UNIVERSIDAD ESTATAL A DISTANCIA

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 N°ACE-004-2023

ESTUDIO SOBRE IMPLEMENTACIÓN DE CONTROLES PARA LA CIBERSEGURIDAD DE LA UNED

2023

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

Índice

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

RESUMEN EJECUTIVO

En el estudio sobre implementación de controles para la ciberseguridad de la UNED realizado para el segundo semestre del 2022, se presentan oportunidades de mejora para los procesos y actividades que se realizan en la DTIC, y que se han venido presentando por la falta de controles establecidos, específicamente lo relacionado con:

Carencia de políticas y lineamientos, para la seguridad de la información y ciberseguridad; control de gestión automatizada de inventario de hardware y software a nivel institucional; plan de protección contra la infiltración de datos y las técnicas de prevención de pérdida de información, para garantizar la privacidad e integridad de los datos sensibles; autoevaluación de Control Interno del periodo 2022, sin considerar las acciones relativas al tema de ciberseguridad, se omite incluir en su plan de mejoras la implementación de los controles sobre Ciberseguridad; cláusulas de confidencialidad en los contratos con los proveedores que brindan servicios de monitoreo o soporte de seguridad a la red datos institucional y la valoración de riesgos del 2022, sin identificar para su análisis y administración, los riesgos relativos a la ciberseguridad.

Las recomendaciones emitidas y dirigidas al Director de la DTIC están relacionadas con:

- Elaborar la política de seguridad de la información y ciberseguridad, en cumplimiento de las leyes, regulaciones y normativa aplicable en materia de TI, considerando establecer cronogramas de trabajo para administrar los tiempos de ejecución que permita evaluar de los avances en el desarrollo de la propuesta. Una vez conformado el documento preliminar, someterlo a la aprobación del ente respectivo y posterior a su aprobación comunicarlos a los funcionarios de la UNED.

- Establecer los controles manuales y/o automatizados (sistema) para la gestión de inventarios de hardware y software institucional que permita un monitoreo continúo y toma de decisiones informada que garantice la seguridad, eficiencia y conformidad de las regulaciones de la institución. En caso de utilizar software libre, igualmente deben efectuarse las evaluaciones de cumplimiento con la normativa institucional y las pruebas respectivas.

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

- Elaborar un plan de protección contra la infiltración de datos y las técnicas de prevención de pérdida de información, para garantizar la privacidad e integridad de los datos sensibles.

- Elaborar e implementar con la asesoría del PROCI la Valoración de Riesgos para la USD e incorporar los riesgos relacionados con la seguridad de la información y la ciberseguridad, considerando, al menos, políticas en ciberseguridad, plan para restablecer los servicios en caso de un ataque cibernético con control de pruebas, manejo de incidentes por error humano, control de gestión de inventarios de Hardware y software, entre otros.

- Realizar con el acompañamiento técnico del PROCI la Autoevaluación de Control Interno e incorporar las actividades relacionadas con la ciberseguridad, un plan de mejora que busque superar las debilidades encontradas. Este plan debe incluir, entre otras cosas, el rediseño, mejora, desaplicación, complementación o, cuando no exista, la implementación de controles como establece el Reglamento para la operación y mantenimiento del sistema de control interno de la Universidad Estatal a Distancia

- Elaborar con la asesoría de la Oficina Jurídica, la cláusula de confidencialidad, para ser incorporadas en los carteles de contratación de los servicios “Outsourcing”, de monitoreo o soporte de la red de datos institucional, así como los contratos de confidencialidad para los servicios de mantenimiento (monitoreos, reportes u otros) interno y externo, que se contraten para los componentes informáticos con información sensible de la institución.

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

INFORME N° ACE-004-2023
(Al contestar refiérase a este número)

INFORME FINAL

ESTUDIO SOBRE IMPLEMENTACIÓN DE CONTROLES PARA LA CIBERSEGURIDAD DE LA UNED

1. INTRODUCCIÓN

1.1 Origen

El estudio corresponde a la función propia de la Auditoría Interna en cumplimiento del Plan Anual de Trabajo, del período 2023.

1.2 Objetivos

Objetivo General

Verificar si la DTIC, como parte de la seguridad digital, ha implementado controles para el resguardo de la información institucional, prevenir alteraciones, sustracción, pérdida o acceso no autorizado, tomando como factores de riesgo las amenazas emergentes, cambios tecnológicos, regulatorios y de terceros, de acuerdo con lo regulado en la normativa interna y externa, así como en mejores prácticas.

Objetivos Específicos

1. Constatar si la Unidad de Seguridad Digital de la DTIC, ha establecido controles lógicos para asegurar que la información que se procesa, almacena y traslada en la red de datos institucional, está protegida razonablemente en caso de un ciberataque.

2. Verificar si los riesgos por ciberseguridad son considerados por la Unidad de Seguridad Digital para su análisis y administración, en la última valoración de riesgos que realiza con el acompañamiento del PROCI.

3. Comprobar si la UNED ha establecido políticas internas para proteger la Red de Datos Institucional, considerando los ciberataques como cambio tecnológico en los riesgos institucionales.

1.3 Alcance del estudio

Segundo semestre del 2022, 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 Sobre la comunicación preliminar y la conferencia final

El informe preliminar y la convocatoria a la conferencia final fueron comunicados por medio del oficio AI-005-2024 del 25 de enero del 2024, al Mag Francisco Duran Montoya, Director de la DTIC.

Al respecto, la conferencia final fue realizada el 19/2/2024, estando presentes los siguientes funcionarios de la Administración: Mag Francisco Duran Montoya, Director de la DTIC, Mag. Johnny Saborío Alvarez, coordinador de la USD.

Mediante el oficio DTIC-2024-014 del 7 de febrero del 2024, la administración presentó observaciones al Informe Preliminar, las cuales se analizaron con detalle en el Anexo N° 3 “Análisis de las Observaciones Recibidas de la Administración”; y el cambio de la observación admitida, se refleja en la recomendación 4.1 del informe. Además, se confeccionó respuesta a la administración mediante oficio AI-022-2024.

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

El trámite de los informes de auditoría se debe realizar de conformidad con lo que establece la Ley General de Control Interno N° 8292, Gaceta No. 169 del 04 de setiembre del 2002), según los artículos:

> ***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 38.-Planteamiento de conflictos ante la Contraloría General de la República.***
>
> *Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de*

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

quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.

La Contraloría General de la República dirimirá el conflicto, en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N° 7428, de 7 de setiembre de 1994.

***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.

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".

2. RESULTADOS DEL ESTUDIO

2.1 Ausencia de políticas para la ciberseguridad

La Universidad carece de políticas y lineamientos, actualizados y formales, para la seguridad de la información y ciberseguridad[1], lo que implica que no se tenga como objetivo proteger los activos informáticos conectados a la red de datos institucional y la información sensible, en caso de un ataque cibernético. Sobre el particular, el director de la Dirección de Tecnología de Información y Comunicación en adelante DTIC, en el oficio DTIC-2023-047 del 26 de mayo 2023, indica:

> *Se está trabajando actualmente en un documento llamado Política de Seguridad de la información y Ciberseguridad, el cual está en una fase de borrador, se espera pronto pueda ser enviado a la CETIC y el Consejo Universitario para su respectivo conocimiento, análisis y posterior aprobación, se adjunta documento. (**El subrayado no es del original)***

Además, hace referencia al documento "*Política de Seguridad Digital*" aprobado en sesión No. 1160-2000, Art. XVIII, del Consejo de Rectoría, en el año 2000, sin embargo, documento que se encuentra desactualizado y, no contempla el tema de la Ciberseguridad,

La condición descrita difiere de lo establecido:

a) La Ley General de Control Interno N° 8292

> ***Artículo 15. —Actividades de control* inciso a)**
> *Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*

[1] La seguridad informática, también conocida como **ciberseguridad**, 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 computadora.
https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica#:~:text=La%20seguridad%20inform%C3%A1tica%20%2C%20tambi%C3%A9n%20conocida,a%20trav%C3%A9s%20de%20las%20redes

Documentar, mantener, actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.

b) Normas de Control Interno para el Sector Público:

1.4. Responsabilidad del jerarca y los titulares subordinados sobre el SCI, inciso 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 Actividades de Control
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….

4.4 Exigencia de confiabilidad y oportunidad de la información
El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente que se recopile, procese, mantenga y custodie información de calidad sobre el funcionamiento del SCI y sobre el desempeño institucional, así como que esa información se comunique con la prontitud requerida a las instancias internas y externas respectivas.

c) Marco de Gobierno y Gestión de TI de la UNED:

Alineación Estratégica y Operativa Determinar las directrices de TI
Esta práctica incluye la identificación, definición, comunicación y socialización de las normas que han de seguirse en la ejecución de las labores de TI. Asimismo, TI define las reglas que se deben seguir, o bien, que se deben ajustar con respecto a las iniciativas, proyectos, conductas y actividades, que se realizan a nivel institucional con el componente de TI.
Actividad

Definir las directrices de TI
Descripción
TI debe definir en forma escrita las normas relacionadas con la función de TI y su gobernabilidad, mismas que se deben cumplir, en el desarrollo de las labores y que a su vez estén acorde con los componentes (principios, valores, visión, entre otros) del marco de gobierno y gestión de TI. Dichas normas o conductas deben de tener como atributos el ser explicitas, simples, realistas, alcanzables. Entre dichas normas están las referentes a seguridad digital, servicios, proyectos, continuidad, relación con terceros de TI, entre otras.

d) Estructura Organizacional y Funcional de la Dirección de Tecnologías de Información y Comunicación:

Funciones
4*. Proponer e implementar directrices que apoyen el cumplimiento de las leyes, regulaciones y normativa aplicable en materia de TI.*
8*. Contribuir en la definición e implementación de acciones orientadas en la mejora de calidad, identificación de riesgos informáticos y para la construcción de un plan de contingencia en materia de TI.*

e) Normas Técnicas para la Gestión y el Control de las tecnologías de información del MICCIT v2:

Perfil del Proceso, ítem 5)
Para asegurar que se realiza una adecuada implementación de cada proceso que soporta la gestión de tecnologías de información, debe asegurarse que cumpla con el siguiente perfil:
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 periodo 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.* ***(el subrayado no es del original)***

Lo anterior se debe a que el documento "Políticas de Seguridad de la Información y Ciberseguridad" está en etapa preliminar.

Por consiguiente, la falta de políticas en ciberseguridad actualizadas, puede tener consecuencias ante limitaciones de definición de amenazas cibernéticas que están en constante evolución; menor eficiencia en detección y capacidad de respuesta; falta de integración de nuevas tecnologías; restringe la educación y concientización del personal sobre amenazas y prácticas seguras.

2.2 Oportunidades de mejora en la implementación de controles para la Ciberseguridad en la UNED

2.2.1-Control de gestión del inventario de Hardware y Software de la red de datos institucional.

La DTIC carece de una gestión de inventario de hardware y software a nivel institucional, lo que provoca la ausencia de control del hardware y licencias de software para maximizar su valor, reducir los costos, identificar los activos de la organización y definir las responsabilidades de protección necesarias.

El director de la DTIC con el oficio DTIC-064-2023 del 26 de junio 2023, adjunta el archivo digital en formato Excel "*Inventario General* de UIT" de la Unidad de Infraestructura tecnológica(UIT), el cual presenta oportunidades de mejora en: uso de encabezados oficial de la DTIC para los documentos de esa dirección o

formularios uniformes, completar los espacios de las celdas requeridas en el registro, número de activo, tipo de servicio, incluir fecha depreciación, fecha de compra, costo del activo, mejoras, seguimiento de mantenimiento, fecha de vencimiento de garantía, nivel de criticidad, entre otros.

2.2.2- Plan de protección contra la infiltración de datos y prevención de pérdida de información.

La DTIC no posee un plan de protección contra la infiltración de datos y las técnicas de prevención de pérdida de información, para garantizar la privacidad e integridad de los datos sensibles. Al respecto, el director de la DTIC por medio del oficio DTIC-064-2023 del 26 de junio 2023, expresa lo siguiente: *"No se tiene conocimiento que la UNED cuente con un Plan de protección que se encuentre debidamente aprobado, contra la infiltración de datos y las técnicas de prevención de pérdida de datos, para garantizar la privacidad e integridad de los datos sensibles". (DTIC-064-2024, Anexo1, pág.5)*

La condición descrita difiere de lo establecido:

a) Ley General de Control Interno N.8292

Artículo N.8 Concepto de sistema de control interno inciso a) *Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.*

b) Normas de Control interno para el Sector Público

4.3 Protección y conservación del patrimonio
El jerarca y los titulares subordinados, según sus competencias, deben establecer, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente la protección, custodia, inventario, correcto uso y control de los activos pertenecientes a la institución.

4.4.2 Formularios uniformes
El jerarca y los titulares subordinados, según sus competencias, deben disponer lo pertinente para la emisión, la administración, el uso y la custodia, por los medios atinentes, de formularios uniformes para la documentación, el procesamiento y el registro de las transacciones que se efectúen en la institución. Asimismo, deben prever las seguridades para garantizar razonablemente el uso correcto de tales formularios.

c) Reglamento para uso de equipo de cómputo e internet de la UNED

Artículo N.5.-De la Dirección de Tecnología Información y Comunicaciones, inciso p)
Mantener el inventario de los recursos informáticos, así como el control de la ubicación de los equipos de cómputo en las dependencias de la
UNED, así como de las licencias de uso del software adquirido…
(El subrayado no es del original)

d) Marco de Gobierno y Gestión de TI de la UNED

Gestionar la plataforma tecnológica
Incluye el mantenimiento y la definición de los planes de renovación de equipamiento, software e infraestructura tecnológica y redes, basado en el Plan de Capacidad de TI.
Actividad
-Monitorear el inventario actualizado de los componentes de la plataforma tecnológica de TI.
-Realizar un control del software necesario para la función Institucional. ***Descripción***
-Dar seguimiento al inventario actualizado del equipamiento (hardware).
-Dar seguimiento al inventario de software (inventario actualizado y detallado) requerido para brindar servicios a la institución.
Recursos
-Inventario actualizado de los componentes de la infraestructura TI.
-Catálogo de aplicaciones y bases de datos.

Evaluar la capacidad de la infraestructura TI
Identificar y definir indicadores y sus posibles valores de medición de la capacidad de la infraestructura TI actual.
Descripción
Además de indicadores y sus posibles valores de medición de la capacidad de la infraestructura actual, se debe contar con información de los servicios TI que se quieran monitorear, así como identificar periodos de tiempo claves para realizar las mediciones, tomando en cuenta los patrones de demanda. ***Recursos***
Inventario actualizado de los componentes de la infraestructura TI.

e) Normas técnicas para la gestión y el control de las tecnologías de información del MICITT v.2

XII Administración Infraestructura Tecnológica
La institución debe implementar prácticas formales que permitan mantener identificados y actualizados los activos de TI, mediante inventarios de recursos tecnológicos instalados en la organización (hardware, software, aplicaciones, comunicaciones), clasificados según el nivel de criticidad, características, configuración, servicios y medidas de protección asociadas.

f) ISO 27001

A.8 Gestión de activos
A.8.1 ***Responsabilidad sobre los activos Objetivo:*** *Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.*
A.8.1.1 Inventario de activos Control
La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario. **(El subrayado no es del original)**

Lo anterior se debe a la ausencia de controles formales, que permitan mantener identificados y actualizados los activos de TI a nivel institucional, formularios uniformes, información completa en la documentación suministrada y para la conformación de un plan de protección contra la infiltración de datos.

Por consiguiente, la falta de control de gestión de inventarios del hardware y software de la red de datos institucional, propicia el riego de perder visibilidad de los activos de hardware y software de la red (servidores, computadoras, dispositivos de red, y software instalado), ineficiencia operativa para rastrear un equipo; garantizar que todos los equipos usan software compatible; dificultad en la planificación de recursos y seguimiento de todos los dispositivos de Tecnologías de Información que tiene la institución. Además, al omitirse un plan de protección contra la infiltración de datos, deja sin establecer formalmente las medidas técnicas, políticas y procesos para garantizar la seguridad de la información en la institución.

2.3 Oportunidad de mejora en la valoración de riesgos para la ciberseguridad.

La Unidad de Seguridad Digital, en adelante USD, omite identificar detalladamente para su análisis y administración, los riesgos para accesos no autorizados a información confidencial, robo de datos, secuestro de información, software malicioso, engaño para que se comparta información, suplantación de identidad mediante el envío de correo electrónicos, identificación de activos y datos críticos, análisis de fallos y búsqueda de soluciones, evaluar amenazas e indicadores que comprometan la seguridad de la información, todos relativos a la ciberseguridad. El documento suministrado por el director de la DTIC con el oficio DTIC-2023-047 del 26 de mayo 2023 hace referencia a la valoración de riesgos del año 2022 de la USD, **(ver Anexo1)** con un planteamiento de forma general.

La condición descrita difiere de lo establecido:

a) Ley General de Control Interno N.8292 artículo N°14. —Valoración del riesgo

En relación con la valoración del riesgo, serán deberes del jerarca y los titulares subordinados, entre otros, los siguientes:

a) *Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, definidos tanto en los planes anuales operativos como en los planes de mediano y de largo plazos.*

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 organizacional aceptable.*

d) *Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar.* ***(El subrayado no es del original).***

b) Ley General de la Administración Pública N°6227

Artículo 4º*.*

La actividad de los entes públicos deberá estar sujeta en su conjunto a los principios fundamentales del servicio público, para asegurar su continuidad, su eficiencia, su adaptación a todo cambio en el régimen legal o en la necesidad social que satisfacen y la igualdad en el trato de los destinatarios, usuarios o beneficiarios.

c) Normas de control interno para el Sector Público (N-2- 2009-CO-DFOE)

3.1 Valoración del riesgo

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, como componente funcional del SCI. Las autoridades indicadas deben constituirse en parte activa del proceso que al efecto se instaure.

d) Marco de Gobierno y Gestión de TI de la UNED

Optimización y gestión del riesgo de TI

Propósit*o*

Producir información que apoye la toma de decisiones orientada a ubicar a la institución en un nivel de riesgo aceptable y así promover, de manera razonable, el logro de los objetivos institucionales. Descripción

La institución 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.

Gestionar riesgos ante amenazas

Debe enfocarse en varios temas, como identificación de riesgos de seguridad de TI y la protección de la información en tránsito y almacenada, educación y compromiso del personal institucional con la seguridad de la información, implementación de controles y detección de vulnerabilidades.

Actividad

Elaborar una gestión del riesgo de seguridad de la información de TI y ciberseguridad.

Seguridad de la información

Propósito

Propiciar, de manera razonable, la confidencialidad, integridad, disponibilidad, autenticidad de la información, conservación, trazabilidad, acceso y servicios utilizados en medios electrónicos, por medio de la toma de decisiones basada en riesgos y tratamiento de la seguridad, asegurando el cumplimiento de la normativa interna y externa de la institución en materia de seguridad de la información.

Procesos de Gestión del Marco de TI
IV. Gestión de riesgos tecnológicos
La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el Marco de Gestión de TI que le resulte aplicable.
La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución.
Ciberseguridad: Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio.

e) Directrices generales para el establecimiento y funcionamiento del sistema específico de valoración del riesgo institucional (SEVRI) D-3-2005-CO-DFOE

Identificación de riesgos. *Primera actividad del proceso de valoración del riesgo que consiste en la determinación y la descripción de los eventos de índole interno y externo que pueden afectar de manera significativa el cumplimiento de los objetivos fijados.*
Evento. *Incidente o situación que podría ocurrir en un lugar específico en un intervalo de tiempo particular.*

f) Estructura organizacional y funcional de la Dirección de Tecnologías de Información y Comunicación (DTIC)

Objetivo General (DTIC)
Determinar las acciones para el desarrollo y sostenibilidad de la Institución, en materia de tecnologías de la información y comunicación (TIC), las cuales son de aplicación general, de forma tal que se contribuya con la mejora en la prestación de los servicios académicos, estudiantiles y administrativos, conforme a las prioridades y los recursos que dicten las autoridades universitarias.

Unidad de Seguridad Digital
Objetivo
Desarrollar nuevas tecnologías de seguridad de la información y ciberseguridad, que contribuyan en la definición, implementación y promoción de las mejores prácticas para la plataforma tecnológica de la DTIC y el software institucional de la Universidad. ***(El subrayado no es del original)***

g) Normas Técnicas para la Gestión y el Control de las Tecnologías de Información 2021 del MICITT[2] v.2

XI. Seguridad y Ciberseguridad
La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.

La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.

La Institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, danos e interferencia a la información y los activos de información de la institución.

Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.

[2] Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones https://www.micitt.go.cr/

La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la informacional Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo, debe contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales. (El subrayado no es del original)

h) ISO 27001

6.1.2 Apreciación de riesgos de seguridad de la información.
*L**a** organización debe definir y aplicar un proceso de apreciación de riesgos de seguridad de la información que:*

a) Establezca y mantenga criterios sobre riesgos de seguridad de la información, incluyendo:
1) Los criterios de aceptación de los riesgos, y
2) Los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información;
a) Asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables;
a) Identifique los riesgos de seguridad de la información:
1)Llevando a cabo el proceso de apreciación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información,
1)Identificando a los dueños de los riesgos;
a) Analice los riesgos de seguridad de la información:
1) valorando las posibles consecuencias que resultarían si los riesgos identificados en el punto 6.1.2 c) 1) llegasen a materializarse,
2) Valorando de forma realista la probabilidad de ocurrencia de los riesgos identificados en el punto 6.1.2 c) 1),
3) determinando los niveles de riesgo;
a) Evalúe los riesgos de seguridad de la información:

1) Comparando los resultados del análisis de riesgos con los criterios de riesgo establecidos en el punto 6.1.2 a),
2) Priorizando el tratamiento de los riesgos analizados.

La condición descrita se debe a que la identificación de los riesgos para la seguridad de la información y ciberseguridad, no son desarrollados en su totalidad para el análisis, administración y seguimiento, existen factores que intervienen en un análisis de riesgos de seguridad de información a considerar, el entorno organizacional, capacitación del personal en el tema, alcance del análisis de riesgos.

Por consiguiente, se limita evaluar los riesgos para la ciberseguridad, las medidas de prevención en caso de robo de datos sensibles, ataques externos que impidan el funcionamiento de los sistemas informáticos y su seguimiento.

2.4 Autoevaluación de la DTIC sin incluir aspectos específicos del tema en estudio

La DTIC en su Autoevaluación de Control Interno del periodo 2022, no considera acciones relativas al tema de ciberseguridad[3], deja de incluir en su plan de mejoras la implementación de los controles sobre Ciberseguridad.

La condición descrita difiere de lo establecido:

a) Ley General de Control Interno N.8292

Artículo 7°. Obligatoriedad de disponer de un sistema de control interno. Los entes y órganos sujetos a esta Ley dispondrán de sistemas de control interno, los cuales deberán ser aplicables, completos, razonables, integrados y congruentes con sus competencias y atribuciones institucionales. Además, deberán proporcionar seguridad en el cumplimiento de esas atribuciones y competencias; todo conforme al primer párrafo del artículo 3 de la presente ley.

Artículo 8°. Para efectos de esta Ley se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:

[3] oficio DTIC-2023-047

a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.
b) Exigir confiabilidad y oportunidad de la información.
c) Garantizar eficiencia y eficacia de las operaciones.
d) Cumplir con el ordenamiento jurídico y técnico.

Artículo 9°. La administración activa y la auditoría interna de los entes y órganos sujetos a esta Ley, serán los componentes orgánicos del sistema de control interno establecido e integrarán el Sistema de Fiscalización Superior de la Hacienda Pública a que se refiere la Ley Orgánica de la Contraloría General de la República.

Artículo 10° Responsabilidad por el sistema de control interno. Serán responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento.

Artículo 17° Que la administración realice, por lo menos una vez al año, las autoevaluaciones que conduzcan al perfeccionamiento del sistema de control interno del cual es responsable. Asimismo, que pueda detectar cualquier desvío que aleje a la organización del cumplimiento de sus objetivos.

b) Normas de Control Interno para el Sector Público (N-22009-CO-DFOE)

6.3.2 Autoevaluación periódica del SCI
El jerarca y los titulares subordinados, según sus competencias, deben disponer la realización, por lo menos una vez al año, de una autoevaluación del SCI, que permita identificar oportunidades de mejora del sistema, así como detectar cualquier desvío que aleje a la institución del cumplimiento de sus objetivos. Las estrategias y los mecanismos para la autoevaluación periódica, deben estar definidos como parte de las orientaciones a que se refiere la norma 6.2. En todo caso, se debe procurar que sea ejecutada sistemáticamente y que sus resultados se comuniquen a las instancias idóneas para la correspondiente toma de acciones y seguimiento de implementación. El jerarca y los titulares subordinados, según sus competencias, deben constituirse en parte activa del proceso que al efecto se instaure.
Sistema de Control Interno (SCI)
También denominado "control interno". Comprende la serie de acciones diseñadas y ejecutadas por la administración activa para

proporcionar una seguridad razonable en torno a la consecución de los objetivos de la organización, fundamentalmente en las siguientes categorías: a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal; b) Confiabilidad y oportunidad de la información; c) Eficiencia y eficacia de las operaciones; y d) Cumplir con el ordenamiento jurídico y técnico.
(el subrayado no es del original)

c) Gestión de los procesos de Valoración del Riesgo Autoevaluación del Sistema de Control Interno y Seguimiento PUNED PROCI 02

4. Definiciones

Las siguientes definiciones son textuales de la Directriz General para el Establecimiento y Funcionamiento del Sistema Específico de Valoración de Riesgo Institucional, Resolución R- C-642005 emitida el 1º de julio del 2005, de la Contraloría General de la República:

***Plan de acción producto de la autoevaluación del SCI**: plan que incluye las acciones que deberán ser ejecutadas para superar las debilidades detectadas al aplicar la autoevaluación del SCI. Este plan incluye la fecha de implementación de cada acción y su responsable.*

Sistema de control interno (SCI):** También denominado "control interno". Comprende la serie de acciones diseñadas y ejecutadas por la administración activa para proporcionar una seguridad razonable en torno a la consecución de los objetivos de la organización, fundamentalmente en las siguientes categorías: a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal; b) Confiabilidad y oportunidad de la información; c) Eficiencia y eficacia de las operaciones; y d) Cumplir con el ordenamiento jurídico y técnico.**(El subrayado no es del original)

d) Reglamento para la operación y mantenimiento del sistema de control interno de la Universidad Estatal a Distancia

***ARTÍCULO 3: GLOSARIO Y TERMINOLOGÍA** Para los efectos de interpretación y aplicación del presente reglamento se entenderá por: **Autoevaluación del Sistema de Control Interno** Actividad periódica que busca el mejoramiento continuo del sistema de*

control interno, en la cual se verifica el cumplimiento, validez y la suficiencia del sistema de control interno y que es realizada por la propia administración.

ARTÍCULO 17: OBJETIVO DE LA AUTOEVALUACIÓN**. El objetivo de la autoevaluación es el verificar el cumplimiento, la validez y la suficiencia del SCII, y que la misma conduzca al perfeccionamiento del SCII detectando cualquier desvío que aleje a la Universidad del cumplimiento de sus objetivos. **(El subrayado no es del original)

ARTÍCULO 18: EJECUCIÓN DE LA AUTOEVALUACIÓN**. La autoevaluación del SCII se aplicará en toda la administración activa al menos una vez al año. La ejecución de este proceso, será asesorada por el PROCI, en la fecha prevista de conformidad – a la planificación aprobada por la CICI. Para la ejecución de la autoevaluación se aplicarán las "Orientaciones y metodologías para la autoevaluación del sistema de control interno de la UNED", aprobadas por el CONRE. **(El subrayado no es del original)

***ARTÍCULO 19: DE LOS TITULARES SUBORDINADOS EN EL PROCESO DE AUTOEVALUACIÓN**. De acuerdo con el objetivo, la metodología y el alcance previsto para la implementación de la autoevaluación anual; los Titulares Subordinados que sean considerados en este proceso, tendrán las siguientes obligaciones:*

- ***a.** Cumplir con las instrucciones para la ejecución de la autoevaluación.*
- ***b.** Realizar la autoevaluación del SCII a lo interno de la dependencia*
- ***c.** Producto de la autoevaluación debe elaborar un informe con los resultados obtenidos y un plan de mejora que busque superar las debilidades encontradas en esta. Este plan debe incluir, entre otras cosas, el rediseño, mejora, desaplicación, complementación o, cuando no exista, la implementación de controles.*
- ***d.** Entregar en la fecha estipulada el informe de resultados y el plan de mejora al Programa de Control Interno. **(El subrayado no es del original)***

La situación descrita se debe a que la DTIC efectúa su autoevaluación administrativa según la plantilla que nos facilita el Programa de Control Interno[4].

[4] Entrevista del 23 de junio de 2023, aplicada al director de la DTIC.

Por consiguiente, se deja sin verificar el cumplimiento, la validez y la suficiencia del SCII de la DTIC en materia de Ciberseguridad y que la misma conduzca al perfeccionamiento del SCII[5], detectando cualquier desvío que aleje a la UNED del cumplimiento de sus objetivos.

2.5 Oportunidad de mejora en los contratos con proveedores que brindan servicios de monitoreo o soporte a la red de datos institucional

La Dirección de Tecnología de Información y Comunicaciones (DTIC) omite establecer cláusulas de confidencialidad en los contratos con los proveedores que brindan servicios de monitoreo o soporte de seguridad a la red datos institucional. El director de la DTIC mediante oficio DTIC-064-2023, informa sobre los proveedores, que tienen acceso a los equipos de la institución y las contrataciones que se manejan en la DTIC para licenciamientos.

Los expedientes de contratación no evidencian el apartado que haga referencia a la cláusula de confidencialidad con los proveedores. Igualmente, se consultó el 30 de noviembre del 2023 mediante correo electrónico a la Oficina Jurídica si existía algún pronunciamiento sobre cláusulas de confidencialidad en las contrataciones de proveedores que brindan servicios de mantenimiento o soporte de seguridad lógica a la red de datos institucional al periodo de alcance del estudio, sin embargo, los documentos aportados no se han relacionado con el tema en estudio.

La situación descrita difiere de lo establecido:

a) Normas de control interno para el Sector Público

> ***5.7.4 Seguridad***
> *Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran**. (El subrayado no es del original)***

[5] Sistema de Control Interno Institucional

b) Normas Técnicas para la Gestión y el Control de las tecnologías de información del MICCIT v.2

XI. SEGURIDAD Y CIBERSEGURIDAD

La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información. ***(El subrayado no es del original)***

c) ISO/IEC 27001: 2017

A.15 Relación con proveedores

A.15.1 Seguridad en las relaciones con proveedores ***Objetivo****: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.*

A.15.1.2 Requisitos de seguridad en contratos con terceros Control

Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura de Tecnología de la Información. ***(El subrayado no es del original)***

La condición descrita se debe a que la DTIC no ha considerado incluir en sus contratos, cláusulas de confidencialidad con los proveedores que tienen accesos a los equipos de la institución y realizan actividades de mantenimientos, monitoreos u otros.

Por consiguiente, la omisión de implementación de cláusulas de confidencialidad en los contratos con los proveedores que puedan acceder a la información institucional, expone a la Institución al riesgo de pérdidas de información, modificaciones no autorizadas por terceros, uso de información sensible para su comercialización, entre otros.

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

3. CONCLUSIONES

3.1 La DTIC carece de políticas y lineamientos actualizados que reglamenten la seguridad de la información y la ciberseguridad, para el resguardo de la información institucional, prevenir alteraciones, sustracción, pérdida o acceso no autorizado, tomando como factores de riesgo las amenazas emergentes y cambios tecnológicos. **(Ver resultado 2.1)**

3.2 La DTIC omite controles manuales o automatizados(sistema) para la gestión de inventarios de hardware y software que permita un monitoreo continúo y toma de decisiones informada que garantice la seguridad, eficiencia y conformidad de las regulaciones de la institución. Además, carece de un plan de protección contra la infiltración de datos y las técnicas de prevención de pérdida de información, para garantizar la privacidad e integridad de los datos sensibles **(Ver resultado 2.2)**

3.3 La DTIC omite en la valoración de riesgos de 2022, los riesgos para la ciberseguridad de forma detallada para su análisis y administración, entre estos: riesgos para accesos no autorizados a información confidencial, robo de datos, secuestro de información, software malicioso, engaño para que se comparta información, suplantación de identidad mediante el envío de correo electrónicos, identificación de activos y datos críticos, análisis de fallos y búsqueda de soluciones, riesgos relativos a seguridad de la información y la ciberseguridad. **(Ver resultado 2.3)**

3.4 La Dirección de Tecnología de Información y Comunicaciones omite incluir en su autoevaluación del sistema de control interno del 2022 el tema de ciberseguridad en todo su ambiente; los aspectos puntualizados están enfocados al personal en lo que respecta a capacitación, y socializarlo con los funcionarios. **(Ver resultado 2.4)**

3.5. La Dirección de Tecnología de Información y Comunicaciones omite el uso de cláusulas de confidencialidad en los contratos aplicables a personal que brinda “Outsourcing”, para el monitoreo o soporte de la red de datos institucional. **(Ver resultado 2.5)**

4. RECOMENDACIONES

De conformidad con las competencias asignadas en el artículo 22 y el artículo 12, su inciso c) de la Ley General de Control Interno, se emiten las siguientes recomendaciones:

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

4.1 Elaborar la política de seguridad de la información y ciberseguridad, en cumplimiento de las leyes, regulaciones y normativa aplicable en materia de TI, considerando establecer cronogramas de trabajo para administrar los tiempos de ejecución que permita evaluar de los avances en el desarrollo de la propuesta. Una vez conformado el documento preliminar, someterlo a la aprobación del ente respectivo y posterior a su aprobación comunicarlos a los funcionarios de la UNED**.** (Ref. 2.1).
Fecha de implementación: Abril 2024 (Esta fecha considera el envío de la propuesta de la política a quien corresponda).

4.2 Establecer los controles manuales y/o automatizados (sistema) para la gestión de inventarios de hardware y software institucional que permita un monitoreo continúo y toma de decisiones informada que garantice la seguridad, eficiencia y conformidad de las regulaciones de la institución. En caso de utilizar software libre, igualmente deben efectuarse las evaluaciones de cumplimiento con la normativa institucional y las pruebas respectivas. (Ref.2.2)**.**
Fecha de implementación: Noviembre 2024 Software Base y Marzo 2025. Software Especializados.

4.3 Elaborar un plan de protección contra la infiltración de datos y las técnicas de prevención de pérdida de información, para garantizar la privacidad e integridad de los datos sensibles. (Ref.2.2)**.**
Fecha de implementación: Agosto 2024.

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

4.4 Elaborar e implementar con la asesoría del PROCI la Valoración de Riesgos para la USD e incorporar los riesgos relacionados con la seguridad de la información y la ciberseguridad, considerando, al menos, políticas en ciberseguridad, plan para restablecer los servicios en caso de un ataque cibernético con control de pruebas, manejo de incidentes por error humano, control de gestión de inventarios de Hardware y software, entre otros. (Ref.2.3).
Fecha de implementación: Inmediata.

4.5 Realizar con el acompañamiento técnico del PROCI la Autoevaluación de Control Interno e incorporar las actividades relacionadas con la ciberseguridad, un plan de mejora que busque superar las debilidades encontradas. Este plan debe incluir, entre otras cosas, el rediseño, mejora, desaplicación, complementación o, cuando no exista, la implementación de controles como establece el Reglamento para la operación y mantenimiento del sistema de control interno de la Universidad Estatal a Distancia. (Ref.2.4)**.**
Fecha de implementación: Inmediata.

4.6 Elaborar con la asesoría de la Oficina Jurídica, la cláusula de confidencialidad, para ser incorporadas en los carteles de contratación de los servicios “Outsourcing”, de monitoreo o soporte de la red de datos institucional, así como los contratos de confidencialidad para los servicios de mantenimiento (monitoreos, reportes u otros) interno y externo, que se contraten para los componentes informáticos con información sensible de la institución. (Ref.2.5).
Fecha de implementación: Febrero 2025.

5.ANEXOS

Anexo 1

Valoración de riesgos 2022
Unidad de Seguridad Digital

Valoración Riesgos USD.pdf

Anexo 2
Autoevaluación DTIC

2-Autoevaluación DTIC 2022.pdf

Anexo 3
Análisis de Observaciones de la Administración

1-Análisis_observaciones.pdf