MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

Normas técnicas para la gestión y el control de las tecnologías de la información

Control de Versiones

Fecha	Versión	Autores	Aprobado	Descripción
10/11/2021	1.0	Ivannia Badilla Picado- Micitt Manuel Montillano Vivas – CCSS Seirys Solís García – Conavi Silvia Chinchilla Sáenz - Comité consultivo ISACA Costa Rica Orlando Tenorio Chacón - Comité consultivo ISACA Costa Rica	Jorge Mora Flores Director de Gobernanza Digital	Oficialización y entrada en vigor de Normas Técnicas para el control de las tecnologías de información
8/11/2022	2.0	Raúl Rivera - Comité consultivo ISACA Costa Rica Silvia Chinchilla Sáenz - Comité consultivo ISACA Costa Rica Luis Gorgona - Comité consultivo ISACA Costa Rica Ana Cecilia Vargas Universidad de Costa Rica	Paula Brenes Ramírez directora Dirección de Gobernanza Digital y Certificadores de Firma Digital	Entrada en vigor de la nueva versión de Normas Técnicas para el control de las tecnologías de información

PAULA FRANCHESKA BRENES RAMIREZ (FIRMA)

Firmado digitalmente por PAULA FRANCHESKA BRENES RAMIREZ (FIRMA)
Fecha: 2022.11.29 15:49:36 -06'00'

_____

Paula Ramírez Brenes
Directora
Dirección Gobernanza Digital y Certificadores de Firma Digital

MARCO NORMATIVO DE GOBIERNO Y GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN

CONTENIDO

ANTECEDENTES

El sector público costarricense presenta una pluralidad de realidades respecto a la gestión de tecnologías de información y comunicación, por lo que la Contraloría General ha señalado que se requiere una respuesta articulada por parte de las autoridades competentes en materia de tecnología y telecomunicaciones, que permita orientar las acciones que deben realizar las instituciones públicas en relación con esta materia. Lo anterior, en procura de direccionar al sector público hacia el aprovechamiento de esas tecnologías para el fortalecimiento de la gestión institucional, suministrando trazabilidad a sus procesos, así como información confiable y sistematizada para la toma de decisiones y la rendición de cuentas. Como parte de esas labores de rectoría en materia de control y fiscalización superior, el Órgano Contralor emitió las Normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE), resolución R-CO-26-2007 de las diez horas del siete de junio de 2007, en las cuales se establecieron criterios de control que debían ser observados como parte de la gestión institucional de las tecnologías de la información. Las Normas de TI, emitidas por la Contraloría General de la República, encontraban fundamento en la ausencia de un marco orientador que regulara tanto la gestión como la definición institucional del marco regulador en materia de tecnologías de información y comunicación, constituyendo en su momento el fundamento para el desarrollo de auditorías sobre la aplicación de controles y prácticas sobre la gestión de tecnologías de información.

Debido a que dicha normativa establece criterios de control que deben ser observados como parte de la gestión institucional de las TI, el jerarca y los titulares subordinados, como responsables de esa gestión deben establecer, mantener, evaluar y perfeccionar ese marco de control de conformidad con lo establecido en la Ley General de Control Interno N° 8292. Asimismo, la Función de TI debe contribuir con ello cumpliendo con dicho marco de control y facilitando la labor estratégica del jerarca. Esta normativa ha sido de acatamiento obligatorio para la Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización, y su inobservancia generaría las responsabilidades que correspondan de conformidad con el marco jurídico que resultara aplicable.

Por otra parte, mediante Directriz 043 del 16 de febrero de 2016, el Poder Ejecutivo emite los "Lineamientos generales para evaluar el estado de situación de las tecnologías de información y comunicación en el sector público costarricense", en los cuales se encomienda al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) la elaboración del diagnóstico del estado de situación del sector de las Tecnologías de la Información y Telecomunicaciones del país, presentar los resultados de ese diagnóstico al Consejo de Gobierno, así como realizar una propuesta de política nacional para el abordaje de las tecnologías de información y comunicación del sector público. En cumplimiento de lo anterior, en el año 2018, el MICITT emite la "Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0.", en la cual plantea el objetivo general del desarrollo del gobierno digital del Bicentenario, como el impulso al uso estratégico de las tecnologías digitales en las instituciones del gobierno de Costa Rica, respondiendo a las necesidades de todos sus habitantes de manera eficiente, transparente e inclusiva. Parte de la estrategia definida por el MICITT contempla el establecimiento de dos ejes estratégicos denominados "Pura Vida Digital" y "CR Inteligente", siendo una de las acciones propuestas en este último eje, la conformación de un Código Nacional de Tecnologías Digitales, consistente en un compendio de políticas que establecen los requisitos mínimos deseables para la adquisición, desarrollo y gestión de las tecnologías y los servicios digitales del sector público costarricense. Por otra parte, el sector público costarricense presenta una pluralidad de realidades con relación al

desarrollo digital que requieren una respuesta articulada de las autoridades competentes en la materia y que oriente las acciones que deben realizar las instituciones en materia de Tecnología y Telecomunicaciones, para enrumbar a todo el sector público en la misma dirección, a fin de lograr el objetivo de uso estratégico de las tecnologías digitales en las instituciones enfocadas en las necesidades de todos sus habitantes de manera eficiente, transparente e inclusiva.

Dentro del contexto descrito, las tecnologías de la información y comunicación son herramientas que contribuyen con las instituciones, suministrando trazabilidad a sus procesos así como información sistematizada y confiable para la toma de decisiones y la rendición de cuentas, por lo que deben atender a las particularidades de cada institución, **y orientadas con la visión definida por el rector en la materia** (MICITT), en consideración al conocimiento de sus actividades y los recursos disponibles. De esta forma, de conformidad con la publicación de la "Derogatoria de las Normas Técnicas para la gestión y el control de las tecnologías de Información (N-2-2007-CO-DFOE) resolución N.°R-CO-26- 2007 y modificación a las Normas de Control Interno para el Sector Público (N-2-2009-CODFOE) resolución N° R-CO-9-2009 ítems 5.9 y 5.10.", así mismo la Ley N° 7169 del 26 de junio de 1990, Ley de promoción del desarrollo científico y tecnológico, en sus artículos 1, 2, 3, 4, 5, 8, 9, 10, 11, 20 y 100, y en los artículos 10 y 11 inciso d) del Decreto Ejecutivo N° 41187-MP-MIDEPLAN, Reglamento de Organización del Poder Ejecutivo, se dispone que corresponde al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, la rectoría de Ciencia, Tecnología, Telecomunicaciones y Gobernanza Digital, y por ende, es el encargado de emitir la política pública en estas áreas, así como y promover la modernización y el aprovechamiento de los recursos tecnológicos que utiliza el Estado, estableciendo la debida coordinación con los demás órganos de la administración pública.

INTRODUCCIÓN

La disponibilidad de las Tecnologías de Información como habilitador son fundamentales para que las instituciones proporcionen la agilidad necesaria para detectar y responder ante las necesidades internas y de la comunidad.

En este ambiente de cambio continuo, la necesidad de implementar un proceso de gobierno, un marco de trabajo integral, que ayude a las entidades públicas a lograr sus objetivos estratégicos mediante el alineamiento de los objetivos de Tecnología con los objetivos institucionales, creando valor y generando beneficios dentro y fuera de la institución. A esta necesidad, se complementa el requerimiento de disponer de un ambiente de control adecuado que permita salvaguardar los datos e información que se gestiona en la institución.

Con la finalidad de generar valor público, es necesario, pasar de un paradigma de TI como recolector y cumplidor de requerimientos de sus grupos de interés, a una gestión de TI enfocada en el apoyo al cumplimiento de la estrategia institucional, lo que se logra más fácilmente cuando se cuenta con un marco de gobierno de TI.

Las Entidades del Estado Central, Municipalidades e Instituciones Autónomas, como a la alta e incremental dependencia tecnológica que tienen para mantener su operativa, se hace necesario contar con un marco orientador de la gestión de las tecnologías de información, que permita garantizar un balance adecuado de las inversiones, organización de recursos y actividades sustantivas, debidamente alineado al marco jurídico y manteniendo relaciones adecuadas con proveedores de bienes y servicios tecnológicos.

El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones – MICITT ha establecido el “Marco Regulatorio de Gobierno y Gestión de las Tecnologías de Información”, con una dirección más ajustada a la realidad en el entorno tecnológico actual, con el fin de coadyuvar a las instituciones en la administración de las I&T.

Los jerarcas, titulares subordinados y auditoría interna, debido a que dicha normativa establece criterios de control que deben ser observados como parte de la gestión institucional de las TI, serán los responsables de esta gestión. Deben establecer, mantener, evaluar y perfeccionar ese marco de gobierno y gestión de las tecnologías de información, de conformidad con lo establecido en la Ley General de Control Interno.

ALCANCE

Este Marco Normativo es de acatamiento obligatorio para las instituciones y órganos sujetos a la fiscalización de la Contraloría General de la República, y su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable.

RESPONSABILIDADES

La responsabilidad de las instancias institucionales en materia de Tecnologías de Información y comunicaciones como ente rector dentro de la organización, es velar por la implementación y seguimiento del Marco Normativo para la aplicación de sanas prácticas y adecuar su realidad basándose en este documento como referencia.

El máximo jerarca institucional, es responsable del establecimiento del Gobierno Corporativo que apoye y supervise la adecuada implementación de Marco Normativo y su gestión, por parte de la instancia competente en materia de I&T.

PRINCIPIO DE CUMPLIMIENTO

El Marco Normativo de Gobierno y Gestión de las Tecnologías de Información orienta a la institución en la implementación de buenas prácticas que permiten la adecuada gestión de los procesos requeridos para brindar de forma oportuna y efectiva los servicios brindados a través del uso y administración de los recursos tecnológicos de forma tal que garanticen la continuidad de las operaciones institucionales, la salvaguarda de la información gestionada, la entrega de valor y el cumplimiento normativo. Para el proceso de implementación es necesario tener conocimiento sobre la gestión institucional, naturaleza, tamaño y complejidad, volumen de operaciones y cómo esta se apoya en su operativa con el uso de los recursos tecnológicos y su nivel de dependencia. Este proceso puede ser progresivo, debidamente planificado, de acuerdo con las prioridades institucionales, criticidad de los procesos y riesgos asociados al uso de recursos tecnológicos y los servicios requeridos que se brindan a través de la gestión de TI.

PERFIL DEL PROCESO

Para asegurar que se realiza una adecuada implementación de cada proceso que soporta la gestión de tecnologías de información, debe asegurarse que cumpla con el siguiente perfil:

1. Debe estar formalmente definido a través de la disposición de un objetivo claro y metas específicas, que sean ejecutables, reales, orientadas a resultados y medibles.
2. La propiedad del proceso debe estar claramente establecida, sobre el diseño, interacción con otros procesos, rendición de cuentas de los resultados finales, medición del desempeño e identificación de mejora
3. Debe estar claramente establecida la secuencia de actividades de forma lógica, consecuente, flexible, y escalable de forma tal que produzca los resultados esperados, considerando el manejo de excepciones y emergencias.

4. Los roles y responsabilidades deben estar exactamente asignados para la ejecución efectiva de las actividades clave y su documentación, además de la rendición de cuentas sobre los entregables finales asociados.
5. Debe disponer de lineamientos y planes debidamente formalizados, revisados, actualizados, aprobados, almacenados, comunicados, publicados y utilizados en forma consecuente, que establezcan las directrices y acciones requeridas. Los lineamientos deben estar accesibles y asegurar el claro entendimiento por parte de los responsables de su aplicación, así como de las partes interesadas. Los lineamientos se constituyen por:
    - Planes de gestión, de trabajo y de acción, que permitan establecer las actividades y tareas para un período específico y el logro de resultados
    - Políticas y directrices que brinden la información necesaria en el más amplio nivel de detalle sobre las normas y mecanismos que se deben cumplir
    - Normas que definan los propósitos generales dentro de un marco o política regulatoria, indicando lo que debe hacerse para su cumplimiento de acuerdo con el entorno de gestión y alcances establecidos por la organización.
    - Procedimientos, para tareas específicas de tipo operativo-administrativo, indicando el cómo se lleva a cabo una actividad o un proceso describiendo con alto grado de detalle el modo de realizar las actividades principales y la parametrización de los componentes e integrantes del proceso que describen.
    - Estándar Técnico, desarrollado como guía para la configuración de valores, reglas, condiciones o características en productos de hardware y software que integran la arquitectura de procesos alcanzados por los requerimientos normativos, regulatorios y legales relacionados con las actividades institucionales.
    - Instructivos, listas de chequeo y formularios, documentación anexa a los procedimientos y que sirven como guía de paso a paso, documento de control y/o registros que presentan resultados obtenidos o proporcionan evidencia de actividades realizadas.
6. Deben contar con indicadores de desempeño, de tal forma que permitan identificar el nivel de logro de las metas. Deben establecerse las formas de recopilación de datos asociados y la presentación de los resultados y acciones para tratar las desviaciones según aplique.

DIAGNÓSTICO

Identificación de la situación actual al nivel de gestión de TI, con el fin de establecer la brecha según buenas prácticas y requerimientos institucionales (tamaño y complejidad de la institución, procesos críticos que se apoyan con las TI, riesgos asociados, entre otros). El diagnóstico puede orientar el nivel de implementación sobre las buenas prácticas de los procesos que se aplicarán para el marco de gestión de TI.

Se recomienda con base en el diagnóstico adicionalmente realizar un análisis de riesgos sobre la gestión y nivel de dependencia que tiene la institución hacia los recursos tecnológicos y el servicio brindado por la unidad de TI institucional, para desarrollar su operativa y el logro de los objetivos institucionales. Este análisis les permitirá priorizar la implementación/mejora de los procesos requeridos y las buenas prácticas asociadas para lograr una adecuada gobernanza y gestión de los servicios al nivel de TI. Si como resultado de esta valoración se identifican prácticas que no aplican a la institución, deberá ser debidamente justificado y respaldado con el análisis de riesgos respectivo.

Se dispone del instrumento: *Perfil de la Gestión de TI*, que permite identificar si se cuenta con los componentes mínimos para establecimiento del Marco de Gestión de las TI Institucional.

DOCUMENTOS DE REFERENCIA

La norma técnica se complementa con **material de referencia adicional**, que puede orientar a la institución y los responsables en la aplicación de buenas prácticas y controles para contar con una garantía razonable de que los procesos que soportan la gestión de las tecnologías son ejecutados adecuadamente, en un ambiente que permite salvaguardar la información y los activos asociados.

Los documentos siguientes, como se indicó anteriormente, fueron diseñados **para apoyar** a la institución en la valoración del estado actual de la gobernanza y gestión de las tecnologías de información, identificación de buenas prácticas para la mejora de los procesos asociados y los controles que permitirán disponer de un marco de seguridad adecuado para la salvaguarda de la información y activos asociados:

- Perfil de la Gestión de TI
- Matriz Guía Implementación Prácticas de Gobierno y Gestión
- Guía de Referencia para la Gestión de la Ciberseguridad
- Matriz de Controles para la Ciberseguridad según buenas prácticas
- Guía de Riesgos asociados a las tecnologías de información

PROCESOS DEL MARCO DE GESTIÓN DE TI

Para asegurar la disponibilidad del Marco de Gestión de Tecnología de Información Institucional, la institución debe establecer los procesos al nivel de Tecnologías de información, que permitan brindar servicios efectivos para mantener la operativa institucional, salvaguardar los datos que se capturan, procesan, organizan, distribuyen y resguardan.

I. GOBERNANZA DE TI

La institución debe disponer de un marco orientador que permita la definición de la acción institucional con un enfoque de valor público. Asimismo, debe considerar en la estrategia institucional la incorporación de iniciativas habilitadas por tecnologías de información.

La entidad pública debe tener un órgano rector que permita establecer las prioridades en cuanto al cumplimiento de estrategias propuestas por tecnologías de información; debidamente conformado por las autoridades institucionales administrativas competentes según corresponda a cada institución, participando a los titulares responsables de la Planificación Institucional y de las tecnologías de información y comunicaciones como un asesor en los modelos de habilitación de los objetivos, necesidades y oportunidades institucionales a través del uso de TI, así como elementos para la rendición de cuentas sobre el uso adecuado de las TI para responder a las necesidades, objetivos y oportunidades institucionales.

La conceptualización de este órgano rector debe ser una instancia de alto nivel que busca habilitar la gobernanza en torno a las Tecnologías de la Información y Comunicaciones (TIC), estableciendo un espacio de diálogo y coordinación entre las gerencias de la institución y la unidad responsable de las Tecnologías de Información y Comunicaciones (DTIC), con el fin de asegurar el apoyo de las TIC a la

gestión y el cumplimiento de la estrategia institucional. Al estar integrado por las máximas autoridades de gobierno y administración de la Institución, junto con la unidad de Tecnologías de la Información y Comunicaciones, y la Dirección de Planificación Institucional asume como cuerpo colegiado, la toma de decisiones sobre temas estratégicos asociados con las TIC que inciden en la prestación de los servicios a los usuarios.

II. GESTIÓN DE TI

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 estratégico y el modelo de arquitectura empresarial:

1. Estructura organizacional, el nivel de responsabilidad jerárquica de la Unidad de TI debe permitir la independencia de sus acciones y priorizar sus servicios de acuerdo con los requerimientos institucionales. Las Unidades deben ser claras y estar asignadas, oficializadas, publicadas y distribuidas a funcionarios que cumplan con el perfil requerido, de forma tal que no impacte la toma de decisiones y el logro de los objetivos de los procesos y servicios de TI.
2. Procesos de TI, establecidos formalmente para el adecuado aseguramiento de entrega de servicios y soporte a la institución.
3. Servicios, formalmente establecidos a través de un catálogo y las relaciones de acuerdos con las unidades funcionales, de forma tal que se pueda administrar adecuadamente la infraestructura tecnológica instalada en la organización para asegurar la continuidad de las operaciones institucionales, el resguardo de la información, el cumplimiento regulatorio y la mejora continua hacia el logro de los objetivos institucionales.
4. Investigación sobre tecnologías emergentes que permitan a través de su eventual incorporación, la innovación y mejora continua al nivel institucional para el logro de los objetivos y la entrega de valor público.
5. Atención (a través de una mesa de ayuda), ya sea solicitudes de nuevos requerimientos o incidentes al nivel de TI, de manera eficaz, eficiente y oportuna; y dicha atención debe constituir un mecanismo de aprendizaje que permita minimizar los costos asociados y la recurrencia. Además de permitir mayor facilidad al usuario el proceso para solicitar la atención. Administración de bienes y servicios prestados por terceros, asegurando que satisfagan los requerimientos en forma eficiente y sean congruentes con las prácticas de calidad, seguridad, seguimiento y evaluación establecidas por la institución.
6. Planificación de trabajo, a través de planes para la asignación de tareas y responsables y que orienten la evaluación del desempeño al nivel individual y el logro de los objetivos establecidos.

III. PLANIFICACIÓN TECNOLÓGICA INSTITUCIONAL

La Institución debe instaurar un modelo estratégico 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, así 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.

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 la línea estratégica institucional establecida

La entidad debe establecer una Política de Innovación e investigación tecnológica donde se determinen los mecanismos necesarios para asegurar el establecimiento de un proceso continuo por medio de la Unidad de TI.

La Unidad de TI debe disponer de un programa de iniciativas institucionales que pueden ser habilitadas a través de la incorporación de recursos y servicios tecnológicos, respaldados debidamente por la valoración de la factibilidad y entrega de valor respectivos.

La Unidad de TI debe desarrollar la planificación anual operativa que oriente las acciones para asegurar la mantenibilidad y disponibilidad de los recursos tecnológicos, la incorporación de nuevas facilidades (a través de proyectos) y el presupuesto asociado a las actividades y tareas, debidamente alineadas con los objetivos estratégicos establecidos por la institución.

La entidad debe optimizar el uso de los recursos financieros invertidos en la gestión de TI procurando el logro de los objetivos de esa inversión, controlando en forma efectiva dichos recursos y observando el marco jurídico que al efecto le resulte aplicable

IV. Gestión de Riesgos Tecnológicos

La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el marco normativo que le resulte aplicable.

La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución.

V. Arquitectura Empresarial

La Institución debe disponer de prácticas formales que permitan gestionar la arquitectura empresarial orientada la gestión de los procesos institucionales para promover la implementación de la estrategia organizacional, en el que se establezca la identificación formal de la estructura de datos clasificada según su nivel de criticidad y uso, la asociación de los procesos institucionales, de acuerdo con el uso de recursos tecnológicos (sistemas de información e infraestructura) para acceder, procesar y almacenar los datos e información.

La entidad debe contar con un modelo de arquitectura que permita visualizar adecuadamente la estructura de procesos institucionales y la relación de uso de recursos instalados (sistemas de información, infraestructura tecnológica) para gestionar los datos e información requeridos en la operativa. El órgano rector de Gobernanza en TI tiene la responsabilidad de establecer el modelo de arquitectura empresarial.

La institución debe disponer de un modelo de clasificación de datos e información, según criterios y requisitos legales, de valor, según el nivel de criticidad y susceptibilidad a divulgación o modificación no autorizada. La Unidad de TI se basará en este modelo para establecer las directrices de seguridad y protección de los datos e información institucionales.

VI. Calidad de los Procesos Tecnológicos

La institución debe implementar prácticas que permitan controlar los procesos organizacionales, posibilitando la mejora continua de productos y servicios, buscando asegurar la satisfacción de las necesidades institucionales, manteniendo estándares de documentación de los lineamientos requeridos, esquemas para la medición del desempeño y control sobre la vigencia de las prácticas aplicables a los procesos.

Igualmente, debe generar servicios de TI de conformidad con los requerimientos de los usuarios con base en un enfoque de eficiencia y mejoramiento continuo de los procesos que habilitan la gestión de las tecnologías de información.

VII. Recursos Humanos

La institución debe disponer de un proceso formal que le permita gestionar los recursos humanos de acuerdo con las necesidades institucionales, en apego a directrices y regulaciones según aplique. Las prácticas deben apoyar el reclutamiento, selección, contratación, inducción y capacitación continua según lo requerido. De igual forma, disponer de modelos que permitan la evaluación del desempeño de los funcionarios y la identificación de funcionarios con responsabilidades críticas y el desarrollo de habilidades en otros colegas que permitan sustituciones para asegurar la continuidad del servicio de las actividades principales.

La Unidad de TI debe constituirse con funcionarios que dispongan de un perfil técnico de acuerdo con sus responsabilidades, así como habilidades de gestión y administrativas que permitan realizar actividades requeridas para asegurar la gobernanza de las TI.

VIII. Contratación y Adquisiciones de Bienes y Servicios Tecnológicos

La institución debe disponer de prácticas formales para establecer los requerimientos de contratación y adquisición de bienes, consultorías y servicios a proveedores externos, cuyo giro de negocio sea orientado al ámbito tecnológico, de forma tal que apoye el desarrollo de iniciativas y mejoras de la infraestructura tecnológica, sistemas de información, seguridad de la información, ciberseguridad y otros relacionados de acuerdo con las necesidades y oportunidades visualizadas al nivel institucional. El modelo debe permitir establecer objetivamente al nivel operativo, técnico, legal y tecnológico entre otros, los términos de referencia, los parámetros de valoración del perfil del proveedor y su oferta para realizar la selección adecuada.

La Unidad de TI debe disponer y aplicar en forma consistente prácticas para la supervisión y evaluación a través de pruebas de aceptación y valoración del cumplimiento contractual en cuanto al servicio y desempeño en la implementación, configuración y administración de los recursos tecnológicos contratados a terceros.

IX. Gestión de Proyectos que implementan recursos tecnológicos

La institución debe gestionar los proyectos que permitan habilitar sus iniciativas para el logro de los objetivos estratégicos, satisfaciendo los requerimientos y en cumplimiento con términos de calidad, tiempo, presupuesto y uso óptimo de los recursos, de acuerdo con las buenas prácticas y estándares preestablecidos.

La Unidad de TI debe establecer el portafolio de proyectos debidamente priorizados, identificando en cada iniciativa el beneficio a generar por la habilitación de tecnologías de información. Su administración a través de la ejecución de los planes asociados, deben permitir obtener el resultado

esperado, minimizando el riesgo asociado a eventos durante la ejecución del proyecto y garantizando la calidad y la entrega de valor para el logro de los objetivos institucionales.

La Unidad de TI debe establecer un modelo estandarizado para la gestión y administración de proyectos de perfil tecnológico, así como su continua actualización, divulgación y capacitación a funcionarios.

X. Desarrollo, Implementación y Mantenimiento de Sistema de Información

La Unidad de TI debe aplicar prácticas formales que permitan ejecutar un proceso consistente para la definición de requerimientos, diseño, adquisición y/o desarrollo, realización de pruebas, migración de datos e información, aprobación, integración de conocimiento e inteligencia de negocios y puesta en marcha de las soluciones, con el fin de asegurar que la institución cuente con sistemas de información y aplicaciones que permitan gestionar adecuadamente la información requerida.

La Unidad de TI debe asegurar la disponibilidad de estándares para programación, gestión de la calidad del software en desarrollo o mantenimiento, cambios por excepción y/o emergencia, llevando un adecuado control de cambios y versiones.

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.

La Unidad de TI debe aplicar las prácticas de aseguramiento del cumplimiento contractual y las prácticas de calidad asociadas para los casos en utilice soluciones desarrolladas y/o implementadas por proveedores externos.

XI. Seguridad y Ciberseguridad

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

Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que 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 Institución, basada 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, lógica 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.

La Institución 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 institución debe implementar medidas de control asociadas a la administración del riesgo de seguridad de la información y ciberseguridad, que permitan el cumplimiento de los objetivos de los procesos, protegiendo la confidencialidad, autenticidad, privacidad e integridad de la información,

La Institución debe realizar una valoración de controles a implementar a través de una declaración de aplicabilidad, que permita contrarrestar los riesgos de seguridad de la información, incluyendo una valoración de madurez (medidas organizativas, técnicas o legales que se aplican) Así mismo, establecer e implementar los mecanismos que permitan contrastar los controles definidos contra los controles que se están aplicando.

La Institución debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios, contemplando contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales.

XII. Administración Infraestructura Tecnológica

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

La Unidad de TI debe establecer prácticas formales para la gestión de la entrega de servicios a través de los recursos tecnológicos instalados en la institución, administrados interna y externamente, gestionando la configuración y mantenimiento del desempeño y capacidad de los activos de TI, de manera que a través de monitoreos y actualizaciones se mantenga el uso óptimo de los recursos y brinden una garantía razonable sobre la continuidad de las operaciones institucionales, establecidos a través de niveles de operación y sostenibilidad para brindar los servicios requeridos.

La Unidad de TI debe disponer de una estructura formal que permita a las unidades usuarias gestionar solicitudes de nuevos servicios (mejoras, mantenimiento, inclusión), reportar incidencias que impacten en la operativa de los procesos; pudiendo ser atendidas y escaladas en un modelo de priorización de respuesta.

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.

XIII. Continuidad y Disponibilidad Operativa de los Servicios Tecnológicos

La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia 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 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.

XIV. Aseguramiento

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 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 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 tecnologías de información sobre los resultados de su gestión 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.

GLOSARIO

Activo - cualquier componente (humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área organizacional.

Activo de información intangible - son aquellos que soportan la información dentro de un activo material, y pueden inutilizar la información, pese a que el activo físico no haya sufrido daño alguno.

Activo de información tangible – recurso que las instituciones consideran importante o de alta validez para la misma, ya que puede contener información importante.

Activo de información material - activos tangibles que contienen información.

Arquitectura Empresarial – modelo integrador de la institución, que brinda una visión sistémica de la institución con enfoque en la tecnología y los negocios. El principal objetivo de la arquitectura empresarial es ayudar a la organización a gestionar procesos de negocio que promuevan la implementación de estrategias institucionales.

Clasificación de la información – ejercicio por medio del cual se determina que los datos e información pertenecen a uno de los niveles de clasificación estipulados en la Institución. Tiene como objetivo asegurar que la información recibe el nivel de protección, las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. La categorización de datos e información se debe realizar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Desempeño - grado de desenvolvimiento que una entidad cualquiera tiene con respecto a un fin esperado.

Evaluación de desempeño - proceso que se lleva a cabo para analizar si un individuo o proceso cumplió con los objetivos fijados.

Gobierno corporativo - conjunto de normas, principios y procedimientos que regulan la estructura y el funcionamiento de los órganos de gobierno de una institución. Establece las relaciones entre la junta directiva, el consejo de administración, los accionistas y el resto de partes interesadas, y estipula las reglas por las que se rige el proceso de toma de decisiones sobre la institución para la generación de valor.

Gobierno de TI - uno o varios procesos que permiten gestionar, administrar y operar de manera más eficiente las tecnologías de información en beneficio de toda la institución. El gobierno de Tecnologías de Información es uno de los elementos del gobierno corporativo, debe estar claramente establecida la autoridad y el modelo de gobierno, darse la ejecución de los proyectos según la dirección dada, realizarse la gestión operativa y estar integrado con las unidades institucionales.

Indicador de gestión - expresión cuantitativa del comportamiento y desempeño de un proceso, cuya magnitud, al ser comparada con algún nivel de referencia, puede estar señalando una desviación sobre la cual se toman acciones correctivas o preventivas según el caso.

Información - datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes de la institución. Asimismo, se refiere a un conjunto organizado de datos contenido en cualquier documento/elemento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Infraestructura Tecnológica - conjunto de elementos para el almacenamiento de los datos de una institución. En ella se incluye el hardware, el software, componentes de comunicación y los diferentes servicios necesarios para optimizar la gestión interna y seguridad de información.

Innovación tecnológica - hace referencia a las mejoras en productos, procesos o servicios que ya existen según los objetivos institucionales, que ofrezcan valor agregado, al actualizar los sistemas de información, renovar herramientas tecnológicas o maquinarias y equipos que permitan aumentar la competitividad de la institución, la gestión de cambios en organización y administración activa.

I&T – Información y Tecnología

Lineamientos – normas, modelos, planes y estándares normativos y técnicos que permiten identificar prácticas y acciones tangibles e intangibles, inmersas en las dimensiones de estrategia y estructura organizacional, procesos institucionales e información, liderazgo y cultura, así como las competencias y los equipos.

Métrica (véase indicador de gestión) - describe la calidad y requiere una base de medición; es aplicable para evaluar cumplimiento y efectividad de procesos y medir el éxito contra objetivos establecidos.

Proceso - secuencia de acciones que se llevan a cabo para lograr un fin determinado.

Propietario de la Información - parte designada de la institución, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente.

Riesgo - exposición a una situación donde hay una posibilidad de sufrir un daño o de estar en peligro. Es la vulnerabilidad o amenaza a que ocurra un evento y sus efectos sean negativos y que alguien o algo puedan verse afectados por él. Cuando se dice que un elemento está en riesgo, es porque se considera que se encuentra en desventaja frente a algo más, bien sea por su ubicación o posición; además de ser susceptible a recibir una amenaza sin importar cuál sea su índole.

TI - proceso que utiliza una combinación de medios y métodos de recopilación, procesamiento y transmisión de datos para obtener nueva información de calidad sobre el estado de un objeto, proceso o fenómeno. El propósito de la tecnología de la información es la producción de información para su análisis por las personas y la toma de decisiones sobre la base de esta para realizar una acción.

Unidad de TI - sector responsable de la administración de los recursos tecnológicos utilizados en una institución, relacionados al tratamiento, almacenamiento y protección de la información.

Valor público - el valor que los ciudadanos dan a los bienes y servicios recibidos del estado para satisfacer una necesidad con calidad y oportunidad.

FIN DEL DOCUMENTO

AGRADECIMEINTO

Equipo Nacional que realizaron la actualización de las Normas técnicas para la gestión y el control de las Tecnologías de Información-2022 propiamente en Seguridad y Ciberseguridad

Silvia Chinchilla Sáenz

Profesional experta en gobierno TI, gestión de riesgos de TI, estrategia corporativa, aseguramiento procesos de gestión TI, Auditoría de TI.

Como formación académica en: Ingeniería en Sistemas de Información, Maestría en Auditoría de Tecnologías de Información, Certificaciones profesionales de reconocimiento internacional en Auditoría de Tecnologías de Información, Gestión de Riesgos y Control sobre TI, Gobierno Empresarial de TI.

Con más de 25 años de experiencia profesional en auditoría interna y externa de tecnologías de información, asesoría en el mejoramiento de procesos aplicando buenas prácticas de gobierno y gestión de tecnologías de información, docencia y coordinación universitaria.

Miembro activo en los equipos de trabajo de ISACA al nivel local y Regional.

Dentro de mis áreas de conocimiento destacan:

- ✓ Auditoría de TI
- ✓ Gobernanza de TI
- ✓ Gestión de Riesgos Tecnológicos
- ✓ Aseguramiento de la gestión de tecnologías de Información
- ✓

Raúl Rivera

Ingeniero en Informática –Máster en Administración de Empresas con Énfasis en Finanzas – Máster en Telemática – Máster Profesional en Ciberseguridad Industrial

Profesional en Gestión de Riesgos & Ciberseguridad IT / OT, con más de 27 años de carrera profesional y experiencia en el sector financiero, servicios y de las tecnologías de la información y comunicación, el cual ha laborado para importantes empresas transnacionales como Hacer, Unisys, PwC, BAC Credomatic y Mastercard, compañía para la cual actualmente labora como Gerente de Productos de Cyber & Intelligence para Costa Rica & Nicaragua. Ha sido miembro de la Junta Directiva de ISACA Costa Rica, así como asesor y vocero en ciberseguridad para la Asociación Bancaria Costarricense. Lidera para Costa Rica el programa de Cybersecurity Nexus de ISACA y el Centro de Ciberseguridad Industrial de España. Ha colaborado para la Organización de Estados Americanos capacitando en Ciberseguridad a personal de gobiernos latinoamericanos, así como en el desarrollo de propuestas de políticas públicas para parlamentos latinoamericanos. Cuenta con más de 8 años de experiencia como conferencista internacional en Seguridad de la Información y Ciberseguridad, además de ser instructor acreditado por APMG Internacional para cursos oficiales de ISACA Global.

Cuenta con varias Certificaciones Internacionales, tales como;

CISA • CISM • CGEIT • CRISC • CDPSE • CSXF • CSXA • Cobit 5F • ITILF • ISO27001 AL • DFIR • KIKF • SFPC • RWVCPC • CSFPC

Luis Gorgona

Egresado de la carrera de Administración de Empresas del ITCR Profesional en ciberseguridad y seguridad de la información.

Cuenta con la acreditación CISA (Certified Information Systems Auditor) de ISACA

Cuenta con la certificación CDPSE (Certified Data Protection Solutions Engineer) también de ISACA.

Exdirector de seguridad de la información para Casa Presidencial (2006-2010)

•Ex instructor del programa de ciberseguridad del CICTE (Comité Interamericano contra el Terrorismo) y de REMJA (Red de ministerios de Justicia de las Américas, Ambos de la Organización de Estados Americanos.

Director de proyecto de la primera implementación de la Norma ISO 27001 en Centros de Datos de Hewlett Packard en los Estados Unidos de América 2011

Oficial de seguridad para la certificación ISO 27001 en el CenAm Center (Costa Rica-Panamá) para Hewlett Packard

Trabajó del 2015 al 2017 como encargado de gobernanza, riesgo y cumplimiento para la región de AMERICAS en McKinsey and Company. Encargado de la certificación ISO 27001 del centro de datos de McKinsey en New Jersey, Estados Unidos de América.

Ana Cecilia

Licenciada en Ciencias de la Computación e Informática de la Universidad de Costa Rica.
Máster en Auditoría de Tecnologías de Información.
Experiencia en Gestión de Riesgos y Seguridad de Centro de Informática de la Universidad de Costa Rica
Experiencia en la implementación de gestión de riesgos de TI y planes de continuidad del Centro de Informática de la Universidad de Costa Rica.
Elaboración de normativas de Directrices técnicas de seguridad de la información de la UCR
Colaboradora en el Marco de Gobierno y Gestión de CONARE y Universidades.
Coordinadora del equipo de implementación del Marco de Gobierno y gestión de TI UCR.