OPTIMIZACIÓN DE RIESGOS. PARTE I

AUTOR: LUIS RAMÍREZ LORÍA

MARZO: 2021

San Marcos

Tabla de contenido

Introdución

Para el tercer módulo se analizará la gestión de riesgos como uno de los elementos del Gobierno de TI en sus distintos niveles, estratégico, táctico y operativo, para lo cual es fundamental la valoración y conocimiento de normas, aspectos de regulación y legales, que se abarcarán en el módulo. Durante la lectura uno del módulo se abordarán los conceptos relacionados con la aplicación de la gestión de riesgos en los niveles estratégico, de cartera, de programa, de proyecto y de operaciones, así como los marcos y normas de gestión del riesgo.

Con el estudio de estos conceptos y normas se busca que el estudiante y futuro profesional en TI logre comprender como dentro de los marcos de Gobierno de TI la aplicación de la gestión de riesgos en la estrategia, carteras, proyectos, programas y operaciones puede generar ventajas significativas y con esto la formación profesional en los conceptos es un requerimiento que permitirá cumplir con aspectos regulatorios y legales en las organizaciones.

En Costa Rica, por ejemplo, para las organizaciones públicas deben cumplir con las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, las cuales en su apartado 1.3 señalan los aspectos a cumplir para una adecuada Gestión de riesgos en materia de Tecnologías de la Información.

Contenido

Dentro de los principios y modelos de Gobernanza de las Tecnologías de la Información se ha establecido que unos de los principales motores de la actividad del Gobierno es el asegurar que las funciones de TI se alineen con las necesidades del negocio, para lo cual se deben abarcar una serie de procesos de la organización que cubren la gestión de servicios, automatización de procesos, el establecimiento y gestión del portafolio de inversiones, las compras, presupuestos, administración de recursos, la estrategia y las operaciones.

Asociado al aseguramiento de los objetivos y metas de negocio se dice que los resultados positivos requieren una adecuada revisión y mejora de servicios, lo cual puede conseguirse si se toman las recomendaciones de las mejores prácticas de gestión, entre ellas aspectos claves como la gestión de los riesgos de TI, la mejora en la comunicación y en las relaciones entre el negocio y TI, son detalles de alta visibilidad y contribución al negocio, por lo cual deben gestionarse de una manera consciente y metódica. En este caso abordaremos los aspectos asociados a riesgos desde la perspectiva de optimización.

Optimización del riesgo

Para determinar adecuadamente lo que refieren las mejores prácticas como el COBIT o el RISK IT, la norma ISO 31000 o el estándar de COSO (con la Gestión de Riesgo Empresarial (ERM)), sobre la optimización de los riesgos, primero debemos entender algunas definiciones iniciales.

En este sentido acorde a los señalado por Helena, tenemos las siguientes definiciones:

- *Riesgo se define como: "el potencial que una amenaza dada aprovechará las vulnerabilidades de un activo o grupo de activos para causar pérdida o daño a los activos."*
- *Riesgo residual se define como: "Riesgo que permanece después de que se han implementado las salvaguardas."*
- *Análisis de riesgo se define como "el proceso de identificar los riesgos de seguridad, determinar su magnitud e identificar las áreas que necesitan salvaguardas".*
- *Gestión del riesgo es "el proceso de evaluar y cuantificar el riesgo y establecer un nivel aceptable de riesgo para la organización"*
- *Principios de gobernanza sobre riesgos:*
    - *"La gestión de riesgos de TI debe formar parte integral de la gestión de riesgos corporativa".*
    - *"Comités de riesgo y auditoría deben asistir a la junta en el cumplimiento de*

sus responsabilidades de TI" (Garbarino Alberti, 2014)

Una adecuada gestión del riesgo de las TI, inicia por la identificación de la utilidad de su gestión por parte de la alta administración (conciencia del riesgo), de manera que se genere el apetito por el riesgo en la organización, y se logre comprender el beneficio del cumplimiento de objetivos de gestión de riesgos, establecer modelos de transparencia en el tratamiento de riesgos (al inicio lo más relevantes por impacto, visibilidad o criticidad del negocio), definir claramente las responsabilidades de su gestión en la organización, de forma que se puede administrar o gerenciar el riesgo (evaluar, mitigar, evitar o aceptar), abarcando desde los procesos críticos de negocio hasta la seguridad de la información (sumamente relevante en la actual revolución 4.0).

Gestionar los riesgos, en la mayor parte de los marcos y mejores prácticas implica en primer lugar establecer los elementos a considerar en el perfil de riesgos de la empresa, mediante una completa descripción de las implicaciones para el negocio, el desarrollo de hipótesis, de métodos para describir los riesgos de forma homologada y comprender las técnicas para cuantificar riesgos y cuáles son los factores que los generan. Complementándose con el alineamiento de los riesgos con los objetivos del negocio y con el establecimiento de la comunicación e impacto de los riesgos de TI.

Otra acción fundamental es propiamente la definición del proceso de gestión de riesgos, sus fundamentos, modelo de gestión, procesos, cadena de valor y de responsabilidades, según los ámbitos estratégicos, tácticos (carteras, portafolios, proyectos), operativos, lo cual implica a nivel de gobernanza de las TI cubrir aspectos como el gobierno del riesgo, la evaluación y las acciones de respuesta, concordando su definición con el alineamiento a los objetivos de negocio.

Aplicación de la gestión de riesgos en los niveles estratégico, de cartera, de programa, de proyecto y de operaciones

Gestión de riesgos en el nivel estratégico

Conforme el desarrollo del curso uno de los factores críticos para una adecuada Gobernanza y Entrega de Valor de TI al negocio es en alineamiento estratégico, por lo cual la desalineación entre las necesidades del negocio y la infraestructura de TI de la organización es un factor a cuidar de manera crítica, ya que puede producir efectos como una infraestructura de TI sobreestimada o subestimada, tiempos de implementación de las soluciones de TI lejana a la expectativa de los usuarios de las áreas de negocios de la organización.

VOLVER A ENFOCARSE EN LOS RIESGOS PARA CONSIDERACIONES TALES COMO CUAN BIEN ALINEADA ESTA LA CAPACIDAD DE LAS TI CON LAS ESTRATEGIAS DE NEGOCIO Y SU APROVECHAMIENTO CON EL FIN DE MEJORAR LA EFICIENCIA O EFECTIVIDAD DE LOS PROCESOS DEL NEGOCIO. (Alvarado Carpio & Zumba Morales, 2015)

La toma de decisiones de TI realizada de forma aislada, de manera que el área de TI no es vista en la organización como estratégica, falta de integración entre las áreas del negocio y las TI. Estos factores pueden generar riesgos tales como:

- “Flujo de información bloqueado debido a los procesos no implementados por TI.”
- “Falta de alineación entre las áreas de TI y de negocios, generando baja eficiencia operacional.”
- “Servicios proporcionados sin la calidad deseada.”
- “Desconocimiento de las necesidades de los nuevos servicios de TI para la atención adecuada del negocio.” (Gaseta, Motta, & Boca Piccolini, 2016)

Gestión de riesgos de cartera

Según lo señalado por Gaseta, (Gaseta, Motta, & Boca Piccolini, 2016), el no realizar una adecuada gestión de la cartera puede generar altos gastos o costos de los servicios, recursos e infraestructura de TI, lo cual puede causar una devaluación y desactualización muy rápida de recursos de TI, la asignación inadecuada de los recursos de TI al negocio, la demora en el proceso de selección, adquisición y entrega de las soluciones de TI, e incluso,

un presupuesto insuficiente para TI. Por lo cual podemos señalar riesgos de alto impacto en el manejo de la cartera, tales como:

- *"Disminuir el lucro de la organización."*
- *"Pérdida del desempeño de las funciones de TI y de los negocios de la organización."* (Gaseta, Motta, & Boca Piccolini, 2016)

Gestión de riesgos de programas

Desde la perspectiva de Gobierno de TI, cuando existe un alineamiento entre el área de TI y el negocio esto se traduce en programas de adquisición de recursos de TI que toman en cuenta el accionar del negocio, la disposición al cambio y se aseguran de entregar al negocio los beneficios previstos, por tanto, el área de TI debe establecer los mecanismos de gestión de riesgos que coadyuven en el cumplimiento de los programas.

Para esto deben aplicarse funciones estándar de la gestión de riesgos, pero aplicadas a los programas tales como:

- Establecer acciones que permitan identificar, controlar, evitar o mitigar el riesgo.
- Cuantificación de los riesgos en términos económicos para la organización, tales como las implicaciones por no ejecutar un programa (falta de financiamiento, falta de priorización) o por costo económico por malos resultados de su ejecución.
- Establecer las políticas para la evaluación, la mitigación y la comunicación de riesgos en los programas de inversión.
- Establecer posibles fondos (reservas, seguros) para los planes de acción de riesgos

Gestión de riesgo en proyectos

LA ADMINISTRACIÓN DE RIESGOS NECESITA ENFOCARSE EN LA HABILIDAD PARA COMPRENDER Y GESTIONAR PROYECTOS COMPLEJOS DE MANERA QUE NO EXISTA UNA DEFICIENTE CONTRIBUCIÓN DE LAS TI PARA LAS NUEVAS SOLUCIONES O MEJORAS. (Alvarado Carpio & Zumba Morales, 2015)

La gestión de riesgo en proyectos implica establecer los mecanismos necesarios para eliminar o minimizar el impacto de la materialización de los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, identificación, análisis, respuesta, monitoreo y control de las actividades del proyecto y de los eventos que tengan el potencial de ocasionar cambios no deseados en el proyecto, sus alcances, avances.

Los riesgos enfrentados por el proceso de administración y gestión de proyectos y por tanto de sus productos entregables se deben establecer y registrar de forma central. También se deberá desarrollar un plan de gestión o de administración de la calidad que describa el sistema de calidad de la gestión de proyectos y cómo será implantado.

Al igual que definen los modelos de gestión de proyectos, el plan de riesgos asociado debe ser revisado y acordado de manera formal por todas las partes interesadas (ej. Usuarios, dirección del negocio, etc.) para luego ser incorporado en el plan integrado de cada proyecto.

Por otro lado, se deben identificar las tareas de aseguramiento y gestión de riesgos requeridos para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado. Estas actividades pueden ser, por ejemplo:

- Identificar los riesgos específicos asociados a los entregables de un proyecto individual, o a la cartera de proyectos.
- Examinar los riesgos y proponer una respuesta a ellos.
- Analizar las prácticas de gestión de proyectos en base al análisis de riesgos.
- Describir el sistema de calidad de la gestión de proyectos (incluyendo los riesgos) y el proceso de cómo será implantado.
- Describir las tareas que aseguren que se satisfagan los requerimientos definidos y reduzcan la incidencia de riesgos.
- Implementar el enfoque de administración de proyectos en la organización y de ser posible las recomendaciones de administración, control y seguimiento para su aseguramiento.

Gestión de riesgos en las operaciones

La gestión de riesgos en las operaciones debe garantizar, en primera instancia, que se cumplan principios de buenas prácticas en las cuales se garanticen aspectos como capacidad, disponibilidad, continuidad, desempeño y seguridad, las mejores prácticas como las propuestas en los marcos de ITSM, Gobierno de TI, seguridad de la información, son una base fundamental para la gestión de riesgos en las operaciones, en los cuales se debe, en principio, identificar las posibles pérdidas operativas y con esto establecer el desarrollo

AQUELLOS RIESGOS QUE PODRÍAN COMPROMETER LA EFECTIVIDAD DE LOS SERVICIOS SOPORTADOS POR TI Y LA INFRAESTRUCTURA DE APOYO. SE DEBE RECORDAR QUE EL RENDIMIENTO Y DISPONIBILIDAD DE LOS SERVICIOS DE TI PUEDEN INFLUIR DIRECTAMENTE EN EL VALOR DE LA EMPRESA LLEGANDO A REDUCIRLO E INCLUSIVE DESTRUIRLO. (Alvarado Carpio & Zumba Morales, 2015)

de los principales indicadores de riesgo operativo.

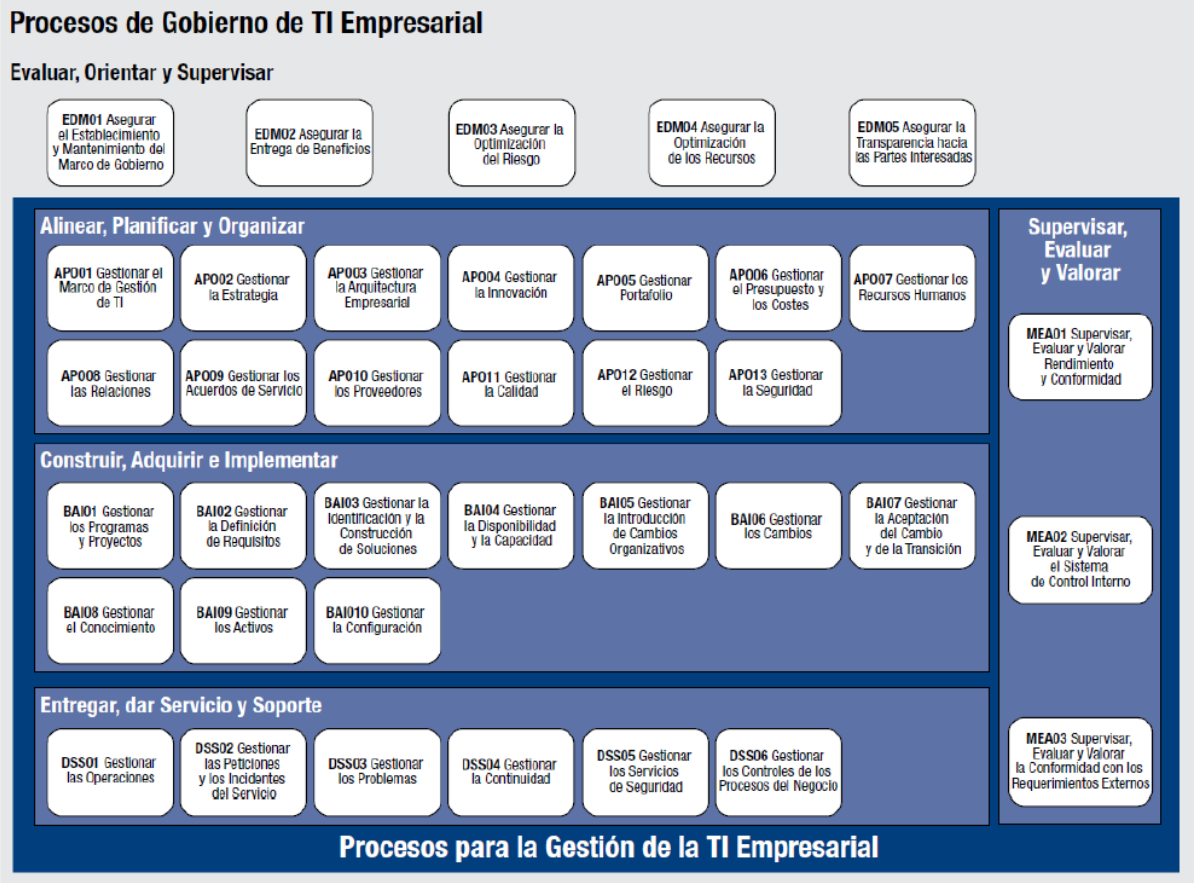
El establecimiento de una cultura de gestión de riesgo promueve su gestión de manera activa en el ámbito de las operaciones, buscando asegurar que los implicados tengan responsabilidades de gestión de riesgos definidas adecuadamente para a asegurar una gestión de riesgos operacional que funcione sobre suposiciones de riesgo constantes y bajo medidas de mejora continua. Al igual que en los otros enfoques una gestión de riesgo en las operaciones implica que las decisiones de riesgos son tomadas por las personas claves, autorizadas, con un enfoque en la gestión organizacional, desempeñando un papel clave en la gestión de los riesgos en el ámbito de las operaciones.

Marcos y normas de gestión del riesgo.

Entre los principales marcos de gestión de riesgos de TI tenemos, al igual que se ha analizado en lecturas anteriores marcos de referencia y mejores prácticas, en algunos casos tales como COBIT 5 en uno de los procesos, el marco de referencia RISK IT también de ISACA, la norma ISO/IEC 27005, ISO/IEC 31000 y otros marcos reconocidos como OCTAVE, MAGERIT, NIST800-30, todos con una serie de recomendaciones importantes sobre la gestión y optimización del riesgo, en resumen, para establecer un enfoque formativo se abarcará de forma resumida las principales, lo cual se puede profundizar con estudios específicos de cada norma y sus actualizaciones recientes.

COBIT 5.

Dentro del modelo de referencia de procesos de COBIT 5, existen una serie de agrupaciones de la mejores prácticas y recomendaciones relacionados con el Gobierno de TI que engloban procesos relacionados con los dominios de Evaluación, Orientación y Supervisión (EDM), Alineamiento, Planificación y Organización (APO), Construcción, Adquisición e Implementación (BAI), Entregar, Dar Servicio y Soportar (DSS) y por último Supervisar, Evaluar y Valorar (MEA), dentro de los cuales se establecen las recomendaciones correspondientes para Gestionar el Riesgo, y para el Aseguramiento de la Optimización del Riesgo.



Modelo de Referencia de Procesos COBIT 5. Fuente: (ISACA®, 2012)

APO12 Gestionar el riesgo

El proceso descrito por ISACA, (ISACA®, 2012), sobre la gestión del riesgo, dispone prácticas adecuadas para identificar, evaluar y reducir los riesgos de TI de una forma continua, y busca mantener estos riesgos / consecuencias, dentro de los niveles de tolerancia establecidos por la dirección de la empresa, incorporando para ellos seis procesos que se describen a continuación:

APO12.01 Recopilar datos

"Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI." (ISACA®, 2012). Esta práctica requiere ejecutar las siguientes actividades, en resumen:

1. Establecer y mantener la metodología de gestión de riesgos, recolección, clasificación y análisis de datos, eventos, categorías y factores de riesgo.
2. Registrar datos relevantes del entorno de operaciones para la gestión de riesgos.

3. Medir y analizar datos históricos, pérdidas, tendencias, datos de la industria.
4. Registrar datos sobre eventos de riesgo en programas, proyectos, operaciones y entrega de servicios de TI.
5. Destacar factores contribuyentes al riesgo en eventos similares o eventos múltiples.
6. Determinar condiciones al momento del riesgo y como afectaban la frecuencia del evento y la magnitud de la pérdida.
7. Analizar eventos periódicamente considerando factores de riesgos nuevos o emergentes y su relación.

APO12.02 Analizar el riesgo

"Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo." (ISACA®, 2012). Esta práctica requiere ejecutar las siguientes actividades, en resumen:

1. Definir amplitud y profundidad en los análisis de riesgo, según el alcance definido por el análisis coste-beneficio.
2. Construir y actualizar regularmente los escenarios de riesgo de TI.
3. Estimar frecuencia y magnitud de las pérdidas asociadas a riesgos de TI.
4. Comparar riesgo residual y margen de tolerancia, identificar exposiciones a riesgos que requieran respuesta.
5. Analiza coste-beneficio de las opciones de respuesta (evitar, reducir, mitigar, transferir, compartir, aceptar, explotar, capturar) y proponer la respuesta óptima.
6. Especificar requerimientos de alto nivel para gestión de riesgos en programas clave.
7. Validar resultados de análisis de riesgos para la toma de decisiones, confirmando el alineamiento de requerimientos con la empresa.

APO12.03 Mantener un perfil de riesgo

"Mantener 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." (ISACA®, 2012). Esta práctica requiere ejecutar las siguientes actividades, en resumen:

1. Inventariar procesos de negocio (personal de soporte, aplicaciones, infraestructura, instalaciones, registros, manuales, críticos, vendedores, proveedores) y sus dependencias de los procesos de gestión de servicios de TI y los recursos de infraestructura de TI.
2. Determinar recursos de TI esenciales para sostener las operaciones, analizar dependencias y eslabones débiles.

3. Agregar escenarios de riesgo actuales (categorías, línea de negocio y área funcional)
4. Capturar información del perfil de riesgo y consolidarla, de forma regular.
5. Definir indicadores de riesgo que permitan una identificación rápida y supervisión de riesgos y sus tendencias.
6. Capturar eventos de riesgo de TI e incluirlos en el perfil de riesgo de la empresa.
7. Incluir información del estado del plan de acción de riesgos de TI en el perfil de riesgo de la empresa.

APO12.04 Expresar el riesgo

"Proporcionar 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." (ISACA®, 2012). Esta práctica requiere ejecutar las siguientes actividades, en resumen:

1. Informar resultados del análisis de riesgos a los interesados (incluir probabilidades, rangos de pérdida, ganancia, niveles de confianza, retorno del riesgo).
2. Informar sobre el peor y más probable escenario de riesgo a los responsables de la toma de decisiones, exponer con la debida diligencia y consideraciones legales, regulatorias y de reputación.
3. Informar la efectividad de la gestión de riesgos, controles, diferencias, inconsistencias, redundancias, remediación e impactos en el perfil de riesgos.
4. Revisar e incluir en el perfil el resultado de evaluaciones de riesgo producto de auditorías y revisiones de aseguramiento de la calidad.
5. Identificar oportunidades relacionadas con TI que habiliten aceptar un mayor riesgo y un crecimiento y retorno mayor.

APO12.05 Definir un portafolio de acciones para la gestión de riesgos

"Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio." (ISACA®, 2012). Esta práctica requiere ejecutar las siguientes actividades, en resumen:

1. Mantener un inventario de actividades de control en curso.
2. Determinar si cada área supervisa y acepta los niveles de riesgo con tolerancias individuales y de sus portafolios.
3. Definir propuestas de proyecto para reducir riesgos incluir oportunidades estratégicas empresariales, considerando coste/beneficio y regulaciones.

APO12.06 Responder al riesgo

"Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI." (ISACA®, 2012). Esta práctica requiere ejecutar las siguientes actividades, en resumen:

1. Preparar, mantener y probar planes de respuesta al riesgo, asegurando que incluyan el escalonamiento en la empresa.
2. Categorizar los incidentes y comparar resultados reales con umbrales de tolerancia al riesgo, comunicar al negocio y a los responsables de toma de decisiones.
3. Aplicar planes de respuesta para minimizar el impacto del riesgo.
4. Examinar eventos adversos, oportunidades perdidas y su causa raíz, requerimientos de respuesta adicionales, mejoras y asegurar que incluyan procesos de gobierno del riesgo.

EDM03 Asegurar la optimización del riesgo

Este proceso es descrito por ISACA, (ISACA®, 2012), como el proceso de TI requerido para asegurar que conceptos como el apetito y la tolerancia al riesgo son entendidos por la organización y esta los articula, comunica y gestiona de forma tal que el riesgo es identificado y gestionado, además que se relacionado con el uso de las TI y el valor para la empresa. Para este proceso de aseguramiento de la optimización del riesgo, la norma propone:

EDM03.01 Evaluar la gestión de riesgos

"Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado." (ISACA®, 2012). Esta práctica requiere ejecutar las siguientes actividades, en resumen:

1. Determinar el nivel de riesgos (TI) que la empresa está dispuesta a asumir (apetito de riesgo).
2. Evaluar y aprobar umbrales de tolerancia al riesgo.
3. Determinar el alineamiento de riesgos de TI y riesgos empresariales.
4. Evaluar riesgos de TI proactivamente previo a la toma de decisiones estratégicas.
5. Determinar que el uso de las TI se sujete a valoraciones de riesgo bajo estándares internacionales.
6. Evaluar las actividades de gestión de riesgo, garantizar el alineamiento a capacidades de la empresa y la tolerancia de los líderes ante pérdidas.

EDM03.02 Orientar la gestión de riesgos

"Orientar 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." (ISACA®, 2012). Esta práctica requiere ejecutar las siguientes actividades, en resumen:

1. Promover una cultura de riesgos en TI, impulsando la identificación proactiva de riesgos, oportunidades e impactos al negocio.
2. Orientar la integración de operaciones y estrategia de riesgos de TI y las empresariales.
3. Orienta la elaboración de planes de comunicación y de acción sobre riesgos.
4. Orientar la implantación de respuesta rápida a riesgos, notificaciones y escalonamiento.
5. Orientar para que el riesgo, oportunidades, problemas y preocupaciones puedan ser reportadas por cualquier persona.
6. Identificar objetivos e indicadores clave de los procesos de gobierno y gestión de riesgos

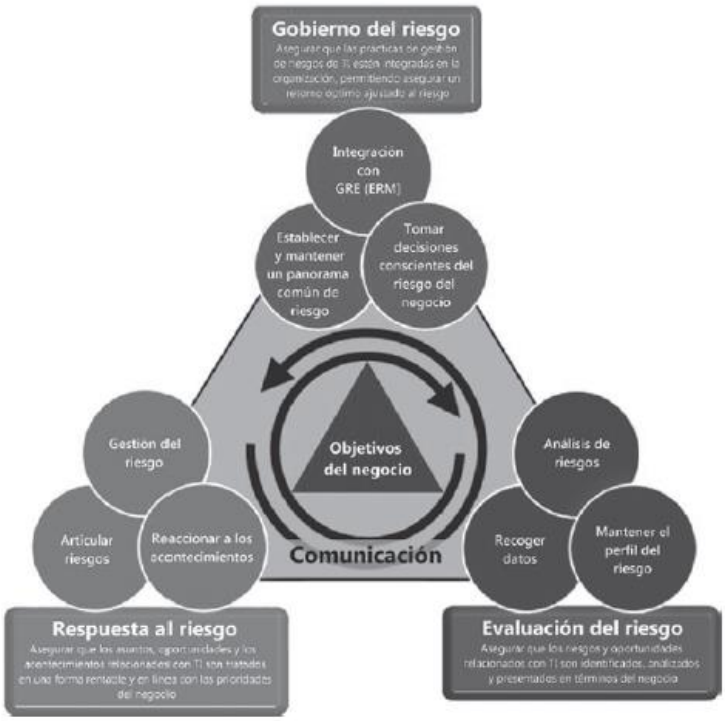
EDM03.03 Supervisar la gestión de riesgos

"Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución." (ISACA®, 2012). Esta práctica requiere ejecutar las siguientes actividades, en resumen:

1. Supervisar que los riesgos (y perfiles) se gestionan según los umbrales de riesgo
2. Supervisar metas y métricas clave de gestión de procesos, analizar causas de desviaciones e iniciar medidas correctivas.
3. Facilitar a los interesados la revisión del progreso hacia objetivos identificados.
4. Informar cualquier problema de gestión de riesgos al Comité de Dirección

RISK TI o RISK FOR COBIT

El marco para la gestión de riesgos de TI, conocido como RISK IT, es también una iniciativa de ISACA, y fue desarrollada como un complemento de COBIT, teniendo en cuenta el marco de controles planteados sobre el Gobierno de TI. Este marco de riesgos (RISK-IT) es un conjunto de principios, guías, procesos de negocio y directrices, el cual está conformado por tres ámbitos y nueve procesos interrelacionados, tal cual se puede ver en la siguiente figura resumida por ISACA:



Fuente: (ISACA IT RISK, 2009)

Según ISACA, (ISACA IT RISK, 2009), "*RISK IT se define y se basa en una serie de guías para la gestión eficaz de los riesgos de TI. Dichas guías se basan en los principios comúnmente aceptados en ERM, que se han aplicado en el ámbito de las TI. El modelo del proceso de los riesgos de TI está diseñado y estructurado para que las organizaciones puedan poner los principios en práctica y comparar sus resultados.*

El marco de RISK IT se basa en los riesgos de TI. En otras palabras, el riesgo organizacional está relacionado con el uso de las TI. La conexión con la organización se basa en los principios en los que se construye el marco, es decir, el gobierno efectivo de la organización y gestión de los riesgos de TI, tales como:

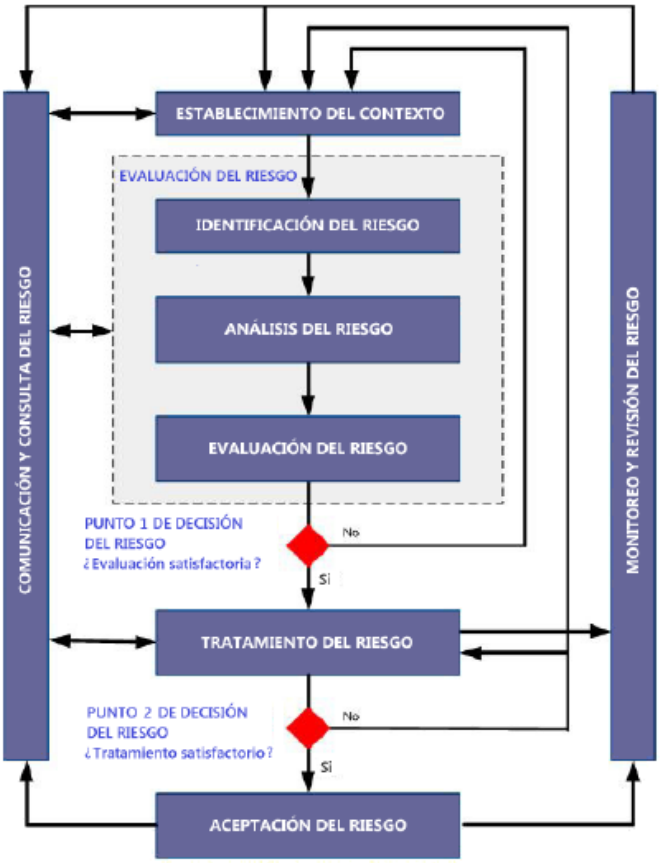
- *Alinear siempre con los objetivos organizacionales.*
- *Alinear la gestión de las TI con el riesgo organizacional análogo con el total de ERM.*
- *Balance de los costes y los beneficios de la gestión de los riesgos de TI.*
- *Promover la comunicación abierta y equitativa de los riesgos de TI.*
- *Establecer el tono correcto desde un enfoque de arriba abajo, definiendo y haciendo cumplir la responsabilidad del personal con los niveles de tolerancia aceptables y bien definidos.*
- *Son un proceso continuo y parte de las actividades diarias."* (ISACA IT RISK, 2009)

ISO/IEC 27000 / 27005

Al igual que otras normas ISO es utilizada para la estandarización y certificación en las directrices asociadas a la gestión de riesgos en los procesos asociados con las Tecnologías de Información, en cuanto a aspectos de sistemas de gestión de seguridad de la información, estas se ubican en la norma ISO/IEC 27001:2013 y a nivel de estructura este es muy similar a la ISO 31000 la cual se explicará adelante en el curso, y propiamente a nivel de directrices sobre gestión de riesgos de seguridad de la información se ubican en la ISO/IEC 27005.

Procedimiento ISO/IEC 27005

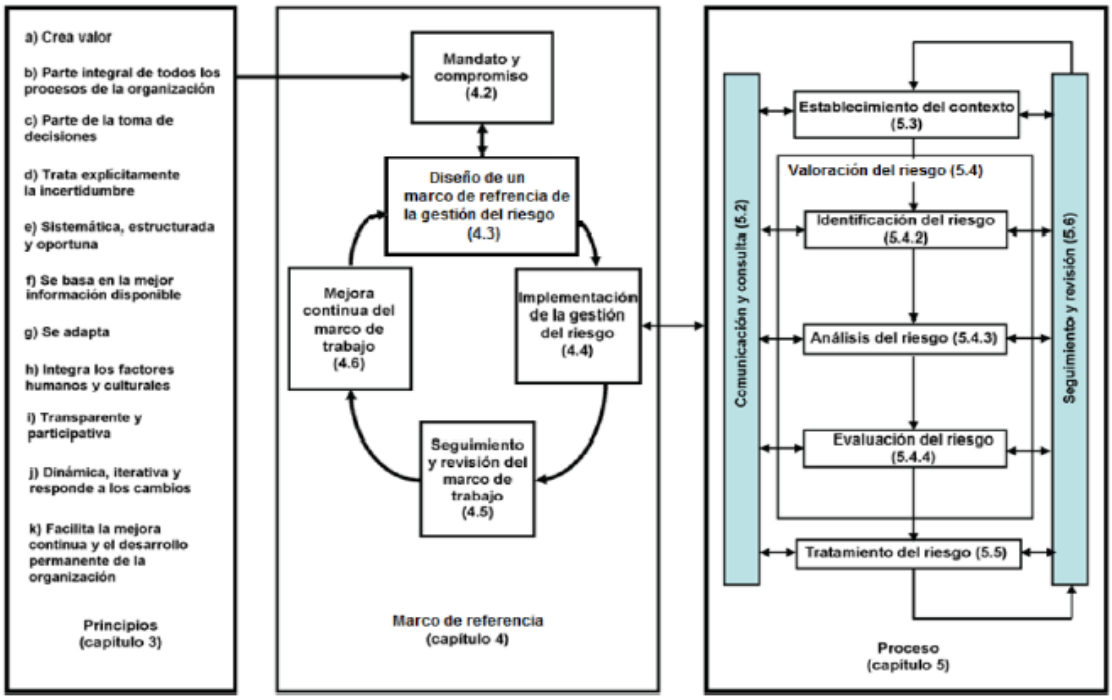
Este procedimiento consiste en a) establecer el contexto (asociado a los procesos de negocio y al riesgo), b) evaluar el riesgo o los riesgos existentes (bajo los pasos de identificación, análisis y evaluación de riesgos), c) establecer el esquema, modelo o acciones de tratamiento del riesgo, d) acepta o gestionar el riesgo residual e) comunicar el riesgo a los interesados d) realizar acciones de revisión y monitoreo, estas dos últimas se ejecutan de manera transversal durante todo el proceso como puede verse en la figura:



Fuente: (Alfaro Campos, 2017)

ISO/IEC 31000

La norma ISO/IEC 31000 se base en tres pilares sobre los cuales se cimienta la gestión de riesgos, el primero refiere a los principios que la empresa establezca para determinar que la gestión de riesgos es eficaz, el segundo tiene relación con el marco de referencia de gestión utilizado para que la información de riesgos pueda utilizarse para la toma de decisiones y responsabilidades, el tercero tiene que ver con el proceso y las actividades a implementar o contemplar para la gestión de los riesgos en la organización. En la siguiente figura se muestra la relación entre los principios, el marco de referencia y el proceso de gestión de riesgo señalado por la norma:



Fuente: (Alfaro Campos, 2017)

Principios

La norma maneja once principios orientados a cumplir con una gestión eficaz de riesgos, los cuales se resumen en:

1. La gestión del riesgo crea y protege el valor
2. La gestión del riesgo es una parte integral de todos los procesos de la organización
3. La gestión del riesgo es parte de la toma de decisiones
4. La gestión del riesgo trata explícitamente la incertidumbre
5. La gestión del riesgo es sistemática, estructurada y oportuna
6. La gestión del riesgo se basa en la mejor información disponible

7. La gestión del riesgo es a la medida
8. La gestión del riesgo integra los factores humanos y culturales
9. La gestión del riesgo es transparente y participativa
10. La gestión del riesgo es dinámica, iterativa, y responde a los cambios
11. La gestión del riesgo facilita la mejora continua de la organización

Marco de referencia

El marco de referencia de la norma en mención contiene cinco componentes que buscan proporcionar las bases y disposiciones que permitan su integración en todos los niveles de la organización, facilitando una gestión eficaz del riesgo mediante la aplicación del proceso de gestión en la organización. Sus componentes son:

1. Mandato y compromiso. Establecer una planificación estratégica y rigurosa con el compromiso fuerte y sostenido de todos los niveles de la organización.
2. Diseño del marco de referencia de la gestión de riesgos, que abarca:
    a. Comprensión de la organización y de su contexto.
    b. Establecimiento de la política de gestión del riesgo
    c. Rendición de cuentas
    d. Integración en los procesos de la organización
    e. Recursos
    f. Establecimiento de los mecanismos internos de comunicación e información
    g. Establecimiento de los mecanismos externos de comunicación y de información
3. Implementación de la gestión del riesgo, lo cual refiere a la:
    a. Implementación del marco de referencia de la gestión del riesgo
    b. Implementación del proceso de gestión del riesgo
4. Seguimiento y revisión del marco de trabajo
5. Mejora continua del marco de trabajo

Proceso

Este proceso de gestión debe formar parte integral en la organización, interactuando con la cultura, prácticas y procesos de negocio de la organización con la gestión de riesgos. Sus actividades incluyen recomendaciones para establecer procesos de gestión asociados a riesgos tales como:

1. Comunicación y consulta
2. Establecimiento del contexto
    a. Interno de la organización

   b. Externo con relación a la organización
3. Establecimiento del contexto del proceso de gestión del riesgo
4. Definición de los criterios de riesgo
5. Valoración del riesgo
   a. Identificación del riesgo
   b. Análisis del riesgo
   c. Evaluación del riesgo
   d. Tratamiento del riesgo
6. Selección de opciones de tratamiento de riesgo
7. Preparación e implementación de los planes de tratamiento de riesgo
8. Seguimiento y revisión

OCTAVE

Por sus siglas en inglés, la norma sobre Operationally Critical Threat, Asset and Vulnerability Evaluation (Evaluación de vulnerabilidades, activos y amenazas operativamente críticas), OCTAVE es una colección de herramientas, técnicas y métodos para evaluar los riesgos de seguridad de la información, desarrollada por el Software Engineering Institute.

Cuenta con tres versiones, variando las fases a ejecutar en el proceso de gestión de riesgos, su concepción y actividades:

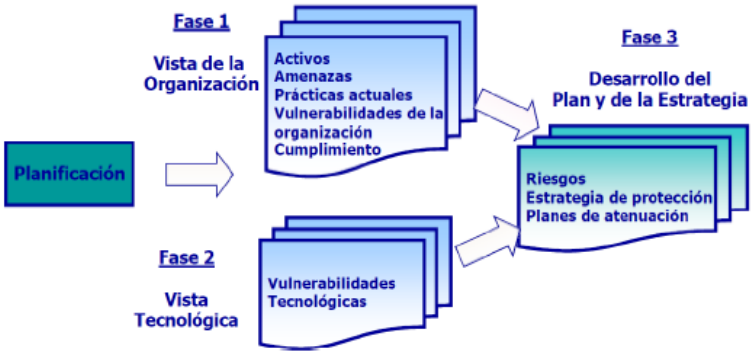
1. OCTAVE
2. OCTAVE-S
3. OCTAVE ALLEGRO

Alfaro Campos, nos señala que OCTAVE es: "*una metodología que mejora la toma de decisiones estableciendo un conjunto de herramientas, técnicas y métodos de información con base en los riesgos. Está diseñada con un enfoque auto dirigido, donde los usuarios pueden aprender y mejorar la postura de seguridad de la organización sin depender de expertos o proveedores*" (Alfaro Campos, 2017). Con lo cual se busca que la organización sea capaz de:

- Dirigir y gestionar sus evaluaciones de riesgos.
- Tomar decisiones con base en sus riesgos.
- Proteger los activos clave de información.
- Comunicar de forma efectiva la información clave de seguridad

Para esto establece tres fases, la primera asociada con la identificación de riesgos

asociados con la organización, sus prácticas, activos y otros, la segunda implica una evaluación de las tecnologías y la seguridad de la información, y la tercera se enfoca en crear e implementar la estrategia para reducir los riesgos de seguridad prioritarios para asegurar el cumplimiento de las regulaciones y objetivos empresariales. Estas fases se representan en la siguiente figura:



Fuente: (Alfaro Campos, 2017)

MAGERIT

Es la metodología de análisis y gestión de riesgos de los sistemas de información, utilizada en la Administración Pública Española, y su cumplimiento es obligatorio por temas de regulación. La misma consta de tres libros referentes a:

- El método de gestión de riesgos. Método.
- El catálogo de elementos y su explicación. Catálogo de elementos.
- La guía de las técnicas utilizadas en la metodología. Guía de técnicas.

Alfaro Campos nos expone que los objetivos de esta metodología son:

- "*Crear conciencia de la existencia de riesgos de TI y de la necesidad de tratarlos, ofrecer un método sistemático para el análisis de riesgos y ayudar en la planificación de medidas oportunas para controlar los riesgos*" (Alfaro Campos, 2017).

Su aplicación a nivel metodológico implica la ejecución de cuatro fases:

1. Planificación del proyecto de riesgos
2. Análisis de riesgos
3. Gestión de riesgos
4. Selección de salvaguardas

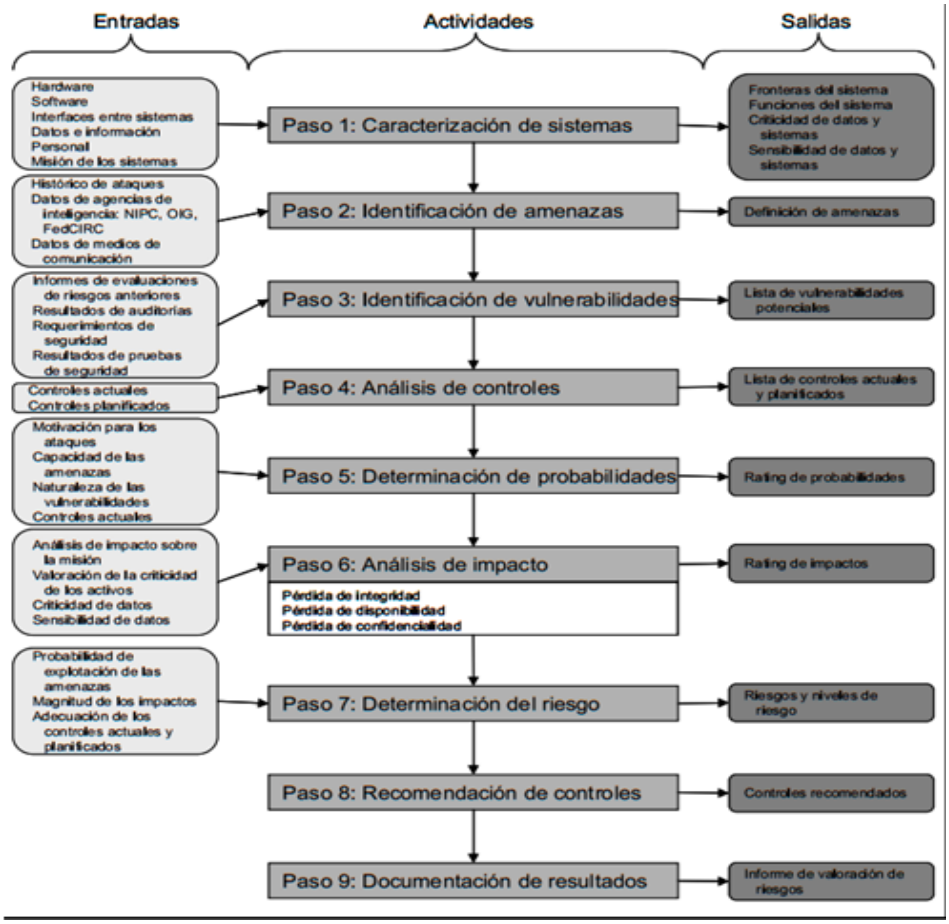
Otro aspecto importante a señalar es que esta metodología es acompañada por un software que da soporte a todo el proceso denominado PILAR.

NIST800-30

Por último, podemos mencionar la guía para la administración de riesgos de Tecnologías de Información del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos. Similar a MAGERIT en el Gobierno Español, esta norma es aplicable a todas las Instituciones gubernamentales de los Estados Unidos y es ampliamente referenciada. Está compuesta por nueve pasos que se aplican para el análisis de los riesgos.

1. Caracterización del sistema.
2. Identificación de amenaza.
3. Identificación de vulnerabilidades.
4. Control de análisis.
5. Determinación del riesgo.
6. Análisis de impacto.
7. Determinación del riesgo.
8. Recomendaciones de control.
9. Documentación de resultados.

La siguiente figura identifica el proceso de análisis de riesgos definido en la metodología:



Fuente: (Valencia Duque, 2016)

Conclusiones y recomendaciones

Puede concluirse a partir de las normas, mejores prácticas y recomendaciones sobre la Gestión de Riesgos de TI, que las Tecnologías de Información y Comunicaciones (TIC) se han convertido en activos estratégicos de las organizaciones actuales y esto aplica al ámbito empresarial de Costa Rica, las tendencias a la automatización, la transformación digital y la nueva realidad de la empresas han generado altos niveles de dependencia de las TIC en el funcionamiento de las organizaciones, lo que las hace imprescindibles para la buena marcha de sus procesos estratégicos, tácticos y operativos, con lo cual la implantación de un Gobierno de TI y una adecuada gestión de riesgos son factores críticos de éxito o de aseguramiento de las operaciones, para reducir la incertidumbre de eventos que pueden afectar las tecnologías de información y por ende procesos internos de las empresas.

La implementación de normas internacionales de gestión de riesgos mejora las capacidades organizacionales y la respuesta a los efectos que el contexto tecnológico incorpora en las perspectivas de análisis de riesgo y gobierno.

Tal como nos señala Francisco, (Valencia Duque, 2016), propiamente en el contexto de riesgos de TI podemos concluir que *“los activos objetos de análisis deben ser identificados, teniendo en cuenta las diferentes capas tecnológicas que hacen parte de las TIC, y que a su vez se vuelven interdependientes para dar una cobertura total, no solo de la información, sino de los activos que le dan soporte.*

Los criterios de impacto, a su vez, son los que le dan la connotación propia del contexto tecnológico para ser pertinentes y disminuir, al menos en cierta medida, la subjetividad al momento de su evaluación”, por tanto, la gestión de riesgos de TI debe considerarse un elemento dentro de la estrategia organizacional.

Referencias bibliográficas

- Alfaro Campos, J. C. (2017). *Metodología para la gestión de riesgos de TI basada en COBIT 5.* Cartago, Costa Rica: Instituto Tecnológico de Costa Rica.
- Alvarado Carpio, D. F., & Zumba Morales, L. A. (2015). *Elaborar un Plan de Gestión de Riesgos de las Tecnologías de Información y Comunicación basada en el Marco COBIT 5 para riesgos aplicado a la Universidad de Cuenca.* Cuenca - Ecuador: Universidad de la Cuenca. Obtenido de http://dspace.ucuenca.edu.ec/handle/123456789/22342
- Garbarino Alberti, H. (2014). *Marco de Gobernanza de TI para empresas PyMEs - SMEsITGF.* Madrid: Universidad Politécnica Madrid.
- Gaseta, E. R., Motta, A. C., & Boca Piccolini, J. D. (2016). *Fundamentos de gobierno de TI*. Obtenido de https://cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI2.pdf
- González, P. (30 de Noviembre de 2018). *COBIT 2019 — El nuevo modelo de gobierno empresarial para información y tecnología.* Obtenido de https://medium.com/: https://medium.com/@ppglzr/cobit-2019-el-nuevo-modelo-de-gobierno-empresarial-para-informaci%C3%B3n-y-tecnolog%C3%ADa-a7bf92b7288b
- Hamidovic, H. (2008). Gobierno de TI. Fundamentos del Gobierno de TI basados en ISO/IEC 38500. *ISACA Bogotá Chapter*, 1-9.
- ISACA. (2012). *Cobit 5. Un marco de negocio para el gobierno y la gestión de las TI de la Empresa.* Estados Unidos: ISACA.
- ISACA IT RISK. (2009). *Marco de Riesgos de TI.* Estados Unidos de América: ISACA.
- ISACA®. (2012). *Cobit 5. Procesos Catalizadores.* Estados Unidos: ISACA.
- Medina Cárdenas, Y. C., Areniz Arévalo, Y., & Rico Bautista, D. W. (2016). Alineación estratégica bajo un enfoque organizacional de gestión tecnológica: ITIL & ISO 20000. *Tecnura*, 82-94. Obtenido de http://revistas.udistrital.edu.co/ojs/index.php/Tecnura/issue/view/805
- Pacheco Garisoain, M. L. (2016). *Tecnologías de la información y la comunicación*. Obtenido de https://elibro.net/es/ereader/usanmarcos/38062
- Real Academia Española. (12 de 12 de 2020). *Diccionario de la Lengua Española*. Obtenido de https://dle.rae.es/
- *UNE-ISO/IEC 38500 Gobernanza Corporativa de la Tecnología de Información.* (2013). Madrid-España: AENOR.
- Valencia Duque, F. J. (Marzo de 2016). Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional. *Gerencia Tecnológica Informática, 15*(41), 65-77. Obtenido de https://www.researchgate.net/publication/311206737
- Vargas Bermúdez, F. A. (2014). Marcos de control y estándares para el gobierno de tecnologías de información (TI). *I+3 Investigación Innovación Ingeniería*, 31-44.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica