IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

FÉLIX ALBERTO ROZO LARA
Universidad Piloto de Colombia
Bogotá, Colombia
felixa79@hotmail.com

Resumen - El análisis, implementación, desarrollo y continua revisión a la implementación de un **SGSI** (Sistema de gestión de seguridad de la información), permite a las entidades privadas y del estado fortalecer sus políticas y procesos encaminados a la seguridad de su información, al compromiso de calidad y confianza hacia sus usuarios, clientes y directivas gerenciales.

A través de la creación y desarrollo gigantesco de tecnologías de comunicación cada día se está más expuesto al fraude y la exposición no autorizada de datos, información y demás activos vitales para cualquier organización.

Si bien es imposible negarse a los constantes cambios de información y tecnologías, si es importante estar preparados ante posibles fallas, cambios o sucesos inesperados o cualquier evento que ponga en riesgo nuestra información y su contenido.

Abstract **–** The analysis , implementation, development and ongoing review of the implementation of an ISMS (*information security management system*, ISMS) , it allows private and state institutions strengthen their policies and processes for the security of information, to commitment to quality and confidence to its users , customers and management directives . Through the creation and massive development of communication technologies every day is more exposed to fraud and unauthorized exposure data, information and other vital assets for any organization.

While it is impossible to refuse to constantly changing information and technology , if it is important to be prepared for possible failures, changes or unexpected events or any event that threatens our information and content.

Índice de Términos **–** Gestión, seguridad, informática e información.

I. INTRODUCCIÓN

Debido a la constante creación de nuevas tecnologías y medios de comunicación, que de manera extraordinaria se generan e implementan, y si bien buscar mejorar de manera vertiginosa los procesos, procedimientos, transacciones, servicios, tareas y minimizando desplazamientos, se ha formado un espacio de ilegalidad que permite a los usuarios sobrepasar los niveles permitidos, esos espacios que son privados, si los relacionamos con la información de cada entidad u organización, deben contar con estándares y sistemas lógicos y físicos de protección, que garanticen la seguridad de los mismo.

Es por eso, que cada día las organizaciones aúnan esfuerzos en concientizar y dar la importancia que requiere la información, como uno de los activos más preciados, para cada una y desde cualquier punto de vista, sin importar su tamaño u objetivo de cada negocio.

Hasta hace poco tiempo la seguridad de la información era tarea de algunos pocos, que no eran conscientes o no conocían los riesgos y amenazas que día a día son materia constante de estudio, por organizaciones que conscientes de la materialización de estas amenazas, han creado verdaderos equipos de trabajo interdisciplinarios y gracias a estándares y procesos sistemáticos se busca establecer metodologías antes la gestión de la seguridad de manera estructura y enfocada a cualquier tipo y tamaño de entidad.

Así las cosas, es importante que se entienda la seguridad de la información de manera global, es decir, como un todo, aunque la gran mayoría de la información de las organizaciones reside en computadores y robustos servidores, un sistema de gestión de seguridad de la información, abarca y esta complementada por todo lo que rodea a una entidad, es decir, documentación física, lógica, conocimiento personal, seguridad perimetral, relación contractual con terceros y todos aquellos datos y procesos propios de un negocio, sin importar su razón de ser o tamaño.

Por todo los anterior y a raíz del crecimiento de amenazas tecnológicas, como hackers, virus, espionaje electrónico, robos de identidad, igualmente se debe pensar en aquellos riesgos que son inherentes y que no existe un alto grado de posibilidad de evadirlos, pero si se debe estar preparado y contar con planes de contingencia y continuidad del negocio ante eventos o desastres naturales como terremotos, inundaciones, asonadas, paros cívicos y demás que pueda afectar o vulnerar

la seguridad de la información y continuidad de una organización.

Gracias a la norma ISO 27001 que se establece con la asistencia del sistema de gestión de seguridad de la información, se puede formalizar y garantizar que la información, sus procesos y contenidos sean confidenciales, integrales y siempre estén disponibles cuando se requieran.

Aunado a lo anterior, es importante que las entidades adopten una guía autorizada, siendo conscientes del completo y efectivo tratamiento que se debe dar a cualquier tipo de información que se considere como relevante o no, para las organizaciones.

II. CONCEPTOS PRELIMINARES

A. Sistema

Son partes o elementos que además de estar organizados deben estar relacionados para que interactúen y así poder lograr los objetivos para el cual fueron creados.

B. Sistema de Información

Puede definirse como el conjunto de componentes interrelacionados que permiten capturar, procesar, almacenar, y distribuir la información para apoyar la toma de decisiones y el control en una institución.

C. Gestión

Es la acción o tramite que hay que llevar a cabo para conseguir o resolver una cosa, también se puede definir como un conjunto de operaciones que se realizan para dirigir y administrar un negocio o una empresa.

D. Información

Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.

E. Seguridad

Se define la seguridad como la ausencia de peligro, daño o riesgo, igualmente es la sensación de confianza que se tiene en algo o alguien.

F. Proyecto

Es un esfuerzo temporal para crear un producto, resultado o servicio único.

III. DESARROLLO

Por sus siglas SGSI, un sistema de gestión de seguridad de la información, y de acuerdo a la norma ISO27001, consiste en la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Cada uno de sus pilares se basa en que la información sea tratada de manera adecuada y se garanticen de acuerdo a los siguientes lineamientos:

Confidencialidad: la información solo está disponible a las entidades, sistemas, procesos y/o personas autorizadas.

Integridad: es el mantenimiento de la exactitud y validez que tiene la información, y que la protege de modificaciones que no han sido autorizadas por su o sus propietarios.

Disponibilidad: es el acceso y utilización de los servicios solo y en el momento que un usuario o entidad así lo requiera.

Así las cosas, una entidad en la cual se da prioridad a la debida gestión de la información, debe anticipar su trabajo, en detallar a todo nivel los riesgos a los cuales se ve expuesto, independiente del tamaño de cada organización, esto le permitirá no solo cuantificar y calificar la gestión de riesgos, sino además, identificar vulnerabilidades, amenazas, identificar los activos y su nivel de exposición, valorar y cuantificar sus activos, conocer que requerimientos de seguridad necesita y definir controles para toda la organización.

Las organizaciones deben, además de definir sus políticas de seguridad, plantear caminos y metas de continuo mejoramiento hacia la seguridad y gestión de la información.

IV. REQUERIMIENTOS DEL SGSI

Es indispensable que todas las organizaciones públicas y privadas, adquieran las destrezas suficientes que permiten reconocer la importancia de porque se debe contar con la implementación, operación, seguimiento, revisión y continuo desarrollo en mejoras de un Sistema de Gestión de Seguridad de la información.

Así mismo, se fortalece y difunde la cultura organización de la seguridad de la información, reduciendo la operatividad de muchos procesos dentro de una entidad, inclusive aumentando el desempeño de varias de sus actividades, si esta cuenta con varias sucursales, filiales y/o plantas en una o varias ciudades del país.

Para todo nuevo proyecto, como lo requiere un sistema de gestión de seguridad de la información, se requiere contar con el apoyo constante de la alta dirección, por consiguiente es necesario que conozcan el vínculo que se tiene entre un sistema de gestión de seguridad de la información y como se alinean con los objetivos de la organización.

Estos fusionados objetivos y beneficios son:

- Reducir los riesgos de seguridad de la información.

- Reducir la probabilidad y el impacto de los incidentes de seguridad.
- Evaluación integral de todos los riesgos que afecten la organización.
- Gobierno integral.
- Obtener una certificación de calidad que genere un buen nombre y confianza hacia sus clientes o usuarios.
- El reconocimiento de buenas prácticas aceptadas en la seguridad de la información.
- Adecuada gestión de costos y calidad.

Aunado a lo anterior se requieren de ciertos compromisos y requerimientos que se deben plantear a la hora de tomar la decisión y realizar un análisis minucioso de lo que se necesita, de acuerdo al tamaño de cada organización o entidad, a continuación se detallan en su gran mayoría los requerimientos que apuntan hacia un SGSI:

- Contar con el compromiso y participación activa de la dirección y/o alta gerencia.
- Cada organización debe definir y detallar la o las políticas y objetivos alineados a las metas negocio.
- Definir el alcance del SGSI en su organización, permitirá que se establezcan los límites de inicio a fin como marco de trabajo, sin que esto implique adicionarse a todos los procesos de la entidad, es ideal avanzar paso a paso.
- Por lo anterior, es muy importante que se defina desde el comienzo el mapa de procesos completo de cada entidad u organización y la implicación de cada uno de sus actores de manera directa o indirecta.
- Detallar el inventario de activos de información de la organización.
- Definir que procedimientos se verán implicados en el SGSI a implementar y así definir los controles.
- Detallar la metodología y plan de tratamiento ante la evaluación de los riesgos, es importante que la entidad vislumbre que el riesgo siempre está latente aunque sea en un mínimo o bajo porcentaje.
- Analizar y evaluar cada uno de los riesgos y su posible impacto ante cualquier eventualidad negativa y su respectiva documentación.
- Identificar amenazas, vulnerabilidades y su impacto real.
- Definir procedimientos ante el manejo, planificación, control de los procesos que impliquen la seguridad de la información y las métricas de los controles y sus resultados.
- Selección los controles en el tratamiento de los riesgos identificados.
- Detallar y documentar todos los hallazgos, avances y resultados de las métricas.
- Definir y detallar todos los procedimientos para la adecuada gestión de la documentación producto del SGSI.
- Definir una declaración de aplicabilidad SOA (Statement Of Applicability) que debe incluir los objetivos de control y controles seleccionados, objetivos de control y controles que ya están implantados y objetivos de control y controles del anexo A excluidos y los motivos de exclusión, nivel de madurez del control, administración aplicabilidad de los controles y la debida aprobación de esa declaración de aplicabilidad.
- Definir procesos y estrategias de comunicación y divulgación de la seguridad de la información a todo el personal de la entidad.
- Realización y documentación de auditorías internas.
- Revisiones frecuentes del tratamiento del riesgo.
- Implantar procedimientos y controles que permitan detectar de manera eficaz una debida respuesta ante incidentes de seguridad.
- Desarrollo y aplicabilidad de un marco normativo, legislación, manuales y procedimientos.
- Plan de mejora, monitoreo y revisión constante al SGSI.
- El monitoreo y la revisión constante permiten detectar a tiempo errores o fallas generados como resultado de procedimientos. Así como, orientar a la dirección en el correcto procesamiento de la información, tal y como se tenía previsto en el alcance.
- Analizar y aprender de los indicadores y sus resultados.
- Igualmente la organización debe propender por la mejora continua, de acuerdo a las mejoras identificadas en el alcance.
- Aplicabilidad y monitoreo al PHVA (planear, hacer, verificar, actuar).

- Monitorear el alcance y efectividad del plan de continuidad del negocio.

V. ESTABLECIMIENTO E IMPLEMENTACIÓN DEL SGSI

Establecer e implementar un sistema de gestión de seguridad de la información implica tomar una serie de responsabilidades en conjunto para una organización, su equipo de trabajo interno y si lo requiere el proyecto, también de una asesoría externa.

Es por eso que anticipadamente se planifica un proyecto bien estructurado, con personal de confianza, profesionales, preferiblemente con experiencia laboral en el tema y con la experticia necesaria para el caso.

Tanto para una organización, el grupo del proyecto y los directos implicados es necesario:

- Contar con la aprobación encaminada a la obtención de un **SGSI.**
- Realizar un análisis de lo que requiere la organización en contexto.
- Comprender las necesidades de los interesados.
- Determinar el alcance del sistema a implementar.
- Definir y establecer las políticas.
- Realizar la matriz de valoración de riesgos.
- Definir los lineamientos para el tratamiento de riesgos.
- Implementar las políticas para el tratamiento de riesgos.

Igualmente las organizaciones deben tener en cuenta aquellas restricciones o contras que se pueden presentar antes o durante el proyecto de implementación de un SGSI:

- Recursos.
- Riesgos.
- Calidad del proyecto.
- Presupuesto.
- No cumplimiento de cronogramas de trabajo.
- El alcance.

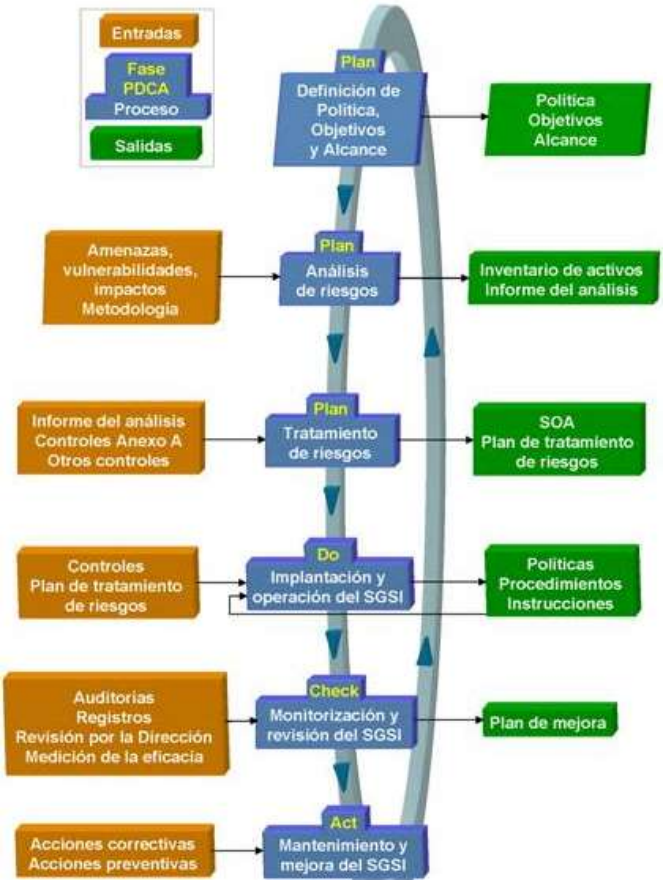
La organización debe contar con un equipo de trabajo que cuente con la experiencia necesaria para liderar el análisis e implementación de un sistema de gestión de seguridad de la información, que mantenga una debida comunicación con todas las áreas involucradas, debe contar con sabiduría organizacional y de grupo, para orientar y direccionar a la entidad hacia el cumplimiento de sus objetivos.

Así las cosas, se deben definir desde el comienzo, tanto los roles como las responsabilidades iniciales que cada actor o involucrado, aplicados al alcance.

Por todo lo anterior se debe planificar el proyecto de acuerdo al tamaño de la entidad y de la siguiente manera:

- Elaborar el plan de proyecto.
- Definir alcance.
- Consulta y análisis de requerimientos.
- Planificar y elaborar un cronograma de trabajo.
- Establecer actividades.
- Planificar la duración del proyecto vs cronograma.
- Planificación e informe de costos.
- Estimación de costos.
- Estimación de duración.
- Elaboración del presupuesto.
- Planificar los procesos de calidad a implementar.
- Plan de adquisiciones.
- Plan de divulgación y comunicaciones.
- Planificación y gestión de riesgos.
- Identificación y gestión de riesgos.
- Plan de respuesta y tratamientos de los riesgos.

Figura No. 1
ENFOQUE A PROCESOS



En la planificación, cada organización en cabeza del gerente del proyecto debe establecer en contexto las actividades globales de la entidad y los riesgos a los cuales es vulnerable.
La organización debe definir desde la planificación el alcance y límites del SGSI.

En la consulta y análisis de requerimientos, el gerente de proyecto debe realizar un estudio detallado con los directos interesados, identificar y documentar las necesidades halladas como resultado del estudio.

Elaborar de acuerdo a la experiencia y a lo planificado un cronograma detallado de trabajo, de acuerdo a los límites de la organización y el alcance del proyecto, analizando la secuencia de actividades, tareas, tiempo, duración, costos y posibles modificaciones o alteraciones en el tiempo. Es conveniente que se siempre se tengan previstos cambios factibles durante la sucesión del proyecto, es decir, el cronograma debe permitir y ser adaptable a procesos de cambios, debidamente controlados por el gerente del proyecto y la entidad.

Aunado a lo anterior, se debe contar con herramientas y estrategias de control de cambios que permitan medir si es posible el cambio, su impacto positivo, impacto negativo, beneficios, el costo monetario, el periodo en tiempo en que afectaría el proyecto, sus resultados, medición y control constante.

Una vez realizado el cronograma, el gerente de proyecto debe identificar y documentar las actividades definidas, para cumplir el objetivo de acuerdo a los entregables del SGSI.

La estimación de los costos asociados al proyecto, le permite al gerente conocer una aproximación de los valores y recursos monetarios necesarios para la construcción del proyecto.

La estimación de la duración del proyecto se puede realizar basándose en experiencias relacionados con casos similares, realizando simulaciones, bases de datos y/o el método de PERT.

El método PERT, permite dirigir y direccionar nuestro proyecto y el sistema de seguridad de la información hacia una adecuada programación, se representa a través de una red de tareas, que de manera organizada y puntual permitirá alcanzar los objetivos trazados en el proyecto.

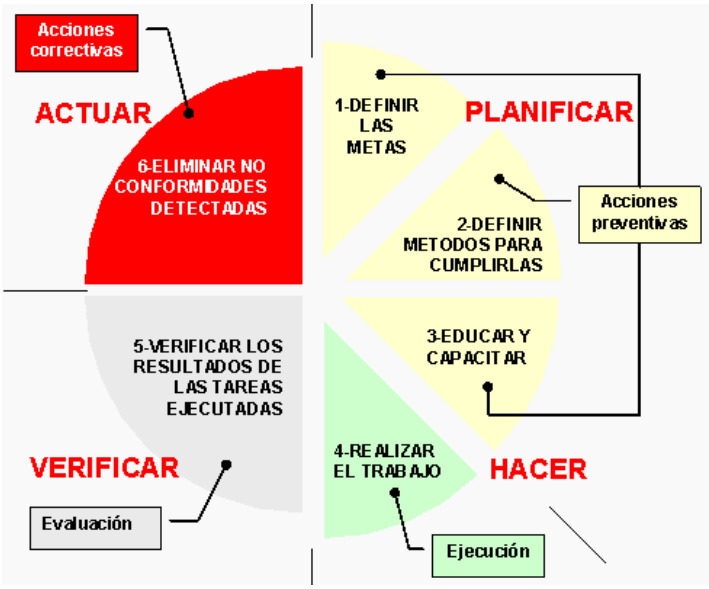
El método debe definir:

- El detalle preciso de todas y cada una de las etapas del proceso.
- Realizar un estimado en el cálculo de cada tarea en tiempo.
- El jefe o jefes de proyecto deben realizar un monitoreo y supervisión constante a cada una de las etapas en su avance y duración.

Cuando se requiere de la elaboración y edificación del presupuesto, el gerente de proyecto debe tener en cuenta la agregación de los costos estimados de cada actividad, y correlacionar que el presupuesto define la línea de control que se tiene para los costos del proyecto durante su duración.

La calidad de los productos o servicios esperados, deben contar con los debidos procesos y revisión de calidad, el gerente de proyecto debe definir las políticas, responsabilidades y los objetivos de forma que lo entregado cumpla con lo pactado y esperado a nivel de calidad. Igualmente un sistema de gestión de seguridad de la información debe ser es objeto constante de auditorías de calidad, mejoras y cumplimiento.

Figura No. 2
CICLO PHVA



Tanto el gerente de proyecto como la organización deben planificar, asegurar y controlar la calidad del **SGSI.**

G. Planear

Se establecen los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requerimientos, políticas y lineamientos de la entidad

H. Hacer

Es la implementación efectiva de los procesos.

I. Verificar

Etapa en la cual se realiza el seguimiento a través de métricas aplicadas a los procesos y productos, correlacionados con las políticas y lineamientos de la organización y siempre documentando y analizando sus resultados.

J. Actuar

Etapa en la cual se toman las determinaciones y acciones encaminadas a mejorar continuamente el desarrollo de los procesos.
En la planificación se identifican requerimientos o lineamientos de calidad del proyecto, los productos, bienes o servicios a entregar y dejar debidamente documentado la manera en que se verificara a completa satisfacción, que se ha cumplido con las solicitudes de la entidad e internamente con cada uno de los dueños del proceso.

Durante la etapa del plan de adquisiciones, el gerente del proyecto en con junto con la alta dirección deben detallar la estrategia de compras, adquisiciones, plan de compras, estudios de mercado y estudio de potenciales proveedores, así como los criterios de selección de acuerdo al valor contractual y la modalidad de contratación, ya sea en empresa privada o pública.

El gerente de proyectos y la administración de la entidad deben planificar todas las comunicaciones enfocadas a sus clientes, empleados, usuarios y personal interno, a través de canales definidos en el respectivo plan de comunicaciones, en el cual definen la estrategia correcta para hacer efectivos los comunicados e información relacionada con el **SGSI** y sus interesados.

El grupo de comunicaciones de cata organización debe, capturar, crear, recolectar, transformar positivamente, distribuir, almacenar y realizar la entrega final de la información a comunicar, en la cual se debe detallar:

- Qué tipo de información se puede comunicar.
- Para quien va la información.
- Cuando y como se necesita la información.
- Para que se hace pública cierta información.
- Donde se necesita la información.

Para la gestión de riesgos, es necesario que se determine a través de una matriz la planificación de la gestión de riesgos, se identifiquen lo riesgos a los que está expuesta la organización, así como el plan de respuesta a los mismos.

- Plan de gestión de riesgos.
- Matriz de riesgos.
- Identificación del riesgo.
- Análisis de impacto del riesgo.
- Plan de respuesta y control al riesgo.

Definitivamente, el cierre y culminación del proyecto puede llegar a ser entre las diferentes etapas, la más importante, esto debido a que se cierra oficialmente el objeto y proceso contractual, relacionado a nuestro proyecto que finaliza también con la implementación del SGSI a nuestra organización.

Figura No. 3
USO DEL SGSI

Previo a esta etapa, se deben haber cumplido con todos los requerimientos iniciales, cambios de momento, procesos de calidad y los respectivos pagos pactados en la etapa contractual, así como la documentación de cierre del proceso y acta de liquidación.

Finalmente y una vez tenemos el **SGSI** trabajando en nuestra organización, las revisiones y mejoras serán constantes, siempre buscando el beneficio en conjunto y demostrando a los usuarios y clientes que se cuenta con una organización que emplea buenas prácticas de seguridad de la información formando canales de confianza y eficiencia en la continuidad y disponibilidad de la organización.

VI. CONCLUSIONES

El éxito de una adecuada implementación de un **SGSI**, requiere del esfuerzo en conjunto de toda una entidad, en cabeza de administrador o administradores de proyectos, que conozca y hagan participe a todas las partes involucradas, con el fin de alinear el Sistema de Gestión de Seguridad de la Información con los objetivos de la entidad y los objetivos propios relacionados con la seguridad de la información.

Un **SGSI** permite a las entidades comprender la importancia y ventajas de proteger toda su información a través de un sistema de seguridad, así como cambiar la actitud de trabajo, ante la consumación de buenas costumbres, implementadas en las políticas de seguridad de la organización.

Las entidades que quieran sobresalir y mantenerse en el mercado actual, deben propender por una mejora continua en la gestión de la seguridad su información y la que los rodea.

REFERENCIAS

[1] ISO 27000.es, disponible en línea en:
http://www.iso27000.es/sgsi_implantar.html#seccion1

[2] Implementación efectiva de un SGSI SO 27001, disponible en línea:
http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf
http://www.gerencie.com/sistemas-de-informacion.html

[3] Tecnologías, disponible en línea en:
http://dle.rae.es/?id=LXrOqrN&o=h
http://www.definicionabc.com/tecnologia/informacion.php
http://www.forodeseguridad.com/artic/discipl/4163.htm

[4] Ciclo PHVA, disponible en línea en:
http://www.gerencie.com/ciclo-phva.html
http://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/

[5] ISO – SGSI, Disponible en línea en:
http://www.gesconsultor.com/iso.html

[6] Figura No. 1 Disponible en línea en:
Portal de ISO en español:
Fuente: www.iso27000.es

[7] Figura No. 2 Disponible en línea en:
Fuente:http://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/

[8] Figura No. 3 Disponible en línea en:
Portal de ISO en español:
Fuente: www.iso27000.es

Autor

Félix Alberto Rozo Lara
Ingeniero de sistemas
Egresado de la Fundación Universitaria Los Libertadores
Bogotá – Colombia
Seminario de Investigación Aplicada Gestión del Riesgo - 2015