMENTARIO: Esta es una labor permanente, se generan espacios a nivel institucional

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
F.5	**31/12/2023**	**B.2 Implementación del Sistema de Seguridad de la Información Riesgo 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.

Recomendación

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.

Comentario de la administración 2024:

Fecha de implementación diciembre 2027.

B.2.1
ESTADO: Proceso
COMENTARIO: ya se inició con el desarrollo de productos que respondan a la implementación del Objetivo de Gobierno "Seguridad de la Información" del Marco de Gobierno y Gestión de TI de la UNED.

B.2.2
Sin iniciar.

Esto le corresponde al Consejo Universitario una vez que cuente con dicha política.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
F.6	**31/12/2023**	**B.3 Informe de revisión de roles y perfiles de usuario** **Riesgo 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.

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.

Comentario de la administración 2024:

B.3.1
Sin iniciar

** Revisar el procedimiento PUNED DTIC-USI 05 Gestión de usuarios y accesos en el AS400 e incorporar las mejoras necesarias (Revisión de roles y mantenimiento de roles).*

** Incorporar en las mejoras del procedimiento la confección al menos una vez al año de un informe sobre roles y accesos de los colaboradores a los sistemas, aplicativos y herramientas de trabajo.*
** Revisar el FUNED DTIC USI 05.00.02 Accesos tramitados en el AS400 para determinar mejoras al formulario y que le permita al Líder de servicio poder registrar los cambios en los roles.*
** Validar las mejoras con algunos Líderes de servicio y Director DTIC.*
Solicitar al CONRE la aprobación de la nueva versión.
** Divulgación de las mejoras con los Líderes de servicio. (1 mes posterior a la aprobación del procedimiento por parte del CONRE)*

B.3.2
Sin iniciar

** Una vez que se cuente con las mejoras aprobadas por parte del CONRE, en el procedimiento PUNED DTIC-USI 05 para generar al menos una vez al año informe sobre roles y accesos de los colaboradores a los sistemas, aplicativos y herramientas de trabajo, el Líder de Servicio tendrá un periodo de al menos un año para construir cierto registro de datos.*

B.3.3
Sin iniciar

** Para esta recomendación se estará analizando si es necesario alguna actualización en algún marco normativo para la revisión de cuentas de usuario y perfiles de acceso.*

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
F.7	**31/12/2023**	**D.1 Manuales de los sistemas sin actualizar o se carecen de los mismos** **Riesgo 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.

Sistemas de información sin manuales de usuario a los sistemas:

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

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.

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.

Comentario de la administración 2024:

D.1.1
ESTADO: PENDIENTE.

COMENTARIO: Se solicitará reunión a vicerrector ejecutivo para analizar el tema, pues no tiene sentido hacer manuales de algo que será sustituido por el GRP

D.1.2
ESTADO: PROCESO.

COMENTARIO: Se optó por cambiar las capacitaciones, por una serie de infografías con la temática principal para comunicarla a los analistas y publicarlas también en la red social de DTIC ágil

D.1.3
ATENDIDA.

Ya se cuenta con el procedimiento "PUNED DTIC-USI 01 Desarrollo y mantenimiento de sistemas de información" donde en Responsabilidades especifica lo siguiente "Por último, es responsable de la generación y actualización de la documentación relacionada con el manual de usuario, el manual técnico de la aplicación desarrollada y cualquier otro artefacto que le corresponda dentro de las actividades definidas en la planificación del sprint.", además, en el Anexo 5. Ejemplo de lista de tareas generales de la planificación del sprint. Se incluye lo siguiente: Generar documentación técnica y Actualizar diccionario de datos (Análisis y Diseño) y Documentar / actualizar el manual de usuario (Desarrollo).

En este sentido ya la recomendación se encuentra ATENDIDA, porque en cada desarrollo se actualiza lo que corresponda del manual de usuario y documentación técnica. Lo que queda pendiente es la D.1.1 que es la generación de los manuales pendientes.

Evidencia:
PUNEDDTIC-USI_01Procedimiento DesyMante sistemasinformación

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.8	**31/12/2023**	**D.2 Informes sobre evaluaciones a los sistemas de información Riesgo 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.

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.

Comentario de la administración 2024:

D.2.1 *Detalle en anexo No. 2 y 4 del oficio DTIC-2024-137.*
ATENDIDA.

Evidencia:
Security Assestment Analysis DB2 (IBMi AS400) Carta de Gerencia CG-TI-2023.

1. Investigar opciones en el mercado para el escaneo de vulnerabilidades de base de datos DB2 IBMi.
2. Solicitar presupuesto para la adquisición de la solución.
3. Realizar trámite de compra de la solución.

D.2.2
ESTADO: ATENDIDA.

COMENTARIO: ya están realizando evaluaciones de vulnerabilidades

D.2.3
Sin iniciar.

1. Investigar opciones en el mercado para el escaneo de vulnerabilidades de base de datos DB2 IBMi.
2. Solicitar presupuesto para la adquisición de la solución.
3. Realizar trámite de compra de la solución.
4. Implementación de la solución.
5. Elaborar la normativa respectiva para el escaneo de vulnerabilidades de base de datos DB2 IBMi.
6. Solicitar la aprobación de la normativa elaborada.
7. Poner en práctica el proceso de escaneo de vulnerabilidades de base de datos DB2 IBMi.

D.2.4 *Detalle en anexo No. 2 y 4 del oficio DTIC-2024-137.*
ATENDIDA.

Dar continuidad al Programa Plan de concienciación de Ciberseguridad ambiente SINPE.

Evidencia:
Programa Plan de concienciación de Ciberseguridad ambiente SINPE

D.2.5 *Detalle en anexo No. 2 y 4 del oficio DTIC-2024-137.*
ATENDIDA.

Evidencia:
Security Assestment Analysis DB2 (IBMi AS400) Carta de Gerencia CG-TI-2023
Aplica las mismas recomendaciones del punto D.3.3

D.2.6
EN PROCESO.

1. Remediación de las brechas detectadas como parte del proceso de mejora continua a partir de las acciones D.2.5.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
F.9	**31/12/2023**	**D.3 Sistemas sin aplicación de pruebas de continuidad** **Riesgo Elevado**	☐	☐	☒

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

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.

Comentario de la administración 2024:

Fecha de implementación septiembre 2026.

D.3.1 Sin iniciar.

D.3.2 Sin iniciar.

D.3.3 Sin iniciar.

D.3.4 Sin iniciar.

** Se solicitó en Inversiones 2025 el presupuesto requerido para adquirir Unidad Hiperconvergente, servidores y equipos de almacenamiento para contar con el espacio requerido. Ya que, lo que se realizará es un reacomodo de equipos para hacer la mayor optimización de los recursos.*

** Entre el 2025 y 2026 se estará adquiriendo una nueva Unidad Hiperconvergente, esto generará mayor espacio para realizar copias de los entornos y realizar las pruebas correspondientes. Este proceso conlleva todas las acciones del pliego de condiciones, adquisición, configuración, entre otros.*

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
F.10	**31/12/2023**	**E.1 Plan de continuidad de negocio** **Riesgo 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 prácticas y el marco regulatorio.

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.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
F.11	**31/12/2023**	**E.2 Plan de capacitación sobre la continuidad de operaciones** **Riesgo 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.

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.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
F.12	**31/12/2023**	**E.3 Pruebas sobre restauración de respaldos** **Riesgo 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.

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.

Comentario de la administración 2024:

E.3.1 Sin iniciar.
Fecha de implementación septiembre 2026.

** En el 2024 se adquirió una unidad nueva de respaldos de información en cinta, que fue implementada a inicios del 2025, esto ayuda a aumentar la capacidad de respaldos en cinta y su velocidad. Esto como proceso de continuidad. De la misma forma que en el punto D.3 Sistemas sin aplicación de pruebas de continuidad, se está la espera de la adquisición de la nueva Unidad Hiperconvergente.*

E.3.2 Sin iniciar.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.13	**31/12/2023**	**E.4 Pruebas de continuidad de negocio** **Riesgo 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.

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.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.14	31/12/2022	**(F.1) Ausencia de un plan de tratamiento de riesgos de seguridad de la información y privacidad.[1]**	☐	☒	☐

Recomendaciones

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 2024:

EN PROCESO. Detalle en anexo No. 2 y 4 del oficio DTIC-2024-137.

Se adjunta correo que evidencia el avance que se lleva.

Seguimiento CG-TI 2022 Auditoría Externa Hallazgo 01 AUSENCIA DE UN PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.15	31/12/2021	**(F.2) Ausencia de un plan para la gestión de la capacidad, disponibilidad y desempeño de la plataforma tecnológica.[1]**	☒	☐	☐

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.

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.

Comentario de la administración 2024:

ESTADO: ATENDIDA

Se cuenta con •DTIC UIT D01 Guía para la gestión de la capacidad de la Infraestructura TI y •DTIC UIT F01 Plan para la gestión de la capacidad de la Infraestructura TI aprobados mediante oficio DTIC-2015-014.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
F.16	31/12/2021	**(F.4) Ausencia de un inventario actualizado de licencias instaladas por equipo.[1]**	☐	☒	☐

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 2024:

Se adjunta "Remisión Oficio DTIC-2023-088 Formalización DTIC UST D01 Condiciones mínimas generales del equipo de cómputo" como parte de los mecanismos.

Se ha realizado un barrido manual, tanto Sede Central como en Sedes Universitarias para garantizar que cuenten con el agente del Aranda y adicionalmente se creó una tarea programada para que desde la consola detecte cuando hay un equipo nuevo en la red institucional, instale el agente, esto permite que se pueda generar varios tipos de reportes en cuanto a software instalado en los equipos.

EN PROCESO. Detalle en anexo No. 2 y 4 del oficio DTIC-2024-137.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.17	31/12/2021	**(F.5) Ausencia de lineamientos documentados para la gestión de infraestructura tecnológico**[1]	☐	☐	☒

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):

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 2024:

Nueva fecha propuesta: noviembre 2025

En vista de que la Institución está enfocada en la implementación del Marco de Gobierno y Gestión de TI (MGGTI-UNED) y en este año 2024 nos hemos apoyado en Servicios de Consultoría en TI (Licitación Reducida 2023LD-000407-0017699999) que está en ejecución, la cual finaliza en noviembre del 2024 y a través de esta licitación se han generado los primeros esfuerzos en materia de Gestión de Servicios TI, se cuenta con un borrador del Catálogo de Servicios de TI y de los acuerdos de nivel de servicio de los Servicios de TI identificados, es que este hallazgo debe ser valorado bajo lo que se está implementado y se espera contar con una segunda contratación así, que por eso se solicitó 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.18	31/12/2021	**(F.7) Debilidades en la definición y administración de acuerdos de servicio.[1]**	☐	☒	☐

Recomendación

1. Elaborar los OLAs faltantes para los servicios de TI con mayor prioridad. Se recomienda 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 2024:

Nueva fecha propuesta: noviembre 2025

Con los avances que se ha tenido este año 2024 en la implementación del Marco de Gobierno y Gestión de TI (MGGTI-UNED), con el apoyo de Servicios de Consultoría en TI (Licitación Reducida 2023LD-000407-0017699999) que está en ejecución, la cual finaliza en noviembre del 2024 y a través de esta licitación se han generado los primeros esfuerzos en materia de Gestión de Servicios TI, se cuenta con un borrador del Catálogo de Servicios de TI y de los acuerdos de nivel de servicio de los Servicios de TI identificados, se está en un proceso de validación interno y se está definiendo una plantilla para los acuerdos de nivel operativo, la cual se empezará a trabajar en noviembre con el equipo de trabajo.

Dado esta situación se solicita que esto sea programado para Noviembre 2025, dado que para los acuerdos de nivel de servicio (SLA) se requiere aprobación del Rector o del CONRE y en el caso de OLA del Director de la DTIC.

EN PROCESO. Detalle en anexo No. 2 y 4 del oficio DTIC-2024-137.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.19	31/12/2021	**(E.9) Debilidades en la gestión de la seguridad de la información[1]**	☒	☐	☐

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 2024.

ATENDIDA.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
F.20	31/12/2021	**(F.10) Debilidades en la gestión de la continuidad de las tecnologías de información**[1]	☐	☒	☐

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 2024:

Nueva fecha propuesta: junio 2027

Es importante respecto al tema de continuidad lo que se detalla en el oficio DTIC-2024-136 que se remitió a la Auditoría Interna, ya que, todo se relaciona de forma integral.

Justificación: Se cuenta con la Política de gestión del riesgo y continuidad de los servicios en la UNED, publicada en el CIBRED, esta política ya cuenta con una actualización para involucrar lo referente a continuidad. El tema de continuidad de negocio (Servicios institucionales), es fundamental para las demás actividades, se visualiza un proceso largo que se espera que sea iniciado en una segunda contratación (2025) que está en curso en la Oficina de Contratación y Suministros y podría abarcar de 2 a 3 años al menos para que la institución cuente con un plan de continuidad de los servicios institucionales identificados como críticos. Se adjunta además un correo "RE Sobre Objetivo de Gestión - Continuidad y disponibilidad operativa de los servicios de TI (MGGTI-UNED)".