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

ACTIVIDADES

DIRECCIÓN DE TELEMÁTICA (DTE)

AÑO 2023

ANDE

MODELO ESTÁNDAR DE CONTROL INTERNO
COMPONENTE CORPORATIVO DE CONTROL ESTRATÉGICO
DIRECCIÓN DE TELEMÁTICA
MACROPROCESO: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

COMPONENTE: ADMINISTRACIÓN DE RIESGOS
PRINCIPIO: IDENTIFICACIÓN DE RIESGOS
FORMATO: Identificación de Riesgos - Actividades
Nº: 70

Actualización: 00
Fecha:25/12/23

(1) ACTIVIDADES	(2) OBJETIVO	(3) RIESGOS	(4) DESCRIPCIÓN	(5) AGENTE GENERADOR	(6) CAUSAS	(7) EFECTOS	(8) UNIDAD RESPONSABLE
PLANIFICACIÓN Y COORDINACIÓN DEL DESARROLLO INFORMÁTICO	Asegurar la planificación y coordinación efectiva del desarrollo informático, alineando los proyectos de software con las estrategias y necesidades organizacionales, garantizando la calidad y seguridad en su implementación.	Error de planificación o coordinación en el desarrollo de sistemas tecnológicos	La probabilidad de cometer errores en la planificación y coordinación del desarrollo informático, lo que puede llevar a una mala gestión de recursos, incumplimiento de los plazos, y desalineación con los objetivos estratégicos y requisitos de seguridad de la organización.	Personas: Inadecuada asignación de recursos, falta de claridad en los objetivos del proyecto, comunicación deficiente entre equipos, y falta de metodologías estandarizadas de desarrollo.	Planificación insuficiente, comunicación ineficaz entre los personales, cambios no controlados en los requisitos, y falta de seguimiento y control adecuado durante el proceso de desarrollo.	Retrasos en la entrega de proyectos, sobrecostos, productos de software que no cumplen con los requisitos o estándares de calidad, y posibles vulnerabilidades de seguridad.	DTE/DTI, DTE/ISC, DTE/DIC
ESTUDIOS TENDIENTES A LA INTEGRACIÓN DE SISTEMAS INFORMÁTICOS	Evaluar y planificar la integración de sistemas informáticos para mejorar la interoperabilidad, eficiencia y consistencia de la información dentro de la organización	Error en estudios de integración de Sistemas informáticos y de telecomunicaciones	Riesgo de errores en la evaluación de compatibilidad, seguridad y eficiencia durante los estudios de integración, lo que puede llevar a la selección de sistemas incompatibles o inseguros.	Personas: Evaluación inadecuada por parte del equipo técnico, falta de conocimiento actualizado sobre las tecnologías disponibles, y comunicación insuficiente entre los departamentos involucrados.	Falta de experiencia o capacitación del personal técnico, comunicación deficiente entre los equipos de TI y otras áreas de la organización, y ausencia de protocolos claros para la evaluación de sistemas.	Selección de sistemas que no se integran bien, problemas de seguridad de la información, incremento en los costos de implementación, y retrasos en la mejora de los procesos organizacionales.	
INGENIERÍA DE IMPLEMENTACIÓN Y CONFIGURACIÓN	Garantizar que la implementación y configuración de soluciones tecnológicas se realicen de manera eficiente, cumpliendo con los estándares técnicos y requisitos del negocio.	Incumplimiento de políticas de implementación y configuración	Riesgo de no cumplir con los estándares técnicos, especificaciones de diseño o requisitos operativos durante la implementación y configuración, lo que puede resultar en fallas funcionales o de seguridad.	Personas: Falta de competencia técnica o experiencia del personal involucrado en la implementación y configuración de soluciones tecnológicas.	Insuficiente capacitación del personal técnico, falta de claridad en los requerimientos técnicos, y deficiencias en la comunicación entre los equipos de desarrollo e implementación.	Fallas en las soluciones implementadas, vulnerabilidades de seguridad, retrasos en la entrega de proyectos y posibles impactos negativos en los procesos empresariales	DTE/DTI, DTE/ISC, DTE/DIC
PLANIFICACIÓN Y ORDENAMIENTO	Asegurar una planificación ordenada y sistemática de las actividades de TI para alinearlas con los objetivos estratégicos de la organización y optimizar los recursos disponibles.	Incumplimiento de planificación	Riesgo de incumplimiento en la ejecución de las actividades planificadas, lo que puede llevar a desviaciones de los objetivos estratégicos, uso ineficiente de recursos y retrasos en los proyectos.	Personas: Falta de compromiso o entendimiento del personal sobre la importancia de seguir la planificación establecida.	Comunicación ineficaz de los planes, falta de claridad en los roles y responsabilidades, y ausencia de seguimiento y evaluación adecuados de las actividades planificadas.	Desalineación con los objetivos estratégicos, desperdicio de recursos, retrasos en la entrega de proyectos y potencial insatisfacción de los usuarios finales.	
CONVENIOS INTERINSTITUCIONALES CON ENFASIS EN LA GESTIÓN INFORMÁTICA CORPORATIVA	Establecer y gestionar convenios con otras instituciones para fortalecer la gestión informática corporativa, promoviendo el intercambio de conocimientos, recursos y mejores prácticas.	Irregularidades en los convenios	Riesgo de irregularidades en la gestión de los convenios, incluyendo incumplimientos, malentendidos o conflictos de intereses, que pueden afectar negativamente la cooperación y los objetivos del convenio.	Personas: Descoordinación entre las partes involucradas y falta de claridad en los términos del convenio.	Falta de comunicación efectiva, ausencia de definiciones claras de roles y responsabilidades, y carencia de mecanismos de seguimiento y control adecuados.	Incumplimiento de los objetivos del convenio, pérdida de oportunidades de colaboración, daño a la reputación de las partes involucradas y potencial desperdicio de recursos.	DTE/DTI, DTE/DSI, DTE/MTI, DTE/DIC, DTE/ISC, DTE/MCO, DTE/MSC
ASESORAMIENTO TÉCNICO A INSTITUCIONES GUBERNAMENTALES EN LA DEFINICIÓN DE SISTEMAS INFORMÁTICOS	Proveer asesoramiento especializado y técnico a instituciones gubernamentales para la definición y desarrollo de sistemas informáticos eficientes y alineados a sus necesidades específicas.	Irregularidades en los convenios	Riesgo de irregularidades en los convenios durante el asesoramiento técnico, lo que puede afectar la legalidad y efectividad de los acuerdos establecidos.	Personas: Falta de comprensión o conocimiento adecuado sobre las regulaciones y estándares aplicables en los convenios..	Inadecuada formación en regulaciones gubernamentales, desconocimiento de estándares técnicos específicos, o supervisión inadecuada.	Convenios que no cumplen con los estándares legales o técnicos, lo que puede llevar a responsabilidades legales, sanciones y pérdida de credibilidad	
VERIFICACIÓN DE EQUIPOS	Realizar revisiones periódicas y sistemáticas de los equipos tecnológicos para asegurar su funcionamiento óptimo y conformidad con los estándares técnicos.	Error en la verificación de equipos	Posibilidad de fallos en equipos por falta de una verificación adecuada.	Personas: Falta de conocimiento técnico o negligencia en la verificación de equipos..	Inadecuada capacitación técnica, falta de procedimientos estandarizados o negligencia.	Fallas en el funcionamiento de los equipos, lo que puede llevar a interrupciones de servicio y aumento en los costos de mantenimiento y reparación.	DTE/DTI, DTE/DSI, DTE/MTI, DTE/DIC, DTE/ISC, DTE/MCO, DTE/MSC
CONTROL Y SUPERVISIÓN	Ejercer un control y supervisión continua de los servicios tecnológicos para garantizar su eficiencia, seguridad y alineación con los objetivos organizacionales.	Omisión en el control o supervisión	Riesgo de suspensión o interrupción de los servicios tecnológicos debido a omisión en el proceso de control y supervisión, lo que puede llevar a problemas de rendimiento, seguridad y cumplimiento.	Personas: Falta de diligencia o supervisión adecuada en las tareas de control.	Falta de claridad en las responsabilidades, inadecuada formación del personal o sistemas de control deficientes.	Interrupción de los servicios tecnológicos, vulnerabilidades en la seguridad de la información, incumplimiento de normativas y estándares, y potenciales pérdidas económicas.	
PLANIFICACIÓN Y COORDINACIÓN DEL DESARROLLO INFORMÁTICO Y DE TELECOMUNICACIONES	Asegurar una planificación y coordinación efectivas de los proyectos de desarrollo informático y de telecomunicaciones, enfocándose en la innovación y en la alineación con los objetivos estratégicos.	Omisión en la planificación o Coordinación	Riesgo de ineficiencias o errores en los proyectos debido a una planificación o coordinación inadecuadas.	Personas: Falta de capacidad o experiencia en la gestión de proyectos de informática y telecomunicaciones.	Planificación deficiente, falta de comunicación efectiva entre los equipos, o recursos insuficientes	Retrasos en los proyectos, sobrecostos y posibles fallas en la implementación de soluciones tecnológicas	DTE/DTI, DTE/ISC, DTE/DIC, DTE/MSC, DTE/MCO
DISEÑO E IMPLEMENTACIÓN DE NORMAS DE CALIDAD EN LOS SISTEMAS INFORMÁTICOS	Desarrollar e implementar un conjunto de normas de calidad robustas y actualizadas para garantizar la excelencia y seguridad de los sistemas informáticos.	Desacierto en el diseño o implementación de normas de calidad	Riesgo de deficiencias en la calidad o no conformidad con los estándares establecidos en los sistemas informáticos.	Personas: Falta de conocimiento o experiencia en estándares de calidad para sistemas informáticos.	Inadecuada comprensión de los estándares de calidad, falta de capacitación o recursos para la implementación efectiva.	Sistemas informáticos que no cumplen con los criterios de calidad, lo que puede resultar en fallos operativos y no conformidades.	

(1)

ESTABLECER PARAMETROS DE ADQUISICIÓN DE EQUIPOS INFORMÁTICOS Y DE TELECOMUNICACIONES	Definir criterios claros y actualizados para la adquisición de equipos informáticos y de telecomunicaciones, asegurando que se alineen con las necesidades y estrategias tecnológicas de la organización.	Omisión de parametros de adquisición de equipos TIC	Riesgo de establecer parámetros inadecuados o insuficientes, lo que puede llevar a adquisiciones no óptimas o no conformes.	Personas: Falta de conocimientos técnicos o experiencia en la definición de parámetros de adquisición.	Inadecuada evaluación de necesidades, falta de conocimiento del mercado o tendencias tecnológicas, o procesos de decisión deficientes	Compra de equipos que no se ajustan a los requisitos o que son tecnológicamente obsoletos, lo que puede resultar en sobrecostos o ineficiencias	DTE/DTI, DTE/ISC, DTE/DIC, DTE/MSC, DTE/MCO
PROMOVER POLÍTICAS INNOVADORAS EN TÉRMINOS DE SERVICIOS A LA INSTITUCIÓN	Fomentar la adopción de políticas innovadoras que mejoren la calidad y eficiencia de los servicios ofrecidos por la institución, alineando las nuevas iniciativas con las necesidades y objetivos estratégicos.	Desacierto en elección de políticas de servicio	Riesgo de resistencia o inadaptación a las nuevas políticas, lo que puede limitar su eficacia e impacto.	Personas: Falta de aceptación o adaptabilidad al cambio por parte de los empleados o directivos.	Resistencia al cambio, falta de comunicación efectiva sobre los beneficios de las políticas innovadoras, o inadecuado proceso de implementación.	Ineficacia en la adopción de nuevas políticas, posible disminución de la moral del personal y falta de mejoras en los servicios.	
RELEVAMIENTO DE NECESIDADES TECNOLÓGICAS	Identificar y documentar de manera sistemática las necesidades tecnológicas de la institución para guiar las decisiones de inversión y desarrollo de proyectos TIC.	Desacierto en el relevamiento de necesidades tecnológicas	Riesgo de no identificar correctamente las necesidades tecnológicas, lo que puede llevar a decisiones inadecuadas en la gestión de TIC.	Personas: Falta de experiencia o conocimiento en la identificación de necesidades tecnológicas.	Inadecuada metodología de relevamiento, falta de comunicación con los usuarios finales o falta de visión estratégica.	Adopción de tecnologías inadecuadas o insuficientes, lo que puede resultar en ineficiencias operativas y gastos innecesarios	DTE/DTI, DTE/DSI, DTE/ISC, DTE/DIC
PROCEDIMIENTO DE ADQUISICIÓN DE EQUIPOS	Establecer y seguir un procedimiento estandarizado y transparente para la adquisición de equipos tecnológicos, asegurando que se cumplan los requisitos de calidad, precio y funcionalidad.	Dolo en el procedimiento de adquisición de equipos TIC	Riesgo de ineficiencias o errores en el proceso de adquisición, lo que puede llevar a compras inadecuadas o sobrecostos.	Personas: Falta de competencia o experiencia en la gestión de adquisiciones.	Procedimientos de adquisición inadecuados, falta de claridad en los requisitos, o insuficiente evaluación de proveedores.	Adquisiciones que no cumplen con los requisitos o que son económicamente desventajosas, impactando la eficiencia operativa y financiera.	
GUÍA TÉCNICA DE IMPLEMENTACIÓN	Proporcionar una guía detallada y estructurada para la implementación de soluciones tecnológicas, asegurando que se sigan los estándares y mejores prácticas de la industria.	Exclusión de guía técnica de implementación	Riesgo de que la guía técnica excluya aspectos críticos o esté desactualizada, lo que podría llevar a implementaciones deficientes o no alineadas con los estándares actuales.	Personas: Errores o falta de actualización en la elaboración de la guía técnica por parte del personal encargado.	Falta de revisión y actualización periódica de la guía, insuficiente retroalimentación de experiencias previas, y carencia de un proceso de validación exhaustivo.	Implementaciones tecnológicas ineficientes, posibles fallos de seguridad, y desviaciones en la consecución de los objetivos tecnológicos de la institución.	DTE/DTI, DTE/DSI
MEJORAS EN EL ALMACENAMIENTO DE DATOS	Optimizar la infraestructura y procesos de almacenamiento de datos para mejorar la eficiencia, seguridad y accesibilidad de la información almacenada.	Desacierto en el diseño de estructuras de Almacenamiento	Riesgo de no lograr una mejora efectiva en el almacenamiento de datos, lo que puede resultar en ineficiencias o vulnerabilidades.	Personas: Falta de habilidades técnicas o experiencia en la gestión de almacenamiento de datos.	Planificación inadecuada, selección incorrecta de tecnologías, o insuficiente inversión en mejoras.	Continuidad de problemas en el almacenamiento de datos, como la lentitud, inaccesibilidad o riesgos de seguridad	
ESTUDIO DE PROBLEMAS Y MEJORAS TECNOLÓGICAS	Analizar y comprender los problemas tecnológicos actuales, proponiendo soluciones y mejoras para optimizar el rendimiento y la eficiencia de los sistemas informáticos.	Desacierto en estudio de problemas y mejoras tecnológicas	Riesgo de desaciertos o errores en el análisis de los problemas y en la propuesta de mejoras, lo que podría resultar en soluciones ineficaces o que introducen nuevos problemas.	Personas: Falta de experiencia o conocimiento técnico adecuado en el personal encargado del estudio.	Insuficiente análisis de los problemas, falta de actualización en las últimas tecnologías y tendencias, y ausencia de una metodología de análisis y resolución de problemas.	Implementación de soluciones que no resuelven eficazmente los problemas, posibles impactos negativos en el rendimiento de los costos operativos.	DTE/DTI, DTE/DSI, DTE/MTI, DTE/DIC, DTE/ISC, DTE/MCO, DTE/MSC
MEJORAMIENTO DE EQUIPAMIENTOS	Modernizar y optimizar los equipamientos tecnológicos para mejorar la eficiencia operativa, la seguridad y la capacidad de respuesta a las necesidades actuales y futuras.	Exclusión de mejoramiento de equipamientos	Riesgo de no lograr mejoras efectivas en los equipamientos, lo que puede resultar en ineficiencias o falta de compatibilidad.	Personas: Falta de competencia técnica o de evaluación adecuada en la mejora de equipamientos.	Evaluación deficiente de las necesidades tecnológicas, selección inadecuada de equipamientos, o restricciones presupuestarias.	Continuación de problemas operativos, obsolescencia tecnológica y posibles incrementos en costos de mantenimiento.	
PLANIFICACIÓN E IMPLEMENTACIÓN DE PROYECTOS	Garantizar que la planificación e implementación de proyectos tecnológicos se realicen de manera eficiente y alineada con los objetivos estratégicos, asegurando la calidad y el cumplimiento de los plazos establecidos.	Conflicto en la planificación o implementación de proyectos TIC	Riesgo de fallos en la planificación o implementación de proyectos, lo que puede llevar a retrasos, sobrecostos o resultados insatisfactorios.	Personas: Falta de habilidades de gestión de proyectos o de comprensión de los objetivos y requisitos.	Planificación deficiente, falta de recursos, o inadecuadas habilidades de gestión de proyectos.	Proyectos que no cumplen con los plazos, presupuestos o estándares de calidad, afectando negativamente los objetivos de la institución.	DTE/DTI, DTE/DSI, DTE/ISC, DTE/DIC
INNOVACIÓN TECNOLÓGICA	Fomentar y gestionar la innovación tecnológica dentro de la institución, buscando constantemente oportunidades para mejorar y transformar los procesos y servicios a través de tecnologías emergentes y soluciones creativas.	Despilfarro en Innovación Tecnológica	Riesgo de implementar innovaciones tecnológicas que no se alineen con las necesidades de la institución o que no generen los beneficios esperados.	Personas: Falta de visión estratégica o comprensión en la selección y aplicación de tecnologías innovadoras.	Selección inadecuada de innovaciones tecnológicas, falta de planificación o evaluación de impacto.	Inversiones en tecnología que no aportan valor, posibles interrupciones en los servicios o ineficiencias operativas.	
ADMINISTRACIÓN DEL STOCK	Gestionar de manera eficiente el stock de equipos y recursos tecnológicos, asegurando su disponibilidad, adecuada conservación y actualización oportuna.	Desacierto en la administración del Stock	Riesgo de gestión ineficiente del stock, lo que puede llevar a escasez o excedentes y afectar la operatividad.	Personas: Falta de habilidades en la gestión de inventarios o en la planificación de necesidades.	Inadecuadas prácticas de gestión de stock, falta de previsión o de sistemas de control eficientes.	Escasez o exceso de stock, inmovilización de recursos financieros y posibles interrupciones en las operaciones.	DTE/DTI, DTE/MTI, DTE/ISC, DTE/MCO
CONTROL DE EQUIPOS A SER SUMINISTRADOS	Asegurar un control riguroso y efectivo de los equipos que serán suministrados, garantizando que cumplan con los requisitos especificados y estén disponibles cuando se requieran.	Omisión en el con trol de equipos suministrados	Riesgo de suministrar equipos que no cumplan con los requisitos o estándares, lo que puede afectar la calidad del servicio.	Personas: Falta de rigurosidad o experiencia en el control de calidad de los equipos..	Procesos de control de calidad deficientes, falta de especificaciones claras o seguimiento inadecuado.	Entrega de equipos inadecuados o defectuosos, lo que puede llevar a fallas operativas y a la insatisfacción de los usuarios	
ADIESTRAMIENTO PERMANENTE DEL PERSONAL	Proporcionar formación continua al personal para mejorar sus habilidades y conocimientos en tecnologías de información y comunicación, asegurando así un rendimiento óptimo y adaptación a las nuevas tecnologías.	Demora en el adiestramiento del personal	Riesgo de inadecuada formación del personal, lo que puede afectar la eficiencia y la calidad del trabajo realizado.	Personas: Falta de adecuación en los programas de formación o falta de compromiso en la capacitación.	Programas de formación obsoletos, falta de recursos para la formación o desinterés del personal en participar.	Personal no capacitado adecuadamente, lo que puede llevar a una disminución en la productividad y calidad del trabajo.	DTE/DTI, DTE/DSI, DTE/DIC, DTE/ISC
MONITOREO DE DESEMPEÑO Y MEJORAS	Realizar un seguimiento continuo y evaluación del desempeño de los sistemas TIC, identificando áreas de mejora y aplicando acciones correctivas para optimizar la eficiencia y la efectividad operativa.	Dolo en el monitoreo de desempeño de mejoras	Riesgo de manipulación o tergiversación de los datos de desempeño, lo que puede resultar en una percepción errónea de la eficiencia y eficacia de los sistemas TIC.	Personas: Conducta engañosa por parte de los responsables del monitoreo, ya sea para ocultar problemas o para presentar un rendimiento artificialmente mejorado.	Falta de transparencia y mecanismos de control en el proceso de monitoreo, y presión para mostrar resultados positivos.	Decisiones basadas en información incorrecta, falta de identificación y corrección de problemas reales, y posibles impactos negativos en la operatividad y la toma de decisiones estratégicas.	

ANÁLISIS DE LAS POLÍTICAS DE IMPLEMENTACIÓN	Evaluar de manera crítica y detallada las políticas de implementación de TIC para asegurar que sean efectivas, eficientes y alineadas con los objetivos estratégicos de la organización.	Desacierto en el análisis de políticas de gobernanza TIC	Riesgo de que las políticas de implementación no reflejen adecuadamente las necesidades o no sean efectivas en la práctica.	Personas: Falta de comprensión o experiencia en el análisis de políticas de implementación.	Evaluación inadecuada de políticas, falta de alineación con objetivos institucionales, o inadecuada comunicación de políticas.	Políticas de implementación inefectivas que pueden llevar a fallas en proyectos o no cumplimiento de los objetivos.	
ESTABLECER CRITERIOS DE TRABAJO	Definir y establecer criterios claros y coherentes de trabajo en el ámbito de las TIC, asegurando que las actividades se realicen de manera eficiente, efectiva y alineada con las políticas y objetivos de la organización. Riesgos (5): Atentados (Información existente, no modificable)	Conflicto para establecer criterios de trabajo	Riesgo de establecer criterios de trabajo que no sean adecuados o no se apliquen efectivamente, lo que puede afectar la productividad y calidad.	Personas: Falta de conocimiento o experiencia en la definición de criterios de trabajo efectivos.	Definición inadecuada de criterios, falta de comunicación o de herramientas para su implementación.	Ineficiencias operativas, confusión entre el personal y posibles discrepancias en la calidad del trabajo.	DTE/DTI, DTE/DSI, DTE/ISC, DTE/DIC
ESTADÍSTICA DE USO DE ACCESOS	Recopilar y analizar estadísticas sobre el uso de los accesos a los sistemas de información para identificar patrones, tendencias y posibles riesgos de seguridad.	Inexactitud en estadísticas de uso de acceso	Riesgo de interpretación errónea o insuficiente de las estadísticas, lo que puede llevar a decisiones inadecuadas en la gestión de accesos.	Personas: Falta de habilidades en análisis estadístico o en la interpretación de datos de accesos.	Análisis insuficiente, falta de herramientas adecuadas para la recolección y análisis de datos, o desconocimiento de las tendencias.	Decisiones basadas en datos incorrectos o incompletos, lo que puede afectar la seguridad y eficiencia de los sistemas.	DTE/DTI, DTE/DSI, DTE/ISC, DTE/DIC
MONITOREO DE POSIBLES RIESGOS EXTERNOS	Vigilar y evaluar continuamente los riesgos externos que puedan afectar a los sistemas y operaciones de TIC, incluyendo amenazas de seguridad cibernética, cambios en la legislación y tendencias del mercado.	Actos malintencionados en el monitoreo de riesgos externos	Riesgo de que actos malintencionados, como ataques cibernéticos, espionaje o vandalismo digital, afecten los activos de TIC de la organización.	Externos: Entidades o individuos fuera de la organización que pueden realizar ataques o acciones malintencionadas contra los sistemas de TIC.	Falta de vigilancia adecuada, vulnerabilidades en los sistemas de seguridad y en las prácticas de gestión de TIC, y cambios en el entorno externo que no son detectados a tiempo.	Compromiso de la seguridad de los sistemas, interrupciones en las operaciones, posibles pérdidas de datos y daños a la reputación de la organización.	
ANÁLISIS DEL ESTADO DE LOS DIFERENTES PROCESOS	Realizar un análisis detallado del estado de los diferentes procesos de TIC para identificar áreas de mejora, oportunidades de eficiencia y posibles riesgos.	Inexactitud en el análisis de procesos	Riesgo de no detectar problemas o áreas de mejora en los procesos, lo que puede afectar la eficiencia y efectividad de las operaciones de TIC.	Personas: Falta de habilidades analíticas o experiencia en la evaluación de procesos de TIC..	Evaluación insuficiente, falta de herramientas analíticas adecuadas, o desconocimiento de las mejores prácticas.	Persistencia de ineficiencias en los procesos, lo que puede llevar a problemas operativos y a una reducción en la calidad de los servicios.	DTE/DTI, DTE/DSI, DTE/ISC, DTE/DIC
ORGANIZACIÓN Y POLÍTICA INFORMÁTICA	Establecer una estructura organizativa efectiva para la gestión de TIC, así como políticas y directrices que guíen la toma de decisiones y acciones en este ámbito.	Desacierto en la organización y política	Riesgo de tomar decisiones inadecuadas o establecer políticas no óptimas que afecten la gestión de la información.	Personas: Falta de conocimiento especializado o experiencia en el diseño de políticas informáticas.	Deficiencias en la formación del personal encargado, falta de una estrategia clara, o carencia de procedimientos establecidos para la elaboración de políticas.	Puede resultar en políticas informáticas ineficientes, falta de cumplimiento de normativas, y posibles brechas en la seguridad de la información.	
ATENCIÓN A USUARIOS	Proporcionar un servicio de atención al usuario eficiente y efectivo, asegurando la resolución rápida de problemas y la satisfacción del usuario.	Demora en la atención a los usuarios	Riesgo de una atención al usuario ineficaz, lo que puede llevar a insatisfacción y problemas no resueltos.	Personas: Falta de habilidades de comunicación o conocimientos técnicos en el personal de atención al usuario.	Formación insuficiente del personal, falta de recursos o sistemas inadecuados para la gestión de consultas.	Insatisfacción de los usuarios, aumento en el número de incidencias no resueltas y posible impacto negativo en la imagen de la institución.	DTE/DTI, DTE/MTI, DTE/MSC, DTE/MCD
PROVISIÓN DE EQUIPAMIENTOS	Asegurar la entrega eficiente y efectiva de equipos tecnológicos necesarios para el óptimo funcionamiento de los servicios de la organización.	Demora en provisión de equipamientos	Riesgo de no proveer equipamientos adecuados o en tiempo oportuno, lo que puede afectar las operaciones.	Personas: Falta de planificación o evaluación adecuada en la provisión de equipamientos.	Inadecuada evaluación de necesidades, retrasos en la adquisición, o selección inadecuada de equipamientos.	Falta de equipamientos necesarios para las operaciones, lo que puede llevar a ineficiencias o interrupciones en el servicio.	
SOPORTE TÉCNICO	Brindar soporte técnico eficaz y oportuno para resolver incidencias y problemas técnicos, asegurando la continuidad y eficiencia de los servicios de TIC.	Demora en el soporte técnico	Riesgo de proporcionar un soporte técnico ineficaz, lo que puede llevar a demoras o resoluciones insatisfactorias de problemas técnicos.	Personas: Falta de conocimientos técnicos o habilidades de comunicación en el equipo de soporte técnico.	Formación insuficiente del equipo de soporte, sistemas de soporte inadecuados, o falta de recursos..	Aumento en el tiempo de resolución de problemas, insatisfacción de los usuarios y posibles interrupciones en las operaciones	DTE/DTI, DTE/MTI, DTE/MSC, DTE/MCD
VIGILANCIA TÉCNICA CONSTANTE AL USUARIO	Implementar una supervisión técnica continua y proactiva sobre los servicios utilizados por los usuarios para garantizar su estabilidad, seguridad y eficiencia..	Desacierto en vigilancia técnica	Riesgo de realizar una vigilancia técnica inadecuada o ineficaz que no identifique o no reaccione adecuadamente a los problemas técnicos, comprometiendo la calidad del servicio.	Personas: Falta de competencia técnica o de recursos adecuados en el equipo de monitoreo.	Insuficiente capacitación en técnicas de monitoreo y vigilancia, falta de herramientas adecuadas para el seguimiento efectivo, o procedimientos ineficientes.	Posibles interrupciones del servicio, brechas de seguridad no detectadas, y una percepción negativa de la calidad del servicio por parte de los usuarios.	
SOPORTE DE SISTEMAS	Proporcionar soporte técnico integral y eficiente a nivel de Sistemas, asegurando la resolución rápida de problemas y el mantenimiento de la operatividad de los sistemas.	Demora en soporte de sistemas	Riesgo de retrasos en la respuesta y solución de problemas técnicos, lo que puede afectar la continuidad operativa y la eficiencia de los sistemas.	Personas: Ineficiencia o sobrecarga en el equipo de soporte técnico.	Recursos insuficientes o inadecuadamente asignados para atender las demandas de soporte, procesos de soporte técnico lentos o ineficaces, o falta de coordinación entre los equipos de soporte.	Interrupciones prolongadas en los servicios de los sistemas, disminución de la productividad y posiblemente impacto negativo en la percepción de la calidad del servicio por parte de los usuarios.	DTE/DTI, DTE/MTI, DTE/MSC, DTE/MCD
MONITOREO TÉCNICO	Implementar un sistema de monitoreo técnico continuo y eficiente para detectar y abordar proactivamente los problemas técnicos, mejorando la confiabilidad y rendimiento de los sistemas TIC.	Omisión en el monitoreo técnico	Riesgo de fallos en el monitoreo técnico, lo que puede llevar a la no detección de problemas o demoras en su resolución.	Personas: Falta de habilidades o recursos para llevar a cabo un monitoreo técnico efectivo.	Insuficiente capacidad de monitoreo, falta de herramientas adecuadas o de personal calificado.	Problemas técnicos no detectados o no resueltos a tiempo, lo que puede llevar a interrupciones del servicio o fallas operativas.	
CONTROL DE FIABILIDAD DE LA RED	Asegurar la estabilidad y fiabilidad constantes de la red a través de un control y gestión adecuados, para garantizar una conectividad ininterrumpida y de alta calidad.	Conflicto en el control de la red	Riesgo de conflictos en la red, como colisiones de datos o incompatibilidades, que pueden causar interrupciones o disminución en el rendimiento de la red.	Equipos: Incompatibilidad entre diferentes componentes de la red o configuraciones inadecuadas.	Uso de equipos o software desactualizados, falta de coordinación en la configuración de la red, o inadecuada planificación en la expansión o actualización de la red.	Interrupciones en el servicio de red, reducción en la calidad de la conectividad, y posibles problemas de comunicación interna o con clientes externos.	DTE/DTI, DTE/MTI, DTE/MSC, DTE/MCD
TRAZABILIDAD DE DESEMPEÑO	Implementar y mantener un sistema efectivo de trazabilidad de desempeño que permita la evaluación y mejora continua de la calidad de los servicios de TIC.	inexactitud de la trazabilidad de desempeño	Riesgo de no evaluar correctamente el desempeño, lo que puede llevar a una comprensión errónea del estado real de los procesos y sistemas.	Personas: Falta de competencias en el análisis y evaluación del desempeño de los sistemas TIC.	Herramientas inadecuadas para el seguimiento del desempeño, falta de indicadores claros o falta de formación en análisis de datos.	Decisiones basadas en información incorrecta o incompleta, lo que puede afectar la calidad y la eficiencia de los servicios TIC.	
CUMPLIMIENTO DE NORMAS	Asegurar el cumplimiento riguroso de todas las normativas y estándares relevantes para garantizar la calidad, seguridad y legalidad de los servicios de TIC.	Incumplimiento de normas	Riesgo de incumplimiento de las normativas, lo que puede llevar a sanciones, ineficiencias o impactos en la calidad del servicio.	Personas: Falta de conocimiento o negligencia en el cumplimiento de las normas.	Falta de claridad en las normativas, insuficiente formación del personal o falta de sistemas de control efectivos.	Posibles sanciones legales, daños a la reputación y problemas en la calidad y seguridad de los servicios TIC	DTE/DTI, DTE/MTI,

(3)

METRICA DE TRABAJOS	Establecer y mantener un sistema de métricas para medir y mejorar el desempeño de los trabajos realizados en el ámbito de TIC, asegurando la eficiencia y calidad del servicio.	Conflicto para establecer metricas de trabajo	Riesgo de utilizar métricas inadecuadas o de interpretar incorrectamente los resultados, lo que puede llevar a decisiones erróneas.	Personas: Falta de conocimiento o habilidades en el desarrollo y análisis de métricas de trabajo.	Selección de métricas inapropiadas, falta de formación en análisis de datos o sistemas inadecuados para el seguimiento.	Decisiones basadas en información errónea, lo que puede afectar la eficacia y la planificación de los trabajos en TIC.	DTE/MSC, DTE/MCO
AUDITORIAS EXTERNAS DE SOFTWARE	Realizar auditorías externas periódicas y meticulosas del software para garantizar su conformidad con los estándares de calidad, seguridad y cumplimiento normativo.	Encubrimiento en auditorias externas de software	Posibilidad de que las auditorías externas no revelen de manera efectiva deficiencias o incumplimientos en el software, lo que podría llevar a riesgos de seguridad y cumplimiento normativo.	Personas: Auditores externos que puedan no realizar una evaluación independiente y exhaustiva.	Parcialidad o falta de competencia en los auditores, Insuficiente supervisión del proceso de auditoría, o posibles conflictos de intereses	Uso continuado de software potencialmente inseguro o no conforme, riesgos de seguridad y cumplimiento, y posibles repercusiones legales o de reputación para la institución.	DTE/MTI, DTE/MCO, DTE/MSC
CONTRATACIÓN DE CONSULTORÍA	Asegurar la selección y contratación de servicios de consultoría de alta calidad que aporten valor y conocimiento especializado a los proyectos de TIC.	Celebración indebida de contratos de consultoría	Riesgo de contratar consultorías que no cumplan con los requisitos o expectativas, afectando la calidad y efectividad de los proyectos.	Personas: Falta de criterio o experiencia adecuada en la selección y contratación de consultorías.	Evaluación inadecuada de proveedores, falta de claridad en los términos de referencia o ineficaz proceso de licitación.	Inversión en consultorías ineficaces, retrasos o fallos en proyectos, y posible desperdicio de recursos financieros	
SUPERVISIÓN PERIODICA	Realizar supervisión periódica y sistemática de los servicios y procesos de TIC para garantizar su adecuación, calidad y alineación con los objetivos estratégicos.	Demora en la supervisión	Riesgo de retrasos o insuficiencias en las actividades de supervisión periódica, lo que puede impedir la detección oportuna de problemas y desviaciones.	Personas: Inadecuada planificación o asignación de recursos para las actividades de supervisión.	Planificación deficiente, recursos insuficientes para la supervisión efectiva, o falta de capacitación adecuada de los supervisores.	Fallos en la identificación temprana de problemas, lo que puede llevar a fallas operativas, incumplimiento de normativas y posibles impactos negativos en la eficiencia y seguridad de los sistemas de TIC.	DTE/MTI, DTE/MCO, DTE/MSC
MONITOREO SOBRE PROCESOS	Implementar un monitoreo continuo y detallado sobre los procesos de TIC para asegurar su eficiencia, efectividad y alineación con los estándares y objetivos organizacionales.	Dolo en el monitoreo de procesos	Riesgo de conductas fraudulentas o engañosas en el monitoreo de procesos, que pueden llevar a evaluaciones incorrectas o a la ocultación de deficiencias.	Personas: Acciones intencionadamente engañosas o manipulativas por parte del personal encargado del monitoreo.	Falta de controles efectivos y de integridad en el personal, conflictos de interés, o falta de transparencia en los procesos de monitoreo.	Informes de monitoreo inexactos o sesgados, fallos en la detección de problemas críticos, y toma de decisiones basadas en información errónea, afectando negativamente la gestión de TIC.	
VIGILANCIA DE PROCESOS	Supervisar y asegurar que los procesos de TIC se adhieran a todos los requerimientos externos, incluyendo estándares de la industria, regulaciones y legislaciones.	Celebración indebida de contratos de vigilancia de procesos	Riesgo de prácticas inadecuadas o irregulares en la gestión de contratos relacionados con los procesos de TIC, lo que puede llevar a acuerdos no beneficiosos o no conformes con las políticas y leyes aplicables.	Personas: Falta de conocimiento o comprensión adecuada de los requerimientos legales y normativos por parte del personal encargado de la supervisión.	Falta de controles adecuados en la gestión de contratos, falta de conocimiento o comprensión de las normativas aplicables, o conflictos de interés en el proceso de toma de decisiones.	Celebración de contratos que no cumplen con los estándares o intereses de la organización, posibles implicaciones legales, y compromiso de la integridad y efectividad de los procesos de TIC.	DTE/MTI, DTE/MCO, DTE/MSC
NORMALIZACIÓN DE PROCESOS	Establecer y mantener un conjunto de procesos estandarizados en TIC para asegurar su eficiencia, coherencia y alineación con las normativas y mejores prácticas del sector.	Incumplimiento de Normas	Riesgo de establecer procesos que no cumplen con las normativas o estándares requeridos, afectando la eficiencia operativa y el cumplimiento normativo.	Personas: Falta de conocimiento o experiencia en la aplicación de normativas y estándares en la normalización de procesos.	Insuficiente comprensión de los requerimientos legales y normativos, falta de directrices claras para la normalización, o deficiencias en la formación del personal.	Implementación de procesos no estandarizados o incompatibles con normativas externas, lo que puede llevar a ineficiencias operativas y riesgos legales o de conformidad.	
DESARROLLO DE ACCIONES DE SEGURIDAD DE LA INFORMACIÓN	Desarrollar e implementar estrategias y medidas efectivas para proteger la integridad, confidencialidad y disponibilidad de la información de la organización.	Conflicto para el desarrollo de acciones de Seguridad	Riesgo de que las acciones de seguridad implementadas no sean efectivas o adecuadas, llevando a vulnerabilidades o brechas de seguridad.	Personas: Falta de conocimiento o experiencia adecuada en el desarrollo e implementación de medidas de seguridad.	Planificación insuficiente, falta de conocimiento técnico actualizado sobre seguridad de la información, o recursos inadecuados.	Posibles brechas de seguridad, pérdida de datos, ataques cibernéticos y otros riesgos de seguridad que pueden afectar gravemente a la organización.	
ANÁLISIS DE DIFERENTES SISTEMAS DE SEGURIDAD	Realizar un análisis exhaustivo de distintos sistemas de seguridad de la información para evaluar su adecuación a las necesidades específicas de la organización y garantizar la máxima protección de datos.	Desacierto en análisis de sistemas de seguridad	Riesgo de realizar un análisis incorrecto o insuficiente de los sistemas de seguridad, llevando a la elección de soluciones inadecuadas.	Personas: Falta de competencia técnica o experiencia en la evaluación de sistemas de seguridad de TIC.	Evaluación superficial, falta de criterios adecuados para la comparación, o desconocimiento de las últimas tendencias y tecnologías en seguridad.	Adopción de sistemas de seguridad ineficaces o incompatibles, lo que puede llevar a vulnerabilidades y riesgos de seguridad para la organización.	DTE/OCS, DTE/DTI, DTE/ISC
RECUPERACIÓN DE SERVICIOS TECNOLÓGICOS	Implementar procedimientos efectivos para la restauración y activación rápida de sistemas tras incidentes o interrupciones, garantizando la mínima afectación a la continuidad operativa.	Demora en la recuperación de servicios tecnológicos	Riesgo de retrasos en la recuperación de servicios tras una interrupción, afectando la continuidad operativa y la eficiencia.	Personas: Falta de preparación o habilidades en el equipo técnico para una rápida recuperación.	Planes de recuperación inadecuados o no actualizados, falta de entrenamiento en procedimientos de recuperación, o recursos insuficientes.	Interrupciones prolongadas en los servicios tecnológicos, lo que puede llevar a pérdidas operativas, impacto en la productividad y posibles daños a la reputación de la institución.	DTE/OCS, DTE/DTI, DTE/ISC
MONITOREO Y OPERACIÓN DE SEGURIDAD	Realizar un seguimiento continuo y detallado de los diversos sistemas de la organización para identificar y responder rápidamente a cualquier problema de seguridad o funcionamiento.	Atentados a servicios tecnológicos	Riesgo de ataques o incidentes de seguridad que no sean detectados o abordados a tiempo debido a fallos en el monitoreo constante.	Personas: Falta de diligencia o competencia técnica del personal encargado del monitoreo.	Falta de capacitación en técnicas de monitoreo avanzadas, insuficientes recursos para el monitoreo efectivo, o sistemas de monitoreo obsoletos.	Vulnerabilidades en la seguridad no detectadas, interrupciones en el funcionamiento de los sistemas y potenciales brechas de seguridad.	

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

(4)

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

Ing. José Vallejos Mernes
Div. de Estudios Energéticos
Jefe

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