



Unidad Organizativa Auditada: Consejo Nacional de Ciencia y Tecnología (CONACYT)

VERSIÓN PÚBLICA - Art. 30 y Art. 6 Lit. "A" de la Ley de Acceso a la Información Pública (LAIP), referente a la supresión de datos personales.

INFORME DE AUDITORIA INTERNA

Ref. IA-NA-005-2023

"EXAMEN ESPECIAL A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DEL CONSEJO NACIONAL DE CIENCIA Y TECNOLOGÍA (CONACYT), AL 31 DE DICIEMBRE DE 2022".

Versión Pública



San Salvador, 03 de noviembre de 2023

MISIÓN DE LA DIRECCIÓN DE AUDITORÍA INTERNA: Somos un Equipo que proveemos servicios de Aseguramiento y Consultoría de forma independiente y objetiva, mediante un enfoque sistemático y disciplinado, evaluando y promoviendo la mejora de los procesos claves del control interno del Ministerio de Educación, Ciencia y Tecnología.

VISIÓN DE LA DIRECCIÓN DE AUDITORÍA INTERNA: Ser un equipo de profesionales que aplique estándares internacionales de auditoría interna; coadyuvando a la mejora de la calidad educativa.

DESTINATARIOS LISTA- DE DISTRIBUCIÓN:

Titulares del Ministerio de Educación, Ciencia y Tecnología (MINEDUCYT):

- Ministro de Educación Ciencia y Tecnología, interino ^(1/) ^(3/) ^(4/)
- Viceministro de Educación y de Ciencia y Tecnología, Ad Honorem y Presidente de Consejo Nacional de Ciencia y Tecnología (CONACYT) ^(1/) ^(2/) ^(4/)

Unidad Organizativa Auditada:

- Consejo Nacional de Ciencia y Tecnología ^(2/) ^(3/)

Unidades Organizativas responsables del Sistema de Control Interno:

- Dirección Ejecutiva del CONACYT ^(2/) ^(4/)
- Observatorio Nacional de Ciencia y Tecnología ^(2/) ^(4/)
- Unidad de Tecnologías de Información ^(2/) ^(3/)
- Unidad de Protocolo y Relaciones Internacionales ^(2/) ^(4/)
- Oficina de Atención y Respuesta ^(2/) ^(4/)
- Unidad de Gestión Documental y Archivo ^(2/) ^(4/)

Funcionarios, Empleados y/o Terceros Relacionados:

- Dirección de Auditoría Cuatro, Corte de Cuentas de la República ^(1/) ^(2/) ^(4/)

(1) Informe de Auditoría notificado [Art. 37 Ley Corte de Cuentas de la República].

(2) Informe de Auditoría notificado [Art. 202 Normas de Auditoría Interna Sector Gubernamental].

(3) Informe de Auditoría comunicado [Art. 5 Reglamento de Normas Técnicas de Control Interno Específicas del MINED].

(4) Informe de Auditoría distribuido en digital



ÍNDICE

I.	INTRODUCCIÓN.....	5
II.	OBJETIVOS DEL EXAMEN	5
III.	ALCANCE DEL EXAMEN.....	6
IV.	RESUMEN DE LOS PROCEDIMIENTOS DE AUDITORÍA APLICADOS	7
V.	PRINCIPALES REALIZACIONES Y LOGROS DE AUDITORÍA	8
VI.	RESULTADOS DEL EXAMEN.....	8
VII.	HALLAZGOS DE AUDITORÍA.....	12
	HALLAZGO N° 01: INADECUADA ORGANIZACIÓN DE LAS TIC.....	13
	HALLAZGO N° 02: FALTA DE GESTIÓN DE RIESGOS RELACIONADO A LAS TIC	22
	HALLAZGO N° 03: VULNERABILIDAD EN EL SITIO WEB DEL CONACYT.....	25
	HALLAZGO N° 04: INADECUADA GESTIÓN Y USO DE LOS SERVICIOS DE TIC.....	29
	HALLAZGO N° 05: DEBILIDADES EN EL USO DE LOS SISTEMAS INFORMÁTICOS	34
	HALLAZGO N° 06: INADECUADA GESTIÓN DE LICENCIAS DE SOFTWARE.....	42
	HALLAZGO N° 07: DEBILIDADES EN LA SEGURIDAD LÓGICA	46
	HALLAZGO N° 08: DEBILIDADES EN LA SEGURIDAD FÍSICA DE LOS SERVIDORES...50	
	HALLAZGO N° 09: INADECUADA GESTIÓN DE CABLEADO ESTRUCTURADO.....	53
	HALLAZGO N° 10: FALTA DE UN INVENTARIO DOCUMENTAL DEL ÁREA DE TIC.	58
	HALLAZGO N° 11: FALTA DE CONTROLES APLICABLES A LAS TIC.....	61
	HALLAZGO N° 12: FALTA DE ESTANDARIZACIÓN DEL SITIO WEB DEL CONACYT. ...	65
	HALLAZGO N° 13: INADECUADA GESTIÓN DEL PORTAL DE TRANSPARENCIA DEL CONACYT.....	68
	HALLAZGO N° 14: INADECUADA GESTIÓN DEL SISTEMA DE REGISTRO Y CONTROL DE LOS BIENES MUEBLES "TECNOLÓGICOS" DEL CONACYT	75
	HALLAZGO N° 15: INADECUADA GESTIÓN DE LAS REDES SOCIALES DEL CONACYT.....	85
	HALLAZGO N° 16: FALTA DE UNA GESTIÓN DOCUMENTAL ELECTRÓNICA.....	89



VIII. SEGUIMIENTO A RECOMENDACIONES DE INFORMES DE AUDITORÍAS ANTERIORES.....	93
IX. RECOMENDACIONES GENERALES.....	93
X. CONCLUSIÓN DEL EXAMEN.....	93
XI. PÁRRAFO ACLARATORIO.....	93
XII. AGRADECIMIENTOS.....	93
XIII. LUGAR Y FECHA.....	94
XIV. FIRMA DE LA RESPONSABLE DE LA DIRECCIÓN DE AUDITORÍA INTERNA.....	94
XV. PERSONAL AUDITOR Y/O FUNCIONARIO QUE EJECUTÓ LA AUDITORÍA.....	94
XVI. ANEXOS.....	95



Versión Pública

I. INTRODUCCIÓN

La presente Auditoría corresponde al “Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022”; y fue realizada según Plan de Trabajo de la Dirección de Auditoría Interna (DAI) del Ministerio de Educación, Ciencia y Tecnología, en adelante MINEDUCYT.

Es la primera auditoría practicada por parte de la Dirección de Auditoría Interna, relacionada a las Tecnologías de la Información y Comunicación en el Consejo Nacional de Ciencia y Tecnología (CONACYT).

El 14 de diciembre de 2012, se aprobó el Decreto Legislativo No.234, publicado en el Diario Oficial No. 34, Tomo No.398 de fecha 19 de febrero de 2013, con el cual se aprobó la Ley de Desarrollo Científico y Tecnológico, derogando la Ley de Creación del CONACYT, que era una institución autónoma, adscrita al Ministerio de Economía.

Mediante Acuerdo Ejecutivo en el Ramo de Educación No. 15-0432-A de fecha 01 de marzo de 2013, Publicado en el Diario Oficial Número 61, Tomo No.399 de fecha 05 de abril del mismo año, se crea el Nuevo Consejo Nacional de Ciencia y Tecnología que podrá denominarse por su siglas “CONACYT”, como una Unidad desconcentrada del Ministerio de Educación bajo la dependencia directa del Viceministerio de Ciencia y Tecnología; y tendrá por objeto ser una entidad implementadora y ejecutora estatal de políticas nacionales en materia de desarrollo científico, tecnológico y de apoyo de la innovación.

A la fecha del desarrollo de la Auditoría, el CONACYT no poseía una unidad informática específica, que de apoyo y administre la plataforma tecnológica de la institución.

II. OBJETIVOS DEL EXAMEN

General:

Evaluar el manejo de los recursos de Tecnologías de Información y Comunicación (TIC) del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022, en función a la normativa aplicable.



Específicos:

1. Verificar el establecimiento y adecuado funcionamiento del Sistema de Control Interno en los procesos y operaciones relacionadas a las Tecnologías de Información y Comunicación.
2. Constatar la adecuada gestión del uso y control de los recursos de Tecnologías de Información y Comunicación.
3. Verificar los elementos que conforman la arquitectura organizacional relacionada a las Tecnologías de Información y Comunicación.
4. Emitir un informe independiente que contenga los resultados de los aspectos evaluados que fortalezcan los controles internos del CONACYT.

III. ALCANCE DEL EXAMEN

Nuestro Examen Especial incluyó una evaluación, al manejo de los recursos de Tecnologías de Información y Comunicación (TIC) del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022.

Realizamos nuestro Examen Especial, de conformidad con las Normas de Auditoría Interna del Sector Gubernamental (NAIG), emitidas por la Corte de Cuentas de la República (CCR), en lo aplicable. Para evaluar el control interno, utilizamos el Reglamento de Normas Técnicas de Control Interno Especificas (NTCIE) MINED; así como lo establecido en las demás normativas aplicables.

Aspectos evaluados:

1. Sistema de Control Interno;
2. Planificación y Organización de las TIC;
3. Estandarización de Sitios Web;
4. Planeación, usabilidad, navegación y seguridad del Sitio Web;
5. Portal de Transparencia del CONACYT;
6. Redes Sociales del CONACYT;
7. Correo Institucional;
8. Uso del Internet e Intranet;
9. Sistemas Informáticos;
10. Licencias de Software;
11. Inventario de Equipo informático y puntos de red;



12. Gobierno Digital;
13. Seguridad física y lógica;
14. Gestión documental de las TIC;
15. Controles establecidos para la gestión de TIC.

IV. RESUMEN DE LOS PROCEDIMIENTOS DE AUDITORÍA APLICADOS

Para el logro de los objetivos del examen, realizamos los procedimientos de auditoría siguientes:

1. Evaluación del Sistema de Control Interno, según marco de control establecido en el Reglamento de Normas Técnicas de Control Interno Específicas del MINED y demás normativa aplicable;
2. Análisis y evaluación de la planificación y estructura organizativa del área relacionada a las "TIC";
3. Verificamos el cumplimiento de la normativa relacionada a los sitios web institucionales de instituciones de gobierno;
4. Revisión del cumplimiento normativo según disposiciones emitidas por el Instituto de Acceso a la Información Pública, respecto a la gestión del portal de transparencia;
5. Verificamos la adecuada administración de redes sociales, de acuerdo con los lineamientos establecidos;
6. Evaluamos la adecuada administración del correo institucional del CONACYT;
7. Constatamos el uso de recursos tecnológicos, relacionados a los servicios de internet e intranet;
8. La utilización de los recursos de tecnología de información, de conformidad a los principios de eficiencia y efectividad;
9. Verificamos que las licencias de software instalados en los equipos de cómputo del personal del CONACYT, este acorde a su licencia física;
10. Contrastamos el inventario del equipo informático de la institución;
11. Verificamos las condiciones de los puntos de red en las instalaciones del CONACYT;
12. Analizamos el grado de aplicabilidad de las "TIC" en el CONACYT, que contribuya al fortalecimiento del gobierno digital;
13. Verificamos la gestión documental relacionadas a las "TIC";
14. Analizamos la implementación de la seguridad física y lógica relacionada a las tecnologías de la institución;
15. Evaluamos los controles realizados por la administración en relación con las actividades relacionadas a las Tecnología de la información y Comunicación.



V. PRINCIPALES REALIZACIONES Y LOGROS DE AUDITORÍA

Durante el desarrollo del Examen Especial de Auditoría, el Consejo Nacional de Ciencia y Tecnología, realizó las siguientes acciones correctivas relacionadas a observaciones comunicadas a los responsables del Sistema de Control Interno:

1. Creación de la Unidad de Tecnologías de Información;
2. Eliminación de riesgos altos y medios relacionados a la seguridad del sitio web www.conacyt.gob.sv;
3. Adecuación parcial de la estandarización de la página web institucional;
4. Actualización parcial de los apartados del portal de transparencia del CONACYT;
5. Retiro de equipos de comunicación inalámbrica personales, instalados en la institución;
6. Establecimiento de contraseña segura para el usuario del sistema ZKTime.Net 3.0;
7. Desactivación de cuenta de usuario de personal que renunció a la institución en el sistema de SIRH;
8. Elaboración de listados de usuarios que utilizan cada uno de los sistemas utilizados por el CONACYT;
9. Retiro la cuenta personal GYFBECAS@hotmail.com del equipo con número de inventario de activo fijo: 40151;
10. Desinstalación de software no acorde a las actividades de los usuarios: SCAM, PushDemo, Skype, DET, Zoom, Dropbox, SQL Server 2005 y Recuva y Spotify;
11. Utilización adecuada del logo de EL Salvador en los perfiles de las redes sociales de la institución;
12. Identificación adecuada de los nombres de los videos y eliminación de "borradores" en el sitio web: <https://www.youtube.com/@CONACYTsvOficial>;

VI. RESULTADOS DEL EXAMEN

1. Evaluación del Control Interno:

Evaluamos el control interno del Consejo Nacional de Ciencia y Tecnología (CONACYT), con base a lo establecido en el Reglamento de Normas Técnicas de Control Interno Específicas del Ministerio de Educación (NTCIE) en lo aplicable y demás normativas relacionadas. Lo anterior fue realizado, utilizando el Método del Cuestionario y la técnica de evaluación establecida en el Manual de Auditoría Interna, de la Dirección de Auditoría Interna del Ministerio de Educación Ciencia y Tecnología, mediante la cual, pudimos ponderar el control con un promedio de 2.02, que calificó el Sistema de Control Interno del CONACYT como: Medio; con una calificación de riesgo Moderado.



2. Inadecuada organización de las TIC.

Se verificó que el CONACYT, no había establecido en su estructura organizativa una Unidad de Tecnologías de Información y Comunicación, sin embargo, dicha condición fue desvanecida como logro de la presente auditoría, con la creación de la "Unidad de Tecnologías de Información" bajo la dependencia jerárquica de la Dirección Ejecutiva del CONACYT, sin embargo, se mantiene observaciones relacionadas a la organización y estructuración de dicha dependencia. Ver Hallazgo 1.

3. Falta de gestión de riesgos relacionado a las TIC.

Se verificó que el CONACYT no elaboró una Gestión de Riesgos de Tecnologías de Información y Comunicación, para el periodo 2013 al 2022. Ver Hallazgo 2.

4. Vulnerabilidad en el sitio web del CONACYT.

Se identificó vulnerabilidades en la seguridad del sitio web "www.conacyt.gob.sv", en cual se determinaron tres riesgos medios y dos riesgos bajos relacionados al servidor y al host remoto. Ver Hallazgo 3.

5. Inadecuada gestión y uso de los servicios de TIC.

Se verificó la gestión y uso de los servicios de Tecnología de la Información y Comunicación, con relación al correo institucional, intranet e intranet, observando que se carece de lineamientos relacionados al uso y gestión de los servicios proporcionados, controles aplicables al monitoreo del uso del servicio, planes de respaldo y resguardo de los archivos compartidos en el internet, soporte de almacenamiento de copias de seguridad ineficiente y pruebas de confiabilidad de pruebas de respaldo. Ver Hallazgo 4.

6. Debilidades en el uso de los sistemas informáticos.

Se verificó los "Sistemas utilizados por el CONACYT", determinado debilidades relacionadas a: carencias de huellas de auditoría, falta de planes de contingencia, falta de asignación de un técnico de parte del CONACYT, ineficiencia e ineficacia de los sistemas diseñados por la institución. Ver Hallazgo 5.



7. Inadecuada gestión de licencias de software.

Se verificó las licencias de software instaladas en los equipos de cómputo del personal del CONACYT y se observó lo siguiente: instalación de licencia en calidad de prueba, sin licencia física que ampare la instalación, softwares desactualizados, licencia Corel Draw x6, sin utilización, activación de opciones de Windows sin supervisión en el equipo y asignación de equipos sin proceder a crear nuevos usuarios en el sistema. **Ver Hallazgos 6.**

8. Debilidades en la seguridad lógica.

Se verificó que la Gestora de Indicadores y Sistemas de Información (período 2013-2022) no realizó un monitoreo a la seguridad lógica de los usuarios de equipo informático del CONACYT, debido a que se observó las siguientes debilidades de seguridad lógica: inicios de sesiones con correos personales o bien sin contraseñas, desactualización del Sistema Operativo y protección de antivirus. **Ver Hallazgo 7.**

9. Debilidades en la seguridad física de los servidores.

Se verificó la seguridad física de los servidores del CONACYT, observando que se carece de lo siguiente: identificación del área, controles de acceso de personal, sistema de video vigilancia y o/alarmas e infraestructura insegura. **Ver Hallazgo 8.**

10. Inadecuada gestión de cableado estructurado.

Se verificó la gestión realizada a la red de datos del CONACYT, observando que se carece de lo siguiente: lineamientos técnicos, control actualizado relacionado a la red de datos y monitoreo de las condiciones físicas del cableado. **Ver Hallazgo 9.**

11. Falta de un inventario documental del área de TIC.

Se verificó la documentación de soporte de las actividades relacionadas a los cargos de Gestor de Sistemas de Información de CyT y Gestor de Indicadores de Sistemas de Información (período 2013 al 2022), observando que carece de una gestión documental acorde a los lineamientos emitidos por la Unidad de Gestión Documental del CONACYT. **Ver Hallazgo 10.**



12. Falta de controles aplicables a las TIC.

Se verificó que el Observatorio Nacional de CyT, no efectuó los suficientes controles que garanticen el adecuado uso de los recursos tecnológicos. **Ver Hallazgo 11.**

13. Falta de estandarización del sitio web del CONACYT.

Se verificó la página web <https://www.conacyt.gob.sv/> observando que no cumple la estandarización de sitios web de instituciones de Gobierno en su totalidad, determinando observaciones relacionadas a los, roles de usuarios y registro de dominio. **Ver Hallazgo 12.**

14. Inadecuada gestión del portal de transparencia de CONACYT.

Se verificó el portal <https://www.transparencia.gob.sv/institutions/conacyt>, observando que la Información publicada no está acorde a las buenas prácticas para la publicación oficiosa de la institución. **Ver Hallazgo 13.**

15. Inadecuada gestión del sistema de registro y control de los bienes muebles "Tecnológicos" del CONACYT.

Se verificó según muestra de auditoría los bienes tecnológicos registrados en el Inventario de control de bienes realizado por la Gerencia de Administración del CONACYT, observando que carece de lo siguiente: Identificación de código de inventario, descargo de licencia con categoría "obsoletas", inadecuada descripción del bien, actualización del estado del bien, actualización de la asignación de equipos al personal, licencias no registradas al encargado de las "TIC", código de inventario repetitivo e inconsistencia en el registro de precio unitario de los bienes, Rack Metálico a la intemperie, duplicidad en asignación del código de inventario de rack, resguardo de documentación vulnerable al desgaste físico, switch en calidad de préstamo por parte del proveedor e inadecuado establecimiento de inventario de activo fijo. **Ver Hallazgo 14.**

16. Inadecuada gestión de las redes sociales del CONACYT.

Se verificó las direcciones de las redes sociales del CONACYT, cuyo vinculo se encuentra en la página web: <https://www.conacyt.gob.sv/>, en el cual se observó que se carece de: autorización de creación de redes sin autorización de la máxima autoridad, instrumentos administrativos que regule la gestión de las redes sociales, nombramiento del administrador y gestor de cada red social, monitoreo, y certificación de cuentas. **Ver Hallazgo 15.**



17. Falta de una gestión documental electrónica.

Se verificó que la Unidad de Gestión documental y Archivo del CONACYT, no ha elaborado conjuntamente con la Unidad de Protocolo y Relaciones Internacionales (Anteriormente RRP y Comunicaciones) y el personal encargado de las TIC los siguientes lineamientos relacionados a: Organización de los documentos electrónicos, buenas prácticas para reducir el consumo de papel; reemplazo de documentos físicos por electrónicos; política de seguridad y privacidad de los datos desarrollados en el sitio web del CONACYT; automatización de procesos, actualización de procedimientos y simplificación de trámites. **Ver Hallazgo 16.**

VII. HALLAZGOS DE AUDITORÍA

Como resultados de los procedimientos de auditoría determinamos los hallazgos indicados a continuación:



HALLAZGO N° 01: INADECUADA ORGANIZACIÓN DE LAS TIC

Importancia del Hallazgo : Riesgo Alto
Componente NTCIE impactado : Entorno de Control

CONDICIÓN:

Se verificó que el CONACYT, no había establecido en su estructura organizativa una Unidad de "TIC", sin embargo, dicha condición fue desvanecida como logro de la presente auditoría, con la creación de la Unidad de Tecnologías de Información bajo la dependencia jerárquica de la Dirección Ejecutiva del CONACYT, sin embargo, se mantiene las siguientes observaciones:

1. Falta de descripción de la organización y funciones relacionadas a las TI, en el Manual de Organización y Funciones del CONACYT;
2. El descriptor de funciones del Gestor de Sistemas de Información de CyT, no proporciona un detalle claro y total de las funciones realizadas en el área de las Tecnologías de Información y Comunicación, además, se observó que no está autorizado por la máxima autoridad del CONACYT;
3. Funciones relacionadas a las TIC, distribuidas en el personal del CONACYT, no acordes al objetivo de las unidades a las cuales pertenecen jerárquicamente. **Ver ANEXO N° 1;**
4. No se visualiza la separación de funciones entre los administradores de base de datos, desarrolladores de sistemas y los que procesa los datos en los sistemas de información;
5. Falta de Nombramiento del personal para actividades específicas de las TIC, con relación a: El coordinador institucional de implementación del plan de ciberseguridad, los Administradores de sistemas y administrador de la base de datos;
6. Se verificó que el CONACYT, no posee en sus controles extracontables la centralización en una sola dependencia de la asignación presupuestaria de todas las proyecciones relacionadas a las Tecnologías de Información y Comunicación;
7. Se verificó que no se poseen metas estratégicas relacionadas a las Tecnologías de Información y Comunicación;
8. Se verificó el Plan Operativo de los años 2013 al 2022, observando que se incorpora metas relacionadas a las TIC, denominadas "Otras Actividades Institucionales" y únicamente se incluye dos actividades permanentes que no abarcan todas las actividades ejecutadas durante el año relacionadas específicamente a las TIC, además no se evidencia la aprobación por la máxima autoridad del CONACYT;



9. Falta de centralización y supervisión de las actividades relacionadas a las TIC, se visualizó que el seguimiento de actividades operativas se realiza por diferentes unidades del CONACYT.
10. No se visualiza un Plan Operativo relacionado a las siguientes unidades que realizan actividades relacionadas a las TIC, para el periodo 2013 al 2022: Oficina de Información y Respuesta, Relaciones Públicas y Comunicaciones;
11. Falta de políticas y procedimientos de controles generales de los sistemas de información, ver ANEXO N° 2.

CRITERIOS:

Política de Ciberseguridad de El Salvador.

Numeral 7, párrafo 3: "Los titulares de cada institución del sector público deberán enviar al ente coordinador de ciberseguridad nacional, la documentación del nombramiento de la persona que ostentará el rol de coordinador institucional de implementación del plan de ciberseguridad. Se sugiere que la persona quien se designe como coordinador institucional de implementación del plan de ciberseguridad posea conocimientos de análisis de riesgo en el uso de TIC, y podrá ser un empleado de la institución, sin embargo, cada institución podrá establecer los roles según sus propias necesidades".

Numeral 8, paso 7: "Implementar el plan de acción. Se determina qué acciones tomar para abordar las brechas, si las hay, identificadas en el paso anterior y luego ajusta sus prácticas actuales de ciberseguridad".

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.

Art. 3: "Cada entidad del sector público debe establecer una Unidad de Tecnologías de Información y Comunicación, ubicada a un nivel jerárquico que le permita ejercer la gobernabilidad e independencia funcional dentro de la entidad, conforme a su nivel de madurez tecnológico y de acuerdo a su tamaño, alcance y ámbito de gestión".

Art. 4: "La entidad debe de definir y mantener actualizado el Manual de Organización y Funciones de la Unidad de TIC y de Puestos para el personal, de manera que las funciones y responsabilidades queden claramente establecidas".



Art. 5: "La Unidad de TIC deberá proponer a la máxima autoridad la adopción de mejores prácticas (estándares abiertos) y controles para la gestión de las TIC, que se requiera para el logro de los objetivos".

Art. 6: "La Unidad de TIC debe realizar un proceso de planificación de TIC de acuerdo con la planeación estratégica institucional, que facilite la consecución de sus logros futuros".

Art. 7: "El Plan Estratégico de TIC debe:

- a) Contener los objetivos e iniciativas estratégicas del área de TIC, que deben estar acordes a los objetivos estratégicos institucionales;
- b) Definir cómo los objetivos estratégicos de TIC serán alcanzados y medidos, establecer los indicadores de desempeño de conformidad con los objetivos estratégicos de TIC;
- c) Contemplar el presupuesto operacional y de inversiones, las estrategias de suministro y de adquisición (contratación de servicios y adquisición de equipos) y los requisitos legales;
- d) Ser formalmente aprobado y divulgado para que sea ejecutado por las partes interesadas".

Art. 8: "La Unidad de TIC debe de elaborar los planes anuales operativos diseñados de tal manera que defina los objetivos a cumplir y alineado con los objetivos estratégicos y/o operativos institucionales, actividades a desarrollar, programación, indicadores de gestión y su seguimiento, recursos de TIC, responsables y fechas de ejecución".

Art. 9: "La gestión de las Tecnologías de Información y Comunicación, es responsabilidad de la máxima autoridad y de la Unidad de TIC, la cual debe contar con los recursos que garanticen el cumplimiento de los objetivos institucionales".

Art. 10: "La Unidad de TIC, elaborará y ejecutará el presupuesto asignado para la gestión de las tecnologías de información y comunicación institucional y los proyectos tecnológicos viables a desarrollar, conforme a su nivel de madurez tecnológico de acuerdo a su tamaño, alcance y ámbito de gestión, los objetivos estratégicos y operativos de la institución y acorde con el plan de compras institucional".

Art. 12: "La Unidad de TIC, se asegurará que los controles internos diseñados mitiguen en gran medida los riesgos residuales obtenidos en el análisis de riesgos, siendo factible y con menor inversión la administración de éstos".



Art. 26: "La máxima autoridad, gerencias y demás jefaturas, deberán asegurar la correcta administración de la seguridad de la información, estableciendo y manteniendo controles que permitan que la información cumpla con las características de confidencialidad, integridad, disponibilidad, confiabilidad y cumplimiento legal".

Art. 27: "La Unidad de TIC administrará adecuadamente la seguridad física y lógica de sus recursos; estableciendo políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos y dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos, así como el resguardo de servidores, switch y otros dispositivos".

Art. 28: "La Unidad de TIC debe de establecer políticas y procedimientos de prevención, detección y corrección de virus; la utilización del correo electrónico; restringir el tráfico de información hacia dentro y fuera de la red institucional (pared de fuego) en todos aquellos puntos con acceso a redes públicas de datos o VPN".

Art. 32: "La Unidad de TIC deberá garantizar la separación de funciones entre los administradores de base de datos, los desarrolladores de sistemas y los que procesan los datos en los sistemas de información automatizados".

Art. 33: "La Unidad de TIC deberá realizar planes de respaldo y resguardo en sitio remoto y procedimientos para la recuperación de datos, que permitan asegurar la información de acuerdo a su importancia y criticidad".

Art. 34: "La Unidad de TIC definirá políticas y procedimientos de seguridad que garantice la confiabilidad, integridad y compatibilidad de la plataforma tecnológica y que contemple el suministro de energía eléctrica para la continuidad del negocio en caso de fallas temporales en la red eléctrica".

Art. 35: "La Unidad de Tecnologías de Información y Comunicación, deberá implementar medidas de seguridad física y lógica para las redes institucionales, esquemas de red con DMZ, consolas de antivirus, manteniéndolos actualizados en la red. Para el caso de los equipos informáticos sin acceso a la red, se deberán de crear políticas para su actualización".

Art. 36: "La Unidad de TIC debe de elaborar y ejecutar un plan de Mantenimiento de Equipo Informático debidamente diseñado, que contenga objetivos, políticas,



prioridades, programación de actividades en el que se identifique a los responsables de ejecutarlas y la determinación de los costos estimados; además, la identificación de metas programadas formuladas de manera precisa, factible, viable y medible, para que se pueda ejercer un seguimiento, evaluación de objetivos y su cumplimiento. Este plan deberá ser comunicado a los niveles responsables de su ejecución”.

Reglamento general de la Ley de Desarrollo Científico y Tecnológico.

Art. 27: “La Presidencia del N-CONACYT tendrá las siguientes funciones: literal k) Aprobar, a propuesta de la Dirección Ejecutiva, las estrategias, programas y planes de trabajo para el cumplimiento de los fines del NCONACYT; (...)”

Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED)

Art. 17: “La máxima autoridad, revisará periódicamente la estructura organizativa institucional, en un plazo no mayor de cinco años o cuando los objetivos y metas institucionales se reorienten, con el propósito de satisfacer los cambios que demande el desarrollo institucional en función de la calidad educativa. (...)”.

Art. 18: “(...) Todas las unidades organizativas, deberán complementar su estructura organizativa con un Manual de Organización y Funciones, que integre claramente el ámbito de control y supervisión, los objetivos y funciones de la Unidad con los niveles jerárquicos establecidos, los canales de comunicación y la delegación de autoridad”.

Art. 20: “En los manuales de Organización y Funciones, se deberá establecer claramente las líneas de autoridad y responsabilidad de cada Unidad organizativa, las cuales responderán de acuerdo a sus funciones ante una sola autoridad”.

Art. 22: “Las funciones de las diferentes unidades organizativas, deberán separarse de tal manera que exista independencia entre las funciones de autorizar, ejecutar, registrar, custodiar y controlar las operaciones asignadas por la Institución. (...)”.

Art. 59: “Los directores y gerentes, evaluarán una vez al año su estructura organizacional, a efecto de determinar si existe algún empleado que esté realizando funciones incompatibles, cuidando que exista la debida segregación de funciones que propicie el adecuado control interno y de rendición de cuentas.



De la realización de dicha actividad de control, cada Director y Gerente, gestionará los cambios que procedieren, tomando en cuenta lo normado en el apartado de separación de funciones incompatibles, de estas Normas. Asimismo, informará a su Jefe inmediato superior de la gestión realizada.

Las unidades organizativas que por su limitado personal deban agrupar funciones, deberán cuidar de no acumular el proceso de custodia, registro y autorización en un solo empleado o funcionario, debiendo buscar alternativas de segregación”.

Art. 289: “Los directores, serán nombrados por Acuerdo Ejecutivo y tendrán firma autorizada, ya sea en forma física o electrónica, en documentos inherentes a su Área de gestión y en las actividades específicas que le designe el Titular. Para los casos de firmas por medios electrónicos, el Director de Área deberá definir las personas autorizadas y contará con un listado actualizado de delegación de firmas”.

Art. 323: “Para las operaciones relacionadas a las tecnologías de información, las unidades de Informática elaborarán documentos de soporte, según la siguiente distribución de responsabilidades:

a) Todas las Unidades Proveedoras de Servicios de Tecnologías de Información:

- * Portafolio de Proyectos y Servicios;
- * Catálogo de Servicio Basado en Tecnología de Información; y
- * Manual de Procedimientos.

b) Gerencia de Informática

- * Plan de Infraestructura Tecnológica, del Ministerio de Educación;
- * Plan de Adquisiciones de Infraestructura Tecnológica;
- * Plan de Contingencia de las Tecnologías de Información;
- * Plan de Mantenimiento de la Infraestructura Tecnológica; y
- * Estándares de Seguridad de Tecnologías de Información.

c) Gerencia de Sistemas Informáticos

- * Documento de Arquitectura de Información del MINED;
- * Portafolio de Sistemas Informáticos;
- * Manual de Desarrollo y Mantenimiento de Sistemas Informáticos; y
- * Metodología para la Identificación de los Riesgos Informáticos.



El Comité Estratégico de Tecnologías de la Información, autorizará los documentos antes mencionados y cualquier otro documento realizado, relacionado a las tecnologías de la información”.

Art. 325: “Las unidades usuarias de los sistemas informáticos, deberán nombrar una persona de su Área como Administrador de Sistemas, quien será responsable de atender las necesidades inmediatas de los usuarios y establecer comunicación con las unidades de Informática, para solicitudes de cambios, capacitaciones y soporte de los sistemas.

La Unidad de Informática, capacitará a los administradores de sistemas en el uso y resolución de problemas, de los sistemas asignados”.

Art. 326: “El acceso a las bases de datos de producción en forma directa, estará restringido sólo para el Administrador de la Base de Datos. Se podrán asignar usuarios de lectura para aplicaciones automatizadas que extraigan datos de manera programada, de acuerdo con lineamientos establecidos y autorizados por el dueño de cada Sistema”.

Art. 334: “Todas las unidades de Informática del MINED, podrán elaborar los catálogos de servicios, basados en tecnologías de información, los cuales deberán actualizarse, por lo menos una vez al año”.

Art. 337: “La Unidad de Informática, encargada de la Infraestructura Tecnológica Central, creará el Plan de Mantenimiento Anual, para los equipos de usuarios finales y el Centro de Datos del MINED, de acuerdo a los recursos disponibles”.

Art. 342: “Las unidades de Informática, promoverán la centralización de los datos institucionales críticos, con el objetivo de protegerlos, llevando el control de respaldos y estableciendo procedimientos de restauración en caso de pérdida”.

Art. 343: “La Unidad de Informática, encargada de la Infraestructura Tecnológica Central, establecerá los estándares y procedimientos para la administración del: Centro de Datos, control de acceso, ordenamiento de equipo de tecnología de informática, inspecciones de sitios y puntos de acceso claves en el MINED Central y direcciones departamentales”.



Art. 364: "La Gerencia de Informática, podrá optar por implementar los estándares y buenas prácticas actualizadas del Ramo de las Tecnologías de Información, que mejoren la gestión de los servicios y proyectos.

La Gerencia de Informática, deberá implementar las leyes externas, regulaciones o requisitos de tecnologías de información que sean requeridos al Ministerio de Educación, por las entidades normalizadoras respectivas, del Gobierno de El Salvador".

CAUSA:

Falta de propuesta por parte de la Dirección Ejecutiva del periodo evaluado en presentar una estructura organizativa adecuada a las necesidades operativas y administrativas, en función de garantizar el adecuado funcionamiento de las Tecnologías de la Información y Comunicación en el CONACYT.

EFFECTOS:

1. Inadecuado funcionamiento de las actividades relacionadas a las Tecnologías de Información y Comunicación.
2. No se poseen claramente líneas de autoridad y responsabilidad de cada Unidad organizativa.
3. Inadecuada supervisión de las actividades y resultados obtenidos en la gestión de Tecnologías de Información y Comunicación.
4. Atribuciones no autorizadas por la máxima autoridad para su ejecución.
5. Falta de control de los recursos ejecutados en concepto de actividades de Tecnologías de la Información y Comunicación de la institución.
6. Realización de actividades, no acorde a las políticas, aspectos legales, procedimientos y controles relacionados a la Tecnologías de la Información y Comunicación, que garanticen una adecuada comunicación y una línea única de acción entre los actores involucrados, para que puedan realizar su trabajo organizada y sistemáticamente.

COMENTARIOS DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED] comentó:

"En respuesta al Acta de Lectura de Borrador de Informe del "Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y



Tecnología (CONACYT), al 31 de diciembre de 2022”, se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados”.

COMENTARIO DE AUDITORÍA INTERNA:

Se verificó el “Plan de Acción 2023”, presentado por la Dirección Ejecutiva del CONACYT, en cual se detallan las actividades a realizar con su respectiva fecha de inicio y finalización; por lo anterior, se procedió a efectuar el análisis de la información contenida en el referido plan, en su numeral uno y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 19/07/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorías posteriores al presente informe. Así mismo, se reconoce como un logro de auditoría la creación de la Unidad de Tecnologías de la Información; no obstante, esta depende organizativamente de la Dirección Ejecutiva del CONACYT, y no de la Máxima Autoridad.

RECOMENDACIÓN DEL HALLAZGO:

A la Directora Ejecutiva del CONACYT:

Implemente las acciones que desvanezcan en el corto plazo, los aspectos reportados en el presente hallazgo.



HALLAZGO N° 02: FALTA DE GESTIÓN DE RIESGOS RELACIONADO A LAS TIC

Importancia del Hallazgo : Riesgo Alto
Componente NTCIE impactado : Valoración de Riesgos

CONDICIÓN:

Se verificó que el CONACYT no elaboró una Gestión de Riesgos de Tecnologías de Información y Comunicación, para el periodo 2013 al 2022.

No obstante, en nota de fecha 02 de febrero de 2023 con referencia de nota No. DE-OBS-001-23, la Coordinadora del Observatorio Nacional de Ciencia y tecnología, presentó una matriz de Riesgos Informáticos "actual" relacionada con los usuarios, servicios y equipos tecnológicos e Informáticos en el CONACYT, observando lo siguiente:

1. Dicha matriz de riesgos no presenta fecha de elaboración, ni personal quien la elaboró, revisó y autorizó;
2. No se identificaron las acciones de Gestión de Riesgos, acciones de contingencia del riesgo y nombre del funcionario responsable de implementar las acciones;
3. No se visualizó la metodología utilizada para la identificación, análisis, administración y evaluación del riesgo en TIC.

CRITERIOS:

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.

Art. 11: "La Unidad de TIC, deberá adoptar una metodología de gestión de riesgos, debiendo documentar el proceso de identificación, análisis, administración y evaluación de riesgos de TIC."

Art. 12: "La Unidad de TIC, se asegurará que los controles internos diseñados mitiguen en gran medida los riesgos residuales obtenidos en el análisis de riesgos, siendo factible y con menor inversión la administración de éstos."



Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 54: "La máxima autoridad, directores nacionales, de staff, departamentales, gerentes y demás jefaturas de todas las unidades organizativas, deberán identificar los factores de riesgo de origen interno o externo que potencialmente pudieran obstaculizar el cumplimiento de los objetivos, metas y actividades institucionales, derivados de situaciones presentes o futuras.

La Dirección de Planificación, brindará la asistencia técnica y facilitará los instrumentos necesarios para que las distintas unidades organizativas, completen la información de los factores de riesgo que hubieren identificado, atendiendo lo establecido en el Modelo para la Administración de Riesgos Institucionales.

Al menos una vez al año, las diferentes direcciones del Ministerio de Educación deberán identificar los riesgos potenciales que afecten el cumplimiento de sus planes operativos y que deberán formar parte de éstos y de los planes estratégicos".

Art. 55: "Cada Unidad Organizativa, procederá a determinar los riesgos, según su importancia, probabilidad de ocurrencia y valoración o pérdida que éstos puedan ocasionar en el cumplimiento de sus planes anuales operativos y estratégicos. El Modelo para la Administración de Riesgos Institucionales, definirá los lineamientos para su análisis".

Art. 56: "La máxima autoridad, directores nacionales, de staff, departamentales, gerentes y demás jefaturas de todas las unidades organizativas, deberán definir los objetivos específicos de control y las actividades asociadas para prevenir, eliminar o minimizar los efectos de los riesgos identificados por medio de un Plan de Acción.

El Modelo para la Administración de Riesgos Institucionales, definirá los lineamientos para su gestión".

CAUSA:

Falta de implementación y fomento de una cultura de riesgos relacionada a las Tecnologías de la Información y Comunicación.

EFEECTO:

Incremento del impacto del riesgo relacionado a las Tecnologías de la Información y Comunicación.



COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED] comentó:

“En respuesta al Acta de Lectura de Borrador de Informe de “Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022”, se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados”.

COMENTARIOS DE AUDITORÍA INTERNA:

Se verificó el “Plan de Acción 2023”, presentado por la Dirección Ejecutiva, en cual se detallan las “actividades que desvanecen lo observado” con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral dos y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/09/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorías posteriores al presente informe. Por lo tanto, la observación se mantiene.

RECOMENDACIÓN DEL HALLAZGO:

Al Jefe de la Unidad de Tecnologías de Información, CONACYT:

Implemente acciones que desvanezcan en el corto plazo, el aspecto de control reportado, respecto a la Gestión de Riesgos de Tecnologías de Información y Comunicación, en función a lo regulado en la normativa aplicable al proceso.



HALLAZGO N° 03: VULNERABILIDAD EN EL SITIO WEB DEL CONACYT

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Actividades de Control

CONDICIÓN:

Se verificó la seguridad del sitio web "www.conacyt.gob.sv", identificando las siguientes amenazas:

Tabla N° 1 Detalle de vulnerabilidades en sitio web de CONACYT

DESCRIPCIÓN DEL RIESGO	VISIÓN DE VULNERABILIDAD/IMPACTO
	MEDIO
	BAJO

Fuente: Elaborado por el auditor.



Versión Pública

Además, se verificó que el CONACYT, posee el dominio del sitio web, <https://www.redisal.org.sv>, el cual posee las siguientes observaciones:

Tabla N° 2 Detalle de observaciones a sitio redisal

DESCRIPCIÓN	OBSERVACIÓN
Dominio https://www.redisal.org.sv	Se puede observar que es un dominio que las personas asocian con organizaciones de beneficencia y otras instituciones sin fines de lucro y no a una institución de gobierno en el cual la estructura de del dominio se identifica con "gob.sv"
Objetivo de REDISAL	Permitir la conformación de redes de investigadores para crear el ambiente necesario favorable a la investigación y estimular el trabajo cooperativo entre investigadores nacionales y científicos extranjeros.
Utilización de logotipo del CONACYT	Se verifica que se utiliza el logotipo de CONACYT (desactualizado)
No conforme a la Estandarización de sitios web de instituciones de gobierno	A pesar de que es un dominio registrado por CONACYT y posee enlace en la web institucional, la dirección www.redisal.org.sv , no está acorde a los estándares de sitios web de instituciones de gobierno.
Falta de acuerdo de aprobación por la máxima autoridad	No se identificó un acuerdo autorizado por la máxima autoridad del CONACYT, en el cual se apruebe la creación de dicha página web y el objetivo de su utilización.

Fuente: Elaborado por el auditor.

CRITERIOS:

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.

Art.5: "La Unidad de TIC deberá proponer a la máxima autoridad la adopción de mejores prácticas (estándares abiertos) y controles para la gestión de las TIC, que se requiera para el logro de los objetivos".

Art. 11: "La Unidad de TIC, deberá adoptar una metodología de gestión de riesgos, debiendo documentar el proceso de identificación, análisis, administración y evaluación de riesgos de TIC".

Art. 12: "La Unidad de TIC, se asegurará que los controles internos diseñados mitiguen en gran medida los riesgos residuales obtenidos en el análisis de riesgos, siendo factible y con menor inversión la administración de éstos".



Guía para estandarización de sitios Web de Instituciones de Gobierno.

3. Manual técnico para el uso de la plantilla

1.3.9: "Asegurarse que el servidor web no tenga vulnerabilidades

Según cifras internacionales acerca de WordPress, el 41% de los sitios web basados en este CMS, son atacados. Por tal motivo, debe escanearse regularmente el servidor, para detectar vulnerabilidades".

CAUSAS:

1. Falta de monitoreo a la seguridad del sitio web: www.conacyt.gob.sv.
2. Creación de sitios web sin autorización de la máxima autoridad.

EFFECTOS:

1. Exposición a potenciales riesgos de seguridad en el sitio web.
2. Al poseer el sitio www.redisal.org.sv, produce efectos como: Identidad diluida, confusión de búsqueda del usuario, falta de asociación de las actividades con el CONACYT.

COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva, [REDACTED] comentó:

"En respuesta al Acta de Lectura de Borrador de Informe de "Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022", se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados".



COMENTARIOS DE AUDITORÍA INTERNA:

Se verificó el "Plan de Acción 2023", presentado por la Dirección Ejecutiva, en cual se detallan las "actividades que desvanecen lo observado" con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral tres y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 09/04/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorías posteriores al presente informe. Por lo tanto, la observación se mantiene.

RECOMENDACIONES DEL HALLAZGO:

Al Jefe de la Unidad de Tecnologías de Información, CONACYT:

1. Implemente acciones que desvanezcan en el corto plazo, el aspecto de control reportado, respecto a la vulnerabilidad en el sitio web "www.conacyt.gob.sv", en función a lo regulado en la normativa aplicable al proceso.
2. Gestionar adecuadamente la eliminación de la página web www.redisal.org.sv con el respectivo justificante que ampare dicha decisión.



HALLAZGO N° 04: INADECUADA GESTIÓN Y USO DE LOS SERVICIOS DE TIC

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Actividades de Control

CONDICIÓN:

Se verificó la gestión y uso de los servicios de Tecnología de la Información y Comunicación, con relación al correo institucional, intranet e internet, observando lo siguiente:

1. Falta de lineamientos relacionados a la solicitud, uso y respaldo de la información de las cuentas de correo con dominio @admin.mined.edu.sv y @mined.gob.sv;
2. No se evidencia una actualización de la "Política para el uso de correo electrónico", a pesar de que se posee cambios significativos relacionado a cargos nuevos, lineamientos apegados a un plan de ciberseguridad entre otros;
3. Falta de control de todos los correos asignados al personal de CONACYT;
4. No se ha realizado el cierre de los correos institucionales del personal que no labora al 31/01/2023 en el CONACYT:
 - a) ██████████@admin.mined.edu.sv,
 - b) ██████████@admin.mined.edu.sv,
 - c) ██████████@admin.mined.edu.sv.
5. Se verificó que no se poseen lineamientos para el uso de internet/intranet en el cual se indique los derechos y responsabilidades de los usuarios en las plataformas digitales;
6. Falta de monitoreo de las conexiones realizadas a internet por los usuarios;
7. No existe restricciones de acceso a sitios web de entretenimiento;
8. Falta de planes de respaldo y resguardo de datos en sitio remoto y procedimiento para la recuperación de los mismos;
9. Se realizó una encuesta de satisfacción del servicio de internet en cual se determinó que 52.6% de usuarios, indican que el servicio es regular, lo cual evidencia que no se realiza un monitoreo por parte del encargado de las TIC, sobre la eficiencia de los recursos tecnológicos;
10. Soporte de Almacenamiento de copia de seguridad, no eficiente debido a que se realiza mensualmente el "Back up" en "DVD", cuya herramienta presenta desventajas, tales como su rápida degradación en el tiempo, la velocidad con la que pueden quedar obsoletos, tasas de error relativamente frecuentes, limitado tamaño o riesgos de seguridad a los que pueden estar sujetos debido a su portabilidad;



11. Se verificó la entrega de copias de seguridad de la información proporcionada a la Dirección Ejecutiva, observando que no se detalla: El contenido del DVD, peso, entre otros detalles, además no se indica que otro personal posee dichas copias de respaldo;
12. Falta de realización de pruebas de confiabilidad del proceso de respaldo;
13. No se evidencia en la entrega del "Back up" a la Dirección Ejecutiva las copias de seguridad de los meses de marzo a diciembre año 2020, enero a diciembre 2021 y abril 2022.

CRITERIOS:

Reglamento de Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 5: "La responsabilidad por el diseño, implantación, evaluación y perfeccionamiento del Sistema de Control Interno, corresponderá a la máxima autoridad del MINED, niveles de Dirección, gerenciales y demás jefaturas en el Área de su competencia institucional".

Art. 342: "Las unidades de Informática, promoverán la centralización de los datos institucionales críticos, con el objetivo de protegerlos, llevando el control de respaldos y estableciendo procedimientos de restauración en caso de pérdida".

Art. 362: "En todos los niveles de la organización, directores, gerentes y jefes responsables, deberán efectuar un monitoreo constante del ambiente interno y externo, de tal manera que les permita tomar las medidas oportunas sobre los factores y condiciones reales o potenciales que pudieran incidir en el desarrollo de sus funciones institucionales, ejecución de planes y cumplimiento de objetivos y metas".

Art. 365: "Las funciones del Comité Estratégico de Tecnologías de Información, estarán orientadas a: Verificar que exista alineación estratégica y entrega de valor de los proyectos e inversiones en Tecnologías de Información y Comunicación (TIC), promover administración eficiente de recursos tecnológicos, administración de riesgo, medición del desempeño y cumplimiento de la legislación y regulación interna relevante a las Tecnologías de Información y Comunicación (TIC)".

Art. 366: "Los directores, gerentes y jefes, deberán analizar y evaluar el funcionamiento de los mecanismos de control interno existentes, al menos una vez al año, con el fin de determinar la vigencia y calidad del control interno, con el propósito de realizar las



modificaciones que sean necesarias para mantener su efectividad. Asimismo, deberán efectuar una evaluación permanente de la gestión, con base a los planes organizacionales y otras disposiciones o regulaciones que fueren aplicables, para identificar oportunamente cualquier desviación y realizar las acciones que sean necesarias para prevenirlas o corregirlas”.

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.

Art. 5: “La Unidad de TIC deberá proponer a la máxima autoridad la adopción de mejores prácticas (estándares abiertos) y controles para la gestión de las TIC, que se requiera para el logro de los objetivos.

Corresponderá a los demás empleados, realizar las acciones necesarias para garantizar su efectivo cumplimiento”.

Art. 21: “La Unidad de TIC, deberá emitir procedimientos de control para monitorear los servicios de enlaces brindados por terceros, asegurándose que se cumpla con la recepción del servicio, la confidencialidad e integridad de la información a la cual tengan acceso, y operación de la infraestructura tecnológica”.

Art. 33: “La Unidad de TIC deberá realizar planes de respaldo y resguardo en sitio remoto y procedimientos para la recuperación de datos, que permitan asegurar la información de acuerdo a su importancia y criticidad”.

Art. 37: “La Unidad de TIC deberá de contar con la documentación de soporte de las operaciones que realicen (físicas o electrónicas), para justificar e identificar la naturaleza, finalidad y resultado de la actividad realizada. La documentación debe estar debidamente custodiada y contar con procedimientos para su actualización oportuna”.

Art. 40: “El Área de TIC debe establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información, que le permitan tener acceso a la misma durante periodos de contingencias, causados por desperfectos en los equipos, pérdida de información u otras situaciones similares”.



Política para el uso de Correo Electrónico, emitido por el CONACYT.

6.1: "Las cuentas institucionales permanecen mientras el usuario ocupa el cargo o función dentro de la institución; por lo que serán utilizadas a lo largo de tiempo".

6.2: "Se podrá solicitar el cierre o cancelación de una cuenta de correo, para ello, el (la) Coordinador (a) de Recursos Humanos deberá notificar por correo electrónico al Gestor (a) de Indicadores de ICT y Sistemas de Información, la baja del empleado por renuncia u otros motivos quién hará efectiva la solicitud.

La cancelación de una cuenta implica la imposibilidad de enviar y recibir nuevos correos".

CAUSA:

Falta de aplicabilidad de un marco de trabajo para la gestión de las tecnologías de la información.

EFFECTOS:

1. La utilización de los dominios diferentes a "@conacyt.gob.sv, genera un riesgo de control sobre la utilización adecuada del usuario, además de subutilizar los recursos de proporcionados por el MINED;
2. Ejecución de actividades no acorde al cumplimiento de los objetivos actuales de la institución;
3. Falta de seguridad razonable en la consecución de los objetivos y metas relacionadas;
4. Uso inadecuado del servicio de correo electrónico por parte de personal que no laborar en la institución.

COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED], comentó:

"En respuesta al Acta de Lectura de Borrador de Informe de "Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022", se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de



hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados”.

COMENTARIOS DE AUDITORÍA INTERNA:

Se verificó el “Plan de Acción 2023”, presentado por la Dirección Ejecutiva, en cual se detallan las “actividades que desvanecen lo observado” con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral cuatro y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/09/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorías posteriores al presente informe. Por lo tanto, la observación se mantiene.

RECOMENDACIÓN DEL HALLAZGO:

Al Jefe de la Unidad de Tecnologías de Información, CONACYT:

Implemente acciones que desvanezcan en el corto plazo, el aspecto de control reportado, respecto a la inadecuada gestión y uso de los servicios de Tecnología de la Información y Comunicación, en función a lo regulado en la normativa aplicable al



HALLAZGO N° 05: DEBILIDADES EN EL USO DE LOS SISTEMAS INFORMÁTICOS

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Actividades de Control

CONDICIÓN:

Se verificó el uso de los "Sistema utilizados por el CONACYT", observando lo siguiente:

Tabla N° 3 Detalle de observaciones a sistemas

SISTEMA	OBSERVACIONES
ZKTime.Net 3.0, utilizado por el departamento de Desarrollo Humano, que interactúa con el dispositivo de marcación utilizado para el registro de entradas y salidas del personal de CONACYT.	a) Modificación de registros de marcación sin registro de huellas de auditoría; b) Falta de un plan de contingencia para el uso del sistema en caso de que faltara el único usuario del sistema; c) Copias de respaldo del sistema no gestionadas por el encargado de TI; d) Falta de asignación de un técnico informático del CONACYT para el seguimiento y monitoreo de las gestiones relacionadas al sistema.
Sistema de Información de Recursos Humanos (SIRH), es un sistema provisto por el Ministerio de Hacienda, que permite la generación de las diferentes planillas de pagos de los empleados de CONACYT.	a) Falta de asignación de un técnico informático del CONACYT para el seguimiento y monitoreo de las gestiones relacionadas al sistema. b) Falta de un plan de contingencia para el uso del sistema en caso de que faltara el único usuario del módulo específico.
Sistema de Administración Financiera Integrado (SAFI), el cual es un sistema provisto por el Ministerio de Hacienda,	
Sistema "REDISAL", cuya utilización es para registrar la información detallada y actualizada sobre los investigadores que requieren ser parte de la "Red de Investigadores"	a) Falta de eficiencia y eficacia de este sistema. b) Falta de asignación de un técnico informático del CONACYT para el seguimiento y monitoreo de las gestiones relacionadas al sistema. c) Falta de un plan de contingencia para el uso del sistema en caso de que faltara el único usuario del módulo específico.
Sistema de Activo Fijo" del CONACYT, el cual básicamente es un archivo en formato de Microsoft Access.	a) Falta de eficiencia y eficacia de este sistema. Ver ANEXO N° 3.

Fuente: Elaborado por el auditor



CRITERIOS:

Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 5: "La responsabilidad por el diseño, implantación, evaluación y perfeccionamiento del Sistema de Control Interno, corresponderá a la máxima autoridad del MINED, niveles de Dirección, gerenciales y demás jefaturas en el Área de su competencia institucional".

Art. 338: "La implementación de soluciones de tecnologías de información, seguirán los lineamientos establecidos por:

- a) Gerencia de Informática: Estándares y procedimientos para adquisición e implementación de equipo informático, a ser utilizado en las oficinas centrales y descentralizadas del MINED;
- b) Gerencia de Sistemas Informáticos: Estándares y procedimientos para adquisición, creación e implementación de sistemas informáticos institucionales a ser utilizados, tanto en las oficinas administrativas del MINED, como en los centros escolares; y
- c) Gerencia de Tecnologías Educativas: Estándares y procedimientos para la implementación de proyectos, adquisición de software licenciado y equipos informáticos, a ser utilizados en los centros escolares y sitios Web institucionales".

Art. 339: "Las unidades de Informática, serán responsables de promover proyectos y procedimientos para proteger la información del MINED.

Las Normas de Seguridad de la Información, estarán definidas en el Documento de Estándares de Seguridad de Tecnologías de Información".

Art. 342: "Las unidades de Informática, promoverán la centralización de los datos institucionales críticos, con el objetivo de protegerlos, llevando el control de respaldos y estableciendo procedimientos de restauración en caso de pérdida".

Art. 346: "La Gerencia de Sistemas Informáticos, llevará el registro de los dueños y administradores de los sistemas. Los dueños de los sistemas, con el apoyo de los administradores de sistemas, serán los responsables de la preparación correcta de los datos que serán ingresados a las aplicaciones, incluyendo los procesos de autorización para ver, ingresar, modificar o eliminar información.



La Gerencia de Sistemas Informáticos, apoyará a los administradores de sistemas, en el desarrollo de capacitaciones que provean los conocimientos básicos a los usuarios, para usar correctamente los sistemas”.

Art. 348: “Los dueños de los sistemas, con apoyo de los administradores de sistemas, deberán establecer los reportes de control necesarios que aseguren la calidad de la información procesada, permitan detectar problemas y ayuden a corregirlos. Será responsabilidad del dueño del Sistema, garantizar que los usuarios utilicen correcta y oportunamente estos reportes de control”.

Art. 351: “El MINED, desarrollará un Sistema de Información, de acuerdo al Plan Estratégico, misión, objetivos y metas establecidos institucionalmente, debiendo ajustarse a requerimientos internos y externos y facilitando información para la rendición de cuentas. (...)”.

Art. 354: “Deberá diseñarse un Sistema de Información que permita identificar, obtener, procesar y divulgar datos relativos a la información financiera, operacional y de cumplimiento legal interno y externo que posibilite la dirección, ejecución y control de sus operaciones, acorde a las necesidades institucionales en un contexto de cambios constantes”.

Art. 355: “Para garantizar la calidad de la información que se genere en las diversas unidades organizativas del MINED y para que sea útil en la toma de decisiones adecuadas, deberá reunir las siguientes características: Apropiada, oportuna, actualizada, exacta y accesible. Cada Unidad organizativa, deberá establecer los puntos de control para verificar y asegurarse que estas características se cumplan, de acuerdo a los procesos que desarrollen”.

Art. 362: “En todos los niveles de la organización, directores, gerentes y jefes responsables, deberán efectuar un monitoreo constante del ambiente interno y externo, de tal manera que les permita tomar las medidas oportunas sobre los factores y condiciones reales o potenciales que pudieran incidir en el desarrollo de sus funciones institucionales, ejecución de planes y cumplimiento de objetivos y metas”.

Art. 364: “La Gerencia de Informática, podrá optar por implementar los estándares y buenas prácticas actualizadas del Ramo de las Tecnologías de Información, que mejoren la gestión de los servicios y proyectos.



La Gerencia de Informática, deberá implementar las leyes externas, regulaciones o requisitos de tecnologías de información que sean requeridos al Ministerio de Educación, por las entidades normalizadoras respectivas, del Gobierno de El Salvador”.

Art. 365: “Las funciones del Comité Estratégico de Tecnologías de Información, estarán orientadas a: Verificar que exista alineación estratégica y entrega de valor de los proyectos e inversiones en Tecnologías de Información y Comunicación (TIC), promover administración eficiente de recursos tecnológicos, administración de riesgo, medición del desempeño y cumplimiento de la legislación y regulación interna relevante a las Tecnologías de Información y Comunicación (TIC)”.

Art. 366: “Los directores, gerentes y jefes, deberán analizar y evaluar el funcionamiento de los mecanismos de control interno existentes, al menos una vez al año, con el fin de determinar la vigencia y calidad del control interno, con el propósito de realizar las modificaciones que sean necesarias para mantener su efectividad. Asimismo, deberán efectuar una evaluación permanente de la gestión, con base a los planes organizacionales y otras disposiciones o regulaciones que fueren aplicables, para identificar oportunamente cualquier desviación y realizar las acciones que sean necesarias para prevenirlas o corregirlas”.

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.

Art.5: “La Unidad de TIC deberá proponer a la máxima autoridad la adopción de mejores prácticas (estándares abiertos) y controles para la gestión de las TIC, que se requiera para el logro de los objetivos.

Corresponderá a los demás empleados, realizar las acciones necesarias para garantizar su efectivo cumplimiento”.

Art. 15: “La Unidad de TIC implementará la metodología para el ciclo de vida del desarrollo de sistemas, asegurando que los sistemas de información sean eficaces, seguros, íntegros, eficientes y económicos, que impidan la modificación no autorizada; asimismo, se ajuste al cumplimiento de las leyes, reglamentos y normativa vigente que les sean aplicables y considerar además lo siguiente:

- a) Se deberá priorizar y fomentar el desarrollo de los sistemas de información con recursos internos de la entidad.
- b) Definir una adecuada separación de las funciones en los ambientes de desarrollo y producción.



c) Procedimientos de actualización en los manuales de usuario y técnico, para el uso de los sistemas en producción y que se encuentra documentado el Control de cambios (versiones del Sistema) y los requerimientos se encuentren autorizados, realizados en el Sistema dentro del mismo”.

Art. 16: “La Unidad de TIC debe contar con políticas y procedimientos para el procesamiento de la información, desde su origen, relacionados con la captura, actualización, procesamiento, almacenamiento y salida de los datos, que asegure que la información sea completa, precisa, confiable y válida para la toma de decisiones”.

Art. 17: “La Unidad de TIC, deberá identificar los cambios en las soluciones automatizadas, conforme a un análisis técnico, económico y operativo, con las diferentes alternativas de solución, analizando el impacto de la implementación de cambios, planificando las pruebas para reducir incidentes, caídas de red, e implementando y documentando los cambios exitosos y en tiempo disponible”.

Art. 21: “La Unidad de TIC, deberá emitir procedimientos de control para monitorear los servicios de enlaces brindados por terceros, asegurándose que se cumpla con la recepción del servicio, la confidencialidad e integridad de la información a la cual tengan acceso, y operación de la infraestructura tecnológica”.

Art. 26: “La máxima autoridad, gerencias y demás jefaturas, deberán asegurar la correcta administración de la seguridad de la información, estableciendo y manteniendo controles que permitan que la información cumpla con las características de confidencialidad, integridad, disponibilidad, confiabilidad y cumplimiento legal”.

Art. 27: “La Unidad de TIC administrará adecuadamente la seguridad física y lógica de sus recursos; estableciendo políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos y dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos, así como el resguardo de servidores, switch y otros dispositivos”.

Art. 31: “La Unidad de TIC deberá garantizar que las bases de datos contengan huellas de auditoría, que registren los eventos de las fechas y actividades que realizan los usuarios, tales como: adición, eliminación, modificación de datos entre otros, con el fin de garantizar la identificación de los accesos a la información”.



Art. 33: "La Unidad de TIC deberá realizar planes de respaldo y resguardo en sitio remoto y procedimientos para la recuperación de datos, que permitan asegurar la información de acuerdo a su importancia y criticidad".

Art. 40: "El Área de TIC debe establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información, que le permitan tener acceso a la misma durante periodos de contingencias, causados por desperfectos en los equipos, pérdida de información u otras situaciones similares".

Art. 42.: "La Unidad de TIC deberá identificar y registrar los incidentes y problemas de TIC, categorizar, diagnosticar, resolver, controlar errores, evaluar problemas graves y reportar los informes que contienen los problemas resueltos y pendientes, el estatus de su procesamiento y las soluciones".

MANUAL DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS INFORMÁTICOS.

2.1. Huellas de Auditoría

"Las huellas de auditoría mínimas se consideran como obligatorias

- **Huellas de auditoría mínimas:**

A cada registro de datos importante se debe agregar los siguientes campos:

- Usuario que crea el registro.
- Fecha de creación del registro.
- Último usuario que modifica.
- Última fecha de modificación del registro.

Según el tipo del sistema y los requerimientos definidos, se podrán añadir las huellas de auditoría sugeridas, u otras que se consideren pertinentes.

- **Huellas de auditoría sugeridas:**

- Crear registro de accesos de usuario al sistema (tabla o archivo log que contiene fecha, usuario, ingreso exitoso o fallido al sistema).
- Dependiendo de la complejidad del sistema se podrá implementar una bitácora de los cambios realizados.
- Dependiendo de la criticidad de los datos se podrá realizar eliminado lógico de los registros."



CAUSA:

Falta de aplicabilidad de los estándares y procedimientos para adquisición, creación e implementación de sistemas informáticos institucionales del CONACYT.

EFFECTOS:

1. Creación de sistemas no acorde a los objetivos de los usuarios.
2. Uso inadecuado de los sistemas utilizados por el CONACYT.

COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED] comentó:

“En respuesta al Acta de Lectura de Borrador de Informe de “Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022”, se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados”.

COMENTARIOS DE AUDITORÍA INTERNA:

Se verificó el “Plan de Acción 2023”, presentado por la Dirección Ejecutiva, en cual se detallan las “actividades que desvanecen lo observado” con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral cinco y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/11/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorías posteriores al presente informe. Por lo tanto, la observación se mantiene.



RECOMENDACIONES AL HALLAZGO:

Al Jefe de la Unidad de Tecnologías de Información, CONACYT:

1. Elabore un plan de contingencia para el uso de los sistemas en caso de que faltara el único usuario;
2. Realice el seguimiento y monitoreo de las gestiones relacionadas a todos los sistemas utilizados por el CONACYT;
3. Para los sistemas "SAFI" y "SIRH", del Ministerio de Hacienda, solicitar por medio del Jefe de la USEFI – CONACYT, la creación de usuario como técnico informático con el fin de poder agregarlo al sistema y que se le notifique sobre los cambios en las aplicaciones que realice el Ministerio;
4. Realice y determine la periodicidad de las copias de respaldo del sistema ZKTime.Net 3.0;
5. Analizar y determinar los privilegios en el sistema ZKTime.Net 3.0 del usuario del Departamento de Desarrollo Humano, con el fin desvanecer cualquier modificación de registro que no posean huellas auditoría;
6. Evalué los sistemas de "REDISAL" y "Activo fijo", con el fin de realizar las mejoras necesarias para considerarlo eficientes y eficaces o bien considerar la sustitución de ambos, por sistemas que satisfagan las necesidades de los usuarios.



HALLAZGO N° 06: INADECUADA GESTIÓN DE LICENCIAS DE SOFTWARE

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Actividades de Control

CONDICIÓN:

Se verificó las licencias de software instaladas en los equipos de cómputo del personal del CONACYT, observando lo siguiente:

- Software instalado "Microsoft Office Profesional 2010" en calidad de prueba caducado; en siete equipos con número de inventario que se detallan a continuación: 32001, 31001, 34052, 24001, 20624, 40145 y 20623.
- Se comprobó que la computadora con código de inventario 60540, tiene instalado el Software ofimático Microsoft Office 2010 y no se posee la licencia física que ampare la instalación de la misma.
- Observamos equipos de cómputo que están desactualizados; debido que, presentaron mensaje de la Seguridad de Windows, donde indica que se necesitan las actualizaciones, según se detalla a continuación:

Tabla N° 4 Listado de equipos con software desactualizado

N°	CÓDIGO DE INVENTARIO	SOFTWARES DESACTUALIZADOS
1	33001	Sistema Operativo Windows 10
2	50644	Sistema Operativo Windows 10 y Software antivirus.
3	60540	Software antivirus.
4	40144	Software antivirus.
5	30520	Software antivirus.
6	40151	Sistema Operativo Windows 10

Fuente: Elaborado por el auditor

- Software instalado y licencia pagada de Corel Draw X6, en la computadora con código de inventario 20624, sin ser utilizada.

CRITERIOS:

Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 5: "La responsabilidad por el diseño, implantación, evaluación y perfeccionamiento del Sistema de Control Interno, corresponderá a la máxima autoridad del MINED, niveles de Dirección, gerenciales y demás jefaturas en el Área de su competencia institucional".



Art. 327: "La Gerencia de Informática, deberá controlar y mantener bajo custodia física los originales de las licencias del Software propiedad del MINED, los informáticos departamentales y cualquier otra Unidad del MINED, deberán registrar cualquier otra licencia adquirida y notificar oportunamente a la Gerencia de Informática sobre su uso. (...)".

Art. 364: "La Gerencia de Informática, podrá optar por implementar los estándares y buenas prácticas actualizadas del Ramo de las Tecnologías de Información, que mejoren la gestión de los servicios y proyectos.

La Gerencia de Informática, deberá implementar las leyes externas, regulaciones o requisitos de tecnologías de información que sean requeridos al Ministerio de Educación, por las entidades normalizadoras respectivas, del Gobierno de El Salvador".

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las entidades del Sector Público.

Art. 5: "La Unidad de TIC deberá proponer a la máxima autoridad la adopción de mejores prácticas (estándares abiertos) y controles para la gestión de las TIC, que se requiera para el logro de los objetivos.

Corresponderá a los demás empleados, realizar las acciones necesarias para garantizar su efectivo cumplimiento".

Art. 26: "La máxima autoridad, gerencias y demás jefaturas, deberán asegurar la correcta administración de la seguridad de la información, estableciendo y manteniendo controles que permitan que la información cumpla con las características de confidencialidad, integridad, disponibilidad, confiabilidad y cumplimiento legal".

Art. 27: "La Unidad de TIC administrará adecuadamente la seguridad física y lógica de sus recursos; estableciendo políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos y dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos, así como el resguardo de servidores, switch y otros dispositivos".

Art. 42: "La Unidad de TIC deberá identificar y registrar los incidentes y problemas de TIC, categorizar, diagnosticar, resolver, controlar errores, evaluar problemas graves y reportar los informes que contienen los problemas resueltos y pendientes, el estatus de su procesamiento y las soluciones".



Art. 43: "La Unidad de TIC deberá emitir procedimientos de control para gestionar la configuración, cambios y liberación de versiones de software mediante la definición de planes y políticas".

Art. 44: "La Unidad de TIC deberá desarrollar procedimientos de control para la instalación y desinstalación de software y dispositivos de información y comunicación, los que deberán ser reinstalados para su funcionamiento y efectividad en el uso".

Art. 45: "Todo el software instalado en la entidad, deberá estar amparado con la respectiva licencia extendida por el fabricante, otorgando a la entidad el derecho de instalación y uso de los mismos, de conformidad a lo establecido por la ley".

Art. 46: "La Unidad de Activo Fijo deberá de elaborar y actualizar un inventario de Software y aplicaciones. La Unidad de TIC deberá controlar el software instalado en cada uno de los equipos informáticos institucionales".

Art. 47: "La Unidad de TIC es la responsable de la instalación de software libre, debiendo justificar los usuarios las necesidades de su uso".

CAUSA:

Falta de control del software instalado en cada uno de los equipos informáticos del CONACYT.

EFFECTO:

Instalación de software ilegal, que pueden venir acompañados de código malicioso que podría provocar infecciones en los equipos locales o incluso fugas de información.

COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED] comentó:

"En respuesta al Acta de Lectura de Borrador de Informe de "Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022", se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa



que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados”.

COMENTARIOS DE AUDITORÍA INTERNA:

Se verificó el “Plan de Acción 2023”, presentado por la Dirección Ejecutiva, en cual se detallan las “actividades que desvanecen lo observado” con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral seis y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/09/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorías posteriores al presente informe. Por lo tanto, la observación se mantiene.

RECOMENDACIÓN DEL HALLAZGO:

Al Jefe de la Unidad de Tecnologías de Información, CONACYT:

Implemente acciones que desvanezcan en el corto plazo, el aspecto de control reportado, respecto a la inadecuada gestión de licencias de software, en función a lo regulado en la normativa aplicable al proceso.



HALLAZGO N° 07: DEBILIDADES EN LA SEGURIDAD LÓGICA

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Monitoreo y Control

CONDICIÓN:

Se verificó que la Gestora de Indicadores y Sistemas de Información (período 2013-2022) no realizó un monitoreo a la seguridad lógica de los usuarios de equipo informático del CONACYT, debido a que se observó las siguientes debilidades de seguridad lógica:

- a) Se verificó el inicio de sesión de cada una de las computadoras de escritorio y portátiles, observando lo siguiente:

Tabla N° 5 Detalle de equipos con debilidades de seguridad lógica

N°.	CÓDIGO DE INVENTARIO	DESCRIPCIÓN	USUARIO	OBSERVACIÓN
1	510699	Computadora		Inicio de sesión de trabajo con el Sistema Operativo con cuenta de correo personal
2	50643	Computadora portátil		Inicio de sesión de trabajo con el Sistema Operativo con cuenta de correo personal
3	50644	Computadora		Inicio de sesión sin contraseña de usuario.
4	34052	Computadora (CPU)		Inicio de sesión sin contraseña de usuario.
5	510674	Laptop		Inicio de sesión sin contraseña de usuario.
6	20627	Laptop		Inicio de sesión sin contraseña de usuario.
7	50549	Computadora (CPU)		Contraseña visible físicamente para cualquier usuario.
8	35050	Computadora (CPU)		Contraseña visible físicamente para cualquier usuario.
9	40145	Computadora (CPU)		Contraseña visible físicamente para cualquier usuario.
10	50643	Computadora portátil		Contraseña visible físicamente para cualquier usuario.

Fuente: Elaborado por el auditor



- b) Equipos trasladados a otros usuarios sin eliminar archivos de trabajo y software a continuación se detallan los números de inventarios: 30520, 501674 y 60540.
- c) Activación de la opción "Protección del Sistema Operativo" de Windows sin supervisión en computadora con código de inventario número 32001.

CRITERIOS:

Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 5: "La responsabilidad por el diseño, implantación, evaluación y perfeccionamiento del Sistema de Control Interno, corresponderá a la máxima autoridad del MINED, niveles de Dirección, gerenciales y demás jefaturas en el Área de su competencia institucional".

Art. 362: "En todos los niveles de la organización, directores, gerentes y jefes responsables, deberán efectuar un monitoreo constante del ambiente interno y externo, de tal manera que les permita tomar las medidas oportunas sobre los factores y condiciones reales o potenciales que pudieran incidir en el desarrollo de sus funciones institucionales, ejecución de planes y cumplimiento de objetivos y metas".

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.

Art. 26: "La máxima autoridad, gerencias y demás jefaturas, deberán asegurar la correcta administración de la seguridad de la información, estableciendo y manteniendo controles que permitan que la información cumpla con las características de confidencialidad, integridad, disponibilidad, confiabilidad y cumplimiento legal".

Art. 27: "La Unidad de TIC administrará adecuadamente la seguridad física y lógica de sus recursos; estableciendo políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos y dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos, así como el resguardo de servidores, switch y otros dispositivos".



Art. 42: "La Unidad de TIC deberá identificar y registrar los incidentes y problemas de TIC, categorizar, diagnosticar, resolver, controlar errores, evaluar problemas graves y reportar los informes que contienen los problemas resueltos y pendientes, el estatus de su procesamiento y las soluciones".

CAUSA:

Falta de controles que aseguren la correcta administración de la seguridad de la información.

EFEECTO:

Daños que el equipo puede sufrir en su estado lógico, perjudicando directamente al software.

COMENTARIOS DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED] comentó:

"En respuesta al Acta de Lectura de Borrador de Informe de "Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022", se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados".

COMENTARIO DE AUDITORÍA INTERNA:

Se verificó el "Plan de Acción 2023", presentado por la Dirección Ejecutiva, en cual se detallan las "actividades que desvanecen lo observado" con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral siete y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/09/2023 al 30/09/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorías posteriores al presente informe. Por lo tanto, la observación se mantiene.



RECOMENDACIÓN DEL HALLAZGO:

Al Jefe de la Unidad de Tecnologías de Información, CONACYT:

Implemente acciones que desvanezcan en el corto plazo, el aspecto de control reportado, respecto a las debilidades en la seguridad lógica, en función a lo regulado en la normativa aplicable al proceso.



Versión Pública

HALLAZGO N° 08: DEBILIDADES EN LA SEGURIDAD FÍSICA DE LOS SERVIDORES

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Monitoreo y Control

CONDICIÓN:

Se verificó la seguridad física de los servidores del CONACYT, observando lo siguiente:

1. El área de los "Servidores", no posee un rotulo que indique el tipo de sala;
2. No poseen un control de acceso del personal que ingresa al área de los "Servidores";
3. Carecen de un control de asignación de llaves del personal que posee los accesos al área;
4. No se posee un sistema de video vigilancia y o/alarmas;
5. Las instalaciones poseen tres puertas: 1. De acceso directo, la segunda es una puerta de acceso a Tesorería (y viceversa) la cual esta sellada con una cinta de tirro, 3. Acceso al baño de Tesorería, cerrada con un pasador (anteriormente el área de servidores era además la oficina del Observatorio Nacional de CYT);
6. Se posee acceso al personal de limpieza, sin supervisión de la actividad a realizar;
7. Se verificó que la documentación de soporte de las actividades del cargo se encuentra resguardado en el área de servidores.

CRITERIOS:

Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 5: "La responsabilidad por el diseño, implantación, evaluación y perfeccionamiento del Sistema de Control Interno, corresponderá a la máxima autoridad del MINED, niveles de Dirección, gerenciales y demás jefaturas en el Área de su competencia institucional".

Art. 362: "En todos los niveles de la organización, directores, gerentes y jefes responsables, deberán efectuar un monitoreo constante del ambiente interno y externo, de tal manera que les permita tomar las medidas oportunas sobre los factores y condiciones reales o potenciales que pudieran incidir en el desarrollo de sus funciones institucionales, ejecución de planes y cumplimiento de objetivos y metas".



Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.

Art.5: "La Unidad de TIC deberá proponer a la máxima autoridad la adopción de mejores prácticas (estándares abiertos) y controles para la gestión de las TIC, que se requiera para el logro de los objetivos.

Corresponderá a los demás empleados, realizar las acciones necesarias para garantizar su efectivo cumplimiento".

Art. 34: "La Unidad de TIC definirá políticas y procedimientos de seguridad que garantice la confiabilidad, integridad y compatibilidad de la plataforma tecnológica y que contemple el suministro de energía eléctrica para la continuidad del negocio en caso de fallas temporales en la red eléctrica".

Art. 35: "La Unidad de Tecnologías de Información y Comunicación, deberá implementar medidas de seguridad física y lógica para las redes institucionales, esquemas de red con DMZ, consolas de antivirus, manteniéndolos actualizados en la red. Para el caso de los equipos informáticos sin acceso a la red, se deberán de crear políticas para su actualización".

CAUSA:

Falta de protección del personal, las instalaciones, el hardware, el software, las redes y los datos frente a acciones y eventos físicos.

EFFECTO:

Daños en el Hardware, dispositivos, periféricos y conexiones.

COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED] comentó:

"En respuesta al Acta de Lectura de Borrador de Informe de "Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022", se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa



que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados”.

COMENTARIO DE AUDITORÍA INTERNA:

Se verificó el “Plan de Acción 2023”, presentado por la Dirección Ejecutiva, en cual se detallan las “actividades que desvanecen lo observado” con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral ocho y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/11/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorías posteriores al presente informe. Por lo tanto, la observación se mantiene.

RECOMENDACIÓN DEL HALLAZGO:

Al Jefe de la Unidad de Tecnologías de Información, CONACYT:

Implemente acciones que desvanezcan en el corto plazo, el aspecto de control reportado, respecto a las debilidades en la seguridad física, en función a lo regulado en la normativa aplicable al proceso.



HALLAZGO N° 09: INADECUADA GESTIÓN DE CABLEADO ESTRUCTURADO

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Actividades de Control

CONDICIÓN:

Se verificó la gestión realizada a la red de datos del CONACYT, observando lo siguiente:

- No se posee, por escrito normativa o lineamientos técnicos respecto a la instalación de cableado estructurado.
- Falta de un control actualizado de la información relacionada a la red de datos del CONACYT, en donde se identifique: Referencia de cable de red, ubicación según estructura organizativa usuario, nombre, cargo, estado (uso, deshabilitado, etc.) entre otra información que facilite su control.
- Falta de monitoreo de las condiciones físicas del cableado de red.
- Se verificó que el 22% de patch cord instalados en el CONACYT (cables de red que van desde el punto de red a la PC) no son certificados, según el siguiente detalle:

Tabla N° 6 Listado de patch cord no certificados

N°.	VIÑETA FÍSICA	UBICACIÓN
1	D02	nivel 1. Contabilidad
2	D07	Nivel 1. RRHH
3	D15	Nivel 1. Tesorería
4	SIN VIÑETA	Nivel 2.
5	N2D08	Nivel 2. Sala de reuniones
6	N2D010	Nivel 2. Promoción y popularización
7	N3D013	Nivel 3. Comunicaciones
8	N3D014	Nivel 3. Comunicaciones
9	N3D021	Nivel 3. Becas
10	SIN VIÑETA	Nivel 3. Becas

Fuente: Elaborado por el auditor.



- e) Inadecuada organización de cables de red (patch cord), según el siguiente detalle:

Tabla N° 7 Inadecuada organización de cables de red

N°.	VIÑETA DOCUMENTO*	UBICACIÓN	OBSERVACIÓN
1	CONACYT_D03	Nivel 1. Contabilidad	Cable tenso, cruzado con las piernas del usuario.
2	CONACYT_D05	Nivel 1. Gerencia Financiera	Sin acceso visual, que contribuya a la verificación física.
3	CONACYT_N2D10	Nivel 2. Promoción y popularización	Cable extenso que rodea el área de conexión con la máquina.
4	CONACYT_N3D23	Nivel 3. Becas	Cableado rodea el área de la oficina, del usuario, (cable extenso)

Fuente: Elaborado por el auditor.

- f) Se verificó los siguientes puntos de red sin identificación:

Tabla N° 8 Detalle puntos de red no identificados

N°.	VIÑETA DOCUMENTO*	VIÑETA FÍSICA	UBICACIÓN
1	CONACYT_D04	SIN VIÑETA	Nivel 1. Presupuesto
2	CONACYT_D18	SIN VIÑETA	Nivel 1. cuarto de servidores
3	CONACYT_N2D04	SIN VIÑETA	Nivel 2.
4	CONACYT_N3D18	SIN VIÑETA	Nivel 3. Comunicaciones
5	CONACYT_N3D19	SIN VIÑETA	Nivel 3. Becas
6	CONACYT_N3D22	SIN VIÑETA	Nivel 2. Becas
7	CONACYT_N3D23	SIN VIÑETA	Nivel 3. Becas

Fuente: Elaborado por el auditor.

- g) Falta de accesibilidad a los puntos de red certificados, según el siguiente detalle:

Tabla N° 9 Puntos de red sin acceso

N°.	VIÑETA DOCUMENTO	UBICACIÓN
1	CONACYT_D05	Nivel 1. Gerencia Financiera
2	CONACYT_Enlace	No se ubicó acceso

Fuente: Elaborado por el auditor.

- h) En el recorrido efectuado a las instalaciones del CONACYT, se observó que se mantiene una red de cableado antiguo, en los tres niveles del edificio, lo cual genera desorden visual y confusión de su utilidad.



CRITERIOS:

Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 5: "La responsabilidad por el diseño, implantación, evaluación y perfeccionamiento del Sistema de Control Interno, corresponderá a la máxima autoridad del MINED, niveles de Dirección, gerenciales y demás jefaturas en el Área de su competencia institucional".

Art. 362: "En todos los niveles de la organización, directores, gerentes y jefes responsables, deberán efectuar un monitoreo constante del ambiente interno y externo, de tal manera que les permita tomar las medidas oportunas sobre los factores y condiciones reales o potenciales que pudieran incidir en el desarrollo de sus funciones institucionales, ejecución de planes y cumplimiento de objetivos y metas".

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.

Art. 27: "La Unidad de TIC administrará adecuadamente la seguridad física y lógica de sus recursos; estableciendo políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos y dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos, así como el resguardo de servidores, switch y otros dispositivos".

Art. 33: "La Unidad de TIC deberá realizar planes de respaldo y resguardo en sitio remoto y procedimientos para la recuperación de datos, que permitan asegurar la información de acuerdo a su importancia y criticidad".

Art. 37: "La Unidad de TIC deberá de contar con la documentación de soporte de las operaciones que realicen (físicas o electrónicas), para justificar e identificar la naturaleza, finalidad y resultado de la actividad realizada. La documentación debe estar debidamente custodiada y contar con procedimientos para su actualización oportuna".

Art. 40: "El Área de TIC debe establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información, que le permitan tener acceso a la misma durante periodos de contingencias, causados por desperfectos en los equipos, pérdida de información u otras situaciones similares".



Art. 42: "La Unidad de TIC deberá identificar y registrar los incidentes y problemas de TIC, categorizar, diagnosticar, resolver, controlar errores, evaluar problemas graves y reportar los informes que contienen los problemas resueltos y pendientes, el estatus de su procesamiento y las soluciones".

CAUSA:

Falta de verificación del cumplimiento de estándares de cableado estructurado.

EFEECTO:

Provocar un colapso en las telecomunicaciones del edificio.

COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva, [REDACTED] comentó:

"En respuesta al Acta de Lectura de Borrador de Informe de "Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022", se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados".

COMENTARIO DE AUDITORÍA INTERNA:

Se verificó el "Plan de Acción 2023", presentado por la Dirección Ejecutiva, en cual se detallan las "actividades que desvanecen lo observado" con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral nueve y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/09/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorias posteriores al presente informe. Por lo tanto, la observación se mantiene.



RECOMENDACIÓN DEL HALLAZGO:

Al Jefe de la Unidad de Tecnologías de Información, CONACYT:

Implemente acciones que desvanezcan en el corto plazo, el aspecto de control reportado, respecto a la inadecuada gestión de cableado estructurado, en función a lo regulado en la normativa aplicable al proceso.



Versión Pública

HALLAZGO N° 10: FALTA DE UN INVENTARIO DOCUMENTAL DEL ÁREA DE TIC

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Actividades de Control

CONDICIÓN:

Se verificó la documentación de soporte de las actividades relacionadas a los cargos de Gestor de Sistemas de Información de CyT y Gestor de Indicadores de Sistemas de Información (período 2013 al 2022), observando lo siguiente:

1. No se evidencia la incorporación de documentos generados por el Gestor de Sistemas de Información de CyT y Gestor de Indicadores de Sistemas de Información (período 2013 al 2022), en el Inventario Documental del año 2022.
2. Falta de elaboración del índice de tipo documental de documentos generados por el Gestor de Sistemas de Información de CyT y Gestor de Indicadores de Sistemas de Información (período 2013 al 2022).
3. La documentación resguardada en el área de servidores no está debidamente ordenada y archivada.
4. No se identifica un control de los respaldos de información.

CRITERIOS:

Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 5: "La responsabilidad por el diseño, implantación, evaluación y perfeccionamiento del Sistema de Control Interno, corresponderá a la máxima autoridad del MINED, niveles de Dirección, gerenciales y demás jefaturas en el Área de su competencia institucional".

Art. 355: "Para garantizar la calidad de la información que se genere en las diversas unidades organizativas del MINED y para que sea útil en la toma de decisiones adecuadas, deberá reunir las siguientes características: Apropiada, oportuna, actualizada, exacta y accesible. Cada Unidad organizativa, deberá establecer los puntos de control para verificar y asegurarse que estas características se cumplan, de acuerdo a los procesos que desarrollen".



Art. 362: "En todos los niveles de la organización, directores, gerentes y jefes responsables, deberán efectuar un monitoreo constante del ambiente interno y externo, de tal manera que les permita tomar las medidas oportunas sobre los factores y condiciones reales o potenciales que pudieran incidir en el desarrollo de sus funciones institucionales, ejecución de planes y cumplimiento de objetivos y metas".

Lineamiento 4 para la Ordenación y Descripción Documental.

Artículo 1: "Las unidades productoras o generadoras deberán conformar expedientes con sus respectivos tipos documentales acordes al proceso de identificación y a los lineamientos de la Unidad de Gestión Documental y Archivos UGDA".

Artículo 2: "Las unidades productoras o generadoras deben determinar los métodos de ordenación: cronológico. alfabético. Numérico. Alfanumérico o mixto: y plasmar en su respectivo manual de procedimientos el método implementado para la ordenación de las series documentales que produce o genera. el cual puede variar entre serie y serie".

Artículo 3: "Las unidades productoras o generadoras deberán foliar los expedientes, estableciendo el método a utilizar que puede ser manual o con sello foliador. principalmente para aquellos expedientes que contengan datos personales, expedientes reglados, expedientes de archivos especializados y otros de valor legal e histórico".

CAUSA:

Falta de cumplimiento a los lineamientos emitidos por la Unidad de Gestión Documental y Archivos del CONACYT.

EFFECTO:

Falta de garantía de la calidad de la información, careciente de las siguientes características: Apropiada, oportuna, actualizada, exacta y accesible.



COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED] comentó:

“En respuesta al Acta de Lectura de Borrador de Informe de “Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022”, se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados”.

COMENTARIO DE AUDITORÍA INTERNA:

Se verificó el “Plan de Acción 2023”, presentado por la Dirección Ejecutiva, en cual se detallan las “actividades que desvanecen lo observado” con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral diez y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/09/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorias posteriores al presente informe. Por lo tanto, la observación se mantiene.

RECOMENDACIÓN DEL HALLAZGO:

Al Jefe de la Unidad de Tecnologías de Información, CONACYT:

Implemente acciones que desvanezcan en el corto plazo, el aspecto de control reportado, respecto a la falta de un inventario documental generada por el gestor de sistemas de información de CyT, en función a lo regulado en la normativa aplicable al proceso.



HALLAZGO N° 11: FALTA DE CONTROLES APLICABLES A LAS TIC

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Monitoreo y Control

CONDICIÓN:

Se verificó que el Observatorio Nacional de CyT, no ha efectuado los siguientes controles para el periodo 2013 al 2022:

1. Cambios en las soluciones automatizadas;
2. Vigencia de garantías de fábrica de los equipos de tecnología de información y comunicación;
3. Monitoreo de los servicios de enlaces brindados por terceros;
4. Software instalado en cada uno de los equipos informáticos de la institución;
5. Cambios de versiones del Sistema;
6. Registro actualizado de la infraestructura tecnológica, licencias de software, aplicativos, manejadores de base de datos;
7. Adquisiciones, contratos y obligaciones de las adquisiciones relacionadas a la infraestructura tecnológica;
8. Conciliaciones efectuadas por el "área de TIC" de los controles de activo fijo y con los registros contables.

CRITERIOS:

Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 5: "La responsabilidad por el diseño, implantación, evaluación y perfeccionamiento del Sistema de Control Interno, corresponderá a la máxima autoridad del MINED, niveles de Dirección, gerenciales y demás jefaturas en el Área de su competencia institucional".

Art. 327: "La Gerencia de Informática, deberá controlar y mantener bajo custodia física los originales de las licencias del Software propiedad del MINED, los informáticos departamentales y cualquier otra Unidad del MINED, deberán registrar cualquier otra licencia adquirida y notificar oportunamente a la Gerencia de Informática sobre su uso. La Unidad de Tecnologías Educativas, deberá controlar y mantener bajo custodia física los originales de las licencias del Software, necesario para los centros escolares".



Art. 344: "La Gerencia de Informática, consolidará los inventarios de software que se utilicen en los equipos oficialmente entregados a las unidades administrativas del MINED. Será responsabilidad de las unidades técnicas del MINED, reportar cualquier licencia que tengan bajo su poder; así como también, de cada usuario mantener su equipo informático con software autorizado. (...)".

Art. 336: "Cada Unidad de Informática, deberá llevar actualizado el control de las adquisiciones, contratos y obligaciones asignadas, respetando los procedimientos definidos en las unidades que los administren".

Art. 362: "En todos los niveles de la organización, directores, gerentes y jefes responsables, deberán efectuar un monitoreo constante del ambiente interno y externo, de tal manera que les permita tomar las medidas oportunas sobre los factores y condiciones reales o potenciales que pudieran incidir en el desarrollo de sus funciones institucionales, ejecución de planes y cumplimiento de objetivos y metas".

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades Del Sector Público.

Art. 15, literal c): "Control de cambios (versiones del Sistema) y los requerimientos se encuentren autorizados, realizados en el Sistema dentro del mismo".

Art. 17: "La Unidad de TIC, deberá identificar los cambios en las soluciones automatizadas, conforme a un análisis técnico, económico y operativo, con las diferentes alternativas de solución, analizando el impacto de la implementación de cambios, planificando las pruebas para reducir incidentes, caídas de red, e implementando y documentando los cambios exitosos y en tiempo disponible".

Art. 20: "La Unidad de TIC deberá contar con registros para el control de la vigencia de las garantías de fábrica que cubran desperfectos y aseguren el funcionamiento de los equipos de tecnología de información y comunicación, para lo cual creará procedimientos en conjunto con la Unidad de Adquisiciones y Contrataciones Institucional".

Art. 21: "La Unidad de TIC, deberá emitir procedimientos de control para monitorear los servicios de enlaces brindados por terceros, asegurándose que se cumpla con la recepción del servicio, la confidencialidad e integridad de la información a la cual tengan acceso, y operación de la infraestructura tecnológica".



Art. 46: "La Unidad de Activo Fijo deberá de elaborar y actualizar un inventario de Software y aplicaciones. La Unidad de TIC deberá controlar el software instalado en cada uno de los equipos informáticos institucionales".

Art. 48: "La Unidad de Tecnologías de Información y Comunicación deberá mantener registros actualizados con las características técnicas de la infraestructura tecnológica, licencias de software, aplicativos, manejadores de base de datos y la documentación de los controles de cambios de los sistemas de información. Estos registros deberán conciliarse con los controles de inventarios de activo fijo y con los registros contables".

CAUSA:

Falta de monitoreo del ambiente interno y externo relacionado a las Tecnologías de la Información y Comunicación.

EFFECTO:

Toma de medidas inoportunas sobre los factores y condiciones reales o potenciales que pudieran incidir en el desarrollo de las funciones, planes y cumplimiento de objetivos y metas del CONACYT.

COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED] comentó:

"En respuesta al Acta de Lectura de Borrador de Informe de "Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022", se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados".



COMENTARIO DE AUDITORÍA INTERNA:

Se verificó el "Plan de Acción 2023", presentado por la Dirección Ejecutiva, en cual se detallan las "actividades que desvanecen lo observado" con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral once y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/09/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorias posteriores al presente informe. Por lo tanto, la observación se mantiene.

RECOMENDACIÓN DEL HALLAZGO:

Al Jefe de la Unidad de Tecnologías de Información, CONACYT:

Implemente acciones que desvanezcan en el corto plazo, el aspecto de control reportado, respecto a la falta de controles aplicables a las actividades relacionadas a las TIC, en función a lo regulado en la normativa aplicable al proceso.



Versión Pública

HALLAZGO N° 12: FALTA DE ESTANDARIZACIÓN DEL SITIO WEB DEL CONACYT

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Información y Comunicación

CONDICIÓN:

Se verificó la página <https://www.conacyt.gob.sv/>, observando lo siguiente:

1. Prestación de servicios del CONACYT, a la Red Nacional de Divulgación en la Ciencia y Tecnología sin ser un proyecto público.
2. No se han definido únicamente un personal para administrador del sitio y gestor de contenido.
3. Se verificó que se registró de contacto un correo electrónico del Director Ejecutivo [REDACTED] el cual no posee nombramiento como funcionario que administrar dichos datos.

CRITERIOS:

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.

Art.26: "La máxima autoridad, gerencias y demás jefaturas, deberán asegurar la correcta administración de la seguridad de la información, estableciendo y manteniendo controles que permitan que la información cumpla con las características de confidencialidad, integridad, disponibilidad, confiabilidad y cumplimiento legal".

Art. 27: "La Unidad de TIC administrará adecuadamente la seguridad física y lógica de sus recursos; estableciendo políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos y dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos, así como el resguardo de servidores, switch y otros dispositivos".

Guía para estandarización de sitios web de Instituciones de Gobierno.

1. Planeación de sitio web

1.1.1. "Gestionar los plazos de vencimiento, claves de acceso y la definición del funcionario que administrar dichos datos. Es importante que, al realizar el registro del dominio se incluya dos personas de contacto, con el fin de garantizar la comunicación oportuna y la continuidad de la operación.



C1 Gestor de Contenido

C.1.1. Roles de administrador

Definición: Son todas las actividades llevadas a cabo por una persona del área de Tecnología, quien será responsable de administrar el sitio web y debe tener los derechos sobre este. (...).

C.1.2. Roles de usuario gestor contenido ("Editor" de WordPress)

Definición: El diseño del sitio como la información publicada debe apegarse a lo que dicta el manual de imagen es recomendable que el responsable de esta actividad pertenezca al área de comunicaciones de la institución, pero será la institución quien lo determine".

C1.3. Colaborador

"Definición: Es una persona que solo gestiona el contenido que ha sido creado por él, y estará sujeto a la aprobación de un usuario del rol "Gestor de Contenido" (...)".

CAUSA:

Gestión inadecuada del portal del sitio web institucional.

EFFECTO:

Sitio web no acorde a los estándares específicos.

COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED] comentó:

"En respuesta al Acta de Lectura de Borrador de Informe de "Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022", se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados".



COMENTARIOS DE AUDITORÍA INTERNA:

Se verificó el "Plan de Acción 2023", presentado por la Dirección Ejecutiva, en cual se detallan las "actividades que desvanecen lo observado" con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral doce y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/06/2023 al 31/07/2023, por lo cual se realizó la respectiva navegación al sitio web del CONACYT, determinando que aún posee características no acordes a los lineamientos establecidos en la materia, sin embargo también se reconoce superación de otros aspectos los cuales se consideraran como un logro de la presente auditoría.

RECOMENDACIONES DEL HALLAZGO:

A la Dirección Ejecutiva del CONACYT:

1. Implemente acciones que desvanezcan en el corto plazo, el aspecto de control reportado, falta de estandarización del sitio web del CONACYT, en función a lo regulado en la normativa aplicable;
2. Atribuir a las actividades de administrador del sitio web institucional al Jefe de la Unidad de Tecnologías de Información del CONACYT, e incorporar las funciones relacionadas a esta actividad en el Manual de Organización y Funciones y Descriptor de puesto de la Unidad de Tecnología de Información;
3. Atribuir las actividades de gestor de contenido, al personal que posee actividades relacionadas a la administración de las comunicaciones institucionales.



HALLAZGO N° 13: INADECUADA GESTIÓN DEL PORTAL DE TRANSPARENCIA DEL CONACYT

Importancia del Hallazgo : Riesgo Medio
 Componente NTCIE impactado : Información y Comunicación

CONDICIÓN:

Se verificó el portal <https://www.transparencia.gob.sv/institutions/conacyt>, observando las siguientes condiciones:

Tabla N° 10 Detalle de observación al portal de transparencia

ÍNDICE/SUB ÍNDICE	OBSERVACIÓN
Índice de Inicio	1. Se visualiza la Institución como una entidad Autónoma.
Inicio/Inicio	1. El nombramiento del oficial de Información es emitido por el Ministerio de Economía en fecha 24 de octubre de 2011.
Marco Normativo/Actas de Consejo	<ol style="list-style-type: none"> 1. No posee un orden cronológico las actas cargadas al sitio; 2. Se cita actas de Consejo Consultivo 2015, sin documento adjunto; 3. Documentos sin la totalidad de las firmas que legalizan la información; 4. Falta de cargar al sitio las actas de los meses: Enero a diciembre 2013, enero, febrero, agosto 2014, abril a diciembre 2015, agosto a octubre de 2016, enero a agosto 2017, febrero 2018, marzo y junio 2019, enero a diciembre 2020, enero a noviembre 2021, abril y diciembre 2022. Además, se verificó que falta cargar las actas de febrero a abril 2023; 5. Se comparten las actas de enero a diciembre del año 2016 en un solo documento y no una por mes como se ha visualizado en los demás años.
Marco Normativo/Manuales básicos de organización	<ol style="list-style-type: none"> 1. Manual de Puestos y Funciones de 2017, a pesar de que se posee la actualización de dicho manual; 2. Documentos con estado vigente a pesar de que son emitidos en calidad del CONACYT autónomo, a continuación, se detallan: Manual de Perfiles emitido en el año 2009, Manual del Desempeño emitido en el año 2008, Código de Ética y Normas de Conducta aprobado en el año 2010; 3. Manual del Desempeño sin autorización de la máxima autoridad.
Marco Normativo/Organigrama	1. No se evidencia organigrama del periodo 2013-2014.
Marco Normativo/Otros Documentos Normativos	1. Manual de Procedimientos Administrativos sin actualización realizadas al año 2022.



ÍNDICE/SUB ÍNDICE	OBSERVACIÓN
<p>Marco Normativo/Procedimientos y resultados de selección</p>	<ol style="list-style-type: none"> 1. En el procedimiento "Reclutamiento, selección, y contratación del personal", no se visualiza fecha de revisión y aprobación, así como también sus respectivas firmas de legalización del documento; 2. Este apartado no indica el cargar al portal de transparencia el procedimiento administrativo, sino más bien las contrataciones efectuadas por la institución.
<p>Marco Presupuestario/Concesiones y Autorizaciones</p>	<ol style="list-style-type: none"> 1. Nombre de archivos cargados, denominados sin contexto del contenido: Concesiones y Autorización de fecha de creación en el portal de transparencia 21/11/2013 y 13/10/2014; 2. Firma de Notas aclaratoria de inexistencia de información oficiosa por parte del Director Ejecutivo, a pesar de que desde el 2013 se ha nombrado un oficial de información y respuesta, dichas notas son del periodo 2014 al 2022; 3. Nota de fecha 07/01/2022 no está acorde al Manual de marca del CONACYT; 4. No se visualiza la nota justificante de inexistencia de la información en el año 2013; 5. Las notas emitidas 2014 al 2022 e inclusive en el año 2023, citan inadecuadamente el art.10 y el numeral que adjudica la obligación; 6. Notas explicativas que describen el contenido no son similares, a pesar de que es el mismo contenido en cada documento cargado al portal.
<p>Marco Presupuestario/Contrataciones y adquisiciones</p>	<ol style="list-style-type: none"> 1. Apartados que incluyen documentación del año 2012; 2. No se evidencia firma de legalización (elaborado, revisado y autorizado) del documento desde el 2013 al 2022 de los archivos de "Informes trimestrales"; 3. No se desarrolla idóneamente el apartado de Contrataciones y adquisiciones ya que no se detalla el contenido de los contratos; 4. No se encuentra homogenizado con el portal de transparencia del MINED, a pesar de ser una entidad desconcentrada.
<p>Marco Presupuestario/Estados Financieros</p>	<ol style="list-style-type: none"> 1. No se evidencia en la descripción del apartado que documentos contiene el archivo pdf, es decir no se detalla cada uno de los nombres de cada documento que componen los Estados Financieros del CONACYT. 2. Documentos compartidos del periodo 2011 al 2012 del CONACYT, autónomo.
<p>Marco Presupuestario/Inventarios</p>	<ol style="list-style-type: none"> 1. Descripción del Inventario no acorde a las descripciones realizadas por el MINED, a pesar de ser una entidad desconcentrada; 2. No se ha divulgado el Inventario de julio a diciembre 2017 a 2020 y marzo a diciembre 2022; 3. No se ha divulgado inventario 2013 y 2014;



ÍNDICE/SUB ÍNDICE	OBSERVACIÓN
	4. Se ha divulgado información de inventario 2012 del CONACYT autónomo; 5. En el documento adjunto de inventarios 2017 al 2020, no se evidencia información adicional que explique la información del documento, como lo es periodo del inventario, valor contable entre otros.
Marco Presupuestario/Presupuesto actual	1. Documentos Adjuntos sin firma jefe UFI; 2. Se ha divulgado información 2012 del CONACYT autónomo.
Marco Presupuestario/Recursos Públicos destinados a privados	1. Apartados sin orden cronológico; 2. Notas aclaratorias con firma del director Ejecutivo a pesar de que se tiene personal nombrado como oficial de información y respuesta.
Marco Presupuestario/Subsidios e incentivos fiscales	1. Notas aclaratorias del periodo 2013 al 2021 con firma del director Ejecutivo a pesar de que se tiene personal nombrado como oficial de información y respuesta.
Marco de gestión estratégica/estadísticas	1. No se visualiza información relacionada a los años 2013 al 2016 y 2022.
Marco de gestión estratégica/ Informes exigidos por disposición legal	1. Notas aclaratorias con firma del director Ejecutivo a pesar de que se tiene personal nombrado como oficial de información y respuesta.
Marco de gestión estratégica/ lista de asesores	1. Notas aclaratorias del periodo 2014 con firma del director Ejecutivo a pesar de que se tiene personal nombrado como oficial de información y respuesta; 2. No se visualiza documentos 2013, 2015 al 2022.
Marco de gestión estratégica/ obras en ejecución	1. Notas aclaratorias con firma del director Ejecutivo a pesar de que se tiene personal nombrado como oficial de información y respuesta.

Fuente: Elaborado por el auditor.

Además, se verificó que la Unidad de OIR del CONACYT, no posee un instrumento administrativo que indique los lineamientos y procedimientos relacionados para recabar y difundir la información oficiosa en el sitio de transparencia del CONACYT.

CRITERIOS:

Ley de Acceso a la Información Pública.

Art. 10: "Los entes obligados, de manera oficiosa, pondrán a disposición del público, divulgarán y actualizarán, en los términos de los lineamientos que expida el Instituto, la información (...)".



Art. 18: "La información oficiosa a que se refiere este capítulo deberá estar a disposición del público a través de cualquier medio, tales como páginas electrónicas, folletos, periódicos u otras publicaciones, o secciones especiales de sus bibliotecas o archivos institucionales.

El Instituto fomentará que los entes obligados utilicen tecnologías de la información y que dentro de un plazo razonable la información esté a disposición del público. No obstante, ninguna institución podrá negar información so pretexto de no contar con la tecnología adecuada".

Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 5: "La responsabilidad por el diseño, implantación, evaluación y perfeccionamiento del Sistema de Control Interno, corresponderá a la máxima autoridad del MINED, niveles de Dirección, gerenciales y demás jefaturas en el Área de su competencia institucional.

Corresponderá a los demás empleados, realizar las acciones necesarias para garantizar su efectivo cumplimiento".

Lineamiento No. 1 para la Publicación de la Información Oficiosa.

Artículo 1: "Las instituciones obligadas a la Ley de Acceso a la Información Pública – en adelante LAIP– deberán publicar la información oficiosa en formato digital disponible en sus sitios o portales web oficiales, ordenada conforme al Art. 44 de la LAIP, lineamiento 8 de Gestión Documental y Archivo, y los lineamientos para la publicación de la información oficiosa emitidos por el Instituto".

Artículo 3: "De acuerdo a lo estipulado en el artículo 50 letra "a" de la LAIP la obtención, sistematización y publicación de la información oficiosa corresponde al Oficial de Información de cada institución, en los casos en que no se haya nombrado uno esta obligación recaerá sobre el titular de la entidad, con independencia de la responsabilidad administrativa que pueda derivar del incumplimiento en el nombramiento del Oficial de Información. Los titulares y las unidades administrativas de cada institución deben proporcionar a los oficiales de información la información oficiosa que generen de manera oportuna y conforme a lo requerido dentro de los plazos para actualizar la información, en los formatos establecidos por el Instituto".



Artículo 4: "Las instituciones obligadas deben publicar la información oficiosa vigente de forma completa y deberán actualizarla como mínimo de manera trimestral, el plazo máximo para dicha actualización vencerá el último día hábil de los meses de enero, abril, julio y octubre de cada año; en la actualización correspondiente al mes de enero deberá incluirse la información oficiosa pendiente de publicación desde la última actualización del año anterior; la actualización trimestral no es aplicable a aquellos casos en los que la ley concede un plazo mayor para la actualización de la información. Las instituciones obligadas deben hacer constar la fecha de la última actualización en los sitios o portales web en los que publican su información oficiosa, de tal forma que permita verificarse la última actualización de cada apartado o documento. Se considerará una buena práctica la actualización mensual de la información oficiosa".

Artículo 5: "La publicación de los documentos relacionados a la información oficiosa que contengan información reservada o confidencial deberá realizarse de forma parcial a través de una versión pública conforme a lo establecido en el Art. 30 de la LAIP, y deberá advertirse expresamente que se trata de una versión pública, consignando además la base legal y circunstancias que justifican su clasificación.

Cuando se trate de reserva parcial deberá consignarse además la referencia correspondiente en el índice de información reservada".

Artículo 6. "Las instituciones obligadas deberán publicar la información de forma clara y precisa; la información deberá disponerse de un modo que permita su fácil identificación y acceso, a través de plantillas, diseños y sistemas que faciliten su ubicación y comprensión de manera sencilla y rápida, sin la necesidad de invertir tiempo y esfuerzo adicional o tener altos conocimientos de informática, esto con el fin de facilitar el acceso por parte de los usuarios.

Además, la información oficiosa deberá ser publicada en formato seleccionable, es decir que permita la copia de datos de forma electrónica para su posterior uso o procesamiento."

CAUSA:

Información publicada no conforme a las buenas prácticas para la publicación oficiosa de la institución.

EFECTO:

Apartados vacíos, información desactualizada e incompleta.



COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED] comentó:

"En respuesta al Acta de Lectura de Borrador de Informe de "Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022", se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados".

COMENTARIOS DE AUDITORÍA INTERNA MINEDUCYT

Se verificó el "Plan de Acción 2023", presentado por la Dirección Ejecutiva, en cual se detallan las "actividades que desvanecen lo observado" con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral trece y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/06/2023 al 31/12/2023, por lo cual se realizó la respectiva navegación del portal de transparencia del CONACYT, determinando que aún posee características no acordes a los lineamientos establecidos en la materia, sin embargo también se reconoce superación de otros aspectos lo cuales se consideraran como un logro de la presente auditoría.

RECOMENDACIONES DEL HALLAZGO:

Al Oficial de información del CONACYT:

1. Realizar actualizaciones constantes dentro del portal de Transparencia a fin ir renovando la información que se pública, los cuales deben estar programadas en el Plan de Trabajo de la unidad de "Oficina de Atención y Respuesta del CONACYT".
2. Revisar cada campo contenga los datos exigidos por la Ley de Acceso a la Información Pública y sus lineamientos, dejar evidencia de que se ha realizado dicha acción;



3. Comunicar al Instituto de Acceso a la Información Pública que el CONACYT, es una entidad desconcentrada pertenecientes al Ministerio de Educación Ciencia y Tecnología y solicitar que el portal de transparencia del CONACYT se ubique en otra categoría distinta a la "autónoma" debido a que esta categoría no corresponde a la figura legal del CONACYT;
4. Solicitar a la Unidad de Fiscalización del Instituto de Acceso a la Información Pública, el seguimiento del "Informe de fiscalización" de fecha 19 de marzo de 2018, con el fin de garantizar el adecuado cumplimiento de las obligaciones de Transparencia;
5. Solicitar al Instituto de Acceso a la Información Pública, capacitaciones relacionadas al tema de transparencia, acceso a la información pública y gestión del portal de transparencia;
6. Implemente acciones que desvanezcan en el corto plazo, el aspecto de control observado.



HALLAZGO N° 14: INADECUADA GESTIÓN DEL SISTEMA DE REGISTRO Y CONTROL DE LOS BIENES MUEBLES "TECNOLÓGICOS" DEL CONACYT

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Actividades de Control

CONDICIÓN:

Se verificó los bienes tecnológicos registrados en el Inventario de control de bienes realizado por la Gerencia de Administración del CONACYT, observando lo siguiente:

- a) Falta de identificación del código de inventario en los bienes registrados por la Gerencia de Administración, a continuación, se detallan:

Tabla N° 11 Detalle de bienes sin código de inventario

Nº.	CÓDIGO DE INVENTARIO	DESCRIPCIÓN
1	50580	Adaptadores macho- hembra XLR
2	50581	Adaptadores macho- hembra XLR
3	30521	Bocinas
4	50583	Cables XLR Macho-Hembra de 20 pies (6 mts)
5	50584	Cables XLR Macho-Hembra de 20 pies (6 mts)
6	50587	Cables XLR Macho-Hembra de 20 pies (6 mts)
7	24001	Computadora (CPU)

Fuente: Elaborado por el auditor

- b) Falta de descargo de licencias obsoletas en el registro de inventario de Activo Fijo, las cuales se detallan a continuación:

Tabla N° 12 Detalle de licencias obsoletas

Nº.	CÓDIGO DE INVENTARIO	DESCRIPCIÓN
1	999956	Certificado SSL
2	999956	Certificado SSL
3	999956	Certificado SSL
4	999956	Certificado SSL
5	999956	Certificado SSL
6	999956	Certificado SSL
7	999956	Certificado TLS
8	999956	Certificado TLS
9	999956	Certificado TLS
10	31001	Computadora (CPU)
11	999955	Licencia (29) Antivirus COMODO



Nº.	CÓDIGO DE INVENTARIO	DESCRIPCIÓN
12	999956	Licencia (29) Antivirus ESET SMART SECURITY BUSINESS EDITION (renovación)
13	999956	Licencia (29) Antivirus SENTINELONE
14	999956	Licencia (29) Antivirus SENTINELONE
15	999956	Licencia Adobe Creative Cloud
16	999956	Licencia Adobe Creative Cloud
17	999956	Licencia Adobe Creative Cloud
18	999956	Licencia Adobe Creative Cloud
19	999956	Licencia Adobe Creative Cloud
20	999956	Licencia Adobe Creative Cloud
21	999956	Licencia FIREWALL
22	999956	Licencia Firewall Fortinet
23	999955	Licencia OPEN Microsoft Office Professional 2007

Fuente: Elaborado por el auditor

- c) Inadecuado registro de descripción del bien en el sistema de Activo Fijo, se observó que los bienes en su descripción física, no coinciden con lo registrado en el sistema, detalle a continuación:

Tabla Nº 13 Registro inadecuado de bienes en sistema de activo fijo

Nº.	CÓDIGO DE INVENTARIO	MARCA DEL BIEN/SERIE/MODELO/DESCRIPCIÓN	MARCA/SERIE/DESCRIPCIÓN REGISTRADA EN EL INVENTARIO
1	50582	CableCreation	Genérico
2	30520	Genius	HP
3	510688	Genius	HP
4	510689	Genius	HP
5	50637	SRD00F1	STDR2000101
6	50638	NAAD5QWV/NA9JAW4C	STDR2000101/ NA9JAVQL
7	510652	Es un Gabinete de Telecomunicaciones que incluye un "CAT 5E enhanced"	Comunicación Switch de 24 puertos 10/100 mbps (Descripción según Activo Fijo)

Fuente: Elaborado por el auditor

- d) Equipo registrado en el Sistema de activo fijo con estado "Bueno", sin utilizar por el personal asignado, a continuación, se detallan:

Tabla Nº 14 Detalle de bienes sin utilizar

Nº.	CÓDIGO DE INVENTARIO	DESCRIPCIÓN
1	50543	Computadora (CPU)
2	24001	Monitor
3	50543	Mouse



Nº.	CÓDIGO DE INVENTARIO	DESCRIPCIÓN
4	510664	Mouse
5	50543	Teclado
6	30546	Teclado
7	50553	UPS
8	24001	USB HUB
9	35050	USB HUB
10	20623	USB HUB
11	20624	USB HUB
12	31001	USB HUB
13	32001	USB HUB
14	33001	USB HUB
15	34052	USB HUB
16	40144	USB HUB
17	40145	USB HUB
18	40146	USB HUB

Fuente: Elaborado por el auditor

- e) Utilización de equipo no asignado en el reporte de Activo Fijo "Personal", a continuación, se detallan:

Tabla N° 15 Utilización de equipo no asignado

Nº.	CÓDIGO DE INVENTARIO	DESCRIPCIÓN	PERSONAL RESPONSABLE	PERSONAL EN USO
1	50568	Audífonos para audio		
2	50546	Cámara de video		
3	20520	Cañón Proyector		
4	510700	Computadora		

Fuente: Elaborado por el auditor

- f) Se verificó que las "Licencias" adquiridas por el CONACYT, se encuentra distribuidas físicamente y registradas en el "Sistema de Activo Fijo", al personal que posee la instalación y no están asignadas al Gestor de Sistemas de Información de CyT, que a continuación se detallan:



Tabla N° 16 Listado de licencias no asignadas al Gestor de Sistemas Informáticos

Nº.	CÓDIGO DE INVENTARIO	DESCRIPCIÓN	PERSONAL RESPONSABLE
1	999956	Licencia Adobe Creative Cloud	
2	999956	Licencia Adobe Creative Cloud	
3	999956	Licencia Adobe Creative Cloud	
4	999956	Licencia Adobe Creative Cloud	
5	999956	Licencia Adobe Creative Cloud	
6	999956	Licencia Adobe Creative Cloud	
	9955	Licencia Corel Draw X6 Graphics Suite X6	
8	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
9	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
10	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
11	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
12	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
13	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
14	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
15	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
16	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
17	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
18	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
19	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
20	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
21	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
22	999955	Licencia FPP Microsoft Office home and bussines 2010 Standard Spanish	
23	999955	Licencia Ms Office 2010 Home Edition	
24	999955	Licencia OEM Small Bussines Español	
25	999955	Licencia OPEN Office para MAC Home and Business	

Fuente: Elaborado por el auditor



Versión Pública

- g) Se verificó que 26 licencias registradas en el sistema de activo fijo se encuentran con código de inventario repetitivo, según el siguiente detalle:

Tabla N° 17 Licencias sin código de inventario

CÓDIGO DE INVENTARIO	CANTIDAD DE LICENCIAS CON CÓDIGO REPETITIVO	TIPO DE LICENCIA
999956	6	Licencia Adobe Creative Cloud
999955	20	Diferentes tipos de licencia

Fuente: Elaborado por el auditor

- h) Inconsistencia en el registro de precio unitario de los siguientes bienes:

Tabla N° 18 Inconsistencia en registro de precio unitario

CÓDIGO DE INVENTARIO	BIEN	PRECIO SEGÚN FACTURA 0175 DE FECHA 21/04/2007	PRECIO SEGÚN REGISTROS DEL INVENTARIO DE ACTIVO FIJO
510652	Comunicación Switch de 24 puertos 10/100 mbps	\$162.00	\$161.91
510653	Comunicación Switch de 24 puertos 10/100 mbps	\$162.00	\$161.91

Fuente: Elaborado por el auditor

- i) Se verificó el bien con código 51014 "Switch marca D-Link", se encuentra sin funcionamiento ya que, a través del proveedor del servicio de Soporte Técnico de mantenimiento preventivo correctivo, se determinó que no funciona y se indicó el estado en calidad de dañado, a pesar de ello en el registro del inventario se establece en el estado como "bueno".
- j) Rack metálico con el código de inventario número 510617, con estado "bueno", según registro en el Inventario de Activo Fijo, el cual se encuentra físicamente a la intemperie con señales claras de deterioro debido a la corrosión.
- k) Se verificó la duplicidad de asignación de código de inventario número 510617, según el siguiente detalle:

Tabla N° 19 Duplicidad de código de inventario

CÓDIGO DE INVENTARIO	FECHA DE ADQUISICIÓN	DESCRIPCIÓN DEL BIEN	VALOR SEGÚN INVENTARIO
510617	01/01/1999	Rack metalico de 4 pies de alto y 19 de ancho, organizador de 8 anillos 24 clips, patch panel integrado de 24 puertos RJ45 CAT5, bandeja metalica de 10"x19", bandeja metalica de 30"x19", Concentrador UTP 16 puertos HUB	\$721.65
510617	-	No posee algún registro en el inventario de bienes del CONACYT.	-

Fuente: Elaborado por el auditor



- l) Se verificó que la documentación del soporte de las actividades relacionadas a la Administración del activo fijo del CONACYT, se encuentra resguarda en el espacio de la ducha del baño de la Gerencia Administrativa, observando lo siguiente:
 - Documentos almacenados en cajas y en el piso de la ducha del baño;
 - Falta un vidrio en la ventana de la ducha del baño;
 - Algunos documentos tienen signos visibles de deterioro.

- m) Se verificó que el Switch marca D-Link modelo DGS-1210-52, no pertenece al CONACYT y se encuentra en calidad de préstamo del proveedor del servicio de soporte técnico de mantenimiento, según reporte emitido por la empresa proveedora " [REDACTED] ", emitido en fecha 24/04/2021.

- n) Se verificó que el CONACYT, posee un Inventario de bienes, en cual no se evidencia una separación en:
 - Inventario de Activos Fijos, iguales o mayores a \$600.00 para el año 2013 al 2022;
 - Inventario de bienes menores a \$600.00;
 - Inventario de Intangibles;
 - Inventario de periféricos.

CRITERIOS:

Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 5: "La responsabilidad por el diseño, implantación, evaluación y perfeccionamiento del Sistema de Control Interno, corresponderá a la máxima autoridad del MINED, niveles de Dirección, gerenciales y demás jefaturas en el Área de su competencia institucional".

Art. 299: "Se considerarán activos fijos, los bienes con valores de adquisición iguales o mayores a Seiscientos Dólares de los Estados Unidos de Norte América (\$600.00), dichos bienes deberán ser controlados de acuerdo a lo normado en el "Instructivo del Sistema de Registro y Control de los Bienes Muebles del Ministerio de Educación".
 Todas las unidades organizativas, estarán obligadas a informar al Área de Activo Fijo, Central o Departamental, las adquisiciones, donaciones, traslados y descargo de bienes muebles, dentro de los cinco días hábiles de efectuada la transacción".

Art. 309: "Para los bienes con valores menores a Seiscientos Dólares de los Estados Unidos de América (\$600.00), se llevará un control administrativo en cada Unidad organizativa.



El Área de Administración, emitirá las políticas que definirán el debido control de dichos bienes, los cuales podrán ser muebles, equipo e intangibles. (..).“

Art. 327: “La Gerencia de Informática, deberá controlar y mantener bajo custodia física los originales de las licencias del Software propiedad del MINED, los informáticos departamentales y cualquier otra Unidad del MINED, deberán registrar cualquier otra licencia adquirida y notificar oportunamente a la Gerencia de Informática sobre su uso. (...)”.

Art. 355: “Para garantizar la calidad de la información que se genere en las diversas unidades organizativas del MINED y para que sea útil en la toma de decisiones adecuadas, deberá reunir las siguientes características: Apropiaada, oportuna, actualizada, exacta y accesible. Cada Unidad organizativa, deberá establecer los puntos de control para verificar y asegurarse que estas características se cumplan, de acuerdo a los procesos que desarrollen”.

Art. 358: “(...) Los directores, gerentes y jefes, serán responsables del adecuado resguardo, conservación, manejo y destrucción de los documentos de sus áreas de gestión y deberán dictar las políticas pertinentes en los casos de documentación que deba resguardarse por criterios propios de su aplicación y por constituir información que el usuario pudiera requerir por lapsos de tiempo largos, como calificaciones, títulos, Prueba de Aprendizaje y Aptitudes para Egresados de Educación Media (PAES) y otros que aplique”.

Art. 362: “En todos los niveles de la organización, directores, gerentes y jefes responsables, deberán efectuar un monitoreo constante del ambiente interno y externo, de tal manera que les permita tomar las medidas oportunas sobre los factores y condiciones reales o potenciales que pudieran incidir en el desarrollo de sus funciones institucionales, ejecución de planes y cumplimiento de objetivos y metas”.

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las entidades del Sector Público.

Art. 26: “La máxima autoridad, gerencias y demás jefaturas, deberán asegurar la correcta administración de la seguridad de la información, estableciendo y manteniendo controles que permitan que la información cumpla con las características de confidencialidad, integridad, disponibilidad, confiabilidad y cumplimiento legal”.



Art. 34: "La Unidad de TIC definirá políticas y procedimientos de seguridad que garantice la confiabilidad, integridad y compatibilidad de la plataforma tecnológica y que contemple el suministro de energía eléctrica para la continuidad del negocio en caso de fallas temporales en la red eléctrica".

Art. 39: "La Unidad de TIC, deberá contar con un plan de contingencia autorizado por la máxima autoridad de la entidad, este plan debe ser viable, que detalle las acciones, procedimientos y recursos financieros, humanos y tecnológicos, considerando los riesgos y amenazas de TIC que afecten de forma parcial o total la operatividad normal de los servicios de la Entidad, categorizando el tipo de acción a realizar en cuanto a la medición en tiempo para el restablecimiento de las operaciones tecnológicas, este plan debe probarse y actualizarse atendiendo la realidad tecnológica de la entidad al menos una vez al año. Deberá ser comunicado a los niveles pertinentes".

Art. 40: "El Área de TIC debe establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información, que le permitan tener acceso a la misma durante periodos de contingencias, causados por desperfectos en los equipos, pérdida de información u otras situaciones similares".

Art. 42: "La Unidad de TIC deberá identificar y registrar los incidentes y problemas de TIC, categorizar, diagnosticar, resolver, controlar errores, evaluar problemas graves y reportar los informes que contienen los problemas resueltos y pendientes, el estatus de su procesamiento y las soluciones".

Art. 46: "La Unidad de Activo Fijo deberá de elaborar y actualizar un inventario de Software y aplicaciones. La Unidad de TIC deberá controlar el software instalado en cada uno de los equipos informáticos institucionales".

Instructivo del Sistema de Registro y Control de los Bienes Muebles del Ministerio de Educación.

"Responsabilidades para la administración de bienes muebles, literal:

- a) El funcionario que administra y controla bienes muebles de cualquier dependencia del MINED, responderá pecuniariamente por la pérdida o deterioro culposo en el uso irracional de ellos, en su defecto podrá restituir el bien dañado o perdido, por otro similar, así también son responsables de verificar que el proceso de control interno previo se haya cumplido.
- e) Será responsabilidad de Directores, Gerentes, Jefes de unidad, Coordinadores y/o Directores de Centros Escolares, codificar y registrar en su inventario todo bien que



adquiera bajo cualquier fuente de financiamiento u otra forma de adquisición, ya que ello constituye parte del patrimonio del Estado;

f) Los Técnicos de Activo Fijo Departamental y los delegados de Activo Fijo de las unidades centrales, están obligados a informar a la instancia superior y al Departamento e Activo Fijo Central sobre los faltantes, deterioros daños u otro tipo de anomalías que se estén generando en la administración de los bienes muebles del MINED. (...)

j) Los Directores Administrativos, Directores de instituciones educativas, Coordinadores o jefes deben velar porque los números de inventario sean estampados con material que garantice su duración, en un lugar visible del bien y además porque dicho código se conserve, aún por causas de mantenimiento, reparación o modificación de los mismos.

r) Las computadoras de escritorio se clasificarán como equipo de cómputo (C.P.U) y así se codificará y registrarán. Los demás periféricos que contiene cada equipo de cómputo será responsabilidad de cada unidad tener su propio control”.

CAUSA:

Falta de evaluación y perfeccionamiento del Sistema de Control Interno relacionada al registro y control de los bienes “Tecnológicos” del CONACYT.

EFFECTO:

Generación de Información no confiable para la toma de decisiones.

COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED] comentó:

“En respuesta al Acta de Lectura de Borrador de Informe de “Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022”, se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT.

No omito manifestar que de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados”.



COMENTARIO DE AUDITORÍA INTERNA:

Se verificó el "Plan de Acción 2023", presentado por la Dirección Ejecutiva, en cual se detallan las "actividades que desvanecen lo observado" con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral catorce y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/06/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorías posteriores al presente informe. Por lo tanto, la observación se mantiene.

RECOMENDACIÓN DEL HALLAZGO:

Al "Encargado de Activo Fijo" del CONACYT:

Implemente las acciones que desvanezcan en el corto plazo, el aspecto de control reportado, respecto a la inadecuada gestión del Sistema de Registro y Control de Bienes, en función a lo regulado en la normativa aplicable al proceso.



HALLAZGO N° 15: INADECUADA GESTIÓN DE LAS REDES SOCIALES DEL CONACYT

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Información y Comunicación

CONDICIÓN:

Se verificó las direcciones de las redes sociales del CONACYT, cuyo vinculo se encuentra en la página web: <https://www.conacyt.gob.sv/>, en las cuales se observó lo siguiente:

- a) Falta de autorización por la máxima autoridad de cada una de las cuentas de las redes sociales;
- b) No se posee un instrumento administrativo sobre el uso de redes sociales institucional;
- c) Falta de una estrategia de participación ciudadana utilizando las redes sociales como medio;
- d) No se posee lineamientos de la calidad de los productos de las redes sociales tanto en su proceso de publicación, como de su contenido;
- e) No se ha determinado la periodicidad de la actualización de redes sociales;
- f) Falta de nombramiento del administrador de las redes sociales y el gestor de contenido, actualmente se poseen tres administradores: Encargada de Relaciones públicas y comunicaciones, Gestora de Promoción y Popularización de CyT y Oficial de Información (control de cuenta oir@conacyt.gob.sv),
- g) No se evidencia monitoreo de las redes sociales por parte de la unidad de Relaciones Públicas y Comunicaciones (Actualmente Unidad de Protocolo y Relaciones institucionales);
- h) Falta de cuentas verificadas para las redes: www.facebook.com/ConacytSV, <https://www.instagram.com/conacytsv/> y <https://twitter.com/CONACYToficial>;

CRITERIOS:

Ley de Procedimientos Administrativos.

Art. 16: "Sin perjuicio de los derechos reconocidos en la Constitución de la República y las Leyes, las personas, en sus relaciones con la Administración Pública, son titulares de los siguientes derechos: Numeral 4: A la garantía de seguridad y confidencialidad de los datos personales que figuren en los ficheros, bases de datos, sistemas y aplicaciones de la Administración Pública;(..)".



Art. 18: "Los órganos de la Administración Pública podrán utilizar tecnologías de la información y comunicación para realizar trámites, diligencias, notificaciones, citatorios o requerimientos, siempre que dichos medios tecnológicos posibiliten la emisión de una constancia, ofrezcan garantías de autenticidad, confidencialidad, integridad, eficacia, disponibilidad y conservación de la información y sean compatibles con la naturaleza del trámite a realizar. (...)".

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las entidades del Sector Público.

Art. 5: "La Unidad de TIC deberá proponer a la máxima autoridad la adopción de mejores prácticas (estándares abiertos) y controles para la gestión de las TIC, que se requiera para el logro de los objetivos".

Art. 26: "La máxima autoridad, gerencias y demás jefaturas, deberán asegurar la correcta administración de la seguridad de la información, estableciendo y manteniendo controles que permitan que la información cumpla con las características de confidencialidad, integridad, disponibilidad, confiabilidad y cumplimiento legal".

Reglamento General de la Ley De Desarrollo Científico y Tecnológico.

Art. 27: "La Presidencia del N-CONACYT tendrá las siguientes funciones: (..) literal j) Aprobar la organización básica, así como las políticas operativas y administrativas que aseguren el adecuado funcionamiento del NCONACYT y que le sean propuestas por la Dirección Ejecutiva".

Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 5: "La responsabilidad por el diseño, implantación, evaluación y perfeccionamiento del Sistema de Control Interno, corresponderá a la máxima autoridad del MINED, niveles de Dirección, gerenciales y demás jefaturas en el Área de su competencia institucional".

Corresponderá a los demás empleados, realizar las acciones necesarias para garantizar su efectivo cumplimiento.

Art. 191: "La Dirección de Comunicaciones, emitirá los lineamientos para la comunicación institucional en congruencia con la política de comunicaciones del MINED".



Art. 355: "Para garantizar la calidad de la información que se genere en las diversas unidades organizativas del MINED y para que sea útil en la toma de decisiones adecuadas, deberá reunir las siguientes características: Apropiada, oportuna, actualizada, exacta y accesible. Cada Unidad organizativa, deberá establecer los puntos de control para verificar y asegurarse que estas características se cumplan, de acuerdo a los procesos que desarrollen".

Art. 361: "La máxima autoridad, los directores, gerentes y demás jefaturas, estarán en la obligación de realizar actividades de supervisión de forma periódica e integrada, previo y durante la ejecución de las operaciones, con el propósito de comprobar que los subalternos realicen sus actividades, de conformidad a los lineamientos establecidos y tomar las acciones correctivas que sean aplicables. Las actividades de control realizadas, deberán documentarse".

Guía para Estandarización de Sitios Web de Instituciones de Gobierno.

"C2.3 Certificados digitales

Definición: Es un fichero informático firmado electrónicamente por un prestador de servicios de certificación, considerado por otras entidades como una autoridad para este tipo de contenido, que vincula unos datos de verificación de firma a un firmante. Es el único medio que permite garantizar legalmente la identidad de una persona en Internet. Se trata de un requisito indispensable para que las instituciones puedan ofrecer servicios seguros a través de Internet. (..)".

CAUSA:

Falta de instrumentos administrativos que regulen la gestión de las redes sociales del CONACYT.

EFFECTO:

Realización de actividades no acorde a los objetivos institucionales.



COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,
[REDACTED] comentó:

“En respuesta al Acta de Lectura de Borrador de Informe de “Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022”, se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados”.

COMENTARIOS DE AUDITORÍA INTERNA:

Se verificó el “Plan de Acción 2023”, presentado por la Dirección Ejecutiva, en cual se detallan las “actividades que desvanecen lo observado” con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral quince y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/07/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorias posteriores al presente informe. Por lo tanto, la observación se mantiene.

RECOMENDACIÓN DEL HALLAZGO:

A la Jefa de Protocolo y Relaciones Internacionales del CONACYT:

Implemente las acciones que desvanezcan en el corto plazo, el aspecto de control reportado.



HALLAZGO N° 16: FALTA DE UNA GESTIÓN DOCUMENTAL ELECTRÓNICA

Importancia del Hallazgo : Riesgo Medio
Componente NTCIE impactado : Información y Comunicación

CONDICIÓN:

Se verificó que la Unidad de Gestión documental y Archivo del CONACYT, no ha elaborado conjuntamente con la Unidad de Protocolo y Relaciones Internacionales (Anteriormente RRP y Comunicaciones) y el personal encargado de los Sistemas de Información de CyT los siguientes lineamientos relacionados a:

- a) Organización de los documentos electrónicos, en cual se indique:
 - Lugar de resguardo (carpeta/s) en la computadora;
 - Disco duro o nombre del servidor donde almacena los documentos;
 - Medidas de economía en el resguardo de la información;
 - Duplicidad de documentos o de copias;
 - Denominación de los documentos;
 - Codificación.
- b) Buenas prácticas para reducir el consumo de papel;
- c) Reemplazo de documentos físicos por electrónicos;
- d) Política de seguridad y privacidad de los datos desarrollados en el sitio web del CONACYT;
- e) Automatización de procesos, actualización de procedimientos y simplificación de trámites.

CRITERIOS:

Ley de Procedimientos Administrativos.

Art. 5: "La comparecencia de los ciudadanos en las oficinas públicas solo será obligatoria por disposición legal. En ese sentido, para la presentación de solicitudes, peticiones o cualquier escrito dirigido a la Administración, no será necesaria la comparecencia del interesado. Si la presentación de escritos dirigidos a la Administración se hace a través de un tercero, será necesario legalizar la firma del interesado".



Art. 18: "Los órganos de la Administración Pública podrán utilizar tecnologías de la información y comunicación para realizar trámites, diligencias, notificaciones, citatorios o requerimientos, siempre que dichos medios tecnológicos posibiliten la emisión de una constancia, ofrezcan garantías de autenticidad, confidencialidad, integridad, eficacia, disponibilidad y conservación de la información y sean compatibles con la naturaleza del trámite a realizar.

La Administración Pública deberá implementar los mecanismos tecnológicos y electrónicos que fueren necesarios para optimizar el ejercicio de sus competencias y los derechos de los administrados. Se deberán crear las estrategias de gobierno electrónico que para tales efectos sean necesarias".

Reglamento Normas Técnicas de Control Interno Específicas del Ministerio de Educación (MINED).

Art. 5: "La responsabilidad por el diseño, implantación, evaluación y perfeccionamiento del Sistema de Control Interno, corresponderá a la máxima autoridad del MINED, niveles de Dirección, gerenciales y demás jefaturas en el Área de su competencia institucional".

Art. 360: "Las unidades que posean datos personales, serán responsables de protegerlos y en relación con éstos, deberán:

- a) Adoptar procedimientos adecuados para recibir y responder las solicitudes de indagatoria, actualización, modificación y supresión de datos personales;
- b) Usar datos exclusivamente en el cumplimiento de los fines institucionales para los que fueron solicitados u obtenidos;
- c) Procurar que los datos personales sean exactos y actualizados;
- d) Rectificar o completar los datos personales que fueren inexactos o incompletos; y
- e) Adoptar medidas que protejan la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

No se podrán difundir, distribuir o comercializar los datos personales contenidos en los archivos o sistemas de información administrados por las unidades, salvo que haya mediado el consentimiento expreso y libre, por escrito o por un medio equivalente, de los individuos a que haga referencia la información".

Art. 362: "En todos los niveles de la organización, directores, gerentes y jefes responsables, deberán efectuar un monitoreo constante del ambiente interno y externo, de tal manera que les permita tomar las medidas oportunas sobre los factores y condiciones reales o potenciales que pudieran incidir en el desarrollo de sus funciones institucionales, ejecución de planes y cumplimiento de objetivos y metas".



Art. 365: "Las funciones del Comité Estratégico de Tecnologías de Información, estarán orientadas a: Verificar que exista alineación estratégica y entrega de valor de los proyectos e inversiones en Tecnologías de Información y Comunicación (TIC), promover administración eficiente de recursos tecnológicos, administración de riesgo, medición del desempeño y cumplimiento de la legislación y regulación interna relevante a las Tecnologías de Información y Comunicación (TIC)".

Reglamento para el uso y control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.

Art.5: "La Unidad de TIC deberá proponer a la máxima autoridad la adopción de mejores prácticas (estándares abiertos) y controles para la gestión de las TIC, que se requiera para el logro de los objetivos.

Corresponderá a los demás empleados, realizar las acciones necesarias para garantizar su efectivo cumplimiento".

LINEAMIENTO 5 DE PAUTAS PARA LA GESTIÓN DOCUMENTAL ELECTRÓNICA.

Artículo 4: "Las unidades productoras o generadoras, bajo la coordinación de la UGDA, deberán organizar los documentos ofimáticos con los mismos criterios que los de soporte en papel tomando en cuenta las siguientes medidas:

> Ordenar las carpetas que contienen los documentos ofimáticos de acuerdo al cuadro de clasificación documental, coherentes con el orden de las versiones finales en soporte de papel y ubicarlas en Mis Documentos o en otras ubicaciones de la computadora, discos o servidores establecidos por la autoridad competente para resguardar los documentos propios de la Unidad, procurando la economía en los respaldos de la información, evitando duplicar las copias a resguardar".

Artículo 6: "La UGDA con apoyo de la unidad de informática y las que se estime conveniente, elaborará e implementará proyectos de digitalización de documentos con base en normas internacionales, tomando en cuenta dos aspectos previos:

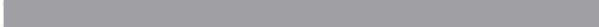
> Determinar los documentos de gestión legalizados que pueden ser digitalizados y enviados por medio del correo electrónico para evitar las copias en papel.

> Digitalizar no sustituye el valor legal del documento, por lo que sólo se digitalizarán documentos para efectos de acceso sin eliminar el soporte original".

Artículo 7: "Los entes obligados deben buscar la creación e implementación de sistemas de gestión de documentos electrónicos siguiendo las normas internacionales, utilizando software libres y pólizas de datos abiertos en la medida que se adopten de manera legal estándares y prácticas que aseguren la fiabilidad, integridad y conservación de la información en este soporte".



COMENTARIO DE LA ADMINISTRACIÓN:

En nota de fecha 12 de septiembre de 2023, suscrita por la Directora Ejecutiva,  comentó:

“En respuesta al Acta de Lectura de Borrador de Informe de “Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022”, se adjunta Plan de Trabajo de Acciones Correctivas, asimismo se presentan algunos documentos de descargo de hallazgos expuestos en el borrador de Informe. En relación al numeral VII se informa que se solicitará al personal responsable de cada uno de los aspectos reportados un plan de acción a corto plazo, con el fin de desvanecer lo observado y fortalecer el control interno de las Tecnologías de la Información y Comunicación del CONACYT. No omito manifestar que, de parte de esta administración, estaremos realizando, el máximo de acciones posibles para subsanar los diferentes hallazgos observados”.

COMENTARIO DE AUDITORÍA INTERNA:

Se verificó el “Plan de Acción 2023”, presentado por la Dirección Ejecutiva, en cual se detallan las “actividades que desvanecen lo observado” con su respectiva fecha de inicio y finalización, por lo anterior se realizó el análisis de la información contenida en dicho plan en su numeral dieciséis y se determina que los comentarios vertidos, establecen acciones correctivas proyectadas en un periodo del 01/07/2023 al 31/12/2023, las cuales se considerarán acciones sujetas a seguimiento en auditorias posteriores al presente informe. Por lo tanto, la observación se mantiene.

RECOMENDACIÓN DEL HALLAZGO:

A la Directora Ejecutiva del CONACYT:

Implemente acciones que desvanezcan en el corto plazo, el aspecto de control reportado, respecto a establecer una adecuada gestión documental electrónica, en función a lo regulado en la normativa aplicable al proceso.



VIII. SEGUIMIENTO A RECOMENDACIONES DE INFORMES DE AUDITORÍAS ANTERIORES

No identificamos Informes de Auditoría para el seguimiento a recomendaciones.

IX. RECOMENDACIONES GENERALES

A la Dirección Ejecutiva del CONACYT:

1. Solicitar al personal responsable de cada uno de los aspectos reportados el cumplimiento oportuno de las acciones presentadas en el "Plan de Trabajo de Acciones Correctivas" presentado por la Dirección Ejecutiva, con el fin de desvanecer lo observado y fortalecer la gestión de las Tecnologías de la Información y Comunicación en la institución.
2. Informar a la presidencia del CONACYT, el plan de acción consolidado y remitir periódicamente el avance de las acciones ejecutadas en cumplimiento al mismo.

X. CONCLUSIÓN DEL EXAMEN

Conforme a los resultados obtenidos, concluimos, que el manejo de los recursos de Tecnologías de Información y Comunicación presenta una alta debilidad en el diseño de la planificación y organización de las TIC, que al ser superada disminuiría las observaciones inherentes al caso y fortalecería el sistema de control interno por lo tanto se deben implementar acciones que garanticen el cumplimiento de la normativa relacionada a los procesos evaluados y el respectivo monitoreo y supervisión.

XI. PÁRRAFO ACLARATORIO

El presente Informe se refiere únicamente a la auditoría por el "Examen Especial a las Tecnologías de la Información y Comunicación del Consejo Nacional de Ciencia y Tecnología (CONACYT), al 31 de diciembre de 2022".

XII. AGRADECIMIENTOS

Hacemos extensivo nuestro agradecimiento al personal del Consejo Nacional de Ciencia y Tecnología, por el apoyo brindado durante la ejecución de nuestra auditoría.



XIII. LUGAR Y FECHA

San Salvador, 03 de noviembre de 2023.

XIV. FIRMA DE LA RESPONSABLE DE LA DIRECCIÓN DE AUDITORÍA INTERNA

DIOS UNIÓN LIBERTAD



[REDACTED]
Directora de Auditoría Interna, MINEDUCYT
direcciondeauditoriainterna@mined.gob.sv

XV. PERSONAL AUDITOR Y/O FUNCIONARIO QUE EJECUTÓ LA AUDITORÍA

- [REDACTED] Directora de Auditoría Interna, MINEDUCYT.
- [REDACTED] Gerente de Auditoría de Gestión, MINEDUCYT.
- [REDACTED] Jefe del Departamento de Auditoría de TIC, MINEDUCYT.
- [REDACTED] Auditora Interna del CONACYT.

Versión Pública

XVI. ANEXOS

ANEXO N° 1: FUNCIONES RELACIONADAS A LAS TIC, DISTRIBUIDAS EN EL PERSONAL DEL CONACYT, NO ACORDES AL OBJETIVO DE LAS UNIDADES A LAS CUALES PERTENECEN JERÁRQUICAMENTE.

Cargo	Funciones relacionadas a las TIC no acorde al objetivo de la Unidad Dependiente Jerárquicamente	Dependencia Funcional/ Objetivo
Gestor de Sistemas de Información de Indicadores de Innovación, Ciencia y Tecnología (ICT) del Observatorio Nacional de Ciencia y Tecnología.	<ul style="list-style-type: none"> Administrar la Plataforma Virtual del Sistema de Información de Vigilancia Científica y Tecnológica del Observatorio de Innovación, Ciencia y Tecnología (ICT) Administrar la plataforma virtual del Registro de Investigadores Científicos de El Salvador Desarrollar otras plataformas virtuales que respondan a Indicadores de ICT. Administrar los servicios de Tecnologías de Información y Comunicación. 	<p><u>Observatorio Nacional de Ciencia y Tecnología</u></p> <p>La finalidad del Observatorio es monitorear, evaluar y difundir conocimiento e información actualizada, sobre la dinámica de la investigación e innovación tecnológica nacional e internacional, políticas, planes, programas y proyectos para impulsar el Desarrollo de la Ciencia y tecnología, a través del Sistema Nacional de Innovación, Ciencia y Tecnología.</p>
Gestor de Indicadores de ICT y Sistemas de Información	<ul style="list-style-type: none"> Administra la red interna del CONACYT y los sistemas de información institucionales (correo, antivirus, sistema informático del activo fijo, entre otros) 	
Oficial de Información	<ul style="list-style-type: none"> Dar soporte Técnico a la red interna de los usuarios del Consejo y dar atención a fallas menores de Hardware y Software. Difundir Información Científica y Tecnológica a través de la Web de CONACYT. Auditar Software del equipo informático de la institución. Colaborar en la administración de la Red. 	<p><u>Oficina de Atención y Respuesta (OAR)</u></p> <p>Promover el acceso y entrega de información pública del N-CONACYT, para todo el ciudadano y ciudadana demande, transparentando así todo el quehacer del N-CONACYT a través de la descripción de las acciones realizadas por las diferentes gerencias y unidades que lo conforman, fortaleciendo así la modernización institucional de acuerdo a LAIP</p>



Versión Pública

Cargo	Funciones relacionadas a las TIC no acorde al objetivo de la Unidad Dependiente Jerárquicamente	Dependencia Funcional/ Objetivo
Gestor de Promoción y Popularización	<ul style="list-style-type: none"> • Administrar y desarrollar el sitio web de Promoción y Popularización de la Ciencia y Tecnología • Administrar la página Web u otros medios de publicación que le sean encomendados por la Gerencia de Promoción y Popularización de la Ciencia y Tecnología • Colaboradora Grafica del sitio web de https://www.conacyt.gob.sv/ https://www.facebook.com/ConacytSV https://twitter.com/CONACYToficial https://www.instagram.com/conacytsv/ https://www.youtube.com/c/CONACYTsvOficial 	<p><u>Gerencia de Promoción y Popularización de la Ciencia y la Tecnología.</u></p> <p>La difusión, promoción y popularización de la Ciencia y Tecnología y las actividades que sean requeridas en el marco de la política de innovación, ciencia y tecnología.</p>
Coordinadora de Recursos Humanos	<ul style="list-style-type: none"> • Brindar asistencia informática al sistema SIRHI • Administrar el SIRHI y el ITR Time Plus. • Manejar sistemas de apoyo, Cerberus y Websoporte 	<p><u>Gerencia Administrativa</u></p> <p>Cumplir con las disposiciones legales y normativas aplicables en los procesos administrativos y mecanismos necesarios para facilitar el cumplimiento de los objetivos institucionales, para velar por el control interno y una sana administración de los recursos institucionales.</p>
Gestor de Becas de Postgrado	<ul style="list-style-type: none"> • Administrar la información sobre oportunidades de formación en ciencia y tecnologías que sea publicada por el CONACYT en las redes sociales, especialmente Facebook y Twitter y dar respuesta a las consultas de las personas interesadas. 	<p><u>Gerencia de Formación y Becas de Posgrado en CYT.</u></p> <p>Coordinar y ejecutar las acciones necesarias para incentivar la formación de profesionales e investigadores altamente calificados en ciencia y tecnología a nivel de postgrados y especialización, así como realizar acciones de formación y difusión de conocimientos en temas que apoyen el desarrollo de la ciencia y la tecnología, la innovación, la investigación y el establecimiento de redes de investigación y cooperación.</p>



**ANEXO N° 2: FALTA DE POLÍTICAS Y PROCEDIMIENTOS DE CONTROLES
GENERALES DE LOS SISTEMAS DE INFORMACIÓN.**

No.	POLÍTICAS Y PROCEDIMIENTOS DE CONTROLES
1	Políticas de seguridad para el acceso y confidencialidad de la información
2	Política de adquisición y asignación del equipo informático
3	Política de software y sistemas de información
4	Política de uso adecuado de recursos de hardware y software
5	Política de Administración de base de datos
6	Política de Control y Acceso a internet
7	Política de acceso y manejo de la Información
8	Política para la asignación y utilización de firmas físicas y/o electrónicas
9	Manual de Procedimientos
10	Manual de Desarrollo y Mantenimiento de Sistemas Informáticos
11	Estándares de Seguridad de Tecnologías de la Información
12	Metodología para la Identificación de los Riesgos Informáticos
13	Lineamientos de Desechos Electrónicos y Eléctricos
14	Programa de ciberseguridad
15	Plan de Infraestructura Tecnológica
16	Plan de Adquisiciones de Infraestructura Tecnológica
17	Plan de Contingencia de las Tecnologías de Información
18	Plan de Mantenimiento de la Infraestructura Tecnológica
19	Plan de respaldo y resguardo en sitio remoto
20	Normas de usos del internet
21	Portafolio de Proyectos de Servicios de Tecnología de Información
22	Portafolio de Proyectos y Servicios
23	Catálogo de Servicios basado en Tecnología de la Información
24	Documento de Arquitectura de Información del CONACYT
25	Portafolio de Sistemas Informáticos



Versión Pública

ANEXO N° 3: DEBILIDADES DEL SISTEMA DE ACTIVO FIJO DEL CONACYT.

Observación	Detalle de lo Observado
a) No se evidencia la documentación de respaldo del desarrollo del sistema informático.	<ul style="list-style-type: none"> • La definición del sistema; • Requerimientos de la unidad técnica solicitante; • Pruebas de aceptación; • Documento de diseño; • Documento de base de datos; • Documento de administración de la configuración; • Manual técnico; • Manual de instalación; • Plan de implementación; • Plan de capacitación.
b) El Manual de Usuario del "Sistema de activo Fijo" del CONACYT, carece de información descriptiva para su análisis y aplicabilidad y no se evidencia la actualización desde su creación en septiembre del año 2019.	<ul style="list-style-type: none"> • Título del Documento; • Fecha de creación; • Control de cambios; • Personal que lo elaboró, revisó y autorizó. • No se visualiza que el documento hubiese sido actualizado, debido que según la información generada en el documento de Word indica el paquete ofimático que la fecha de creación es registrada en fecha 27/09/2012 y fecha de última modificación es de 27/09/2012, con usuario 16:25. • No se describió cada opción del "módulo Estadísticas" en el "Manual de Usuario". • No se describió el funcionamiento de cada una de las opciones del sistema, sino que solamente se muestra el nombre de la opción con la imagen correspondiente, sin una explicación apropiada, orientativa y los criterios relacionados con dicha opción necesarios para que cualquier usuario antiguo o nuevo le sirva de consulta sobre los procesos mecanizados en cada una de las opciones de este sistema.
c) Inadecuado diseño del sistema.	<ul style="list-style-type: none"> • Inadecuado diseño de la interfaz gráfica del usuario, no proporcionando una imagen limpia, bien organizada, intuitiva y no se visualiza una actualización de acuerdo a los parámetros de logos y colores autorizados por la institución; • No se desarrolló opciones visibles para que el usuario pudiese interactuar con el sistema a través de las opciones básicas como "Nuevo", "Modificar", "Eliminar" y "Guardar"; • y en colones sin la equivalencia respectiva en la base de datos.
d) Falta de actualización de los reportes que genera el sistema	<ul style="list-style-type: none"> • Las opciones de reportes no son utilizables ya que no presentan todos los bienes respectivos, poseen logos del MINEC y no del MINEDUCYT y hacen una mezcla de expresión monetaria en colones.

Versión Pública



Observación	Detalle de lo Observado
<p>e) Falta de eficiencia y eficacia del Sistema</p>	<ul style="list-style-type: none"> • Actividades fuera de las opciones del usuario final: Informes de depreciación de bienes de Activo Fijo. <ul style="list-style-type: none"> ○ Actualización de registros de bienes (Asignar precio a bienes en la base de datos). ○ Emitir listados en formato Excel de la siguiente información: <ul style="list-style-type: none"> ➤ Bienes no depreciables. ➤ Bienes depreciables. ➤ Bienes intangibles amortizables. ➤ Bienes intangibles no amortizables ○ Ingresar al sistema personal nuevo y asignarle bienes de activo fijo. ○ Separar el inventario del CONACYT del inventario del proyecto ICSU. ○ Eliminar registros del inventario de Activo Fijo de CONACYT. ○ Informe de bienes inservibles y obsoletos en formato Excel. ○ Asignar código e ingresar a la base de datos los bienes adquiridos. ○ Eliminación de "Responsables de Activo Fijo". ○ Emitir el informe del inventario general de los Activos Fijos. ○ Actualización de registros de bienes fuera de uso. ○ Informes en formato Excel de "Licencias amortizables y no amortizables".
<p>f) Falta de incorporación de la conversión monetaria (colones a dólares) de la base de datos.</p>	<ul style="list-style-type: none"> • Se verificó la existencia de un único campo denominado "Valor" conteniendo cifras expresadas en Colones salvadoreños a pesar de que las facturas únicamente están expresadas en Dólares Americanos.
<p>g) Falta de calidad de la información generada por el sistema.</p>	<ul style="list-style-type: none"> • La información no es útil para la toma de decisiones adecuada, debido a que los reportes generados presentan inconsistencias en el valor de algunos bienes, como resultado de la conversión obligada de dólares de a colones y su transformación posterior de colones a dólares. • La información generada no es exacta y apropiada ya que es necesaria la intervención de otros usuarios de la institución a fin de corregir problemas de aproximación de decimales causados por la doble conversión descrita en el numeral anterior. • No se establecen puntos de control para verificar y asegurarse que se cumplan las características de la información que son desarrolladas en el proceso de "Activo Fijo". • A través del documento fecha el 19 de diciembre de 2022 y con referencia "DE-GA-045-2022", se estableció que la Ingeniera Doris de Alens, "... el problema es que, para calcular



Observación	Detalle de lo Observado
	<p>los valores de depreciación, la base automáticamente aproximadamente trabajo con 8 decimales, y en la impresión del informe se emite con dos decimales, por lo que no se puede corregir". Por lo tanto, se corroboró la imposibilidad de la "Responsable de la Base de datos de activo fijo", de corregir el problema generado en el cálculo de depreciación, lo que provocó el doble trabajo en el área de Contabilidad para corregir las diferencias en los montos de la depreciación de bienes.</p>
<p>h) Falta de depuración y documentación de objetos en la base de datos (Archivos en formato Access)</p> <p>i) Falta de calidad en la información generada en el sistema.</p>	<ul style="list-style-type: none"> • Se identificaron un total de 26 objetos de tipo Tabla en el archivo de Access, sin embargo, se verificó que para el sistema solamente son de utilidad 4 de ellas, los restantes se han identificado como "información sin documentar" ya que pudieron ser pruebas o la creación de subconjuntos de información creados por el informático a cargo sin documentar porque las creó, para qué las utilizó y la razón dejarlas almacenadas creando falta de claridad en el esquema de información. • Consultas. En el archivo de Access se encuentran almacenadas 55 consultas a la base de datos en su mayoría utilizadas por la persona Informática encargada de este sistema. • Formularios. En el archivo de Access se encuentran almacenados 15 formularios, de los cuales se han identificado 3 de ellos que son utilizados en el menú que se le presenta al usuario final. • Informes. Se han identificado 60 objetos de tipo Informes en la base de datos o archivo en formato Access, de los cuales solo 9 forman parte del menú de acceso del usuario final, es decir, que los restantes eran de uso únicamente del informático a cargo del sistema. • Macros. Se identificaron 7 macros almacenadas en Access, de las cuales solo a una de ellas se hace referencia en el menú principal, precisamente para Salir del Sistema. De las demás se carece de información para determinar su utilización.
<p>j) Falta de un esquema de seguridad.</p>	<ul style="list-style-type: none"> • No cuenta con un esquema de seguridad. En la verificación de la documentación de este sistema no se ha encontrado evidencia de un esquema de seguridad que permita la creación de usuarios y contraseñas de tal manera que permita dar los accesos correspondientes a sus diferentes roles de acción dentro del mismo como pueden ser de administrador, operador, consulta, entre otros.
<p>k) Falta de registro de cambios o bitácoras.</p>	<ul style="list-style-type: none"> • Falta de un registro de cambios o bitácora. En la documentación verificada no se ha encontrado evidencia del registro de información de los cambios realizados a la información almacenada.



Observación	Detalle de lo Observado
l) Desarrollo de sistema sin tomar en cuentas las mejores prácticas y controles para la gestión de las Tecnologías de la Información y Comunicación.	<ul style="list-style-type: none"> Desarrollado sin tomar en cuenta las mejores prácticas y controles para la gestión de las TIC. Este sistema con aproximadamente más de 15 años de uso fue desarrollado sin tomar en cuenta las mejores prácticas y controles para la gestión de las TIC. De acuerdo con los manuales verificados, no cuenta con la definición de los requerimientos, documentación de las fases de su desarrollo, utilización de estándares de programación, seguridad, documentación actualizada de diseño, desarrollo, instalación, de usuario, técnica, de instalación, entre otras.
m) Riesgos de corrupción de archivo.	<ul style="list-style-type: none"> Se verificó que existen posibilidades de riesgo de corrupción del archivo en formato de Access que contiene la base de datos y el Sistema de Activo Fijo, ya que puede ser accedido desde diferentes sistemas operativos, teniendo como consecuencia la pérdida parcial o total de la información ahí almacenada.
n) Fallas en los reportes de depreciación y amortización	<ul style="list-style-type: none"> En la verificación y consulta con los usuarios se determinó que existen inconsistencias en el cálculo de los valores generados por este proceso.

