ANDE

ADMINISTRACIÓN NACIONAL DE ELECTRICIDAD

DIRECCIÓN DE PLANIFICACIÓN Y ESTUDIOS (DP)

DIVISIÓN DE ORGANIZACIÓN, SISTEMAS Y PROCESOS (DP/DO)

DEPARTAMENTO DE DESARROLLO DE POLÍTICAS Y SISTEMAS DE GESTIÓN (DP/DPS)

IDENTIFICACIÓN DE RIESGOS
PROCESOS y SUBPROCESOS

DIRECCIÓN DE TELEMÁTICA (DTE)

AÑO 2023

ANDE

mecip 2015 | Norma de Requisitos Mínimos para Sistemas de Control Interno

MODELO ESTÁNDAR DE CONTROL INTERNO
IDENTIFICACIÓN DE RIESGOS / SUBPROCESOS
DIRECCIÓN DE TELEMÁTICA
MACROPROCESO: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

COMPONENTE: CONTROL DE LA PLANIFICACIÓN
PRINCIPIO: IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS
FORMATO: Identificación de Riesgos - Subprocesos
Nº: 69

Actualización: 00
Fecha: 4/12/2023

(1) PROCESO	(2) SUBPROCESO	(3) OBJETIVO	(4) RIESGOS	(5) DESCRIPCIÓN	(6) AGENTE GENERADOR	(7) CAUSAS	(8) EFECTOS	UNIDADES INVOLUCRADAS
PLANIFICACIÓN Y ORGANIZACIÓN DE TIC	GESTIÓN ESTRATÉGICA DE TIC	Definir los servicios estratégicos y la metodología de gestión de cada uno de ellos, siguiendo las recomendaciones y standares internacionales.	Error en la Gestión Estratégica	Probabilidad de que errores en la recopilación, interpretación o comunicación de la información estratégica de TIC obstaculicen la alineación de los servicios tecnológicos con las metas institucionales, lo que puede resultar en implementaciones ineficientes y desviaciones de los objetivos estratégicos.	Personas: Individuos o equipos responsables de la estrategia TIC	Falta de formación adecuada en prácticas de gestión de TIC, uso de sistemas de información estratégica desactualizados o inadecuados, y procesos de comunicación interna deficientes que conducen a una mala interpretación de los datos estratégicos.	Retrasos significativos en la entrega de proyectos de TIC, desalineación de los esfuerzos tecnológicos con las necesidades institucionales, recursos desperdiciados en iniciativas no estratégicas	DTE/DTI, DTE/ISC, DTE/DIC
	ESTRATEGIA Y ARQUITECTURA DE TECNOLOGÍA INFORMÁTICA	Definir la arquitectura de la infraestructura tecnológica de la empresa y la estrategia para su mantenimiento, siguiendo las recomendaciones y standares internacionales.	Incumplimiento de Estrategias	No cumplir con los objetivos de establecer y mantener una arquitectura de TIC adecuada y alineada con la estrategia de la organización, lo que puede resultar en incompatibilidades sistémicas, redundancias y dificultades en la integración de nuevas tecnologías.	Personas: Jefes, Proyectistas y Proveedores de servicios	Asignación inadecuada de responsabilidades, carencia de conocimientos especializados, falta de seguimiento y control, y la ausencia de un marco de trabajo claro para la implementación de la arquitectura de TIC.	Desviación de los planes de TIC, interrupciones en la continuidad del servicio, aumento en los costos por retrabajos, y una posible pérdida de eficiencia operativa y de la capacidad de respuesta ante las demandas del mercado o cambios tecnológicos.	DTE/DTI, DTE/ISC, DTE/DIC
	GESTIÓN DE ACUERDOS DE SERVICIO	Gestionar y mantener los acuerdos que sean necesarios para disponibilizar los servicios, cuidando los recursos y la integridad de la Institución.	Irregularidades en Acuerdos de Servicios	Irregularidades en la gestión de los acuerdos de servicio debido a actos intencionales o negligencias que alteren los términos, condiciones o la calidad esperada del servicio TIC, afectando negativamente la operatividad y los estándares de servicio acordados.	Personas: administradores de contratos, proveedores de servicios y supervisores de cumplimiento	Fallas en el proveedor de la información	Demoras en la entrega de servicios, infracciones de los niveles de servicio acordados, disputas contractuales, y potencialmente, repercusiones financieras y legales, así como un impacto negativo en la reputación de la empresa.	DTE/DTI, DTE/DSI, DTE/MTI, DTE/DIC, DTE/ISC, DTE/MCO, DTE/MSC
	ADMINISTRACION DE SERVICIOS TECNOLÓGICOS	Definir las políticas a seguir para administrar los servicios y los recursos necesarios para la buena y completa administración de dichos servicios.	Error en la Administración de Servicios	Este riesgo involucra errores en la gestión y coordinación de los servicios tecnológicos, como la asignación ineficiente de recursos, la mala ejecución de las políticas y la falta de seguimiento de los procedimientos establecidos.	Personas: El riesgo puede ser generado por el personal de administración de servicios tecnológicos debido a la falta de capacitación, experiencia insuficiente o una mala interpretación de las políticas y procedimientos.	Las causas pueden incluir la falta de capacitación adecuada del personal, una deficiente comunicación interna, la ausencia de una supervisión efectiva y la inadecuada asignación de responsabilidades.	Los efectos pueden ser variados, incluyendo la interrupción de servicios tecnológicos, la reducción de la eficiencia operativa, el incremento de costos por errores y retrabajos, y la posible pérdida de datos o fallas de seguridad.	DTE/DTI, DTE/DSI, DTE/MTI, DTE/DIC, DTE/ISC, DTE/MCO, DTE/MSC

GESTIÓN DE INNOVACIÓN	**GESTIÓN DE INVESTIGACIÓN Y DESARROLLO (I+D)**	Recopilar y analizar datos de toda la Institución que pueden ser útiles para la identificación de oportunidades de mejora en los procesos y nuevas tecnologías, así como datos de otras instituciones que pudieran ser útiles en este proceso y en ocasiones se reciben solicitudes de innovación.	Omisión en la Investigación o desarrollo	Riesgo de omitir componentes clave en la investigación y desarrollo, lo que podría conducir a resultados incompletos o inexactos, impactando negativamente la innovación y el avance tecnológico.	Personas: Investigadores y desarrolladores cuya falta de experiencia, conocimientos insuficientes o sobrecarga de trabajo podrían conducir a la omisión de pasos críticos en el proceso de investigación y desarrollo.	Falta de experiencia o formación adecuada entre el personal de investigación y desarrollo, sobrecarga de trabajo, y posiblemente una deficiente definición de roles y responsabilidades en los proyectos de I+D.	Consecuencias como la generación de información incompleta o inexacta, retrasos en el desarrollo de nuevos servicios o mejoras, y potencialmente, pérdidas económicas o daños a la reputación de la institución debido a la falta de innovación efectiva.	DTE/DTI, DTE/ISC, DTE/DIC, DTE/MSC, DTE/MCO
	INTELIGENCIA DEL NEGOCIO	Investigar y desarrollar diseños (ante-proyectos) de nuevos productos o tecnologías para mejorar los procesos de la Institución.	Conflicto de Intereses	Conflictos internos o externos que pueden surgir durante la fase de investigación y desarrollo de inteligencia de negocio. Esto puede deberse a desacuerdos en la interpretación de datos o en las estrategias a seguir, lo que puede entorpecer la toma de decisiones basada en datos y el desarrollo de iniciativas de negocio informadas.	Entorno: departamentos internos con objetivos desalineados, competencia por recursos entre proyectos, o discrepancias con proveedores externos o partes interesadas en cuanto a expectativas y resultados de la inteligencia de negocio.	Designación inadecuada de responsables de ejecutar tareas clave, falta de comunicación efectiva, y ausencia de una estructura de gobernanza clara para la gestión de la inteligencia de negocio.	Retrasos en la entrega de análisis de inteligencia de negocio, pérdida de oportunidades por no actuar a tiempo sobre información crítica, y potencial desaprovechamiento de recursos al no capitalizar adecuadamente las perspectivas de negocio.	DTE/DTI, DTE/ISC, DTE/DIC, DTE/MSC, DTE/MCO
MPLEMENTACIÓN DE TIC	**GESTIÓN DE PROYECTOS DE TECNOLOGÍA Y COMUNICACIÓN**	Administrar proyectos TIC para desarrollar o implementar soluciones tecnológicas utilizando herramientas de gestión y de seguimiento de proyectos.	Desacierto en la Gestión de Proyectos TIC	Este riesgo involucra errores en la planificación, ejecución y control de proyectos de tecnología y comunicación, pudiendo llevar a la no consecución de los objetivos del proyecto, sobrecostos y retrasos.	Personas: Gestores de proyectos y miembros del equipo de proyecto, cuya falta de habilidades, experiencia o comprensión adecuada de los requisitos del proyecto pueden conducir a errores en la gestión.	Incluyen una planificación inadecuada, estimaciones incorrectas de tiempo y recursos, una mala gestión de riesgos y cambios, y comunicación deficiente entre los interesados.	Pueden ser variados, incluyendo la no entrega de proyectos dentro del tiempo y presupuesto establecidos, baja calidad del producto final, insatisfacción de los usuarios, y en casos graves, la cancelación del proyecto.	DTE/DTI, DTE/DSI, DTE/ISC, DTE/DIC
	GESTIÓN DE SOLUCIONES INFORMÁTICAS Y TELECOMUNICACIONES	Buscar las mejores soluciones disponibles en el mercado local, de acuerdo a los recursos disponibles.	Exclusión de la Gestión de Soluciones TIC	Exclusión de soluciones informáticas críticas o idóneas debido a procesos de selección inadecuados o a la falta de acceso a la información correcta, lo que podría resultar en la implementación de tecnologías subóptimas y no alineadas con las necesidades de la organización.	Entorno: Factores del entorno tecnológico y de mercado, como limitaciones de los proveedores de información, sesgos en la evaluación de soluciones o la falta de un proceso de toma de decisiones inclusivo que considere todas las opciones disponibles.	Comunicación deficiente con los proveedores de soluciones informáticas, una evaluación inadecuada de las necesidades tecnológicas o un proceso de selección que no considera todas las soluciones potenciales.	Demoras en la implementación de proyectos de TIC, mayores costos por la adopción de soluciones ineficientes, y una posible falta de competitividad debido a la falta de innovación tecnológica o adaptabilidad a nuevas tendencias del mercado.	DTE/DTI, DTE/DSI
	IMPLEMENTACIÓN DE SOLUCIONES INFORMÁTICAS Y DE TELECOMUNICACIONES	Implementar las soluciones tecnológicas siguiendo las recomendaciones y mejores prácticas de cada caso.	Desacierto en Implementación de Soluciones TIC	Desacierto en la implementación de soluciones informáticas, que puede ser el resultado de decisiones erróneas o juicios equivocados durante el proceso de implementación, llevando a una ejecución deficiente que no cumple con los requisitos o expectativas del proyecto.	Personas: miembros del equipo de proyecto, incluyendo gerentes de proyecto, desarrolladores y analistas, cuyas acciones o decisiones directas impactan la calidad y el éxito de la implementación de soluciones informáticas.	Asignación inadecuada de roles y responsabilidades, falta de competencias o experiencia del personal asignado, comunicación deficiente entre los equipos, o una planificación y análisis previos insuficientes.	Retrasos en los plazos de entrega, sobrecostos, funcionalidades defectuosas o ineficientes, y la posible necesidad de realizar costosas correcciones post-implementación, afectando la satisfacción del usuario final y los resultados empresariales.	DTE/DTI, DTE/DSI, DTE/MTI, DTE/DIC, DTE/ISC, DTE/MCO, DTE/MSC

(2)

DESARROLLO/ADQUISICIÓN E IF	**DISEÑO E IMPLEMENTACIÓN DE CAMBIOS TECNOLÓGICOS**	Analizar y definir las mejores estrategias para realizar los cambios tecnológicos, buscando mantener a la ANDE en la vanguardia en implementaciones tecnológicas.	Error en el Diseño e Implementación de Cambios Tecnológicos	Este riesgo implica errores en el proceso de diseño y ejecución de cambios tecnológicos, lo que puede resultar en soluciones que no cumplen con los requisitos, son incompatibles con los sistemas existentes, o introducen nuevos problemas.	Personas: Ingenieros de sistemas y diseñadores de TIC, cuya falta de comprensión detallada de los requisitos del sistema o limitaciones en habilidades técnicas pueden llevar a errores en el diseño e implementación.	Las causas pueden incluir una planificación deficiente, falta de análisis de impacto, comunicación insuficiente entre los equipos de diseño y operaciones, y una evaluación inadecuada de los riesgos asociados con los cambios.	Los efectos pueden abarcar desde fallas en el sistema, interrupciones operativas, aumento de los costos de corrección, hasta la insatisfacción de los usuarios y posibles brechas de seguridad.	DTE/DTI, DTE/DSI, DTE/ISC, DTE/DIC
	GESTIÓN DE ACTIVOS TECNOLÓGICOS	Definir y desarrollar procedimientos para gestionar los activos TIC de la ANDE con herramientas que faciliten la gestión del mismo.	Demora en la Gestión de Activos Tecnológicos	Demoras en la gestión de activos informáticos, lo que puede afectar la disponibilidad y el rendimiento de los recursos tecnológicos de la organización, llevando a un cumplimiento tardío de los objetivos de IT y posiblemente afectando la continuidad del negocio.	Entorno: fallas en la cadena de suministro, procesos internos ineficientes y la gestión inadecuada del ciclo de vida de los activos informáticos, que pueden retardar las actualizaciones, el mantenimiento y la sustitución de los equipos tecnológicos.	Fallas en la comunicación con los proveedores de información, procesos de aprobación lentos, y la falta de procedimientos estandarizados para la gestión de activos, lo que puede resultar en una asignación ineficiente de los recursos informáticos.	Demoras en la gestión de activos informáticos pueden ser retrasos significativos en la entrega de proyectos de TIC, disminución en la productividad del personal, aumento de costos operativos por el uso prolongado de equipos obsoletos y un mayor riesgo de fallas de seguridad debido al hardware o software desactualizado.	DTE/DTI, DTE/MTI, DTE/ISC, DTE/MCO
	GESTIÓN DE CALIDAD DE TIC	Definir, desarrollar e implementar procedimientos y herramientas para gestionar la calidad de TIC dentro de la ANDE.	Dolo en la Gestión de la Calidad de TIC	Implica la presentación engañosa o falsificación de la conformidad con los estándares de calidad y las mejores prácticas, lo que puede resultar en la implementación de soluciones que no cumplen con los requisitos necesarios o que son inadecuadas para los procesos de la organización.	Entorno: procedimientos de control de calidad deficientes, falta de transparencia en los procesos de auditoría y evaluación, y posibles conflictos de interés que pueden comprometer la integridad de la gestión de calidad.	Dependencia de información incorrecta o incompleta proporcionada por los proveedores, falta de controles internos robustos, y la ausencia de una cultura de calidad que promueva la mejora continua en las TIC.	Retrasos en la entrega de proyectos, la adopción de tecnologías que no se ajustan a los estándares de la industria, vulnerabilidades de seguridad y posibles impactos negativos en la operatividad y reputación de la organización.	DTE/DTI, DTE/DSI, DTE/DIC, DTE/ISC
ÓN DEL GOBIERNO DE TIC	**IMPLEMENTACIÓN Y MONITOREO DEL MARCO DE GOBIERNO DE TIC**	Implementar herramientas de monitoreo para facilitar la gestión del Gobierno TIC	Omisión en el Gobierno TIC	Este riesgo implica la falta de implementación o seguimiento adecuado de las políticas y procedimientos del marco de gobierno de TIC, lo que podría llevar a una gestión ineficiente y a una alineación deficiente con los objetivos estratégicos de la organización.	Personas: La dirección y el personal de TIC, cuya falta de compromiso o comprensión inadecuada de las políticas de gobierno de TIC pueden resultar en la omisión de su correcta implementación y monitoreo.	Las causas pueden incluir la falta de claridad en las políticas de gobierno de TIC, la ausencia de responsabilidad definida, la resistencia al cambio dentro de la organización, y la insuficiente formación del personal en gobierno de TIC.	Los efectos pueden incluir una alineación deficiente de las TIC con las estrategias empresariales, incremento en los riesgos relacionados con las TIC, ineficiencias operativas, y posiblemente, el incumplimiento de normativas y estándares relevantes.	DTE/DTI, DTE/DSI, DTE/ISC, DTE/DIC
	ADMINISTRACIÓN DE RIESGOS DE TIC	Establecer los criterios adecuados para medir los riesgos de cada servicio.	Desacierto en la Administración de Riesgos TIC	Este riesgo se refiere a fallos en la correcta identificación, evaluación y tratamiento de los riesgos asociados a las TIC, lo que puede llevar a una gestión ineficiente de los mismos y a una exposición innecesaria a amenazas.	Personas: Personal encargado de la gestión de riesgos de TIC, cuya falta de experiencia, conocimiento o aplicación inadecuada de métodos de gestión de riesgos pueden llevar a una administración ineficaz.	Las causas pueden incluir una falta de capacitación adecuada, ausencia de herramientas o metodologías apropiadas para la gestión de riesgos, y una mala comunicación entre los departamentos involucrados.	Los efectos pueden incluir decisiones basadas en información incorrecta o incompleta, aumento de la vulnerabilidad a incidentes de seguridad, y potenciales pérdidas financieras o daños a la reputación de la organización.	DTE/DTI, DTE/DSI, DTE/ISC, DTE/DIC

GESTI	**GESTIÓN DE TRANSPARENCIA DE LA INFORMACIÓN**	Definir y propiciar la implementación los mecanismos para disponibilizar los datos y lograr la transparencia ante los demás sectores e instituciones de control.	Desacierto en la Gestión de Transparencia	Desacierto en la toma de decisiones debido a la falta de transparencia en la información gestionada, lo que puede conducir a decisiones mal informadas o basadas en datos incompletos o incorrectos.	Personas: Individuos encargados de la recopilación, procesamiento y distribución de información dentro de la organización, que pueden incluir personal de IT, analistas de datos, y responsables de la toma de decisiones que dependen de esta información.	La falta de un sistema de información adecuado que asegure la transparencia y precisión de los datos, carencia de políticas de gestión de datos claras y efectivas, y la ausencia de controles y auditorías regulares que validen la calidad y la disponibilidad de la información.	Retrasos en los procesos operativos, decisiones estratégicas subóptimas, y la pérdida de confianza de las partes interesadas debido a la falta de claridad y veracidad en la información proporcionada.	DTE/DTI, DTE/DSI, DTE/ISC, DTE/DIC
DE SERVICIOS Y SOPORTE DE TIC	**GESTIÓN DE SERVICIOS DE TIC**	Definir e implementar la gestión de los servicios TIC, siguiendo las normativas y mejores prácticas internacionales.	Error en la Gestión de Servicios de TIC	Errores en la gestión de servicios de TIC que pueden originarse por la adopción de ideas, opiniones o creencias incorrectas, o por acciones que resulten en la desobediencia de normas establecidas, lo cual puede impactar negativamente la calidad y conformidad de los servicios de TIC.	Entorno: El entorno que incluye los estándares de TIC, las expectativas de conformidad, y la dinámica del mercado. Cualquier cambio o malinterpretación en estos factores puede ser un agente generador de errores en la gestión de servicios.	Las fallas en el proveedor de la información que llevan a la desinformación o mala interpretación de las normativas, así como la falta de procesos actualizados para evaluar y aplicar las mejores prácticas internacionales de gestión de servicios de TIC.	No cumplimiento de los plazos críticos, retrasos en la entrega de servicios y proyectos, y en el incumplimiento de objetivos operativos y estratégicos, afectando la eficiencia y la efectividad de la organización en su conjunto.	DTE/DTI, DTE/MTI, DTE/MSC, DTE/MCO
	GESTIÓN DE ASISTENCIA TÉCNICA A USUARIOS	Gestionar los recursos necesarios y las capacidades requeridas para lograr un correcto y completo mantenimiento correctivo, preventivo y predictivo de los sistemas y equipos TIC.	Desacierto en la Gestión de Asistencia Técnica a Usuarios	Desacierto en la toma de decisiones relacionadas con la gestión de asistencia técnica a usuarios, lo que puede llevar a la implementación de soluciones de soporte inadecuadas, insuficientes o erróneas, afectando la eficiencia y la satisfacción del usuario.	Entorno: Factores ambientales y circunstancias externas que afectan la gestión de asistencia técnica, incluyendo limitaciones en la información proporcionada por proveedores externos y cambios en las necesidades o expectativas de los usuarios.	Fallos en el proveedor de la información, falta de entendimiento claro de las necesidades del usuario, y procesos de gestión de asistencia técnica deficientes o desactualizados.	Incumplimiento de los plazos de respuesta, disminución en la calidad del servicio al usuario, frustración del usuario, y potencial impacto en la productividad general debido a la ineficacia del soporte técnico.	DTE/DTI, DTE/MTI, DTE/MSC, DTE/MCO
	GESTIÓN DE MANTENIMIENTO DE TIC	Gestionar los recursos necesarios y las capacidades requeridas para lograr una correcta y completa asistencia a los usuarios de la red informática CORPORATIVA y SCADA.	Demora en la Gestión del Mantenimiento de TIC	Demoras en el mantenimiento de las TIC, que puede llevar a una extensión de los tiempos de inactividad o a un rendimiento subóptimo de los sistemas tecnológicos, afectando la continuidad operativa y la eficiencia de la organización.	Entorno: fallas de los proveedores en la entrega de servicios de mantenimiento, restricciones presupuestarias que afectan la frecuencia y la calidad del mantenimiento, o limitaciones de recursos internos.	Falta de coordinación con los proveedores de servicios de mantenimiento, procesos de gestión de mantenimiento deficientes, o la ausencia de un plan de mantenimiento preventivo adecuado.	Incumplimiento de los plazos para la realización de tareas críticas de mantenimiento, aumento en los riesgos de seguridad por la falta de actualizaciones, y un impacto negativo en la productividad debido a la indisponibilidad de sistemas esenciales.	DTE/DTI, DTE/MTI, DTE/MSC, DTE/MCO

GESTIÓN	**GESTIÓN DE ESTRATEGIAS DE CONTINUIDAD DE TIC**	Definir y gestionar las estrategias a seguir para lograr la continuidad de los servicios TIC, siguiendo las recomendaciones y mejores prácticas internacionales.	Conflicto en la Gestión de estrategias de Continuidad	Conflictos en la gestión de estrategias de continuidad de TIC, lo cual puede generar desacuerdos o falta de alineación en las acciones y políticas para mantener la operatividad de los sistemas de información ante situaciones adversas.	Entorno: El entorno organizacional y operativo que influye en la continuidad de las TIC, incluyendo la falta de claridad en las responsabilidades, discrepancias en la comprensión de los requisitos de continuidad y posibles fallos en la comunicación entre las partes involucradas.	Fallas en la información proporcionada por proveedores sobre soluciones de continuidad, la ausencia de procesos de gestión de continuidad bien definidos y la falta de participación de todos los stakeholders en el proceso de planificación de la continuidad.	No implementación oportuna de estrategias de continuidad, la falta de preparación ante incidentes que afecten la disponibilidad de TIC y, en última instancia, un impacto negativo en la capacidad de respuesta y recuperación de la organización frente a interrupciones.	DTE/DTI, DTE/MTI, DTE/MSC, DTE/MCO
	GESTIÓN DE CONTROLES DE PROCESOS DE TIC	Definir y gestionar los controles a seguir sobre los servicios TIC, siguiendo las recomendaciones y mejores prácticas internacionales.	Omisión de Gestión de Controles de Procesos	Este riesgo se refiere a la falta de implementación o seguimiento adecuado de los controles necesarios en los procesos de TIC, lo que puede resultar en procesos ineficientes, no conformes y vulnerables a errores y fallas.	Personas: El personal de TIC encargado de la implementación y supervisión de los controles de procesos, cuya falta de experiencia o conocimientos adecuados puede llevar a una omisión en la gestión efectiva de estos controles.	Incluyen la falta de claridad en los procedimientos de control, la insuficiente formación del personal en prácticas de control de procesos, y la ausencia de una supervisión y revisión periódica de los controles establecidos.	Puede resultar en el funcionamiento inadecuado de los procesos de TIC, aumento del riesgo de fallas y errores, y potencialmente, en impactos negativos en la prestación de servicios de TIC y en la seguridad de la información.	DTE/DTI, DTE/MTI, DTE/MSC, DTE/MCO
SUPERVISIÓN Y MONITOREO DE TIC	**REVISION INDEPENDIENTE DE TIC**	Fortalecer y mejorar los niveles de confianza, así como de seguridad del entorno de Control Interno Informático de la ANDE, ejecutando revisiones externas independientes a intervalos regulares.	Defraudaciones en Revisión Independiente de TIC	Implica la posibilidad de actos intencionados para manipular o alterar los resultados de las revisiones independientes de TIC, ya sea mediante acceso no autorizado, alteración de los sistemas de control, o por medio de prácticas fraudulentas que distorsionen la realidad del estado de seguridad y confiabilidad de los sistemas de TIC.	Entorno. El entorno en el que se realizan las revisiones, que puede incluir a terceros malintencionados, personal interno con conflictos de interés o proveedores de servicios que puedan tener el incentivo o la capacidad de manipular los resultados de las revisiones.	Las fallas en el proveedor de la información, que pueden incluir la falta de transparencia, la inadecuada verificación de la información recibida o la no detección de manipulaciones en los datos o sistemas evaluados.	No cumplimiento de los plazos para la corrección de vulnerabilidades, la implementación de medidas de seguridad inadecuadas y una falsa sensación de seguridad que puede llevar a brechas o fallas significativas en los sistemas de TIC.	DTE/MTI, DTE/MCO, DTE/MSC
	SUPERVISIÓN Y MONITOREO DE CONTROL INTERNO DE TIC	Supervisar y evaluar de forma continua el estado y funcionamiento de los sistemas y equipos TIC por medio de herramientas tecnológicas.	Dolo en la Supervisión y Monitoreo de Control Interno de TIC	Implica la posibilidad de que se cometan actos intencionados de fraude, simulación o engaño durante la supervisión y el monitoreo de los controles internos de TIC. Esto puede llevar a informes falsos sobre el estado y funcionamiento de los sistemas y equipos TIC, afectando la toma de decisiones y la integridad de las operaciones de TIC.	Personas: personales involucradas en la supervisión y el monitoreo de los controles internos de TIC, como los auditores internos, los administradores de sistemas y los operadores de red, pueden convertirse en agentes generadores de riesgos si actúan con intención de fraude o desinformación.	Designación inadecuada del responsable de la elaboración de informes y del monitoreo de los controles internos puede llevar a un conflicto de intereses, a la falta de objetividad en las evaluaciones y a la posibilidad de manipulación de información.	No cumplimiento de los plazos para la detección y corrección de problemas, lo que podría comprometer la seguridad, eficiencia y confiabilidad de los servicios de TIC y, en última instancia, afectar a toda la organización.	DTE/MTI, DTE/MCO, DTE/MSC

	MONITOREO DE CUMPLIMIENTO DE REQUERIMIENTOS EXTERNOS	Evaluar el cumplimiento de requisitos legales, regulatorios y contractuales, tanto en los procesos de Tecnología de Información (TI) así como de Seguridad de Información (SI), para identificar los requisitos de cumplimiento y monitorear que los mismos se cumplan y hayan sido integrados con los procesos de cumplimiento de la ANDE en general.	Celebración indebida de contratos	Implica acuerdos o compromisos establecidos sin cumplir con los requisitos legales, regulatorios o contractuales necesarios. Este riesgo puede llevar a compromisos no autorizados, ineficaces o inválidos que podrían exponer a la organización a consecuencias legales o financieras.	Personas: responsables de la gestión y supervisión de los contratos y acuerdos, incluyendo a los gerentes de proyecto, los responsables de la contratación y los oficiales de cumplimiento, cuyas acciones pueden influir en la validez y la adecuación de los contratos celebrados.	Designación de responsables que no están adecuadamente informados o equipados para llevar a cabo la elaboración y revisión de contratos de forma que se asegure el cumplimiento de todos los requisitos externos necesarios.	Pueden ser múltiples y adversos, incluyendo retrasos en la ejecución de proyectos de TIC, posibles conflictos legales, repercusiones financieras por sanciones o litigios, y un impacto negativo en la reputación y la credibilidad de la organización.	DTE/MTI, DTE/MCO, DTE/MSC
SEGURIDAD DE LA INFORMACIÓN	**DISEÑO DE PLANES DE SEGURIDAD DE TIC**	Definir las políticas y procedimientos de la Seguridad de la información, establecer configuraciones y arquitecturas seguras para las conexiones e intercambios de datos, la medición de la madurez y capacitación de los funcionarios.	Error en Diseño de Planes de Seguridad TIC	Este riesgo implica errores o deficiencias en el proceso de diseño de planes de seguridad de TIC, lo que puede llevar a planes ineficaces, incompletos o que no abarquen todas las áreas críticas de la seguridad de la información.	Personas: Especialistas en seguridad de TIC, cuya falta de experiencia o conocimiento en estándares y mejores prácticas de seguridad puede resultar en un diseño inadecuado de los planes de seguridad.	Las causas pueden incluir una inadecuada comprensión de los riesgos de seguridad de TIC, falta de alineación con los objetivos de negocio, y una inadecuada evaluación de las necesidades y vulnerabilidades de la infraestructura de TIC.	Los efectos pueden ser variados, incluyendo vulnerabilidades en la seguridad de la información, posibles brechas de datos, y la incapacidad para responder eficazmente a incidentes de seguridad.	DTE/OCS, DTE/DTI, DTE/ISC
	GESTIÓN DE SERVICIOS DE SEGURIDAD INFORMÁTICA	Operativizar los lineamientos de la política de seguridad de la información, estableciendo criterios y controles para copias de seguridad, actualización de sistemas, escaneo de vulnerabilidades, así como el monitoreo constante y planes de acción de recuperación ante eventos cibernéticos.	Atentados a la Gestión de Servicios de Seguridad TIC	Posibilidad de acciones deliberadas que podrían comprometer la seguridad de la información y la infraestructura de TIC, como ataques cibernéticos que buscan explotar vulnerabilidades, o incidentes internos que resultan en la pérdida o el daño de activos de datos críticos.	Personas: ya sean internas o externas a la organización, con la capacidad de perpetrar atentados contra la infraestructura de TIC. Esto incluye hackers, empleados descontentos o negligentes y terceros con acceso inadecuado a sistemas críticos.	Falta de medidas de seguridad robustas, entrenamiento insuficiente del personal en prácticas de seguridad, sistemas desactualizados o mal configurados, y la inadecuada gestión de acceso a la información y sistemas críticos.	Pérdida de datos confidenciales, interrupciones en las operaciones críticas de la organización, daño a la reputación corporativa, y posibles sanciones legales y costos de recuperación.	DTE/OCS, DTE/DTI, DTE/ISC

Elaborado por:	Fecha:
Revisado por:	Fecha:
Aprobado por:	Fecha:

ING. LUIS A. ZÁRATE M.
Jefe de Ofic. de Apoyo a la Gestión de
la Dirección de Telemática (DTE/OAG)
26/12/2023

ING. LUIS POISSON SPESSOT
Director de Telemática

Ing. Tito Ocariz Krauer
Dirección de Planificación y Estudios
DIRECTOR

Lic. María Natalia Ferreira
Jefa Dpto. de Desarrollo de Políticas
y Sistemas de Gestión

Econ. Walter Gustavo Luraghi
Div. de Org., Sistemas y Procesos

Ing. Tito Ocariz Krauer
Dirección de Planificación y Estudios
DIRECTOR