Auditoría Interna
Tel: 2527 2276
Telefax: 2224 9684
Apdo. 474-2050 / San Pedro de Montes de Oca

UNED
UNIVERSIDAD ESTATAL A DISTANCIA
Institución Benemérita de la Educación y la Cultura

AUDITORÍA INTERNA UNIVERSIDAD ESTATAL A DISTANCIA

INFORME FINAL

ESTUDIO SOBRE SEGURIDAD FÍSICA y LÓGICA EN EL SITIO ALTERNO DEL DATA CENTER DE LA UNED

ACE-001-2021

2021

Auditoría Interna
Tel: 2527 2276
Telefax: 2224 9684
Apdo. 474-2050 / San Pedro de Montes de Oca
UNED
UNIVERSIDAD ESTATAL A DISTANCIA
Institución Benemérita de la Educación y la Cultura

Tabla de Contenido

Auditoría Interna
Tel: 2527 2276
Telefax: 2224 9684
Apdo. 474-2050 / San Pedro de Montes de Oca

UNED
UNIVERSIDAD ESTATAL A DISTANCIA
Institución Benemérita de la Educación y la Cultura

INFORME FINAL N° ACE-001-2021
(Al contestar refiérase a este número)

ESTUDIO SOBRE SEGURIDAD FÍSICA Y LÓGICA EN EL SITIO ALTERNO DEL DATA CENTER DE LA UNED

RESUMEN EJECUTIVO

Esta auditoría de carácter especial es relativa al Centro de Datos Alterno ubicado en el Centro Universitario de Cartago, se evalúan la seguridad física y lógica del lugar por la inversión realizada, aproximadamente $915,807.66, en equipo y software: VxBlock 350, servicios conexos, equipos de comunicación y de respaldo de la información de los procesos críticos de la institución.

El Centro de Datos Alterno presenta oportunidades de mejora en la seguridad ambiental y física, al facilitar el personal del Centro Universitario la llave de entrada sin que medie una bitácora de control; existe acumulación de objetos de limpieza, cajas y cables cerca de la puerta de ingreso; el recinto está expuesto a filtraciones de agua de lluvia, exceso de humedad, moho y óxido en las barras y placas del entrepiso. Situación que expone a la institución a pérdidas económicas por concepto de activos y a un posible acceso sin autorización previa e incumplimiento de lo establecido en la "*Directriz en cuanto al acceso a las instalaciones de la DTIC y DATACENTER por parte de terceros*". Por tal razón, se recomienda al director de la Dirección de Tecnología, información y comunicaciones en adelante DTIC, informar mediante oficio o correo electrónico al personal del CU de Cartago los lineamientos establecidos en la citada "Directriz" relacionada con el acceso a los centros de datos e implementar una bitácora o control equivalente, para registrar el ingreso de funcionarios y visitantes al Centro de Datos Alterno. A la Vicerrectora Ejecutiva quién ejerce por subrogación la jefatura a.i. de SERGE, gestionar las acciones de mantenimiento solicitadas mediante oficio DTIC-UIT-2021-015, considerando el riesgo materializado en el sitio; efectuar la calendarización y luego, la ejecución de los mantenimientos preventivos para resguardo de la seguridad física y ambiental del Centro de Datos Alterno, considerando el criterio técnico de la Unidad de Infraestructura Tecnológica en adelante UIT y el presupuesto necesario para cumplir con lo programado.

El sitio alterno carece de un procedimiento o instructivo formal para la gestión de respaldo de los datos guardados en los equipos informáticos "SERVIDORES",

elaborado bajo la orientación técnica del Centro de Planificación y Programación Institucional, en adelante CPPI y aprobado por la autoridad correspondiente; condición que dificulta la verificación del control, su cumplimento, logro de los objetivos, fiscalización del proceso, consulta y evaluación, se recomienda elaborar con la guía y acompañamiento técnico del CPPI, un procedimiento que regule el proceso de respaldo de la información de los servicios informáticos del Centro de Datos Alterno, elevarlo a la aprobación correspondiente y mantener su contenido actualizado. Al menos debe contener el propósito, procesos, responsables, mantenimientos y tiempo de recuperación deseables.

Además, la Oficina de Servicios Generales, en adelante SERGE, carece de una valoración de riesgos del tema objeto de estudio, condición que ha materializado eventos asociados con la seguridad ambiental, se recomienda realizar con el acompañamiento técnico del Programa de Control Interno, en adelante PROCI y la asesoría técnica de la UIT, la valoración de riesgos específica para la seguridad física y ambiental del Centro de Datos Alterno, que incluya al menos, la identificación de riesgos, probabilidad, acciones o medidas de mejora para la adecuada administración y minimizar su impacto, considerar recursos y procedimientos internos para dar seguimiento.

También se determinó que los puestos y funciones para “administrador de infraestructura de respaldos de información” y “administrador de infraestructura de servidores de datos Windows” y “Linux” están sin formalizar en la Estructura Orgánica y Funcional de la DTIC, aprobada en el acuerdo tomado por el Consejo Universitario en sesión No. 2862-2021, Art. II, inciso 6), celebrada el 28 de junio de 2021, tampoco en el documento “Roles y Funciones” aprobado por la CETIC en sesión No. 016-2018, Art. I, inciso 3), celebrada el 08 de octubre de 2018 ni en el Manual Descriptivo de Puestos de la UNED, se recomienda al director de la DTIC realizar en coordinación con el CPPI y la CETIC la actualización de los puestos que defina la DTIC para sus unidades, y someterla a la aprobación correspondiente.

La gestión del personal de la Unidad de Seguridad Digital, en adelante USD, para controlar, verificar e investigar incidentes de seguridad de la información en los Servidores de Datos de la UNED presenta limitaciones de acceso, generando que el personal de la USD tenga restricciones en el cumplimiento de funciones. Se recomienda al director de la DTIC, otorgar los permisos necesarios al personal de la USD -con los controles requeridos-, para que sean efectuadas las gestiones de seguridad lógica en la atención de incidentes en todos los servidores de datos de la

UNED, de acuerdo a lo establecido en la “Estructura orgánica y funcional de la DTIC”, e instrumento “Roles y Funciones.

1. INTRODUCCIÓN

1.1. Origen

El estudio corresponde a la función propia de la Auditoría Interna en cumplimiento del Plan Anual de Trabajo, período 2021.

1.2. Objetivos

Objetivo General

Evaluación de la Seguridad Física y Lógica del Sitio Alterno del Data Center de la UNED.

Objetivos Específicos

1. Verificar sí las condiciones de seguridad física y lógica del Sitio Alterno del Data Center que se ubica en Cartago, cumplen con la normativa nacional y mejores prácticas.

2. Determinar el uso (salvaguarda de procesos críticos), la existencia de un plan de recuperación y sus pruebas.

1.3. Alcance del estudio

Esta auditoría incluye el Centro de Datos Alterno, ubicado en el Centro Universitario de Cartago, específicamente en las áreas DTIC y SERGE, segundo semestre del 2020, ampliándose en los casos que se considere necesario.

1.4. Estudio realizado de acuerdo con la Normativa

La auditoría se realiza en cumplimiento de las normas, leyes y reglamentos que rigen los procedimientos de la Auditoría Interna en el Sector Público; además de conformidad con las “Normas Generales de Auditoría para el Sector Público” (R-DC064- 2014), publicada en la Gaceta N° 184 del 25 de setiembre de 2014.

1.5. Comunicación preliminar de los resultados de la Auditoría y Conferencia Final

El estudio fue presentado a la Vicerrectora Ejecutiva, en carácter de informe preliminar mediante el oficio AI-109-2021, del 25 de agosto del 2021, y recibido en esa fecha.

La comunicación preliminar de los resultados, conclusiones y recomendaciones producto de la auditoría a la que alude el presente informe fue efectuada el 14 de setiembre del 2021, a las 08:00 a.m., en forma virtual mediante la plataforma MS-TEAMS, en presencia de la Vicerrectora Ejecutiva quien ocupa por subrogación el puesto de la Jefatura de SERGE, el Coordinador de la UIT de la DTIC y el Coordinador la Unidad de Mantenimiento, en adelante UMI.

El director de la DTIC no convocó a la conferencia o presentación oral de los resultados del presente Informe. Las recomendaciones emitidas al director de la DTIC fueron aceptadas con una propuesta en redacción en la 4.5 mediante oficio DTIC-2021-329. Esta observación fue analizada por esta Auditoría Interna mediante oficio AI-124-2021 del 15 de setiembre del año en curso y lo resuelto se consigna en el Anexo No. 4 de este Informe.

1.6. Deberes en el trámite de informes y plazos que se deben observar

"ARTÍCULO 36.- Informes dirigidos a los titulares subordinados

Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:

a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.
b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de

su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.
c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda".

"ARTÍCULO 39.-Causales de responsabilidad administrativa

El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios. El jerarca, los titulares subordinados y los demás funcionarios públicos incurrirán en responsabilidad administrativa, cuando debiliten con sus acciones el sistema de control interno u omitan las actuaciones necesarias para establecerlo, mantenerlo, perfeccionarlo y evaluarlo, según la normativa técnica aplicable. Asimismo, cabrá responsabilidad administrativa contra el jerarca que injustificadamente no asigne los recursos a la auditoría interna en los términos del artículo 27 de esta Ley. Igualmente, cabrá responsabilidad administrativa contra los funcionarios públicos que injustificadamente incumplan los deberes y las funciones que en materia de control interno les asigne el jerarca o el titular subordinado, incluso las acciones para instaurar las recomendaciones emitidas por la auditoría interna, sin perjuicio de las responsabilidades que les puedan ser imputadas civil y penalmente. El jerarca, los titulares subordinados y los demás funcionarios públicos también incurrirán en responsabilidad administrativa y civil, cuando corresponda, por obstaculizar o retrasar el cumplimiento de las potestades del auditor, el subauditor y los demás funcionarios de la auditoría interna, establecidas en esta Ley. Cuando se trate de actos u omisiones de órganos colegiados, la responsabilidad será atribuida a todos sus integrantes, salvo que conste, de manera expresa, el voto negativo"

1.7. Limitaciones y antecedentes

La Auditoría Interna realizó en 2011 el estudio X-24-2011-02 “Seguridad física y lógica del Data Center de la UNED, ubicado en ese entonces, en las oficinas de la DTIC en el tercer piso del edificio B.

Actualmente, la institución cuenta con un Centro de Datos Alterno ubicado en el Centro Universitario de Cartago, con la finalidad de tener una opción confiable para respaldar los servicios informáticos prioritarios del Centro de Datos Principal en Sabanilla. Con la iniciativa número 8 del Acuerdo de Mejoramiento Institucional (AMI), se logra contar con este sitio desde octubre de 2019.

2. RESULTADOS DEL ESTUDIO

2.1. Oportunidad de mejora para el control en la seguridad física y ambiental del Centro de Datos Alterno

El Centro de Datos Alterno que respalda la información de los procesos críticos de la institución presenta oportunidades de mejora en la seguridad ambiental y física, la condición se evidencia en los siguientes aspectos:

1. El personal del Centro Universitario de Cartago facilita la llave de entrada al recinto del Centro de Datos Alterno, sin que medie una bitácora de control.

2. Almacenamiento y acumulación de objetos de limpieza, cajas plásticas y de cartón con repuestos y cables en la esquina derecha, cerca de la puerta. **(Ver Anexo N.1)**

3. El sitio se encuentra en el primer piso, cerca de la entrada principal, está expuesto a riesgo de filtraciones de agua de lluvia, al carecer de protección (techo más amplio) para evitar que ingrese agua a los corredores frontales y de costado. **(Ver anexo N.2)**

4. Exceso de humedad, moho y óxido en las barras y placas del entrepiso. El Coordinador de la UIT, con el oficio DTIC-UIT-2021-015 del 3 de marzo del año en curso, solicitó al jefe de la UMI, las acciones para corregir las debilidades detectadas en el piso falso, cableado y la humedad del lugar, puntualizando lo siguiente:

> *"…cables de fibra óptica con humedad y con moho, dentro del encapsulado donde se encuentran conectados en los equipos de comunicación del centro de datos.*
>
> *…óxido en las barras y placas que sostienen el entrepiso, principalmente en las partes que no poseen pintura.*
>
> *… en el entrepiso insectos como ciempiés, propios de la humedad del ambiente.*
>
> *… dentro del centro de datos, se percibe un olor a humedad bastante pronunciado.*
>
> *… La puerta principal del centro de datos la encontramos también con ciertas muestras de humedad.*

Durante la visita al Centro de Datos Alterno el 13 de mayo del año en curso, los problemas citados por el Coordinador de la UIT aún estaban sin solucionarse. Se requirió a la Vicerrectoría Ejecutiva mediante el oficio AI-066-2021 del 18 de mayo 2021, el estado de las acciones ejecutadas para atender la solicitud, estableciendo el jefe de la UMI en el oficio UMI-065-2021 del 16 de junio, la existencia de un proceso de licitación para que una empresa especializada brinde el mantenimiento respectivo, proceso que podría durar varios meses en adjudicarse mientras los problemas de seguridad ambiental avanzan.

El apartado 4.3 "Protección y conservación del patrimonio"; el 4.3.1 "Regulaciones para la administración de activos" inciso a) de las normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE); y el apartado 1.4.3 seguridad física y ambiental incisos b), d), f), g) y h) de las normas técnicas para la gestión y el control de las tecnologías de Información (N-2-2007-CO-DFOE) emitidas por la Contraloría General de la República, señalan lo siguiente:

> *"El jerarca y los titulares subordinados, según sus competencias, deben establecer, evaluar y perfeccionar las actividades de control interno pertinentes a fin de asegurar razonablemente la protección, custodia, inventario, correcto uso y control de los activos pertenecientes a la institución…*
>
> *El Jerarca y los titulares subordinados, según sus competencias, deben establecer, actualizar y comunicar las regulaciones pertinentes con respecto al uso, conservación y custodia de los*

activos pertenecientes a la institución. Deben considerarse al menos los siguientes asuntos:

a. La programación de las necesidades de determinados activos, tanto para efectos de coordinación con las instancias usuarias, como para la prevención de sustituciones, reparaciones y otros eventos.

La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos.

Como parte de esa protección debe considerar:

b. La ubicación física segura de los recursos de TI.

d. El debido control de los servicios de mantenimiento.

f. La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas.

g. El acceso de terceros.

h. Los riesgos asociados con el ambiente".

Esta situación se debe a falta de seguimiento en las acciones de mejora e incumplimiento de los objetivos establecidos para la administración de riesgos del Centro de Datos Alterno. Además, la gestión para atención de solicitudes de mantenimiento correctivo por parte de SERGE carece de premura y se omite una planificación anual preventiva, que considere la inversión realizada en los equipos e infraestructura que se ubican en el lugar.

El almacenamiento de implementos para limpieza y repuestos se debe a que la UIT no posee un sitio en el C.U. de Cartago para guardar los implementos y repuestos requeridos para sustento técnico de la infraestructura e higiene del lugar, por último, el director de la DTIC menciona que desconocía la situación con el personal del Centro Universitario de Cartago cuando se solicita la llave de ingreso al centro de datos. Lo que muestra la omisión de un control para el dispositivo que se encuentra en custodia por parte del personal del C.U. de Cartago.

Por consiguiente, el Centro de Datos Alterno presenta problemas en la estructura del piso falso, cables de fibra óptica con humedad y moho dentro del encapsulado donde se encuentran conectados los equipos de comunicación, óxido en las barras y placas que sostienen el entrepiso en donde no poseen pintura e insectos como ciempiés, propios de la humedad del ambiente, situación que expone

a la institución a pérdidas económicas por concepto de activos valorados aproximadamente en $915,807.66, equipo y software: VxBlock 350, Servicios Conexos, Equipos de comunicación y software.

Además, la ausencia de control en el manejo de la llave del Centro de Datos que actualmente custodia el personal del CU en Cartago expone a un posible acceso sin autorización previa e incumplimiento de lo establecido en la "*Directriz en cuanto al acceso a las instalaciones de la DTIC y DATACENTER por parte de terceros*" incluida en el Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones de la Universidad Estatal a Distancia.

2.2. Normativa para la gestión del proceso de respaldo y lineamientos relacionados con el Centro de Datos Alterno de Cartago

El Centro de Datos Alterno de la UNED ubicado en el C.U. de Cartago, carece de un procedimiento o instructivo formal para la gestión del respaldo de los datos albergados en los equipos informáticos "SERVIDORES", elaborado bajo la orientación técnica del CPPI, y aprobado por la autoridad correspondiente.

El director de la DTIC comunica que los aspectos relacionados con la recuperación de información y actividad diaria de los equipos del Centro de Datos Alterno, corresponden a las descritas en el archivo digital titulado "*Manual Usuario SITE RECOVERY MANAGER*" que adjuntó con el oficio DTIC-2021-063. Sin embargo, el instructivo no coincide con los lineamientos internos para la conformación de procedimientos establecido por el CPPI; el documento en mención es de la empresa SONDA S.A, proveedora del software para el proceso de respaldos en ese sitio.

Además, se aportó el "*Instructivo para respaldo de información del Centro de Datos principal 2019*", aprobado por el Consejo de Rectoría en sesión No. 2064-2020, Artículo IV, inciso 5), celebrada el 20 de enero del 2020 (REF.: CR-2020-0086), en este caso, tal como lo indica su título, es relativo al Centro de Datos Principal ubicado en el Edificio Ii+D de Oficinas Centrales en Sabanilla y no hace referencia al Centro de Datos Alterno.

En lo que respecta a lineamientos de seguridad en TI se determina que el *"Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones de la Universidad Estatal a Distancia*" aprobado por el Consejo de Rectoría en sesión No. 1950-2017, Artículo V, inciso 3), celebrada el 26 de junio del 2017 está desactualizado, al hacer mención solo al Centro de Datos, quedando pendiente de incluir los temas relacionados con el Centro de Datos Alterno. Este

archivo digital está publicado en la página web de la UNED, y consigna su fecha para revisión al 26 de junio del 2019.

Además, este Manual de Procedimientos para la Seguridad en TI, establece en el apartado de anexos una "*Directriz en cuanto al acceso a las instalaciones de la DTIC y DATACENTER por parte de terceros relacionada con el acceso a los centros de datos*", emitida por el director de la DTIC, y que no se comunica a los funcionarios de la UNED. Se notificó al personal de la DTIC, mediante nota circular DTIC-2018-197 del 24 de setiembre de 2018 "CIRCULAR Manual de Gestión TI y Manual de Seguridad de TI", cuando el alcance establece:

> *"De cumplimiento obligatorio para todos los funcionarios de la UNED, en relación al acceso a estas áreas restringidas con las que se cuenta actualmente, así como las implicaciones por los daños que puedan ocasionar*."

La situación descrita difiere de lo establecido en el artículo N.15 "Actividades de Control" inciso a) y b) apartado ii, de la Ley General de Control Interno N. 8292 publicada en la Gaceta N.169 del 4 de setiembre de 2002 y los apartados 1.4 "Responsabilidad del jerarca y los titulares subordinados sobre el SCI" en su inciso c), 4.1 "Actividades de Control", 4.4 "Exigencia de confiabilidad y oportunidad de la información", todas de las Normas de control interno para el Sector Público (N-2-2009CO-DFOE) emitidas por la Contraloría General de la República detallan:

> *(…)*
> *"Respecto a las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*
> *a) Documentar, mantener actualizado y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional…*
>
> *b) <u>Documentar</u>, <u>mantener actualizados</u> y <u>divulgar</u> internamente tanto las políticas como los procedimientos que definan claramente entre otros asuntos, los siguientes:*
>
> *ii. La protección y conservación de todos los activos institucionales*
>
> *1.4 c) La emisión de instrucciones a fin de que las políticas, normas y procedimientos para el cumplimiento del SCI, estén debidamente documentados, oficializados y actualizados, y sean divulgados y puestos a disposición para su consulta".*

> *4.1 "El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales" ….*

Además, los conceptos para el sistema normativo de la UNED, aprobado por el Consejo Universitario en sesión No.447, artículo VI, inciso 1 de 13 de setiembre de 1983 instituyen:

> *"…MANUALES E INSTRUCTIVOS*
> *Son conjuntos de disposiciones sobre aspectos de la organización y funcionamiento de la Universidad, aprobados por el órgano competente y subordinados a los Reglamentos".*

La "Guía para el Desarrollo de Documentación PUNED CPPI 01", Centro de Planificación y Programación Institucional actualizada mediante acuerdo tomado por el Consejo de Rectoría en sesión No. 2150-2021, Artículo IV, inciso 4, del 17 de marzo de 2021 define:

> *"…1. Propósito*
> *Asegurar que la documentación relacionada a los procesos de las dependencias de la Universidad Estatal a Distancia (UNED), se desarrolle, se apruebe, se distribuya y se controle de una manera estandarizada y efectiva. Asimismo, evitar su uso cuando esté obsoleta o desactualizada, para que contribuya a que los servicios o productos de las dependencias cumplan con los objetivos por los cuales fueron creados".*

La situación descrita, según el director de la DTIC obedece a que: "…*las actividades de respaldo se realizan directamente en el Centro de Datos Principal debido a que en el Centro de Datos Alterno en Cartago existe una copia de la información de este sitio principal. Sin embargo, se está planificando contar con un sistema de respaldos de la misma manera en Cartago por lo que, aún no se cuenta con un documento similar para el Centro de Datos Alterno. Es algo que se debe conformar*", menciona el director de la DTIC. Además, considera que *la "Directriz en cuanto al acceso a las instalaciones de la DTIC y DATACENTER por parte de terceros relacionada con el acceso a los centros de datos, es un control interno, y que, en caso de ser solicitado el acceso, se debe aplicar. Por tal razón, solo se comunicó al personal de esa Dirección mediante el Oficio DTIC-2018-109 CIRCULAR del 28 de setiembre de 2018".*

Por consiguiente, la omisión de estándares de conformación de documentos de procesos internos formalmente establecidos y aprobados dificulta la verificación del control, su cumplimento, logro de los objetivos, debilita la fiscalización del proceso, consulta y evaluación. Además, el divulgar únicamente a lo interno de la DTIC la "*directriz para el acceso a las instalaciones de la DTIC y al DATACENTER por parte de terceros relacionada con el acceso a los centros de datos*" e incluirla como anexo en el Manual de Procedimientos para la Seguridad en TI conformado de 267 páginas, podría limitar al resto de los funcionarios de la institución conocer las medidas de control que rigen para el sitio, a pesar de que su contenido establece que es de "*cumplimiento obligatorio para todos los funcionarios de la UNED*", y su objetivo señala…"*ofrecer a la comunidad universitaria una guía sobre las características y requerimientos mínimos que deben ser cumplidos respecto al acceso a estas áreas restringidas que tiene actualmente la Universidad Estatal a Distancia (UNED), como también las implicaciones por los daños que puedan ocasionar* ".

2.3. Valoración de riesgos de SERGE no incluye el tema objeto de estudio y se materializan daños en la estructura del piso falso y cableado.

El Centro de Datos Alterno en Cartago carece de una valoración de riesgos específica que muestre el análisis, acciones de mejora, y seguimiento para la seguridad física y ambiental del sitio. Los resultados aportados por SERGE para 2018 establecen 16 procesos en general, entre los que podrían relacionarse con el Centro de Datos Alterno están el "mantenimiento de equipo electrónico", "mantenimiento eléctrico" y "mantenimiento eléctrico en general". **(Ver anexo N.3)**

La información suministrada para las medidas establecidas por SERGE en el 2018 para el proceso N.7 "*mantenimiento eléctrico y general*" hace mención a: "***2-****Comenzar a incluir en la planificación el mantenimiento preventivo en las instalaciones nuevas*" el cual podría incluir al Centro de Datos Alterno por ser un edificio reciente, sin embargo, se solicitó información con el oficio AI-066-2021 a la Vicerrectora Ejecutiva, relacionada con la planificación del mantenimiento preventivo para el Centro de Datos Alterno correspondiente al 2019 y 2020, y con el oficio UMI-65-2021, solo se detallan los trabajos realizados sin que se aporte lo requerido.

Sin embargo, el informe y plan de administración de riesgos para 2020 de mantenimiento de SERGE, puntualiza como medida de control del riesgo:

> *"Poner en ejecución contratos de mantenimiento puntual y preventivo institucional para Ii+D, data center, plantas generadoras, ups, elevadores, aires acondicionados, plantas de tratamiento, edificios nuevos."* (El subrayado no es del original)

El oficio UMI-65-2021 del 16 de junio del año en curso, emitido por el jefe de la Unidad de Mantenimiento informa sobre la condición del proceso para contratación de servicios de mantenimiento preventivo de equipo que incluye al Data Center Alterno, en los siguientes términos:

> *"…me permito informarle que desde mediados del año 2020 se inició con el levantamiento de las características de los equipos y tipo de mantenimiento preventivo adecuado; para el 2021 se logró publicar el cartel en la Plataforma del SICOP (LICITACIÓN PÚBLICA NACIONAL 2021LN-000003-0017699999, UNIVERSIDAD ESTATAL A DISTANCIA OFICINA DE SERVICIOS GENERALES UNIDAD DE MANTENIMIENTO "Servicio de Mantenimiento de Equipos"), el cual pasó por todas las etapas y al viernes 7 de junio del presente a*ño se entregó a la oficina de Contratación y Suministros la revisión del estudio de ofertas presentadas por las empresas interesadas en ofrecer el servicio. (Ver Anexos)"

La condición expuesta difiere de lo normado en el Artículo N°14- "Valoración de riesgo" de la Ley General de Control Interno N.8292, en los incisos b, c y d; el apartado 3.1 "Valoración del riesgo" de las Normas de Control Interno para el Sector Público (N-22009-CO-DFOE) y el ítem 1.3 Gestión de riesgos de las Normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE) mencionan al respecto:

> *"…b) Analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran, y decidir las acciones que se tomarán para administrarlos.*
> c) Adoptar las medidas necesarias para el funcionamiento adecuado del sistema de valoración del riesgo y para *ubicarse por lo menos en un nivel de riesgo institucional aceptable.*
> *d)Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar.*
>
> *3.1 El jerarca y los titulares subordinados, según sus competencias, deben definir, implantar, verificar y perfeccionar un proceso permanente y participativo de valoración del riesgo institucional…*

1.3 La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable".

La situación descrita se debe a que los riesgos son analizados por SERGE en forma general, y no incluye el Centro de Datos Alterno, a pesar de la gran inversión en equipo e infraestructura realizada en el lugar. Los seguimientos, las gestiones de mejora, los riesgos en la parte eléctrica tampoco son específicos. Además, los eventos que comprometen la seguridad física y ambiental para el sitio alterno no cuentan con el acompañamiento requerido del personal de la UIT, como área experta en infraestructura tecnológica.

Por consiguiente, se han materializado eventos asociados con la seguridad ambiental del Centro de Datos Alterno. El oficio DTIC-UIT-2021-015 del 03 de marzo de 2021 del coordinador de la UIT de la DTIC, solicita al jefe de la Unidad de Mantenimiento de la UNED, la acción correctiva para el Centro de Datos Alterno al informarle una serie de anomalías entre ellas: *"cables de fibra óptica con humedad y con moho, dentro del encapsulado donde se encuentran conectados en los equipos de comunicación del centro de datos; óxido en las barras y placas que sostienen el entrepiso, principalmente en las partes que no poseen pintura; insectos como ciempiés, propios de la humedad del ambiente; olor a humedad bastante pronunciado, lo cual nos parece que puede ser producido por el ambiente donde se encuentra el edificio; puerta principal del centro de datos la encontramos también con ciertas muestras de humedad".*

Esta condición expone a la UNED a pérdidas económicas de activos valorados aproximadamente en $915,807.66, por concepto en equipo y software: VxBlock 350, servicios conexos, equipos de comunicación y software, sobre todo, amenaza la continuidad de las operaciones y el propósito u objetivo de creación del Centro de Datos Alterno.

2.4. Puestos y funciones de la UIT sin definir dentro de la Estructura Orgánica y Funcional de la DTIC, ni en el documento "Roles y Funciones".

Los puestos y funciones denominados "administrador de infraestructura de respaldos de información" y "administrador de infraestructura de servidores de datos Windows y Linux" que ejerce el personal de la UIT que administra el Centro de Datos

Alterno, están sin formalizar en la Estructura Orgánica y Funcional de la DTIC, aprobada en el acuerdo tomado por el Consejo Universitario en sesión No. 2862-2021, Art. II, inciso 6), celebrada el 28 de junio de 2021, tampoco en el documento "Roles y Funciones" aprobado por la CETIC[1] en sesión No. 016-2018, Art. I, inciso 3), celebrada el 08 de octubre de 2018 ni en el Manual Descriptivo de Puestos de la UNED.

El director de la DTIC mediante oficio DTIC-2021-085 del 28 de abril del año en curso, indica que el personal de la UIT tiene a cargo las actividades de administración del Centro de Datos Alterno. Sus funcionarios tienen asignada una clave de administrador con los siguientes puestos:

> *"1-Administrador de Infraestructura en Servidores Windows (2 funcionarios).*
> *2- Administrador de Infraestructura en Servidores Linux (2 funcionarios).*
> *3- Administrador de Infraestructura de Respaldos de Información (1 funcionario)".*

Además, para efecto del tema en estudio menciona que el cargo de "Administrador de infraestructura de respaldos de Información", realiza la siguiente gestión:

> *"El especialista en Respaldos de Información es responsable de participar en el resguardo, restauración, control, monitoreo y logística en general de la información que se procesa en los Centros de Datos de la UNED. Además, deberá sugerir y elaborar mejoras para el mantenimiento y resguardo de la información, así como de las herramientas y tecnologías de Respaldo que se utilicen en el mercado".*

Según el documento "Roles y Funciones" aprobado por la CETIC el 08 de octubre del 2018, define 2 roles para la UIT a saber: Coordinador de la UIT y Técnico de servicios informáticos, por tanto, los puestos Administrador de Infraestructura de Servidores e Infraestructura de Respaldos de Información no corresponde a los mencionados en el citado instrumento.

La condición difiere de lo regulado en el apartado 2.5 "Estructura Organizacional", 4.2 "Requisitos de las actividades de control" inciso e) de las normas del control interno para el Sector Público (N-2-2009-CO-DFOE) publicado en la Gaceta N°26 del 6 de febrero de 2009, además el apartado 4.2 "Administración y operación

[1] Comisión Estratégica de Tecnología de Información y Comunicaciones.

de la plataforma tecnológica inciso a)" de las normas técnicas para la gestión y el control de las Tecnologías de Información que puntualizan lo siguiente:

> "*El jerarca y los titulares subordinados, según sus competencias y de conformidad con el ordenamiento jurídico y de las regulaciones emitidas por los órganos competentes, deben procurar una estructura que defina la organización formal, sus relaciones jerárquicas, líneas de dependencia y coordinación, así como la relación con otros elementos que conforman la institución, y que apoyen el logro de los objetivos….*
>
> *Las actividades de control deben reunir los siguientes requisitos:*
> *e)* ***Documentación****. Las actividades de control deben documentarse mediante su incorporación en los manuales de procedimientos, en la descripción de puestos y procesos, o en documentos de naturaleza similar…*
>
> *…a) Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma".*

La situación descrita se debe a que el Director de la DTIC creó un nuevo puesto y funciones de "administrador de infraestructura en servidores *y de respaldos de información",* sin embargo, en la "*Estructura orgánica y funcional de la DTIC*" que se actualizó recientemente no se incluye el "Administrador de Infraestructura de Respaldos de Información", "Administrador de Infraestructura en Servidores Windows" ni "Administrador de Infraestructura en Servidores Linux", estos puestos y funciones específicas, tampoco son incluidos en el documento "Roles y funciones" emitido por la CETIC el 08 de octubre del 2018.

Por consiguiente, las funciones realizadas por el personal de la UIT en los puestos mencionados anteriormente quedan al margen de la "Estructura orgánica y funcional de la DTIC", aunque conllevan la exigencia de las responsabilidades que implican un compromiso con la gestión de equipos y la confidencialidad de la información que se almacena y se procesa en la institución.

2.5. Atención de incidentes de la seguridad de la información por parte del personal de la USD en los servidores de datos de la UNED.

La gestión del personal de la USD, para controlar, verificar e investigar incidentes de seguridad de la información en los Servidores de Datos de la UNED presenta limitaciones de acceso. El oficio DTIC-2021-085 del 28 de abril del año en curso, enviado por el director de la DTIC, señala:

> *"…Hay que manifestar que los funcionarios de la USD no cuentan con acceso físico a los centros de datos de la universidad, ni acceso lógico a los servidores de la plataforma institucional*".

Las tareas establecidas para el personal de la UIT conciernen las funciones para atención de infraestructura y eventos de seguridad de información[2] relacionado con hardware y el entorno.

Por otro lado, la USD posee funciones establecidas en la "Estructura Organizacional y Funcional de la DTIC" aprobada por el Consejo Universitario, en sesión No. 28622021, Art. II, inciso 6), celebrada el 28 de junio de 2021, donde se asigna a esta unidad la seguridad lógica de la plataforma tecnológica institucional, a saber: "*Realizar la gestión de incidentes de seguridad informática[3] que afecten a los recursos de información de la UNED*".

Además, el contenido del documento "Roles y Funciones" aprobados por la CETIC en sesión No. 016-2018, Art. I, inciso 3), celebrada el 08 de octubre de 2018 define lo siguiente:

- *"Controlar e investigar incidentes o violaciones de seguridad, analizando bitácoras, pistas de auditoria, generando reportes de violación y de actividades de seguridad.*
- *Coordinar las funciones relacionadas a la seguridad, como seguridad física del Centro de Datos, seguridad del personal y seguridad de la información almacenada.*
- *Establecer las medidas de seguridad para el almacenamiento de los respaldos".*

[2] Evento de seguridad de la información: Cualquier ocurrencia relacionada con los activos o el entorno que indique un posible compromiso de las políticas o la falla de los controles, o una situación no asignada que pueda afectar a la seguridad. Fuente: https://www.escuelaeuropeaexcelencia.com/2020/04/definiciones-de-eventoincidencia-o-no-conformidad-en-iso-27001/

[3] **La seguridad informática**, también conocida como ciberseguridad o seguridad de tecnología de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras. https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

Además, la DTIC ha invertido en capacitación para el personal de la USD en Ciberseguridad", ISO 27001, "Fortinet y tecnologías que colaboren con el cumplimiento de los objetivos asignados, los funcionarios también cuentan con el perfil profesional para atender incidentes de seguridad informática sin intermediarios.

La separación de las funciones se refiere a que el conocimiento y los privilegios son necesarios, para completar el proceso de división entre varios usuarios. El control estándar requiere que las funciones que sean conflictivas y las áreas con responsabilidades distintas se deben segregar con el fin de reducir el riesgo de modificación o el uso no autorizado o involuntario, todo esto considerando la supervisión y aprobación por parte del director de la DTIC, ante situaciones que son detectadas por el área en seguridad digital designada.

La condición descrita difiere de lo establecido en el apartado 2.5.3 "Separación de funciones incompatibles y del procesamiento de transacciones" de las normas de control interno para el sector público (N-2-2009-CO-DFOE), además los puntos 1.4 "Gestión de la seguridad de la información" y 4.5 "Manejo de incidentes", de las Normas técnicas para la gestión y el control de las tecnologías de información (N-22007-CO-DFOE) que regulan lo siguiente:

> *"2.5.3 El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que las funciones incompatibles, se separen y distribuyan entre los diferentes puestos; … de modo tal que una sola persona o unidad no tenga el control por la totalidad de ese conjunto de labores...*
>
> *1.4 La organización debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI. Además, debe darles el seguimiento pertinente, minimizar el riesgo de recurrencia y procurar el aprendizaje necesario.*
>
> *4.5 La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales… Para ello debe… asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:*
> *- El compromiso del personal con la seguridad de la información.*
> *- La seguridad en las operaciones y comunicaciones"*

La situación descrita según el director de la DTIC se debe a que años atrás varios funcionarios de la DTIC contaban con clave “Administrador” y cuando se modificó un indicador o valor en un servidor no se pudo determinar el responsable. En vista de esto, el Coordinador de la UIT para garantizar que ellos podrían controlar y mantener el orden en estos equipos, se acuerda que solo ellos mantuvieran ese acceso para las actividades en los servidores de datos.

Por consiguiente, el personal de la USD tiene limitaciones en el cumplimiento de funciones asignadas, y que se han externado por el Coordinador de la USD al director de la DTIC en la minuta del 5 de abril del año en curso, que revela la restricción de acceso a ciertas plataformas, y que al otorgárseles permisos se han atendido varias alertas, como se observa en el siguiente párrafo:

> *“…• Se indica que gracias al acceso y los permisos suministrados por Francisco al usuario jsaborio@uned.ac.cr al Centro de Administración de Office 365 se logra tener acceso a las siguientes herramientas e información:*
> *5.b..1. Cloud App Security: herramienta utilizada para atender:*
> *5.b..1.1. Alertas de Riesgo*
> *5.b..1.2. Alertas de protección de identidad de Microsoft 5.b..1.2.1. Nueva detección de usuarios en riesgo.*
> *5.b..1.2.2. Detección de inicios de sesión riesgos*
> *5.b..2. Seguridad de Microsoft 365*
> *5.b..2.1. Actividad inusual en archivos de parte de usuarios externos*
> *5.b..3. Se atendieron varias alertas y se cambiaron contraseñas como medida de protección de las cuentas. Se logró detectar acceso desde Holanda y Costa Rica en un mismo espacio de tiempo.*
> *5.b..4. Hay que valorar brindar los mismos accesos a Michael y Alejandro para que puedan realizar acciones similares al usuario jsaborio@uned.ac.cr en Microsoft 365”.*

Además, el proceso de atención de incidentes de seguridad lógica cuando son detectados eventos por parte del personal de la USD mediante el Fortinet, se retrasa en su solución al tener que elaborarse un tiquete de atención o concretar una reunión por chat con el personal de la UIT para que sea visto el caso, solución que al final dependerá de la disponibilidad del funcionario de la UIT al que se le solicita la atención. También, se aumenta la posibilidad de no ser evidenciados errores involuntarios, sucesos irregulares en las gestiones internas de la UIT durante el proceso verificación de la seguridad lógica de la información.

3. CONCLUSIONES

3.1. El Centro de Datos Alterno de Cartago presenta vulnerabilidades en su seguridad ambiental comprometiendo la estructura del piso falso, producto de la excesiva humedad que ocasiona herrumbre, cables de fibra óptica encapsulados con relente y moho; condición que expone a la institución a pérdidas económicas en activos valorados en aproximadamente $915,807.66. Aunado a esto, una deficiente atención de la Administración para ejecutar mantenimientos preventivos y correctivos incrementan el riesgo. Además, la seguridad física se compromete sin una bitácora para control de la llave convencional que custodia el personal del Centro Universitario de Cartago; y el personal de la U.I.T no tiene un sitio para almacenaje de objetos de limpieza, cajas plásticas y cartón con repuestos y cables.

3.2. El Centro de Datos Alterno de Cartago carece de documentación formal aprobada por la autoridad competente para el proceso de respaldo que se realiza en los equipos “SERVIDORES”. El documento aportado como instrucciones del proceso corresponde a un Manual de usuario de la empresa SONDA S.A. proveedora del software para el proceso de respaldos en ese sitio. Además, el director de la DTIC estableció una directriz para el control de acceso a los Centros de Datos de la UNED, sin embargo, su divulgación se realiza con anexo del Manual de Seguridad de TI, sin que medie una comunicación directa a todos los funcionarios de la UNED, considerando que el alcance de dicha restricción, es de acatamiento obligatorio para todos los funcionarios, tal como se indica en su contenido.

3.3. El Centro de Datos Alterno de Cartago carece de una valoración de riegos para administrar las amenazas y establecer controles para la seguridad física y ambiental del sitio. La desatención, aunada a la falta de ejecución de un plan de mantenimiento preventivo y correctivo ya ocasiona problemas en la infraestructura materializados en su piso falso, puerta de seguridad y herrumbre por el ambiente con excesiva humedad**,** exponiendo a la institución a pérdidas económicas de activos valorados aproximadamente en $915,807.66, y en especial, amenaza la continuidad de las operaciones y el propósito u objetivo de creación del Centro de Datos Alterno.

3.4. Las funciones y puestos definidos por el Director de la DTIC denominados "administrador de infraestructura de respaldos de información", "administrador de infraestructura de Servidores Windows" y "Linux" de la UIT están sin formalizar en la "Estructura Orgánica y Funcional de la DTIC", aprobada con el acuerdo tomado por el Consejo Universitario en sesión No. 2862-2021, Art. II, inciso 6), celebrada el 28 de junio de 2021, tampoco en el documento denominado "Roles y Funciones" aprobados por la CETIC en sesión No. 016-2018, Art. I, inciso 3), celebrada el 08 de octubre de 2018 ni en el Manual Descriptivo de Puestos de la UNED.

3.5. El personal de la USD tiene restricción en acceso lógico a los servidores de datos de la UNED cuando se requiere verificar incidentes que son alertados por la plataforma "FORTINET". La ejecución de funciones asignadas a la USD con el impedimento de acceso lógico a los Servidores Institucionales limita la ejecución rápida en el cumplimiento de sus funciones. El Director de la DTIC crea un puesto de "administrador de infraestructura de respaldos de información" para el resguardo, restauración, control, monitoreo y logística en general de la información que se procesa en los Centros de Datos de la UNED con responsabilidades similares a las asignadas a la USD; por ejemplo, establecer las medidas de seguridad para el almacenamiento de los respaldos; además, al ser detectadas situaciones de amenazas o incidentes con algún usuario, el personal de la USD debe solicitar a la UIT su atención, para conjuntamente ver el caso, generando atrasos en la atención de situaciones al depender de la disponibilidad del personal de la UIT.

4. RECOMENDACIONES

Al Mag. Francisco Durán Montoya, director de la DTIC o a quien ocupe el puesto.

4.1. Informar mediante oficio o correo electrónico al personal del Centro Universitario de Cartago los lineamientos establecidos mediante "*Directriz en cuanto al acceso a las instalaciones de la DTIC y DATACENTER por parte de terceros relacionada con el acceso a los centros de datos*" emitida por el director de la DTIC al personal mediante circular DTIC-2018-197. **(Resultado 2.1)**

4.2. Implementar una bitácora o control equivalente, para registrar el ingreso de funcionarios y visitantes al Centro de Datos Alterno. En caso de mantenerse vigente la llave, dicho control puede ser manual, no obstante, cuando se migre a un sistema de ingreso por tarjeta el control debe ser digital. **(Resultado 2.1)**

4.3. Elaborar con la guía y acompañamiento técnico del CPPI, un procedimiento que regule el proceso de respaldo de la información de los servicios informáticos del Centro de Datos Alterno de la UNED, elevarlo a la aprobación correspondiente y mantener su contenido actualizado. Al menos debe contener el propósito, procesos, responsables, mantenimientos y tiempo de recuperación deseables. **(Ver Resultado 2.2)**

4.4. Comunicar a la Comunidad Universitaria, mediante oficio o correo electrónico institucional, las directrices que emita esa dirección, cuando en su alcance establezcan que son de cumplimiento obligatorio para todos los funcionarios de la Institución. **(Ver Resultado 2.2)**

4.5. Proceder con la actualización de los roles de la DTIC para las respectivas unidades y someterla a la aprobación correspondiente. (**Ver Resultado 2.4)**

4.6. Otorgar los permisos necesarios al personal de la USD *-con los controles requeridos-*, para que sean efectuadas las gestiones de seguridad lógica en la atención de incidentes en todos los servidores de datos de la UNED, de acuerdo a lo establecido en la "Estructura orgánica y funcional de la DTIC", e instrumento "Roles y Funciones". **(Ver resultado 2.5)**

A la Mag Heidy Rosales Sánchez, jefe a.i de SERGE o a quien ocupe el puesto.

4.7. Gestionar las acciones de mantenimiento solicitadas por el Coordinador de la UIT mediante oficio DTIC-UIT-2021-015 del 3 de marzo 2021, considerando el riesgo de los activos que se albergan en el sitio alterno. **(Resultado 2.1)**

4.8. Efectuar la calendarización y luego, la ejecución de los mantenimientos preventivos para resguardo de la seguridad física y ambiental del Centro de Datos Alterno, considerando el criterio técnico de la UIT y el presupuesto necesario para cumplir con lo programado. **(Resultado 2.1).**

4.9. Realizar con el acompañamiento técnico del PROCI y la asesoría técnica de la UIT, la valoración de riesgos específica para la seguridad física y ambiental del Centro de Datos Alterno en Cartago, que incluya al menos, la identificación de riesgos, probabilidad, acciones o medidas de mejora para la adecuada administración y minimizar su impacto, considerar recursos y procedimientos internos para dar seguimiento. (**Ver resultado 2.3)**

5. ANEXOS

ANEXO N.1

Objetos de limpieza y almacenaje de cable y demás
Centro de Datos

Fecha: 13/5/2021
Fuente: Fotografía tomada el día de visita al Centro de Datos Alterno

Auditoría Interna
Tel: 2527 2276
Telefax: 2224 9684
Apdo. 474-2050 / San Pedro de Montes de Oca

ANEXO N.2

Pasillo frente al Centro de Datos Alterno ingreso de agua de lluvia
CU Cartago

Fecha: 13/5/2021
Fuente: Fotografía tomada el día de visita al Centro de Datos Alterno

Pasillo frente y costado del sitio donde se ubica el Centro de Datos Alterno CU Cartago, ya se había limpiado el agua de lluvia que estaba en este corredor

Fecha: 13/5/2021
Fuente: Fotografía tomada el día de visita al Centro de Datos Alterno

ANEXO N.3

Procesos que se relacionan con el tema en estudio

Proceso	Evento	Riesgo	Factor	Medidas para la Administración del Riesgo
N.7 Mantenimiento eléctrico y general	Que no se ejecute mantenimiento preventivo en todas las áreas que lo requieren.	Efectividad	Programación o Planificación del Trabajo	**1.** Al reparar daños se mejoran las instalaciones y se implementan las normas eléctricas actuales. Coordinador Unidad de Mantenimiento Permanente Mantenimiento preventivo **2.** Comenzar a incluir en la planificación el mantenimiento preventivo en las instalaciones nuevas.
N.16 Mantenimiento en General	Que no especifiquen los requerimientos de mantenimiento en las construcciones nuevas.	Comunicación	Comunicación defectuosa	Solicitar a la Vicerrectoría Ejecutiva que se establezca una mejor comunicación entre la Unidad de Proyectos y la Unidad de Mantenimiento para coordinar ciertos aspectos propios de la Unidad de mantenimiento

Fuente: Elaboración propia con la información suministrada.

Fecha: 21 abril 2021

Auditoría Interna
Tel: 2527 2276
Telefax: 2224 9684
Apdo. 474-2050 / San Pedro de Montes de Oca
UNED
UNIVERSIDAD ESTATAL A DISTANCIA
Institución Benemérita de la Educación y la Cultura

ANEXO N.4

Análisis de Observaciones de la Administración

Valoración de las observaciones recibidas de la Administración al informe en carácter de "Preliminar" Estudio sobre Seguridad Física y Lógica en Sitio Alterno de Data Center de la UNED, Código ACE-001-2021, mediante oficios DTIC-2021-329 y DTIC-351-2021.

Detalle en el Informe Preliminar	**Recomendación** 4.5 Realizar en coordinación con el CPPI y la CETIC la actualización de los puestos que defina la DTIC para sus unidades, y someterla a la aprobación correspondiente**. (Ver Resultado 2.4)**					
Detalle de la observación de la Administración	Cabe mencionar que para la recomendación 4.5, la DTIC actualmente cuenta con un documento de roles y funciones que colabora como apoyo a las funciones establecidas en el manual de puestos institucional, en este sentido le hago saber que se remitió a la CETIC la versión 1.2 mediante oficio DTIC-2021-068 con la propuesta de actualización por parte de la DTIC, dada esta situación se solicita tomar en cuenta la sugerencia de redacción de esta recomendación: **Propuesta**: "Proceder con la actualización de los roles de la DTIC para las respectivas unidades y someterla a la aprobación correspondiente" Respuesta con el oficio DTIC-351-2021 del 29 de setiembre del año en curso, se establece la implementación para diciembre 2021.					
¿Se acoge?	SÍ	X	NO		Parcial	
Argumento(s) de la Auditoría Interna.	Se realiza respuesta con el oficio AI-124-2021 del 15 de setiembre 2021, en los términos: "*El mencionado oficio DTIC-2021-068 no se adjunta, siendo un aporte significativo para determinar el estado de la gestión recomendada, es decir, si la actualización está en proceso o fue tramitada. Es importante señalar que el hallazgo se realiza*					

	en una fecha específica de la actividad de examen y puede variar su condición, debido al tiempo que transcurre hasta la fecha de presentación del informe preliminar. *Si el documento "Roles y Funciones" ya fue actualizado a su versión 1.2 en los términos sugeridos en la recomendación 4.5, es decir, incluye las funciones y puestos definidos por el director de la DTIC denominados "administrador de infraestructura de respaldos de información", "administrador de infraestructura de Servidores Windows" y "Linux" de la UIT, la recomendación estaría cumplida.* *Obsérvese que el objetivo de este proceso de actualización es concordar la teoría con la práctica, al oficializar por parte de la CETIC la nueva versión del documento "Roles y Funciones V. 1.2" que contiene, entre otros aspectos, los tres puestos y las funciones que fueron creados en la UIT, según información proporcionada mediante oficio DTIC-2021-085 del 28 de abril 2021, que a la fecha se evidenció quedan sin incluirse en la Estructura Orgánica y funcional de la DTIC, recientemente aprobada por el Consejo Universitario en sesión No. 2862-2021, Art. II, inciso 6) celebrada el 28 de junio de 2021, ni en el instrumento "Roles y Funciones", versión 1.1 del 31 de mayo del 2017, de vigencia actual.* *Por tal razón, debe aportar como evidencia documental de su implementación el oficio DTIC-2021-068 y el acuerdo de la CETIC que aprueba la actualización del documento "Roles y funciones" en su Versión 1.2. El plazo de implementación se define en el oficio DTIC-2021-329".*

Detalle en el Informe Preliminar	**Recomendación 4.6** Otorgar los permisos necesarios al personal de la USD -con los controles requeridos-, para que sean efectuadas las gestiones de seguridad lógica en la atención de incidentes en todos los servidores de datos de la UNED, de acuerdo a lo establecido en la "Estructura orgánica y funcional de la DTIC", e instrumento "Roles y Funciones". (**Ver resultado 2.5)**

Detalle de la observación de la Administración	Adicionalmente en lo que respecta a la recomendación 4.6, otorgar permisos es parte de una de las actividades que habría que considerar como parte de una gestión integral y oportuna en incidentes de seguridad, por lo tanto, se solicita tomar en cuenta la sugerencia de redacción de esta recomendación. **La propuesta es la siguiente:** **4.6** Buscar los mecanismos necesarios con los controles requeridos, para que sean efectuadas las gestiones de seguridad lógica en la atención de incidentes en todos los servidores de datos de la UNED, de acuerdo a lo establecido en la "Estructura orgánica y funcional de la DTIC", e instrumento "Roles y Funciones". (**Ver resultado 2.5**) Respuesta con el oficio DTIC-351-2021 del 29 de setiembre del año en curso, se establece la implementación para **setiembre 2022**					
¿Se acoge?	SÍ		NO	X	Parcial	
Argumento(s) de la Auditoría Interna.	Se responde con el oficio AI-124-2021 del 15 de setiembre 2021, en los siguientes términos: "*La estructura de las recomendaciones de Auditoría conlleva una serie de consideraciones, tanto de fondo como de forma, en apego a la ley de control interno, normativa de la CGR e interna, en concordancia con los hallazgos y conclusiones del informe.* *La recomendación 4.6. está enfocada en subsanar la debilidad de control evidenciada en las funciones de seguridad lógica asignadas con la "Estructura Orgánica y Funcional de la DTIC" y el documento "Roles y funciones" a la USD, en lo que respecta a los Servidores Institucionales.* *Desde ese contexto, al evidenciar las limitaciones del Coordinador de esta Unidad para gestionar la verificación de alertas notificadas con las herramientas de monitoreo existentes, se recomienda que sean brindados los permisos necesarios con los respectivos controles para el cumplimiento de sus funciones.*					

	La actividad de seguridad lógica recae en la USD, por lo tanto, debe ser específicamente en esa Unidad donde sea atendida la recomendación según el hallazgo. *Su propuesta de redacción a la recomendación 4.6., sugiere un cambio a la esencia de la condición y no define acciones concretas, sino generales que podrían tornarse en difusas, en su implantación y seguimiento.* *En razón de que la recomendación de la Auditoría, responde a la generación de acciones concretas para reducir las deficiencias de control, se considera que la recomendación inicial debe persistir, a pesar de considerarse como una actividad más dentro de las que puede impulsar esa Dirección en el proceso de gestión integral y oportuna de incidentes de seguridad, por lo que su redacción se mantiene".*