Formulario Matriz de Evaluación Auditoría Externa TI		Versión 1.0
Escrito por:	Aprobado por:	Fecha aprobación:
Comité Supervisores de TI	**Comité de Supervisión Consolidada**	**20-abr-17**

Contenido

Nombre	Descripción
Alcance:	Las disposiciones establecidas en este documento son aplicables a las entidades supervisadas por la SUGEF, SUPEN, SUGESE y SUGEVAL.
Definiciones:	**Tecnología de información (TI):** Acrónimo de Tecnologías de Información, definidas como el conjunto de técnicas para la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos de negocios, de manera que pueda ser organizada y utilizada en forma consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad, entre otros.
	Entidad supervisada: Entidad del sector financiero supervisada por un órgano supervisor costarricense
	Marco de Gestión de TI: Conjunto de procesos destinados a gestionar las tecnologías de información que la entidad supervisada debe adoptar como referencia para la gestión integral de sus riesgos tecnológicos, considerando su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos y la dependencia tecnológica que éstas tienen en procesos de TI.
	Proceso de negocio: Cadena de actividades que agregan valor y permiten la generación de un producto o servicio bajo determinadas condiciones y plazo.
Responsabilidades:	Es responsabilidad de la entidad supervisada suministrar este insumo a los encargados de la Auditoría Externa de TI en la forma y el plazo establecido en los Lineamientos Generales del Reglamento General de Gestión de Tecnología de Información.
Exoneración de responsabilidades:	Se exonera de responsabilidad a las superintendencias por cualquier cambio que la entidad o los encargados de las Auditorías Externas de TI realice a la estructura de la Matriz de Evaluación de la Auditoría Externa de TI.
Especificaciones generales:	Para efectos de una adecuada cumplimentación de la matriz se debe seguir lo establecido en la "Guía para completar la matriz de evaluación de Gestión TI" que se encuentra disponible en los sitios web de cada superintendencia.

Información General

DATOS DE LA ENTIDAD	NOMBRE COMPLETO	CÉDULA JURÍDICA

CONTRAPARTE EN LA ENTIDAD DURANTE LA AUDITORIA EXTERNA	NOMBRE COMPLETO	PUESTO	TELÉFONO	EXTENSIÓN	CORREO ELECTRÓNICO
PRINCIPAL					
SECUNDARIO					

PERIODO DE AUDITORÍA	FECHA DESDE	FECHA HASTA

EJECUCIÓN DE AUDITORÍA	FECHA DE INICIO	FECHA DE FIN	HORAS EFECTIVAS

DATOS DEL AUDITOR CISA	NOMBRE COMPLETO	EMPRESA	NÚMERO CISA

ENTREGA FINAL DEL INFORME	FECHA

RESULTADOS DE LA EVALUACIÓN

Criterios de Evaluación

La Gestión de Riesgos se califica como fuerte, aceptable, mejorable y débil, conforme el siguiente detalle:

Fuerte

Las características de la función tales como las responsabilidades, estructura, recursos, metodologías y prácticas, superan lo que se considera necesario, dada la naturaleza, complejidad, importancia sistémica y perfil de riesgo de la entidad, y su desempeño ha sido altamente efectivo y consistente. Las características y el desempeño de la función son superiores a las mejores prácticas utilizadas por la industria.

Aceptable

Las características de la función, tales como las responsabilidades, estructura, recursos, metodologías y prácticas, cumplen con lo necesario, dada la naturaleza, complejidad, importancia sistémica y perfil de riesgo de la entidad y su desempeño ha sido efectivo. Las características y el desempeño de la función cumplen con las mejores prácticas utilizadas por la industria.

Mejorable

Las características de la función, tales como las responsabilidades, estructura, recursos, metodologías y prácticas, generalmente cumplen con lo necesario, dada la naturaleza, complejidad, importancia sistémica y perfil de riesgo de la entidad. El desempeño de la función ha sido generalmente efectivo, pero existen áreas que necesitan mejoras. Esas mejoras no son suficientemente relevantes como para causar preocupaciones, siempre y cuando sean atendidas oportunamente. Las características y el desempeño no cumplen sistemáticamente con mejores prácticas utilizadas por la industria.

Débil

Las características de la función, tales como las responsabilidades, estructura, recursos, metodologías y prácticas, no cumplen de manera significativa con lo necesario, dada la naturaleza, complejidad, importancia sistémica y perfil de riesgo de la entidad. El desempeño de la función ha demostrado serias debilidades que necesitan ser atendidas de inmediato. Las características y el desempeño frecuentemente no cumplen con las mejores prácticas utilizadas por la industria.

IDENTIFICADOR	PROCESOS	DESCRIPCION
1.1	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Analizar y articular los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.
1.2	Asegurar la Entrega de Beneficios	Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a un costo aceptable.
1.3	Asegurar la Optimización del Riesgo	Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.
1.4	Asegurar la Optimización de Recursos	Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un costo óptimo.
1.5	Asegurar la Transparencia hacia las Partes Interesadas	Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.
2.1	Gestionar el Marco de Gestión de TI	Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.
2.2	Gestionar la Estrategia	Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.
2.3	Gestionar la Arquitectura Empresarial	Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costos potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.
2.4	Gestionar el portafolio de servicios	Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.
2.5	Gestionar el presupuesto y los costos	Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, costo y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costos a la empresa. Consultar a las partes interesadas para identificar y controlar los costos totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.
2.6	Gestionar los recursos humanos	Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.
2.7	Gestionar las relaciones entre TI y el negocio	Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.
2.8	Gestionar los acuerdos de niveles de servicio	Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.
2.9	Gestionar los servicios de los proveedores de TI	Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.
2.10	Gestionar la Calidad	Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.
2.11	Gestionar el riesgo de TI	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
2.12	Gestionar la seguridad	Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.
3.1	Gestionar programas y proyectos	Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.
3.2	Gestionar la definición de requerimientos	Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costos y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.
3.3	Gestionar la identificación y construcción de soluciones	Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.
3.4	Gestionar la disponibilidad y capacidad	Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costos. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.
3.5	Gestionar los cambios	Gestionar todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.
3.6	Gestionar la aceptación del cambio y la transición	Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.
3.7	Gestionar los activos de TI	Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un costo óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia.
3.8	Gestionar la configuración	Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarias para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.
4.1	Gestionar las operaciones	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.
4.2	Gestionar peticiones e incidentes de servicio	Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.

4.3	Gestionar los problemas	Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.
4.4	Gestionar la continuidad	Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.
4.5	Gestionar servicios de seguridad de la información	Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.
4.6	Gestionar controles de proceso de negocio	Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.
5.1	Supervisar, evaluar y valorar el rendimiento y la conformidad	Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.
5.2	Supervisar, evaluar y valorar el sistema de control interno	Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.
5.3	Supervisar, evaluar y valorar la conformidad con los requerimientos externos	Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
1.1	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno

Descripción del Proceso

Analizar y articular los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La evaluación del Sistema de Gobierno: asegurar que se Identifique y comprometa continuamente con las partes interesadas de la empresa, que se documente la comprensión de los requerimientos y se realice una estimación del actual y futuro diseño del gobierno de TI de la empresa.
2. La orientación del Sistema de Gobierno: asegurar que se informe a los líderes y obtengan su apoyo, su aceptación y su compromiso. Asimismo, garantizar que las estructuras, procesos y prácticas para el gobierno de TI estén en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno. Adicionalmente, asegurar que se defina la información necesaria para una toma de decisiones informadas.
3. La supervisión del Sistema de Gobierno: asegurar que se supervise la ejecución y la efectividad del gobierno de TI de la empresa. Asimismo, garantizar que se analice si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionen una supervisión apropiada de TI.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios

Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo

Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
1.2	Asegurar la Entrega de Beneficios

Descripción del Proceso
Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a un costo aceptable.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La evaluación de la optimización de valor: asegurar que se evalúe continuamente las inversiones, servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa y aportar valor a un coste razonable. Asimismo, garantizar que se Identifique y juzgue cualquier cambio en la dirección que necesita ser dada a la gestión para optimizar la creación de valor.

2. La orientación de la optimización de valor: asegurar que se orienten los principios y las prácticas de gestión de valor para posibilitar la realización del valor óptimo de las inversiones TI a lo largo de todo su ciclo de vida económico.

3. La supervisión de la optimización de valor: asegurar que se supervise los indicadores clave y sus métricas para determinar el grado en que el negocio está generando el valor y los beneficios previstos de los servicios e inversiones TI. Asimismo, garantizar que se identifiquen los problemas significativos y consideren las acciones correctivas.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios

Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo

Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
1.3	Asegurar la Optimización del Riesgo

Descripción del Proceso
Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La evaluación de la gestión de riesgos: asegurar que se examine y evalúe continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Asimismo, garantizar que si el apetito de riesgo de la empresa es apropiado y si el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.
2. La orientación de la gestión de riesgos: asegurar que se oriente el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo.
3. La supervisión de la gestión de riesgos: asegurar que se supervisen los objetivos y las métricas clave de los procesos de gestión de riesgo y que se establezca cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
1.4	Asegurar la Optimización de Recursos

Descripción del Proceso

Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un costo óptimo.

INFORMACIÓN REQUERIDA

Evaluación

Pendiente de Evaluar

Criterios de Evaluación

1. La evaluación de la gestión de recursos: asegurar que se examine y evalúe continuamente la necesidad actual y futura de los recursos relacionados con TI, las opciones para la asignación de recursos (incluyendo estrategias de aprovisionamiento) y los principios de asignación y gestión para cumplir de manera óptima con las necesidades de la empresa.
2. La orientación de la gestión de recursos: asegurar la adopción de principios de gestión de recursos para permitir un uso óptimo de los recursos de TI a lo largo de su completo ciclo de vida económica.
3. La supervisión de la gestión de recursos: asegurar que se supervisen los objetivos y métricas clave de los procesos de gestión de recursos y se establezca cómo serán identificados, seguidos e informados para su resolución las desviaciones o los problemas.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios

Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo

Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
1.5	Asegurar la Transparencia hacia las Partes Interesadas

Descripción del Proceso

Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.

INFORMACIÓN REQUERIDA

Evaluación

Pendiente de Evaluar

Criterios de Evaluación

1. La evaluación de los requisitos de elaboración de informes de las partes interesadas: asegurar que se examinen y verifiquen continuamente los requisitos actuales y futuros de comunicación con las partes interesadas y de la elaboración de informes, incluyendo tanto los requisitos obligatorios (p. ej. de regulación) de elaboración de informes como la comunicación a otros interesados. Asimismo, garantizar que se establezcan los principios de la comunicación.

2. La orientación de la comunicación con las partes interesadas y la elaboración de informes: asegurar que se garantice el establecimiento de una comunicación y una elaboración de informes eficaces, incluyendo mecanismos para asegurar la calidad y la completitud de la información, vigilar la elaboración obligatoria de informes y crear una estrategia de comunicación con las partes interesadas.

3. La supervisión de la comunicación con las partes interesadas: asegurar que se supervise la eficacia de la comunicación con las partes interesadas. Asimismo, se evalúen los mecanismos para asegurar la precisión, la fiabilidad y la eficacia y determinar si se están cumpliendo los requisitos de los diferentes interesados.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios

Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo

Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
2.1	Gestionar el Marco de Gestión de TI

Descripción del Proceso

Alinear los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos y las cuentas asociadas para que sean comprendidos por todos, con la identificación de las opciones estratégicas de TI, estructurados e integrados con los planes de negocio.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. El establecimiento de a estructura organizativa: asegurar que se establezca una estructura organizativa interna y extensa que refleje las necesidades del negocio y las prioridades de TI. Asimismo, garantizar que se implementen las estructuras de gestión requeridas (p. ej., comités) para permitir que la toma de decisiones se lleve a cabo de la forma más eficaz y eficiente posible.

2. El establecimiento de los roles y las responsabilidades: asegurar que se establezca, acuerde y comunique los roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades en las TI corporativas, que reflejen claramente las necesidades generales del negocio y los objetivos de TI, así como la autoridad, las responsabilidades y la rendición de cuentas del personal relevante.

3. El mantenimiento de los elementos catalizadores del sistema de gestión: asegurar que se mantengan elementos catalizadores del sistema de gestión y del entorno de control de la TI de la empresa y garantizar que están integrados y alineados con la filosofía y el estilo operativo de gobierno y de gestión de la empresa. Estos elementos catalizadores incluyen una comunicación clara de expectativas/requisitos. Asimismo, garantizar que el sistema de gestión fomente la cooperación interdepartamental y el trabajo en equipo, y promueva el cumplimiento y la mejora continua y trate las desviaciones en el proceso (incluidos los fallos).

4. La comunicación de los objetivos y la dirección de gestión: garantizar que se comunique la sensibilización y la comprensión de los objetivos y la dirección de TI a las partes interesadas y usuarios pertinentes a lo largo de toda la empresa.

5. La optimización de la ubicación de la función de TI: asegurar que se posicione la capacidad de TI en la estructura organizativa global para reflejar en el modelo de empresa la importancia de TI en la organización, especialmente su criticidad para la estrategia empresarial y el nivel de dependencia de TI. Asimismo, asegurar que la línea de reporte del CIO sea proporcional a la importancia de las TI en la empresa.

6. El establecimiento de la propiedad de la información (datos) y del sistema: garantizar que se defina y mantenga las responsabilidades de la propiedad de la información (datos) y los sistemas de información. Asimismo, asegurar que los propietarios tomen decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación.

7. La gestión de la mejora continua de los procesos: asegurar que se evalúe, planifique y ejecute la mejora continua de procesos y su madurez para garantizar que son capaces de entregarse conforme a los objetivos de la empresa, de gobierno, de gestión y de control. Asimismo, asegurar que se consideren las directrices de la implementación de procesos , estándares emergentes, requerimientos de cumplimiento, oportunidades de automatización y la realimentación de los usuarios de los procesos, el equipo del proceso y otras partes interesadas. Adicionalmente, garantizar que se actualicen los procesos y se considere el impacto en los catalizadores del proceso.

8. El mantenimiento del cumplimiento con las políticas y procedimientos: asegurar que se ponga en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Asimismo, garantizar que se sigan las tendencias y el rendimiento y sean considerados en el diseño futuro y la mejora del marco de control.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
2.2	Gestionar la Estrategia

Descripción del Proceso

Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La comprensión de la Dirección de la empresa: asegurar que se considere el entorno actual y los procesos de negocio de la empresa, así como la estrategia y los objetivos futuros de la compañía. Asimismo, garantizar que se tome también en cuenta el entorno externo a ella (motivadores de la industria, reglamentos relevantes, bases para la competencia).

2. La evaluación del entorno, capacidades y rendimiento actuales: asegurar que se evalúe el rendimiento del negocio interno actual y las capacidades de TI y los servicios externos de TI para desarrollar un entendimiento de la arquitectura empresarial en relación con TI. Asimismo, garantizar que se identifiquen los problemas que se están experimentando y generen recomendaciones en las áreas que pueden beneficiarse de estas mejoras. Adicionalmente, asegurar que consideren los aspectos diferenciadores y las opciones de proveedores de servicios y el impacto financiero, los costes y los beneficios potenciales de utilizar servicios externos.

3. El establecimiento del objetivo de las capacidades de TI: asegurar que se defina el objetivo del negocio, las capacidades de TI y los servicios de TI necesarios. Asimismo, garantizar que este basado en el entendimiento del entorno empresarial y sus necesidades; la evaluación de los actuales procesos de negocio, el entorno de TI y los problemas presentados; considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes o propuestas de innovación.

4. La realización del análisis de diferencias: asegurar que se identifiquen las diferencias entre el entorno actual y el deseado y considerar la alineación de activos (las capacidades que soportan los servicios) con los resultados de negocio para optimizar la inversión y la utilización de la base de activos internos y externos. Asimismo, garantizar que se consideren los factores críticos de éxito que apoyan la ejecución de la estrategia.

5. El establecimiento del plan estratégico y la hoja de ruta: asegurar que se cree un plan estratégico que defina, en cooperación con las partes interesadas más relevantes, cómo los objetivos de TI contribuirán a los objetivos estratégicos de la empresa. Asimismo, garantizar que se incluya cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, servicios y activos de TI. Adicionalmente, asegurar que se orienten las tecnologías para definir las iniciativas que se requieren para cerrar las diferencias, la estrategia de abastecimiento y las medidas que se utilizarán para supervisar el logro de los objetivos, para dar prioridad a las iniciativas y combinarlas en una hoja de ruta a alto nivel.

6. La comunicación de la estrategia y la dirección de TI: asegurar que se cree conciencia y comprensión del negocio y de los objetivos y dirección de TI, como se encuentra reflejada en la estrategia de TI, a través de comunicaciones a las partes interesadas adecuadas y a los usuarios de toda la empresa.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios

Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo

Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
2.3	Gestionar la Arquitectura Empresarial

Descripción del Proceso

Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costos potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. El desarrollo de la visión de la arquitectura de empresa: asegurar que la visión de la arquitectura proporcione una primera descripción de alto nivel de las arquitecturas de partida y objetivo, cubriendo los dominios de negocio, información, datos, aplicaciones y tecnología. La visión de la arquitectura proporciona al promotor la herramienta clave para vender los beneficios de la capacidad propuesta a las partes interesadas de la empresa. La visión de la arquitectura de información describe como nuevas capacidades permitirán alcanzar las metas de la empresa y los objetivos estratégicos y considera la preocupaciones de las partes interesadas en su implementación.

2. El establecimiento de la arquitectura de referencia: asegurar que la arquitectura de referencia describa la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.

3. La selección de las oportunidades y las soluciones: asegurar la racionalización de las desviaciones entre las arquitecturas de referencia y objetivo, considerando tanto la perspectiva técnica como la del negocio y agrupándolos a ambos en paquetes de trabajo del proyecto. Asimismo, que se integre el proyecto con todos los programas de inversión relacionados con TI para asegurar que las iniciativas relacionadas con la arquitectura estén alineadas y que estas iniciativas sean parte del cambio general en la empresa. Adicionalmente, garantizar que se haga de ello un esfuerzo en colaboración con las partes interesadas clave de la empresa y en TI para evaluar el grado de preparación de la empresa para su transformación e identificar las oportunidades, soluciones y todas las restricciones de la implementación.

4. El establecimiento de la implementación de la arquitectura: asegurar que se cree un plan de implementación y de migración viable acorde con la cartera de proyectos y programas. Asegurar que el plan está coordinado de cerca para garantizar que se proporciona el valor y que se disponen de los recursos necesarios para finalizar los trabajos.

5. La provisión de los servicios de arquitectura empresarial: asegurar que la provisión de los servicios de arquitectura empresarial incluya las guías y supervisión de los proyectos a implementar, la formalización de las maneras de trabajar mediante los contratos de arquitectura, la medición y comunicación de los valores aportados por la arquitectura y la supervisión del cumplimiento.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
2.4	Gestionar el portafolio de servicios

Descripción del Proceso

Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. El establecimiento de la mezcla del objetivo de inversión: asegurar que se revise y garantice la claridad de las estrategias y servicios actuales corporativos y de TI. Asimismo, garantizar que se defina una adecuada mezcla de inversión, basada en los costes, la alineación con la estrategia y medidas financieras, tales como coste, retorno de inversión esperado a lo largo de todo el ciclo de vida económico, grado de riesgo y tipo de beneficio para los programas del portafolio. Adicionalmente, garantizar que se ajusten las estrategias corporativas y de TI cuando sea necesario.

2. La determinación de la disponibilidad y las fuentes de fondos: asegurar que se determinen las fuentes potenciales de fondos, diferentes opciones de financiación y las implicaciones de las fuentes de financiación sobre las expectativas del retorno de inversión.

3. La evaluación y selección de los programas a financiar: asegurar basado en los requisitos de la mezcla general del portafolio de inversión, se evalúe y priorice casos de negocio de programas y decidan sobre las propuestas de inversión. Asimismo, garantizar que se dediquen fondos e inicien los programas.

4. La supervisión y optimización del rendimiento del portafolio de inversiones: asegurar que regularmente, se supervise y optimice el rendimiento del portafolio de inversiones y de los programas individuales a lo largo de todo el ciclo de vida de inversión.

5. La mantención de los portafolios: asegurar que se mantengan los portafolios de programas y proyectos de inversión, servicios de TI y activos de TI.

6. La gestión de la consecución de beneficios: asegurar que se supervisen los beneficios de proporcionar y mantener servicios y capacidades TI apropiadas, basadas en el caso de negocio acordado actual.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
2.5	Gestionar el presupuesto y los costos

Descripción del Proceso

Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, costo y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costos a la empresa. Consultar a las partes interesadas para identificar y controlar los costos totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1.La gestión de las finanzas y la contabilidad: asegurar que se establezca y mantenga un método de contabilización para todos los costes, inversiones y depreciaciones relacionadas con las TI, como parte integral de los sistemas financieros empresariales y el plan de cuentas para administrar las inversiones y los costes de TI. Asimismo, garantizar que se capturen y asignen los costes reales, se analicen las desviaciones entre las previsiones y los costes reales, e informen usando los sistemas empresariales de medición financiera.

2. La priorización de la asignación de recursos: asegurar se implemente un proceso de toma de decisiones para priorizar la asignación de recursos y definir las reglas para las inversiones discrecionales por parte de unidades de negocio individuales. Asimismo, garantizar que se Incluya el uso potencial de proveedores de servicio externos y se consideren las opciones de compra, desarrollo y alquiler.

3. La creación y mantención de los presupuestos: asegurar que se prepare un presupuesto que refleje las prioridades de inversión que apoyen los objetivos estratégicos basado en la cartera de programas habilitados por TI y servicios de TI.

4. La asignación del modelo de costes: asegurar que se establezca y utilice un modelo de costes de TI basado en la definición del servicio, que asegure que la asignación de costes de los servicios es identificable, medible y predecible, que fomente el uso responsable de los recursos, incluyendo aquellos proporcionados por proveedores de servicio. Asimismo, se garantice que se revise regularmente y se compare la idoneidad del modelo de costes/prorrateo de costes para que se mantenga su pertinencia y adecuación al negocio en evolución y las actividades de TI que le dan soporte.

5. La gestión de costes: asegurar que se implemente un proceso de gestión de costes comparando los costes reales con los presupuestos. Asimismo, garantizar que los costes sean supervisados y comunicados y, en el caso de desviaciones, identificados oportunamente, así como evaluado su impacto en los procesos y servicios empresariales.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
2.6	Gestionar los recursos humanos

Descripción del Proceso

Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. El mantenimiento de la dotación de personal suficiente y adecuada: asegurar que se evalúen las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos empresariales. Asimismo, garantizar que el personal incluya recursos tanto internos como externos.

2. La identificación del personal clave de TI: asegurar que se identifique el personal clave de TI a la vez que se reduzca al mínimo la dependencia de una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión y el respaldo (backup) del personal.

3. El mantenimiento de las habilidades y competencias del personal: asegurar que se defina y gestionen las habilidades y competencias necesarias del personal. Asimismo, garantizar que se verifique regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y se verifique que estas competencias se mantengan, con programas de capacitación y certificación en su caso. Adicionalmente, garantizar que se proporcione a los empleados aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales.

4. La evaluación del desempeño laboral de los empleados: asegurar que se **l**leven a cabo oportunamente evaluaciones de rendimiento de manera regular respecto a los objetivos individuales derivados de los objetivos de la empresa, las normas establecidas, las responsabilidades específicas del trabajo y el marco de habilidades y competencias. Asimismo, garantizar que los empleados reciban preparación sobre el desempeño y conducta siempre que sea apropiado.

5. La planificación y seguimiento del uso de recursos humanos de TI y del negocio: asegurar que se comprenda y realice un seguimiento de la demanda actual y futura de recursos humanos para el negocio y TI con responsabilidades en TI corporativa. Asimismo, garantizar que se identifiquen las carencias y proporcionen datos de entrada a los planes de aprovisionamiento, planes de abastecimiento de procesos de contratación del negocio y de TI y procesos de contratación del negocio y de TI.

6. La gestión del personal contratado: asegurar que los consultores y el personal contratado que apoyan a la empresa con capacidades de TI, conocen y cumplen las políticas de la organización así como los requisitos contractuales previamente acordados.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios

Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo

Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
2.7	Gestionar las relaciones entre TI y el negocio

Descripción del Proceso

Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. El entendimiento de las expectativas del negocio: asegurar que se entienda el enfoque y expectativas actuales del negocio para TI. Asimismo, asegurar que los requisitos son entendidos, gestionados y comunicados y su estado acordado y aprobado.
2. La identificación de las oportunidades, riesgos y limitaciones de TI para mejorar el negocio: asegurar que se identifiquen oportunidades potenciales para que la TI sea catalizadora de la mejora del rendimiento empresarial.
3. La gestión de las relaciones con el negocio: asegurar que se gestione la relación con los clientes (representantes del negocio). Asimismo, asegurar que los roles y responsabilidades de la relación están definidos, asignados y se facilita la comunicación.
4. La coordinación y comunicación: asegurar que se trabaje con las partes interesadas y se coordine de extremo a extremo la entrega de los servicios TI y las soluciones proporcionadas al negocio.
5. La provisión de los datos de entrada para la mejora continua de los servicios: asegurar que se mejore y evolucione continuamente los servicios basados en TI y la entrega del servicio a la empresa para alinearlos con unos cambiantes requisitos de empresa y tecnológicos.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
2.8	Gestionar los acuerdos de niveles de servicio

Descripción del Proceso

Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La identificación de los servicios de TI: asegurar que se analicen los requisitos del negocio y el modo en que los servicios TI y los niveles de servicio soportan los procesos de negocio. Asimismo, garantizar que se discuta y acuerden servicios potenciales y niveles de servicio con el negocio y que sean comparados con la cartera actual para identificar servicios nuevos o modificados, u opciones de nivel de servicio.

2. El catalogo de servicios basados en TI: asegurar que se definan y mantengan uno o más catálogos de servicios para grupos de clientes objetivo relevantes. Asimismo, garantizar que se publiquen y mantengan los servicios TI activos en los catálogos.

3. La definición y preparación de los acuerdos de servicio: asegurar que se definan y preparen los acuerdos de servicio basándose en las opciones de los catálogos de servicio. Asimismo, garantizar que se incluyan acuerdos de nivel de operaciones interno.

4. La supervisión y comunicación de los niveles de servicio: asegurar que se supervisen los niveles de servicio, se informe de las mejoras y se identifiquen tendencias. Asimismo, garantizar que se proporcione información de gestión adecuada para ayudar a la gestión del rendimiento.

5. La revisión de los acuerdos de servicio y contratos: asegurar que se lleven a cabo revisiones periódicas de los acuerdos de servicio y sean revisados cuando sea necesario.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios

Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo

Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
2.9	Gestionar los servicios de los proveedores de TI

Descripción del Proceso

Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La identificación y evaluación de las relaciones y contratos con proveedores: asegurar que se identifiquen proveedores y contratos asociados y se categoricen por tipo, relevancia y criticidad. Asimismo, garantizar que se establezca un criterio de evaluación de contratos y proveedores y se evalúe la cartera general de proveedores y contratos actuales y alternativos.
2. La selección de los proveedores: asegurar que se seleccionen proveedores de acuerdo a prácticas justas y formales que aseguren la selección del que mejor se adapte a los requisitos. Asimismo, garantizar que los requisitos sean optimizados con las aportaciones de nuevos proveedores potenciales.
3. La gestión de los contratos y relaciones con proveedores: asegurar que se formalice y gestionen las relaciones con cada proveedor. Asimismo, garantizar que se gestione, mantenga y supervisen los contratos y la entrega de servicios. Asegurar que los nuevos contratos o los cambios son conformes a las normas de la empresa, las leyes y las regulaciones. Adicionalmente, garantizar que se gestionen los conflictos contractuales.
4. La gestión del riesgo en el suministro: asegurar que se identifiquen y gestionen los riesgos relacionados con la capacidad de los proveedores de proporcionar de manera continua una entrega del servicio segura, eficaz y eficiente.
5. La supervisión del cumplimiento y el rendimiento del proveedor: asegurar que se revise periódicamente el rendimiento general de los proveedores, el cumplimiento con los requisitos contractuales y el valor de lo pagado y se traten las incidencias identificadas.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
2.10	Gestionar la Calidad

Descripción del Proceso
Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. El establecimiento de un sistema de gestión de la calidad (SGC): asegurar que haya una aproximación a la gestión de la calidad para la información, la tecnología y los procesos de negocio que sea continua, estandarizada, formal y que esté alineada con los requerimientos del negocio y con la gestión de la calidad a nivel corporativo.

2. La definición y gestión de los estándares, procesos y prácticas de calidad: asegurar que se Identifiquen y mantengan los requisitos, normas, procedimientos y prácticas de los procesos clave para orientar a la organización en el cumplimiento del SGC. Asimismo, garantizar que este en consonancia con los requisitos del marco de control TI. Adicionalmente, garantizar que se considere la posibilidad de certificar los procesos, las unidades de la organización, los productos o los servicios clave.

3. El enfoque de la gestión de la calidad en los clientes: asegurar que se enfoque la gestión de la calidad en los clientes, mediante la determinación de sus necesidades y se asegure el alineamiento con las prácticas de gestión de calidad.

4. La supervisión de los controles y revisiones de la calidad: asegurar que se supervise la calidad de los procesos y servicios de forma permanente como se defina en el SGC. Asimismo, garantizar que se defina, planifique y apliquen medidas para supervisar la satisfacción del cliente con la calidad, así como el valor que proporciona el SGC. Adicionalmente, asegurar que la información recogida sea utilizada por los propietarios de los procesos para mejorar la calidad.

5. La integración de la gestión de la calidad en la implementación de soluciones y la entrega de servicios: asegurar que se incorporen las prácticas pertinentes de gestión de la calidad en la definición, supervisión, notificación y gestión continua de los desarrollo de soluciones y los servicios ofrecidos.

6. La mantención de una mejora continua: asegurar que se mantenga y comunique regularmente un plan de la calidad global que promueva la mejora continua. Asimismo, garantizar que se incluya la necesidad y los beneficios de una mejora continua y que se recoja y analicen datos sobre el SGC y mejore su eficacia. Adicionalmente, asegurar que se corrijan las no conformidades para prevenir la recurrencia y se promueva una cultura de mejora continua de la calidad.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
2.11	Gestionar el riesgo de TI

Descripción del Proceso
Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La recopilación de datos: asegurar que se identifiquen y recopilen datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.
2. El análisis del riesgo: asegurar que se desarrolle información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.
3. La mantención del perfil de riesgo: asegurar que se mantenga un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.
4. La comunicación del riesgo: asegurar que se proporcione información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.
5. La definición del portafolio de acciones para la gestión de riesgos: asegurar que se gestionen las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.
6. La respuesta al riesgo: asegurar que se responda de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
2.12	Gestionar la seguridad

Descripción del Proceso
Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. El establecimiento y mantención de un SGSI: asegurar que se establezca y mantenga un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que se encuentre alineado con los requerimientos de negocio y la gestión de seguridad en la entidad.

2. La definición y gestión del plan de tratamiento del riesgo de la seguridad de la información: asegurar que se mantenga un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asimismo, garantizar que las recomendaciones para implementar las mejoras en seguridad se basen en casos de negocio aprobados, se implementen como parte integral del desarrollo de soluciones y servicios y se operen, después, como parte integral de las operaciones del negocio.

3. La supervisión y revisión del SGSI: asegurar que se mantenga y comunique regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Asimismo, garantizar se recolecte y analicen datos sobre el SGSI y la mejora de su efectividad. Adicionalmente, asegurar que se corrijan las no conformidades para prevenir recurrencias y se promueva una cultura de seguridad y de mejora continua.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios

Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo

Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
3.1	Gestionar programas y proyectos

Descripción del Proceso

Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. El mantenimiento de un enfoque estándar para la gestión de programas y proyectos: asegurar que se mantenga un enfoque estándar para la gestión de programas y proyectos que posibilite revisiones y tomas de decisión de gobierno y de gestión y actividades de gestión de la entrega, enfocadas en la consecución de valor y de objetivos (requisitos, riesgos, costos, cronograma y calidad) para el negocio de una forma consistente.

2. El inicio del programa: asegurar que se inicie un programa para confirmar los beneficios esperados y para obtener la autorización para proceder. Esto incluye los acuerdos sobre el patrocinio del programa, confirmar el mandato del programa a través de la aprobación del caso de negocio conceptual, designar a los consejeros o los miembros del comité del programa, generar el expediente del programa, revisar y actualizar el caso de negocio, desarrollar un plan de realización de beneficios y obtener la aprobación de los patrocinadores para empezar.

3. La gestión del compromiso de las partes interesadas: asegurar que se gestione el compromiso de las partes interesadas que garantice un intercambio activo de información precisa, consistente y oportuna, que llegue a todos las partes interesadas relevantes. Esto incluye la planificación, identificación y el compromiso de las partes interesadas y la gestión de sus expectativas.

4. El desarrollo y mantenimiento del plan de programa: asegurar que se formule un programa para definir las bases iniciales y posicionarlo para una ejecución exitosa mediante la formalización del alcance del trabajo a ser efectuado e identificando los entregables que satisfarán sus objetivos y la entrega de valor. Asimismo, garantizar que se mantenga y actualice el plan del programa y el caso de negocio a lo largo del ciclo de vida económico completo del programa, asegurando el alineamiento con los objetivos estratégicos y reflejando el estado actual y los conocimientos obtenidos hasta el momento.

5. La ejecución del programa: asegurar que se lance y ejecute el programa para adquirir y dirigir los recursos necesarios para lograr las metas y beneficios definidos en el plan del programa. Asimismo, garantizar de acuerdo con los criterios de revisión de lanzamiento o cambio de fase (stage-gate), se preparen los cambios de fase, las revisiones de las iteraciones o versiones para informar del progreso del programa y se establezcan los fundamentos para la financiación de la siguiente etapa después de la

informar del progreso del programa y se establezcan los fundamentos para la financiación de la siguiente etapa después de la revisión del lanzamiento o de cambio de fase (stage-gate).

6. La supervisión, control y comunicación de los resultados del programa: asegurar que se supervise y se controle el rendimiento del programa (entrega de soluciones) y de la organización (valor/resultado) versus el plan durante el ciclo de vida económico completo de la inversión. Asimismo, garantizar que se informe del rendimiento al comité estratégico del programa y a los patrocinadores.

7. El lanzamiento e inicio de proyectos dentro de un programa: asegurar que se defina y documente la naturaleza y alcance del proyecto para confirmar y desarrollar entre las partes interesadas un entendimiento común o el alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa general de inversiones de TI. Asimismo, garantizar que la definición esté formalmente aprobada por el patrocinador del programa y del proyecto.

8. La planificación de proyectos: asegurar que se establezca y mantenga un plan de proyecto formal, aprobado e integrado (que cubra los recursos del negocio y de TI), para guiar la ejecución del proyecto y controlarlo durante toda su vida. Asimidmo, garantizar que el alcance de los proyectos esté claramente definido y vinculado claramente a la construcción o aumento de la capacidad del negocio.

9. La gestión de la calidad de los programas y proyectos: asegurar que se prepare y ejecute un plan y procesos y prácticas de gestión de la calidad, alineadas al SGC que describe el enfoque de calidad del programa y el proyecto y cómo será implementado. Asimismo, garantizar que el plan esté formalmente revisado y acordado por todas las partes afectadas y, después, incorporado en los planes integrados del programa y los proyectos.

10. La gestión del riesgo de los programas y proyectos: asegurar que se elimine o minimice los riesgos específicos asociados con los programas y proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta, supervisión y control de las áreas o eventos que tienen el potencial de causar cambios no deseados. Asimismo, garantizar que los riesgos enfrentados por la administración del programa y los proyectos sean establecidos y registrados en un único punto.

11. La supervisión y control de proyectos: asegurar que se mida el desempeño del proyecto versus los criterios clave de rendimiento del proyecto, tales como la planificación, la calidad, el costo y los riesgos. Asimismo,garantizar que se evalue el impacto de las desviaciones en el proyecto y el programa general y se informe los resultados a las partes interesadas clave.

12. La gestión de los recursos y los paquetes de trabajo del proyecto: asegurar que se gestionen los paquetes de trabajo mediante requerimientos formales de autorización y aceptación de los paquetes de trabajo, y asignando y coordinado los recursos de negocio y de TI adecuados.

13. El cierre de un proyecto o iteración: asegurar que se solicite a las partes interesadas del proyecto, al final de cada proyecto, versión o iteración, que evalúen si el proyecto, la versión o la iteración entregaron los resultados y valor planeados. Asimismo, garantizar que se identifique y comunique cualquier actividad pendiente necesaria para lograr los resultados del proyecto y los beneficios del programa planeados, que se identifique y documenten las lecciones aprendidas para futuros proyectos, versiones, iteraciones y programas.

14. El cierre de un programa: asegurar que se elimine el programa del portafolio de inversiones activas cuando haya acuerdo de que el valor deseado ha sido logrado o cuando esté claro que no será logrado con los criterios de valor establecidos para el programa.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
3.2	Gestionar la definición de requerimientos

Descripción del Proceso

Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costos y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La definición y mantención de los requerimientos técnicos y funcionales de negocio: asegurar que se basen en un caso de negocio, para identificar, priorizar, especificar y acordar los requerimientos de información de negocio, funcionales, técnicos y de control que cubra el alcance/entendimiento de todas las iniciativas necesarias para alcanzar los resultados esperados de la solución de negocio de TI propuesta.

2. La realización de un estudio de viabilidad y soluciones alternativas: asegurar que se realice un estudio de viabilidad de las potenciales soluciones alternativas, evaluando su viabilidad y seleccionando la opción preferida. Asimismo, si se considera, garantizar que se implemente la opción seleccionada como un piloto para determinar posibles mejoras.

3. La gestión de los riesgos de los requerimientos: asegurar que se identifique, documente, priorice y mitiguen los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa y solución propuesta.

4. La obtención de la aprobación de los requerimientos y soluciones: asegurar que se coordine la realimentación de las partes interesadas afectadas y, en las fases clave predeterminadas, se obtenga la aprobación y la firma del patrocinador o propietario del producto y cierre de los requerimientos técnicos y funcionales, de los estudios de viabilidad, de los análisis de riesgos y de las soluciones recomendadas.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
3.3	Gestionar la identificación y construcción de soluciones

Descripción del Proceso

Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. El diseño de las soluciones de alto nivel: asegurar se desarrolle y documenten diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas. Asegurar que haya un alineamiento con la estrategia TI y la arquitectura empresarial. Asimismo, garantizar que se revalore y actualicen los diseños cuando sucedan cuestiones significativas durante las fases de diseño detallado o de construcción o según la solución evolucione y asegurar que las partes interesadas participen activamente en el diseño y en la aprobación de cada versión.

2. El diseño de los componentes detallados de la solución: asegurar que se desarrollen, documenten y elaboren diseños detallados progresivamente usando técnicas de desarrollo ágiles o por fases acordadas previamente considerando todos los componentes (procesos de negocio y automatización relacionada y controles manuales, aplicaciones soporte de TI, servicios de infraestructura y productos tecnológicos y proveedores/fabricantes). Asimismo, asegurar que el diseño detallado incluya los acuerdos de niveles de servicio (SLA) y acuerdos de servicio entre áreas (OLA) internos y externos

3. El desarrollo de los componentes de la solución: asegurar que se desarrollen los componentes de la solución progresivamente conforme el diseño detallado siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación. Asimismo, asegurar que se consideren todos los requerimientos de control en los procesos de negocio, soportando las aplicaciones TI y servicios de infraestructura, productos tecnológicos, servicios y proveedores/suministradores.

4. La obtención de los componentes de la solución: asegurar que se obtengan los componentes de la solución sobre la base del plan de adquisiciones y conforme a los requerimientos y diseños detallados, principios de arquitectura y estándares y en los procedimientos generales contractuales y de adquisiciones de la empresa, requerimientos de calidad (QA) y aprobación de estándares. Asimismo, asegurar que todos los requerimientos legales y contractuales son identificados y cumplidos por el proveedor.

5. La construcción de soluciones: asegurar que se instalen y configuren las soluciones y se integren con las actividades de

los procesos de negocio. Asimismo, garantizar que se implementen controles, medidas de seguridad y 'auditabilidad' durante la configuración y durante la integración del hardware e infraestructura del software para proteger los recursos y se asegure la disponibilidad e integridad de los datos. Adicionalmente, garantizar que se actualice el catálogo de servicios para reflejar la nueva situación.

6. La realización de los controles de calidad: asegurar que se desarrolle y ejecute un plan de calidad (QA) alineado con el SGC para obtener la calidad especificada en la definición de los requerimientos y de acuerdo a las políticas y procedimientos de calidad de la empresa.

7. La preparación de pruebas de la solución: asegurar que se establezca un plan de pruebas y entornos necesarios para probar los componentes individualmente y de la solución integrada incluyendo los procesos de negocio y servicios, aplicaciones e infraestructura que los soportan.

8. La ejecución de pruebas de la solución: asegurar que se ejecuten pruebas continuamente durante el desarrollo, incluyendo pruebas de control, en concordancia con el plan de pruebas y con las prácticas de desarrollo en el entono apropiado. Asimismo, garantizar que se hagan partícipes a los dueños de los procesos de negocio y usuarios finales en el equipo de pruebas. Adicionalmente, asegurar que se identifique, registre y prioricen los errores e incidentes identificados durante las pruebas.

9. La gestión de cambios a los requerimientos: asegurar que se haga un seguimiento del estado de los requerimientos individuales (incluyendo todos los requerimientos rechazados) a través de todo el ciclo de vida del proyecto y gestionar la aprobación de los cambios a los requerimientos.

10. La mantención de las soluciones: asegurar que se desarrolle y ejecute un plan para el mantenimiento de la solución y componentes de la infraestructura. Asimismo, garantizar que se incluyan revisiones periódicas respecto a las necesidades de negocio y requerimientos operacionales.

11. La definición de los servicios TI y mantención del catálogo de servicios: asegurar que se defina y acuerden nuevos servicios TI o cambios y opciones de nivel de servicio. Asimismo, garantizar que se documenten nuevas definiciones o cambios en los servicios y opciones de nivel de servicio que serán actualizadas en el catálogo de servicios.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios

Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
3.4	Gestionar la disponibilidad y capacidad

Descripción del Proceso

Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costos. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La evaluación de la disponibilidad, rendimiento, capacidad actual y creación de una línea de referencia: garantizar que se evalúe la disponibilidad, el rendimiento y la capacidad de los servicios y recursos para asegurar que se encuentra disponible una capacidad y un rendimiento justificables en costos para dar soporte a las necesidades del negocio y para entregar el servicio de acuerdo a los acuerdos de nivel de servicio (SLA). Asimismo, garantizar que se creen líneas de referencia para la disponibilidad, el rendimiento y la capacidad para comparaciones futuras.

2. La evaluación del impacto en el negocio: asegurar que se identifiquen los servicios importantes para la empresa, mapear los servicios y recursos con los procesos de negocio e identifiquen las dependencias del negocio. Asegurar que el impacto de la indisponibilidad de recursos está acordado y aceptado por el cliente. Asegurar que, para las funciones vitales del negocio, los requisitos de disponibilidad definidos en el acuerdo de nivel de servicio (SLA) pueden ser satisfechos.

3. La planificación de los requisitos de servicios nuevos o modificados: asegurar se planifique y prioricen las implicaciones en la disponibilidad, el rendimiento y la capacidad de cambios en las necesidades del negocio y en los requerimientos de servicio.

4. La supervisión y revisión de la disponibilidad y la capacidad: asegurar que se supervise, mida, analice, informe y revise la disponibilidad, el rendimiento y la capacidad. Asimismo, garantizar que se identifiquen desviaciones respecto a las líneas de referencia establecidas. Adicionalmente, garantizar se revisen informes de análisis de tendencias identificando cualquier cuestión y variación significativa, iniciando acciones donde sea necesario y asegurando que se realiza el seguimiento de todas las cuestiones pendientes.

5. La investigación y abordaje de las cuestiones de disponibilidad, rendimiento y capacidad: asegurar que se aborden las desviaciones investigando y resolviendo las cuestiones identificadas relativas a disponibilidad, rendimiento y capacidad.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
3.5	Gestionar los cambios

Descripción del Proceso

Gestionar todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La evaluación, priorización y autorización de las peticiones de cambio: asegurar que se evalúen todas las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI, y se analice si el cambio afectará negativamente al entorno operativo e introducirá un riesgo inaceptable. Asegurar que los cambios son registrados, priorizados, categorizados, analizados, autorizados, planificados y programados.

2. La gestión de cambios de emergencia: asegurar que se gestione cuidadosamente los cambios de emergencia para minimizar futuras incidencias y asegurar que el cambio está controlado y se realiza de forma segura. Asimismo, garantizar que se verifique que los cambios de emergencia son evaluados debidamente y autorizados una vez hecho el cambio.

3. El seguimiento y comunicación de los cambios de estado: asegurar que se mantenga un sistema de seguimiento e informe que documente los cambios rechazados, comunique el estado de cambios aprobados y en proceso y de cambios completados. Asegurar que los cambios aprobados son implementados como esté previsto.

4. El cierre y documentación de los cambios: Siempre que el cambio haya sido implementado, asegurar que se actualice, de manera consecuente, la documentación de la solución y del usuario, así como los procedimientos a los que afecta el cambio.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
3.6	Gestionar la aceptación del cambio y la transición

Descripción del Proceso

Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. El establecimiento de un plan de implementación: asegurar que se establezca un plan de implementación que cubra la conversión de datos y sistemas, criterios de aceptación de las pruebas, comunicación, formación, preparación del lanzamiento, paso a producción, soporte inicial en producción, plan de marcha atrás o de contingencia y una revisión post-implantación. Asimismo, garantizar que se obtenga la aprobación de las partes relevantes.

2. La planificación de la conversión de procesos de negocio, sistemas y datos: asegurar que se prepare la migración de procesos de negocio, datos de los servicios de TI e infraestructuras como parte de los mecanismos de desarrollo de la empresa, incluyendo registros de auditoría y un plan de recuperación para el caso de que la migración fallara.

3. La planificación de las pruebas de aceptación: asegurar que se establezca un plan de pruebas basado en estándares corporativos que defina roles, responsabilidades, y criterios de entrada y salida. Asegurar que el plan es aprobado por las partes relevantes.

4. El establecimiento de un entorno de pruebas: asegurar que se defina y establezca un entorno seguro de pruebas que sea representativo del proceso de negocio y entorno de operaciones de TI planeados, en cuanto a rendimiento y capacidad, seguridad, controles internos, prácticas de operación, calidad de los datos y requisitos de privacidad y carga de trabajo.

5. La ejecución de pruebas de aceptación: asegurar que se prueben los cambios independientemente, de acuerdo con el plan de pruebas definido, antes de migrar al entorno de producción.

6. El pase a producción y gestión de los lanzamientos: asegurar que se pase la solución aceptada al negocio y las operaciones. Donde sea apropiado, ejecutar la solución como un proyecto piloto o en paralelo con la solución antigua durante un período de tiempo definido y comparar su comportamiento y resultados. Asimismo, si se dieran problemas significativos, asegurar que se reinstaure el entorno original de acuerdo al plan de marcha atrás o alternativo. Adicionalmente, garantizar que se gestionen los lanzamientos de los componentes de la solución.

7. La prevención del soporte en producción: asegurar que se proporcione soporte desde el primer momento a los usuarios y a las operaciones de TI durante un periodo de tiempo acordado para tratar cualquier incidencia y ayudar a estabilizar la nueva solución.
8. La ejecución de la revisión post-implantación: asegurar que se **l**leve a cabo una revisión post-implantación para confirmar salidas y resultados, se identifiquen lecciones aprendidas y desarrollen un plan de acción. Asimismo, garantizar que se evalúe y verifique el rendimiento actual y las salidas del servicio nuevo o modificado respecto al rendimiento y salidas previstas (es decir, el servicio esperado por el usuario o el cliente).

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
3.7	Gestionar los activos de TI

Descripción del Proceso

Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un costo óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La identificación y registro de los activos actuales: asegurar que se mantenga un registro actualizado y exacto de todos los activos de TI necesarios para la prestación de servicios y garantizar su alineación con la gestión de la configuración y la administración financiera.

2. La gestión de los activos críticos. asegurar que se identifiquen los activos que son críticos en la provisión de capacidad de servicio y que se den los pasos para maximizar su fiabilidad y disponibilidad para apoyar las necesidades del negocio.

3. La gestión del ciclo de vida de los activos: asegurar que se gestionen los activos desde su adquisición hasta su eliminación para garantizar que se utilizan tan eficaz y eficientemente como sea posible y que son contabilizados y protegidos físicamente.

4. La optimización del costo de los activos: asegurar que se revise periódicamente la base global de activos para identificar maneras de optimizar los costos y se mantenga el alineamiento con las necesidades del negocio.

5. La administración de licencias: asegurar que se administren las licencias de software de forma que se mantenga el número óptimo de licencias para soportar los requerimientos de negocio y el número de licencias en propiedad sea suficiente para cubrir el software instalado y en uso.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
3.8	Gestionar la configuración

Descripción del Proceso

Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarias para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. El establecimiento y mantención del modelo de configuración: asegurar que se establezca y mantenga un modelo lógico de la infraestructura, activos y servicios y la forma de registrar los elementos de configuración (CIs del inglés, configuration items) y las relaciones entre ellos. Asimismo, garantizar que se incluyan los CIs considerados necesarios para gestionar eficazmente los servicios y se proporcione una sola descripción fiable de los activos en un servicio.
2. El establecimiento y mantención del repositorio de configuración y la base de referencia: asegurar que se establezca y mantenga un repositorio de gestión de la configuración y se creen unas bases de referencia de configuración controladas.
3. La mantención y control de los elementos de configuración: asegurar que se mantenga un repositorio actualizado de elementos de configuración rellenado con los cambios.
4. La generación de informes de estado y configuración: asegurar que se defina y elaboren informes de configuración sobre cambios en el estado de los elementos de configuración.
5. La verificación y revisión de la integridad del repositorio de configuración: asegurar que se revise periódicamente el repositorio de configuración y se verifique la integridad y exactitud con respecto al objetivo deseado.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
4.1	Gestionar las operaciones

Descripción del Proceso

Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La ejecución de procedimientos operativos: asegurar que se mantenga y ejecuten procedimientos y tareas operativas de forma confiable y consistente.
2. La gestión de servicios externalizados de TI: asegurar que se gestione la operación de servicios externalizados de TI para que se mantenga la protección de la información empresarial y la confiabilidad de la entrega del servicio.
3. La supervisión de la infraestructura de TI: asegurar que se supervise la infraestructura TI y los eventos relacionados con ella. Asimismo, garantizar que se almacene la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones.
4. La gestión del entorno: asegurar que se mantengan las medidas para la protección contra factores ambientales. Asimismo, se instale el equipamiento y dispositivos especializados para supervisar y controlar el entorno.
5. La gestión de las instalaciones: asegurar que se gestionen las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
4.2	Gestionar peticiones e incidentes de servicio

Descripción del Proceso

Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La definición de los esquemas de clasificación de incidentes y peticiones de servicio: asegurar que se definan esquemas y modelos de clasificación de incidentes y peticiones de servicio.
2. El registro, clasificación y priorización de las peticiones e incidentes: asegurar que se identifiquen, registren y clasifiquen peticiones de servicio e incidentes, y se asigne una prioridad según la criticidad del negocio y los acuerdos de servicio.
3. La verificación, aprobación y resolución de peticiones de servicio: asegurar que se seleccionen los procedimientos adecuados para peticiones y se verifique que las peticiones de servicio cumplen los criterios de petición definidos.
4. La investigación, diagnostico y localización de incidentes: asegurar que se identifique y se registren síntomas de incidentes, se determinen posibles causas y se asignen recursos a su resolución.
5. La resolución y recuperación de incidentes: asegurar que se documente, solicite y prueben las soluciones identificadas o temporales y se ejecuten acciones de recuperación para restaurar el servicio TI relacionado.
6. El cierre de peticiones de servicio e incidentes: asegurar que se verifique la satisfactoria resolución de incidentes y/o satisfactorio cumplimiento de peticiones, y cierre.
7. El seguimiento del estado y emisión de informes: asegurar que se haga seguimiento, analice e informe de incidentes y tendencias de cumplimiento de peticiones, regularmente, para proporcionar información para la mejora continua.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
4.3	Gestionar los problemas

Descripción del Proceso

Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La identificación y clasificación de problemas: asegurar que se defina e implementen criterios y procedimientos para informar de los problemas identificados, incluyendo clasificación, categorización y priorización de problemas.

2. La investigación y diagnóstico de problemas: asegurar que se investigue y diagnostiquen problemas utilizando expertos en las materias relevantes para valorar y analizar las causas raíz.

3. El levantamiento de errores conocidos: Tan pronto como las causas raíz de los problemas se hayan identificado, asegurar que se creen registros de errores conocidos y una solución temporal apropiada, e identifiquen soluciones potenciales.

4. La resolución y cierre de problemas: asegurar que se identifiquen e inicien soluciones sostenibles refiriéndose a la causa raíz, levantando peticiones de cambio a través del proceso de gestión de cambios establecido si se requiere para resolver errores. Asegurarse de que el personal afectado está al tanto de las acciones tomadas y de los planes desarrollados para prevenir que vuelvan a ocurrir futuros incidentes.

5. La realización de una gestión de problemas proactiva: asegurar que se recojan y analicen datos operacionales (especialmente registros de incidentes y cambios) para identificar tendencias emergentes que puedan indicar problemas. Asimismo, garantizar que se registren problemas para permitir la valoración.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
4.4	Gestionar la continuidad

Descripción del Proceso

Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La definición de una política de continuidad de negocio, objetivos y alcance: asegurar que se defina la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas.

2. **El mantenimiento de una estrategia de continuidad:** asegurar que se evalúen las opciones de gestión de la continuidad de negocio y se escoja una estrategia de continuidad viable y efectiva en costo, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.

3. El desarrollo e implementación de una respuesta a la continuidad del negocio: asegurar que se desarrolle un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas.

4. El ejercicio, prueba y revisión del Plan de Continuidad (BCP): asegurar que se prueben los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.

5. La revisión, mantención y mejora del plan de continuidad: asegurar que se realice una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para garantizar su continua idoneidad, adecuación y efectividad. Asimismo, asegurar que se gestionen los cambios en el plan de acuerdo al proceso de control de cambios para que el plan de continuidad se mantenga actualizado y refleje continuamente los requerimientos actuales del negocio.

6. La capacitación y formación en el plan de continuidad: asegurar que se proporcione a todas las partes implicadas, internas y externas, de sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción.

7. La gestión de acuerdos de respaldo: asegurar que se mantenga la disponibilidad de la información crítica del negocio.

8. La ejecución de las revisiones post-reanudación: asegurar que se evalúe la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
4.5	Gestionar servicios de seguridad de la información

Descripción del Proceso
Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La protección contra software malicioso (malware): asegurar que se **i**mplemente y mantengan efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).

2. La gestión de la seguridad de la red y las conexiones: asegurar que se utilicen medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.

3. La gestión de la seguridad de los puestos de usuario final: asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) estén asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.

4. La gestión de la identidad del usuario y el acceso lógico: asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinen con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.

5. La gestión del acceso físico a los activos de TI: asegurar que se defina e implementen procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. Asimismo, garantizar que el acceso a locales, edificios y áreas este justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.

6. La gestión de los documentos sensibles y dispositivos de salida: asegurar que se establezcan salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (token) de seguridad.

7. La supervisión de la infraestructura para detectar eventos relacionados con la seguridad: asegurar que se usen herramientas de detección de intrusiones, se supervise la infraestructura para detectar accesos no autorizados y aseguren que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
4.6	Gestionar controles de proceso de negocio

Descripción del Proceso
Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La alineación de actividades de control embebidas en los procesos de negocio con los objetivos corporativos: asegurar que se evalúe y supervise continuamente la ejecución de las actividades de los procesos de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de controles está alineado con las necesidades del negocio.

2. El control del procesamiento de la información: asegurar que se opere la ejecución de las actividades de proceso de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de la información es válido, completo, preciso, oportuno y seguro (es decir, refleja el uso de negocio autorizado y legitimado).

3. La gestión de roles, responsabilidades, privilegios de acceso y niveles de autorización: asegurar que se gestionen los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Asimismo, garantizar que se autorice el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio, de TI y de terceras partes. Esto asegura que el negocio sabe donde están los datos y quien los está manejando en su nombre.

4. La gestión de errores y excepciones: asegurar que se gestionen las excepciones y errores de los procesos de negocio y facilite su corrección. Asimismo, garantizar que se incluyan escalada errores y excepciones en los procesos de negocio y la ejecución de acciones correctivas definidas. Esto proporciona garantía de precisión e integridad del proceso de información del negocio.

5. El aseguramiento de la trazabilidad de los eventos y responsabilidades y de información: asegurar que la información de

negocio pueda ser rastreada hasta los responsables y eventos de negocio que la originan. Esto permite trazabilidad de la información a lo largo de su ciclo de vida y procesos relacionados. Proporciona garantías de que la información que conduce el negocio es de confianza y ha sido procesada acorde a los objetivos definidos.

6. El aseguramiento de los activos de información: asegurar que los activos de información accesibles por el negocio a través de los métodos aprobados, incluyendo la información en formato electrónico (tales como métodos para crear nuevos activos en cualquier forma, dispositivos portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en formato físico (tales como documentos fuente o informes de salida) e información en tránsito. Esto beneficia al negocio proporcionando una salvaguarda de la información de comienzo a fin.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
5.1	Supervisar, evaluar y valorar el rendimiento y la conformidad

Descripción del Proceso

Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. El establecimiento de un enfoque de la supervisión: asegurar que se involucre a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Asimismo, garantizar que se integre este enfoque con el sistema de gestión del rendimiento de la compañía.
2. El establecimiento de los objetivos de cumplimiento y rendimiento: asegurar que se colabore con las partes interesadas en la definición, revisión periódica, actualización y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento.
3. La recopilación y proceso de los datos de cumplimiento y rendimiento: asegurar que se recopilen y procesen datos oportunos y precisos de acuerdo con los enfoques del negocio.
4. El análisis e informe sobre el rendimiento: asegurar que se revise e informe de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de supervisión.
5. El aseguramiento de la implantación de medidas correctivas: asegurar que se apoye a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios

Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
5.2	Supervisar, evaluar y valorar el sistema de control interno

Descripción del Proceso

Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La supervisión del control interno: asegurar que se realice, de forma continua, la supervisión, los estudios comparativos y la mejora el entorno de control de TI y el marco de control para alcanzar los objetivos organizativos.
2. La revisión de la efectividad de los controles sobre los procesos de negocio: asegurar que se revise la operación de controles, incluyendo la revisión de las evidencias de supervisión y pruebas, para garantizar que los controles incorporados en los procesos de negocio operen de manera efectiva. Asimismo, asegurar que se incluyan actividades de mantenimiento de evidencias de la operación efectiva de controles a través de mecanismos como la comprobación periódica de controles, supervisión continua de controles, evaluaciones independientes, centros de mando y control y centros de operación de red. Esto proporciona al negocio de la seguridad de la efectividad del control para satisfacer los requisitos relativos al negocio y a las responsabilidades sociales y regulatorias.
3. La realización de autoevaluaciones de control: asegurar que se estimule a la Dirección y a los propietarios de los procesos a tomar posesión de manera firme del procedimiento de mejora del control, a través de programas continuos de autoevaluación que valoren la completitud y efectividad del control de la Dirección sobre los procesos, políticas y contratos.
4. La identificación y comunicación de las deficiencias de control: asegurar que se identifiquen deficiencias de control y analicen e identifiquen las causas raíz subyacentes. Asimismo, garantizar que se escalen las deficiencias de control y sean comunicadas a las partes interesadas.
5. La garantía que los proveedores de aseguramiento son independientes y están cualificados: asegurar que las entidades que realizan el aseguramiento sean independientes de la función, grupo u organización en el alcance. Asimismo, garantizar que las entidades que realizan el aseguramiento demuestren una actitud y apariencia apropiadas y adecuada competencia en las habilidades y conocimientos que son necesarios para realizar el aseguramiento y la adherencia a los códigos de ética y los estándares profesionales.
6. La planificación de las iniciativas de aseguramiento: asegurar que se planifiquen las iniciativas de aseguramiento basándose en los objetivos empresariales y las prioridades estratégicas, riesgo inherente, restricciones de recursos y suficiente conocimiento de la compañía.
7. El estudio de las iniciativas de aseguramiento: asegurar que se defina y acuerde con la dirección el ámbito de la iniciativa de aseguramiento, basándose en los objetivos de aseguramiento.
8. La ejecución de las iniciativas de aseguramiento: asegurar que se ejecute la iniciativa de aseguramiento planificada. Asimismo, garantizar que se informe de los hallazgos identificados y que se provean opiniones de aseguramiento positivo, cuando sea oportuno, y recomendaciones de mejora relativas a los riesgos residuales identificados en el desempeño operacional, el cumplimiento externo y el sistema de control interno.

Fortalezas del proceso

Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso

Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso

Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios

Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo

Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

RESULTADOS DE LA EVALUACIÓN

Estado Evaluación	Seleccionado
NO INCLUIDO EN ALCANCE	NO

Número	Proceso valorado
5.3	Supervisar, evaluar y valorar la conformidad con los requerimientos externos

Descripción del Proceso

Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.

INFORMACIÓN REQUERIDA

Evaluación
Pendiente de Evaluar

Criterios de Evaluación

1. La identificación de los requisitos externos de cumplimiento: asegurar que se identifique y supervise, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos externos de obligado cumplimiento en el área de TI.

2. La optimización de la respuesta a requisitos externos: asegurar que se revisen y ajusten políticas, principios, estándares, procedimientos y metodologías para garantizar la adecuada gestión y comunicación de los requisitos legales, regulatorios y contractuales. Asimismo, asegurar que se consideren qué estándares sectoriales, códigos de buenas prácticas y guías de mejores prácticas pueden adoptarse y adaptarse.

3. La confirmación del cumplimiento de requisitos externos: asegurar que se confirme el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requisitos legales, regulatorios y contractuales.

4. La obtención de la garantía del cumplimiento de requisitos externos: asegurar que se obtengan y notifiquen garantías de cumplimiento y adherencia a políticas, principios, estándares, procedimientos y metodologías. Asimismo, garantizar que se confirme que las acciones correctivas para tratar las diferencias en el cumplimiento son cerradas a tiempo.

Fortalezas del proceso
Se incluyen las capacidades especiales con las que cuenta el proceso, por ejemplo, las sanas practicas en las actividades que desarrolla el proceso cuanto a productos innovadores, sistemas de información, seguridad informática, plataforma e infraestructura de TI, entre otros.

Debilidades del proceso
Se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso.

Identificación de Riesgos del Proceso
Se incluye el detalle de la condición (estado), causa (origen) y efecto (impacto) por cada riesgo del proceso evaluado.

Comentarios
Se incluyen observaciones con respecto al diseño, la implementación, la operación y oportunidades de mejora de controles de TI del proceso.

Referencia a papeles de trabajo
Se incluye los documentos fuente (en formato electrónico y firmados digitalmente), registros e información de corroboración utilizados para apoyar la auditoría del proceso. Adicionalmente, se incluye los procedimientos, pruebas de cumplimiento, pruebas sustantivas y las técnicas de auditoría utilizadas (ej. cuestionarios, entrevistas, lista de verificación, matriz de riesgo, método de muestreo, otros).

Seleccionado	Identificador	Proceso valorado	Estado de la valoración
NO	1.1	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	**NO INCLUIDO EN ALCANCE**
NO	1.2	Asegurar la Entrega de Beneficios	**NO INCLUIDO EN ALCANCE**
NO	1.3	Asegurar la Optimización del Riesgo	**NO INCLUIDO EN ALCANCE**
NO	1.4	Asegurar la Optimización de Recursos	**NO INCLUIDO EN ALCANCE**
NO	1.5	Asegurar la Transparencia hacia las Partes Interesadas	**NO INCLUIDO EN ALCANCE**
NO	2.1	Gestionar el Marco de Gestión de TI	**NO INCLUIDO EN ALCANCE**
NO	2.2	Gestionar la Estrategia	**NO INCLUIDO EN ALCANCE**
NO	2.3	Gestionar la Arquitectura Empresarial	**NO INCLUIDO EN ALCANCE**
NO	2.4	Gestionar el portafolio de servicios	**NO INCLUIDO EN ALCANCE**
NO	2.5	Gestionar el presupuesto y los costos	**NO INCLUIDO EN ALCANCE**
NO	2.6	Gestionar los recursos humanos	**NO INCLUIDO EN ALCANCE**
NO	2.7	Gestionar las relaciones entre TI y el negocio	**NO INCLUIDO EN ALCANCE**
NO	2.8	Gestionar los acuerdos de niveles de servicio	**NO INCLUIDO EN ALCANCE**
NO	2.9	Gestionar los servicios de los proveedores de TI	**NO INCLUIDO EN ALCANCE**
NO	2.10	Gestionar la Calidad	**NO INCLUIDO EN ALCANCE**
NO	2.11	Gestionar el riesgo de TI	**NO INCLUIDO EN ALCANCE**
NO	2.12	Gestionar la seguridad	**NO INCLUIDO EN ALCANCE**
NO	3.1	Gestionar programas y proyectos	**NO INCLUIDO EN ALCANCE**
NO	3.2	Gestionar la definición de requerimientos	**NO INCLUIDO EN ALCANCE**
NO	3.3	Gestionar la identificación y construcción de soluciones	**NO INCLUIDO EN ALCANCE**
NO	3.4	Gestionar la disponibilidad y capacidad	**NO INCLUIDO EN ALCANCE**
NO	3.5	Gestionar los cambios	**NO INCLUIDO EN ALCANCE**
NO	3.6	Gestionar la aceptación del cambio y la transición	**NO INCLUIDO EN ALCANCE**
NO	3.7	Gestionar los activos de TI	**NO INCLUIDO EN ALCANCE**
NO	3.8	Gestionar la configuración	**NO INCLUIDO EN ALCANCE**
NO	4.1	Gestionar las operaciones	**NO INCLUIDO EN ALCANCE**
NO	4.2	Gestionar peticiones e incidentes de servicio	**NO INCLUIDO EN ALCANCE**
NO	4.3	Gestionar los problemas	**NO INCLUIDO EN ALCANCE**
NO	4.4	Gestionar la continuidad	**NO INCLUIDO EN ALCANCE**
NO	4.5	Gestionar servicios de seguridad de la información	**NO INCLUIDO EN ALCANCE**
NO	4.6	Gestionar controles de proceso de negocio	**NO INCLUIDO EN ALCANCE**
NO	5.1	Supervisar, evaluar y valorar el rendimiento y la conformidad	**NO INCLUIDO EN ALCANCE**
NO	5.2	Supervisar, evaluar y valorar el sistema de control interno	**NO INCLUIDO EN ALCANCE**
NO	5.3	externos	**NO INCLUIDO EN ALCANCE**

FORTALEZAS RELEVANTES PROCESOS

DEBILIDADES RELEVANTES PROCESOS

CONCLUSIÓN GENERAL