Instituto de Desarrollo Rural

Informe Auditoría de Sistemas de Información
Carta de Gerencia de TI - 2023
Informe Final

INFORME DE AUDITORÍA BASADA EN RIESGOS DE LAS TENOLOGÍAS DE INFORMACIÓN

Contenido

San José, 4 de julio 2024

Señores
Junta Directiva
Presidencia
Departamento de Tecnologías de Información
INSTITUTO DE DESARROLLO RURAL
Presente

Estimados señores:
Según nuestro contrato de servicios, efectuamos la auditoría externa del período 2023 al Instituto de Desarrollo Rural (en adelante INDER o la Institución) y en el examen efectuado, revisamos aspectos referentes al sistema de control interno y procedimientos de Tecnología de Información para la administración de los sistemas de información que soportan la gestión financiera, cuyo resultado sometemos a consideración de ustedes en esta carta de gerencia CG TI-1-2023.

Considerando el carácter de pruebas selectivas en que se basa nuestro examen, ustedes pueden apreciar que se debe confiar en métodos adecuados de comprobación y de control interno. Los resultados indicados en este informe no son puntuales a los diferentes funcionarios de la Institución y por el contrario debe ser considerado como una base para el mejoramiento y fortalecimiento de los procedimientos de control interno y los aspectos relacionados al Área de Tecnologías de la Información.

Agradecemos una vez más la colaboración brindada por los funcionarios y colaboradores del INDER y estamos en la mejor disposición de ampliar o aclarar el informe adjunto en una sesión conjunta de trabajo.

MURILLO Y ASOCIADOS, S.A.
CONTADORES PÚBLICOS AUTORIZADOS

ESTEBAN MURILLO DELGADO (FIRMA)
PERSONA FISICA, CPF-01-0905-0622.
Fecha declarada: 16/07/2024 05:32:40 PM
Esta es una representación gráfica únicamente,
verifique la validez de la firma.

Lic. Esteban Murillo Delgado
Contador Público Autorizado Nº 3736
Póliza de Fidelidad Nº 0116FID000697712
Vence el 30 de setiembre de 2024

"Exento de timbre de Ley número 6663 del Colegio de Contadores Públicos de Costa Rica, por disposición de su artículo número 8".

I. OBJETIVO

Como parte de la evaluación de los estados financieros de la Organización, procedimos a realizar la evaluación de los controles generales de la gestión de Tecnología de Información, con el objetivo de medir el riesgo de la información en lo que respecta a seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica.

La evaluación la realizamos considerando el Marco Regulatorio de Gobierno y Gestión de Tecnologías de Información, emitidas por el MICITT, y en general las mejores prácticas globales para el gobierno y gestión de tecnología de información.

II. ALCANCE

En esta visita el trabajo fue enfocado principalmente a las siguientes áreas:

- Valoración del proceso establecido para cumplir con las disposiciones de la nueva norma técnica emitida por el MICITT respecto al gobierno y gestión de las tecnologías de información con el desarrollo de los Sistemas Contables, su participación y acción a efecto de que los estados financieros se lleven a cabo en forma, oportuna, eficaz y con la seguridad requerida, para la emisión de los Estados Financieros. Además, evaluamos la Unidad de Tecnología de la información, sus funciones, áreas de control, reportes, asistencia técnica, conformación, personal, métodos de trabajo, control interno sobre los equipos en uso y en desuso, recambio de partes y su control.
- Oportunidades de mejora identificadas en la evaluación.
- Seguimiento a los compromisos establecidos en la carta de gerencia anterior.

III. PERÍODO DEL ESTUDIO

El estudio se realizó durante los meses de mayo y julio de 2024 y corresponde con el periodo comprendido entre el 1 de enero y el 31 de diciembre de 2023.

IV. LIMITACIONES DEL ESTUDIO

No hubo.

V. ENFOQUE Y METODOLOGÍA

El enfoque general utilizado para llevar a cabo esta evaluación, se enmarcó dentro los términos establecidos en el Marco Regulatorio de Gobierno y Gestión para las tecnologías de información publicado por el MICITT el 10 de noviembre del 2021.

Para el desarrollo del trabajo de campo, se emplearon una variedad de instrumentos metodológicos, dentro de los que destacan los siguientes:

- Delimitación del marco conceptual, legal, administrativo, organizacional y de ejecución por medio del cual se efectuará la evaluación.
- Identificación y obtención de documentación que resultara relevante para la evaluación.
- Otras técnicas, herramientas o métodos necesarios para mejorar la comprensión o el análisis de la información obtenida, a utilizar según criterio profesional de los consultores asignados a este proyecto.

VI. RESULTADOS

A continuación, se muestran los resultados de los procedimientos previamente indicados:

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
1	Si bien el INDER ha efectuado algunas acciones para iniciar con la implementación de las normas del MICITT, al momento de nuestra revisión pudimos observar que la entidad no ha efectuado un análisis que le permita determinar las brechas que tiene con respecto al cumplimiento del Marco de Gestión de TI del MICITT publicado en el año 2021.	Tomamos como referencia las disposiciones para aplicar las Normas técnicas para la gestión y el control de las Tecnologías de Información que sustituyen las Normas técnicas para la gestión y el control de las Tecnologías de Información (N2-2007-CODFOE) derogadas por la Contraloría General de la República mediante la resolución resolución N° R-DC-17-2020 del diecisiete de marzo del dos mil veinte.	Es conveniente efectuar el análisis indicado para determinar las brechas que tiene el INDER con respecto al marco de gestión de TI del MICITT. Con base en el estudio anterior, definir planes de acción (hoja de ruta) para implementar dicha normativa según lo establecido por el MICITT.	Mediante oficio NDER-GG-TI-022-2022, la Unida de TI eleva a la Gerencia General la solicitud para que la institución proceda con la *"**declaración, aprobación y divulgación"***, establecida por la Contraloría General de la República en el Transitorio I de la resolución R-CO-26-2007, para la implementación de dicho marco de gestión, previo a iniciar las acciones que correspondan.
2	Como parte de nuestros procedimientos de revisión, logramos observar que el INDER no ha establecido controles que le permitan asegurar que las recomendaciones de las cartas de Gerencia enviadas por la auditoría externa de	Utilizamos como referencia lo indicado en la sección de Aseguramiento del Marco de Gestión de TI del MICITT:	Es conveniente que la Institución establezca en sus lineamientos de control interno las normas y las responsabilidades necesarias	Se le comunicará al área de Control Interno de la Dirección de la Secretaría Técnica de Desarrollo Rural (SETER) lo

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
	TI son atendidas y se les brinda seguimiento para su corrección. Como ejemplo de lo anterior, el área de TI no nos pudo proporcionar un reporte con el estado de implementación de las recomendaciones de los informes de las auditorías externas de años anteriores.	*"La institución debe disponer de prácticas formales que permitan la valoración de la disponibilidad y adecuada aplicación de un sistema de control interno para el uso eficiente de los recursos tecnológicos de la institución para lograr mantener la continuidad de las operaciones, salvaguarda y protección de la información y los activos asociados a su captura, procesamiento, consulta, almacenamiento y transferencia y la gestión apropiada de los riesgos asociados. Adicionalmente, debe asegurar que las unidades institucionales disponen y aplican prácticas e instrumentos que le permitan evaluar la adecuada gestión de los procesos y servicios a través de métricas de rendimiento y metas para generar valor a la institución y apoyar en el logro de los objetivos y metas institucionales.* *La institución debe estar comprometida en la aplicación de*	para asegurar que las brechas detectadas por entes de control sean atendidas por las áreas responsables en plazos razonables en concordancia con el riesgo relacionado.	recomendado, por cuanto es un aspecto a implementar a nivel institucional y no únicamente TI.

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		buenas prácticas y seguimiento en la gestión de las TI estableciendo criterios efectivos para el cumplimiento de regulaciones internas y externas, así como disposiciones contractuales. *La Unidad de TI debe incorporar prácticas de valoración para el aseguramiento sobre la entrega de servicios y el uso óptimo de los recursos tecnológicos instalados para apoyar a la institución en la continuidad de sus operaciones, salvaguarda y protección de la información y activos asociados y la implementación de iniciativas para el logro de los objetivos institucionales.* *La institución debe disponer de informes de resultados sobre las diferentes valoraciones que le permitan identificar desviaciones y áreas de mejora sobre la gestión de TI en la entrega de servicios, la disponibilidad y protección de los recursos tecnológicos. La Unidad*		

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		de TI debe establecer acciones para el mejoramiento continuo con base en los resultados de las evaluaciones que se deben incorporar a sus planes de trabajo. La Unidad de TI debe informar formalmente al órgano rector sobre tecnolog.as de informaci.n sobre los resultados de su gesti.n de acuerdo con los planes establecidos, identificando el nivel de alineación y entrega de valor y beneficios según lo definido para el logro de los objetivos institucionales."		
3	Al momento de nuestra revisión y con base en los requerimientos solicitados observamos que el INDER no cuenta con controles que le permitan actualizar la documentación relacionada con los procesos que dan soporte a las plataformas tecnológicas de la entidad. Como ejemplo de lo anterior, observamos procesos de TI con más de 6 años sin revisión y actualización. Algunos de estos procesos son los siguientes:	Usamos de referencia la sección de Gestión de TI según el Marco de Gestión del MICITT: "*La institución debe implementar y mantener prácticas de gestión de las TI, que defina formalmente los siguientes componentes para la entrega de servicios al nivel de tecnologías de información en alineación con el marco*	Es necesario implementar los controles necesarios para que se efectúen revisiones periódicas de los procesos para mantenerlos vigentes y actualizados, además de que los mismos queden debidamente documentados como parte de los procesos de mejora continua.	Se procederá con el cumplimiento, una vez que se haya adoptado, por parte del INDER, el nuevo Marco de Gestión de TI establecido por el MICITT y los documentos se ajusten a las pautas establecidas en dicho marco.

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
	• Cumplimiento regulatorio, actualizado por última vez en 2019. • Marco de Control Interno de TI, actualizado por última vez en 2019. • Administración y liberación de cambios, actualizado por última vez en 2017. • Gestión de la calidad, actualizado por última vez en 2017. • Metodología de desarrollo, actualizado por última vez en 2017. • Plan de Continuidad de TI, actualizado por última vez en 2017.	*estratégico y el modelo de arquitectura empresarial:* *Procesos de TI, establecidos formalmente para el adecuado aseguramiento de entrega de servicios y soporte a la institución"*		
4	Al momento de nuestra revisión, luego de efectuar nuestras pruebas, identificamos que el INDER no ha establecido un rol independiente que tenga las responsabilidades de Seguridad de la Información y Ciberseguridad, de manera que pueda ejercer actividades de control a las operaciones de TI, así como asegurar la vigencia y el cumplimiento de la política de seguridad de la información en la organización. Como consecuencia de lo anterior, identificamos lo siguiente:	Tomamos como referencia los aspectos indicados en el apartado de Seguridad y ciberseguridad de las Normas técnicas para la gestión y el control de las Tecnologías de Información del MICITT: "*La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita*	Es conveniente que el INDER establezca el rol y las responsabilidades de la función de seguridad de la información y ciberseguridad de la organización. También debe establecer controles para asegurar que se otorguen accesos administrativos a las	Se nombró a la compañera Rosa Fernández Zumbado como Oficial de Seguridad de TI. Se procederá con la elaboración planes de acción para el cumplimiento de lo recomendado en los aspectos operativos y

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
	• Al momento de nuestra revisión observamos nombres de usuario cuyos dueños ya no laboraban para la organización o bien que ya no eran requeridos dentro de los sistemas analizados. Como ejemplo de lo anterior observamos 2 usuarios administradores (Pablo H y R E) que no requerían dichos accesos en la consola del sistema de antivirus (Trellix). Cabe mencionar que dichos usuarios fueron eliminados durante la visita de esta auditoría. También, observamos al menos 14 nombres de usuario genéricos (por ejemplo: ADMIN_DB, adminepo, ADministrator, admservers, entre otros) que tenían permisos de administración en el Directorio Activo de la entidad; lo anterior, sin que el INDER nos pudiera proporcionar una justificación técnica razonable para mantener dichos usuarios con esos permisos. Cabe mencionar que el grupo de administración del dominio tenía al menos 22 usuarios registrados, situación que aumenta el riesgo de	*establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.* *La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.*	diferentes plataformas de la entidad considerando el menor privilegio posible. Además, deben implementar controles que les permitan asegurar que los accesos se desactiven oportunamente ante la salida de un funcionario o proveedor. Es importante que se establezca monitoreo de las actividades clave de los usuarios administradores. Es relevante establecer controles para asegurar la detección y atención oportuna de las vulnerabilidades en los dispositivos de TI de la entidad. La entidad debe establecer procedimientos formales y las actividades pertinentes	administrativos indicados.

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
	cambios no autorizados, a la vez que contraviene las buenas prácticas de otorgar el menor privilegio posible. • Como complemento a lo anterior, evidenciamos que algunas de las claves de los usuarios genéricos en el Directorio Activo mencionados anteriormente, no están siendo administradas de forma segura, ya que son del conocimiento de un funcionario en algunos casos, mientras que en otros no se cuenta con la clave del todo. • También, observamos que no se han implementado procedimientos de monitoreo que le permitan a la entidad detectar situaciones de riesgo que se efectúen con los usuarios administradores previamente mencionados, tanto en el Directorio Activo como en las herramientas de control indicadas (Trellix para antivirus y Palo Alto para los firewalls). Dicha situación se agrava en la medida que los usuarios administradores pueden eliminar las bitácoras del Directorio Activo. Es importante mencionar que la entidad cuenta con proveedores que	*La Institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución.* *Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.* *La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir*	que le permitan asegurar que los controles de seguridad cibernética están funcionando en todos los dispositivos de la entidad. Ante migraciones o cambios, debe asegurar que todos los dispositivos mantengan la protección necesaria para mitigar los riesgos asociados.	

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
	tienen la posibilidad de ingresar con permisos de administración a las herramientas de seguridad (Trellix y Palo Alto). • Adicionalmente, observamos que el INDER no está efectuando un proceso formal de detección, análisis y corrección de vulnerabilidades, de manera que pueda disminuir el riesgo de explotación de estas. • También, como parte de la revisión evidenciamos que el INDER no cuenta con controles que le permitan conocer si la totalidad de los dispositivos conectados a la red cuentan con antivirus instalado y actualizado. Lo anterior en la medida que la entidad no nos pudo proporcionar el estado de actualización del antivirus de uno de los servidores del Directorio Activo (IP 172.1.1.16). Como complemento de lo anterior, tampoco nos pudieron proporcionar un plan actualizado de migración de los servidores y computadores de usuario final a la nueva herramienta de antivirus.	*transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.* *La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales."*		

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
5	Al realizar nuestros procedimientos de auditoría, evidenciamos que si bien el INDER cuenta con alguna documentación relacionada con la gestión de riesgos de TI, no nos pudo proporcionar evidencia de un listado actualizado de los riesgos y controles más relevantes definidos por TI para sus procesos y la tecnología asociada que reflejen los riesgos emergentes de la actualidad (por ejemplo: computación en la nube, phishing, ransomware, ingeniería social, ciberataques, entre otros).	Al respecto consideramos los lineamientos de Gestión de riesgos tecnológicos según las Normas técnicas para la gestión y el control de las Tecnologías de Información del MICITT: "*La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el Marco de Gestión de TI que le resulte aplicable.* *La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios,*	Es necesario que la entidad cumpla con las normas políticas y procedimientos de la gestión de riesgos de TI que ha establecido y que documente y le brinde tratamiento a los riesgos emergentes de TI a los que está expuesta.	Se cuenta con una persona responsable de la gestión de riesgos de TI, quien procederá con la elaboración de un plan de acción para el cumplimiento de lo recomendado.

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución."		
6	Al finalizar nuestros procedimientos de revisión, logramos identificar que el Plan Estratégico de TI (PETI) del INDER no se encuentra alineado con el plan estratégico de la entidad. Lo anterior en la medida que el PETI proporcionado fue elaborado previo al nuevo plan estratégico del INDER.	Para poder evaluar lo anterior consideramos la sección de Planificación Tecnológica Institucional de las Normas técnicas para la gestión y el control de las Tecnologías de Información del MICITT: "*La Institución debe instaurar un modelo estraégico formal que permita establecer la dirección organizacional, iniciativas a corto, mediano y largo plazo, incorporando las necesidades y oportunidades tecnológicas que permita establecer los requerimientos al nivel tecnológico para la sostenibilidad de las operaciones institucionales, as.*	Es importante establecer los controles necesarios para la revisión periódica del PETI y que el mismo logre alinearse a los objetivos institucionales de manera que se pueda garantizar la continuidad del negocio.	Se encuentra en proceso de contratación la solicitud de compra en SICOP #0062024004900010 para la *Elaboración del Plan Estratégico de Tecnologías de la Información (PETI) del Inder*, el cual cuenta con el presupuesto requerido a fin de ser ejecutada en el 2024. Este trámite se lleva a cabo una vez que la Secretaría Técnica de Desarrollo Rural (SETER) publicara en el 2023 el nuevo (Plan

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		como cambio y mejora a los recursos tecnológicos instalados y las oportunidades de crecimiento y entrega de valor público. *Adicionalmente, que incorpore indicadores que permitan valorar el nivel de cumplimiento de los objetivos estratégicos, las acciones de revisión y ajuste a la estrategia."*		Estratégico Institucional) PEI institucional 2023-2030, precisamente para que el nuevo PETI se encuentre alineado a los objetivos y necesidades estratégicas institucionales.
7	Al efectuar nuestra revisión, si bien observamos que el INDER cuenta con documentación relacionada con la Continuidad de TI, no nos pudo proporcionar evidencia actualizada que permita determinar que se están efectuando pruebas de forma periódica para asegurar que el plan de recuperación de desastres se mantiene vigente y cumple con los objetivos de continuidad establecidos por la entidad.	Al respecto usamos como referencia lo relativo a la Continuidad y Disponibilidad Operativa de los servicios según las Normas técnicas para la gestión y el control de las Tecnologías de Información del MICITT: "*La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia*	Es necesario que la institución establezca y documente las normas relacionadas con las pruebas del plan de recuperación de desastres y su frecuencia. Además, debe efectuar dichas pruebas dejando evidencia de los resultados, así como de los planes de remediación en caso de encontrar brechas.	Se encuentra conformado un equipo de trabajo que está en proceso de revisión y actualización del Plan de Continuidad de TI. En este momento se está realizando el Análisis de Impacto del Negocio (BIA, por sus siglas en inglés) para proceder con las demás tareas establecidas en el

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas. *La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.* *La Unidad de TI debe definir acciones formales que permitan brindar una garantía razonable*		procedimiento de actualización del Plan de Continuidad de TI.

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		sobre la continuidad de los servicios tecnológicos internos y los administrados por terceros, procesos ante situaciones de contingencia y restablecimiento de los recursos tecnológicos, ante una interrupción; manteniendo adicionalmente acuerdos de servicio con los proveedores de bienes y servicios que le permitan solventar situaciones de interrupción."		
8	Si bien el INDER cuenta con un contrato de servicios con el proveedor del SIFAT (RACSA), al momento de nuestra revisión no obtuvimos evidencia acerca de los procedimientos de control que le permiten al INDER verificar que dicho contrato se está cumpliendo según lo solicitado en lo relativo a los aspectos de seguridad de la información. Además, no pudimos determinar que el INDER haya efectuado una revisión independiente de forma recurrente al proveedor del SIFAT (RACSA), con el propósito de asegurar que tenga implementados políticas y procedimientos de seguridad de la información	Tomamos como referencia los aspectos indicados en el apartado de Seguridad y ciberseguridad de las Normas técnicas para la gestión y el control de las Tecnologías de Información del MICITT: "*La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad*	Es conveniente establecer los controles que el proveedor debe cumplir tomando como referencia buenas prácticas de la industria (por ejemplo: ISO 27001, CCM del CSA, NIST u otro que el INDER considere aplicable). Una vez definidos dichos controles y establecidos contractualmente, efectuar un seguimiento al cumplimiento de los	Se coordinará con el Director Administrativo-Financiero, quien es el Administrador del Contrato con la empresa RACSA, para el cumplimiento de lo recomendado.

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
	para administrar la infraestructura tecnológica del sistema. Tampoco, el INDER pudo generar evidencia que el proveedor del SIFAT (RACSA) efectúe auditorías de terceros que certifiquen que las políticas y procedimientos para administrar la infraestructura tecnológica de dicho sistema son seguros.	*debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.* *La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.* *La Institución debe propiciar un ambiente seguro, considerando la*	requerimientos de seguridad por parte del proveedor (RACSA).	

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución. *Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.* *La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e*		

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información. *La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales."*		
9	Como resultado de nuestras pruebas logramos identificar que el INDER no cuenta con normas políticas y procedimientos para la administración general de las bitácoras de los	Para elaborar nuestras pruebas consideramos lo establecido en las normas de Seguridad y ciberseguridad emitidas como normativa por el MICITT:	Es conveniente establecer y documentar las normas políticas y procedimientos de la gestión de bitácoras y su monitoreo en la Entidad.	Se coordinará con el Director Administrativo-Financiero, quien es el Administrador del Contrato con la empresa

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
	sistemas, de manera que puedan efectuar actividades de monitoreo de estas. Como ejemplo de lo anterior, el INDER no nos pudo proporcionar bitácoras de la gestión de los accesos en el SIFAT. Tampoco nos pudo proporcionar evidencia que está efectuando respaldos de las bitácoras del Directorio Activo, así como un monitoreo de las situaciones de mayor riesgo en dicha plataforma.	"*La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.* *La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como*		RACSA, para el cumplimiento de lo recomendado en cuanto al SIFAT. Respecto a los sistemas administrados por TI, se elaborarán planes de acción para el cumplimiento de lo indicado.

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información. *La Institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución.* *Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.*		

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información. *La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o involucramiento de los usuarios finales, dueños de*		

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		procesos y responsables de los diferentes procesos y servicios institucionales."		
10	Luego de revisar el proceso de gestión de accesos en el sistema SIFAT, observamos que el INDER no ha definido controles que le permitan asegurar que los accesos que tienen los funcionarios al sistema son los requeridos para el desempeño de sus funciones y que a la vez cumplen con el principio del menor privilegio posible. En relación con lo anterior evidenciamos lo siguiente: • El INDER no ha definido cuáles son los permisos sensibles o que podrían tener conflicto entre sí, de manera que se puedan detectar situaciones de riesgo desde antes de otorgar los permisos. • Tampoco, ha establecido controles periódicos de certificación de accesos que le permita a las áreas de negocio revisar y confirmar que los accesos están otorgados según las normas establecidas y con el menor riesgo posible. Como ejemplo de lo anterior, para el periodo en evaluación (año 2023) el INDER no pudo entregarnos	Para poder evaluar lo anterior consideramos la sección de Seguridad y ciberseguridad de las Normas técnicas para la gestión y el control de las Tecnologías de Información del MICITT: "*La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.*	Es conveniente establecer y documentar las normas políticas y procedimientos que le permitan asegurar que los accesos que tienen los funcionarios al sistema SIFAT, son los requeridos para el desempeño de sus funciones y cumplen con el principio del menor privilegio. Además, es necesario efectuar una revisión de la estructura de roles y permisos en el sistema de manera que puedan identificar permisos en conflicto, permisos sensibles y asegurar que dichas situaciones de riesgo no se presenten o cuenten con los controles adecuados.	Se coordinará con el Director Administrativo-Financiero, quien es el Administrador del Contrato con la empresa RACSA, para el cumplimiento de lo recomendado en cuanto al SIFAT.

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
	evidencia que la revisión de accesos fue efectuada por áreas que usan el SIFAT.	*La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.* *La Institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución.* *Los procesos institucionales deben considerar los requerimientos de*	Es conveniente efectuar certificaciones de los accesos de forma periódica.	

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución. *La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.*		

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
		La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales."		
11	Luego de efectuar nuestras pruebas, evidenciamos que el INDER no ha establecido controles que le permitan efectuar la renovación tecnológica de los sistemas de forma oportuna. Como consecuencia de lo anterior, observamos que el INDER tenía en su infraestructura sistemas operativos cuyo soporte por parte del proveedor ya había vencido. Como ejemplo de lo anterior identificamos servidores con Windows Server 2012 y Windows Server 2008, cuyo soporte finalizó desde octubre de 2023 y enero de 2020, respectivamente.	La sección de Planificación Tecnológica Institucional del Marco de Gestión del MICITT indica lo siguiente: "*La Unidad de TI debe disponer de un plan de infraestructura e inversiones que permita proyectar los requerimientos de licenciamiento, mantenimiento de infraestructura tecnológica (preventiva, por obsolescencia, mejora), adquisición de nuevos recursos tecnológicos, basados en*	Es conveniente que la entidad establezca los controles necesarios para que la actualización de las versiones y de los parches de todos los sistemas se efectúe de forma oportuna.	Se elaborarán planes de acción para el cumplimiento de lo recomendado.

No.	Situación observada	Criterio	Recomendación	Comentario de la administración
	Además, como complemento de lo anterior evidenciamos que el INDER no cuenta con controles que le permitan actualizar oportunamente los computadores de usuario final y los servidores de la entidad con los parches de seguridad emitidos por el fabricante. Al respecto, identificamos que más de 8952 actualizaciones de seguridad y 1517 actualizaciones críticas, estaban pendientes de ser aplicadas en la entidad. Tampoco el INDER nos pudo proporcionar un plan de trabajo que permita conocer los plazos que le tomará a la entidad efectuar la actualización correspondiente.	*la línea estratégica institucional establecida"*		

VII. SEGUIMIENTO A CARTA DE GERENCIAS ANTERIORES

No.	Condición	Recomendación del 2021	Estado
1	Gestión de TI	**11.1.** Dar seguimiento periódico a los SLAs definidos para validar el cumplimiento de los acuerdos tomados. En caso de incumplimientos, realizar las respectivas acciones para brindar los servicios de acuerdo con las necesidades y acuerdos con las áreas usuarias. **11.2.** Comunicar a la administración y a los interesados del acuerdo de nivel de servicio, los resultados de la revisión y el análisis de indicadores respectivo. **Responsables:** Unidad de TI / Responsables Unidades de Gestión Institucional	Atendido
2	Gestión de TI	**12.1.** Mejorar la herramienta utilizada para la gestión de incidentes de modo que lleve un control y haga mediciones de acuerdo con las métricas definidas en el procedimiento. **12.2.** Generar mediciones periódicas como parte del proceso de calidad de forma que se informe si existen desviaciones en la gestión de incidentes realizada o si se requieren ajustes para mejorar su gestión. **Responsables:** Unidad de TI	Pendiente
3	Planificación tecnológica	**09.1** Dar seguimiento a los planes de TI de acuerdo con los lineamientos establecidos para estas actividades. Dicho seguimiento debe quedar documentado con el objetivo de dar trazabilidad de la actividad. **09.2** Presentar el seguimiento documentado ante el Comité de TI, para dar a conocer los cambios en la estrategia de la Dirección de TI, ajustar las posibles desviaciones del plan y dar a conocer el avance de su ejecución a los miembros de dicho comité. **09.3** Alinear los proyectos del plan anual operativo de TI y el plan estratégico de TI de modo que se pueda hacer una vinculación directa entre lo que se ejecuta con la estrategia de TI. De este modo, se puede verificar que el PAO se encuentra en función de lo planificado estratégicamente por TI. **Responsables:** Planificación Institucional / Unidad de TI	Pendiente

No.	Condición	Recomendación del 2021	Estado
4	Gestión de riesgos de TI	***2021.02*** Realizar un análisis exhaustivo del proceso de gestión de riesgos al nivel de TI, de forma tal que se logre homologar las prácticas aplicables (en la medida de lo posible contar con solo una línea de gestión) **Responsables:** Responsables gestión de riesgo institucional / Unidad de TI	Pendiente
5	Arquitectura empresarial	**06.1** Documentar y detallar el modelo de arquitectura de información considerando los siguientes aspectos: Modelos de proceso de negocio: relacionado a identificar la misión, visión, valores y objetivos de la organización. Así como la visión de la arquitectura empresarial y la gestión de los interesados. Modelo de datos: relacionado a la gestión de la información y procesos. Así como la comprobación del ciclo de vida de la información y las trasformaciones recibidas de los datos durante su recepción y procesamiento. Modelo de aplicaciones: relacionado a la gestión de aplicaciones corporativas y externas, desarrollo de aplicaciones y sistemas. Así como la debida gestión de la funcionalidad de cada aplicación encontrada en la organización. Modelo de tecnología: relacionado a la gestión de la tecnología y sistemas de información. Así como la visualización y diagramación de procesos tecnológicos plasmados en la infraestructura, servicios externos o facilitadores del negocio. **06.2** Revisar el modelo de arquitectura de información periódicamente para garantizar que el mismo se mantenga actualizado de acuerdo con los cambios presentados en el Unidad de TI, la información y los procesos de negocio. **Responsables:** Gerencia General / Unidad de TI **06.3** Efectuar las gestiones para que el modelo de arquitectura cuente con la aprobación formal de la administración y sea comunicado a los interesados. **06.4** Valorar el uso de marcos de referencia como guía para crear un modelo de arquitectura de información robusto.	Cumple parcialmente El modelo no ha sido revisado desde el 2018 acorde con la evidencia aportada. Una vez revisado y actualizado se deben actualizar los demás documentos en consecuencia.

No.	Condición	Recomendación del 2021	Estado
6	Calidad de los procesos tecnológicos	**2021.01** Aprovechando el proceso de adopción del Marco Regulatorio de Gobierno y Gestión de las TI recientemente emitido por MICITT, incorporar el proceso de revisión, adecuación real a los procesos que se realizan al nivel de TI y actualización de la documentación pertinente. Para esto debe montarse un plan formal que como se establecen en las disposiciones de la Contraloría General de la República, debe estar formalmente aplicado máximo en diciembre 2023. Este desarrollo debe convertirse en componente estratégico institucional, ya que el debido cumplimiento normativo no es de competencia exclusiva de la Unidad de TI, sino más bien de toda la institución, para lo cual debe conformarse un equipo multidisciplinario para analizar y establecer las vías de cumplimiento de las directrices establecidas en el marco regulatorio **Responsable:** Gerencia General / Unidad de TI	Pendiente
7	Calidad de los procesos tecnológicos	**2021.01** Aprovechando el proceso de adopción del Marco Regulatorio de Gobierno y Gestión de las TI recientemente emitido por MICITT, incorporar el proceso de revisión, adecuación real a los procesos que se realizan al nivel de TI y actualización de la documentación pertinente. Para esto debe montarse un plan formal que como se establecen en las disposiciones de la Contraloría General de la República, debe estar formalmente aplicado máximo en diciembre 2023. Este desarrollo debe convertirse en componente estratégico institucional, ya que el debido cumplimiento normativo no es de competencia exclusiva de la Unidad de TI, sino más bien de toda la institución, para lo cual debe conformarse un equipo multidisciplinario para analizar y establecer las vías de cumplimiento de las directrices establecidas en el marco regulatorio **Responsable:** Gerencia General / Unidad de TI	Pendiente
8	Calidad de los procesos tecnológicos	**02.1** Ejecutar evaluaciones de calidad periódicas a los servicios de TI en función de lo establecido en el proceso de gestión de la calidad para determinar las mejoras que requieren dichos servicios	Pendiente

No.	Condición	Recomendación del 2021	Estado
		02.2 Presentar a la administración los informes y mejoras planteadas según los resultados obtenidos producto de las mediciones realizadas, de modo que se dé aprobación y se analicen los planes de mejora presentados **Responsables:** Unidad de TI	
9	Calidad de los procesos tecnológicos	**Recomendación:** Realizar el análisis y actualización del Marco de Gestión a la realidad actual de la Unidad. En primera instancia, por el tipo de servicio que se brinda, se puede visualizar como una unidad de Soporte, así los procesos pueden orientarse y actualizarse específicamente al aseguramiento de la mantenibilidad de la operativa institucional que se apoya con tecnologías, tal y como se ha venido realizando. **Responsable:** Gerencia General / Unidad de TI	Pendiente
10	Seguridad de la información y ciberseguridad	**08.1** Dar seguimiento de manera periódica al cumplimiento de la política de seguridad de la información de modo que se pueda identificar las brechas y/o aspectos más vulnerables en la organización. Se debe documentar los resultados para mantener una trazabilidad en la revisión de la política. **08.2** Divulgar la política y capacitar al personal de la institución para que estos conozcan y entiendan los lineamientos establecidos y la importancia de cumplir con estos. Dichas capacitaciones deben ser sobre la política de seguridad de la información implementada. **Responsables:** Unidad de TI / Gerencia General	Pendiente
11	Administración de la infraestructura	**05.1** Elaborar un catálogo de software el cual contenga la lista de programas que son permitidos a nivel de la institución, evaluando que software no representa un problema de seguridad de la información o legal a nivel institucional. **05.2** Implementar un control del software instalado en cada uno de los equipos de la institución, con el fin de tener una mejor gestión del software y verificar que cada uno sea permitido por la institución y que cuente con la respectiva licencia.	Cumple parcialmente Según la evidencia aún está pendiente la verificación periódica del

No.	Condición	Recomendación del 2021	Estado
		05.3 Verificar periódicamente el software instalado con el fin de identificar el software instalado que no es permitido. Si se detectan casos durante la verificación, se debe ejecutar una medida de mantenimiento para desinstalar el software identificado. **Responsables:** Unidad de TI	software instalado.
12	Administración de la infraestructura	**07.1** Generar un modelo de monitoreo como parte de un procedimiento para la gestión de la capacidad y disponibilidad de la plataforma tecnológica **Responsables:** Unidad de TI **Observación:** Esta práctica es parte del modelo de administración y operaciones de la infraestructura tecnológica que debe aplicarse de manera formal, asignada a los responsables de la administración de estos recursos. Adicionalmente, debe coordinarse con los proveedores externos de servicios para que brinden los reportes requeridos en los recursos que le competen. **Estado cumplimiento:** Pendiente	Pendiente
13	Continuidad de los servicios tecnológicos	**03.1** Definir un plan pruebas para el plan de contingencias y continuidad de tecnologías de información, el cual sea ejecutado al menos una vez al año. Producto de los resultados de las pruebas se debe actualizar el plan de continuidad de TI. **03.2** Capacitar periódicamente, al menos una vez al año, a los funcionarios de la organización (involucrados en el proceso de continuidad de TI) para que conozcan sus respectivos roles en la ejecución del plan de contingencias y continuidad. **Responsables:** Unidad de TI / Gerencia General	Pendiente
14	Aseguramiento	**2021.04** Establecer modelos prácticos y formales que permitan a las unidades de gestión institucional y en el caso que nos refiere a la Unidad de TI, realizar autoevaluaciones periódicas sobre su gestión, identificando áreas de mejora y estableciendo planes de acción. Estas prácticas deben asociarse con el proceso de gestión de calidad institucional (según VI. Calidad de los procesos tecnológicos del Marco de gobierno y gestión de las TI del MICITT). Su adecuada aplicación se utiliza	Pendiente

No.	Condición	Recomendación del 2021	Estado
		como insumo en la rendición de cuentas sobre la gestión, así como la identificación de oportunidades y acciones para la mejora continua de la ejecutoria operativa y la entrega de servicios esperada por la Unidad. Es recomendable que esta valoración sea realizada en forma oportuna previo al establecimiento del plan anual operativo, de forma tal que las acciones de mejora sean incorporadas en este, **Responsables:** Gerencia General / Auditoría Interna / Unidad de TI	