IX Congreso iberoamericano
de seguridad informática
Universidad de Buenos Aires
Ciudad Autónoma de Buenos Aires, Argentina
1 al 3 de noviembre de 2017

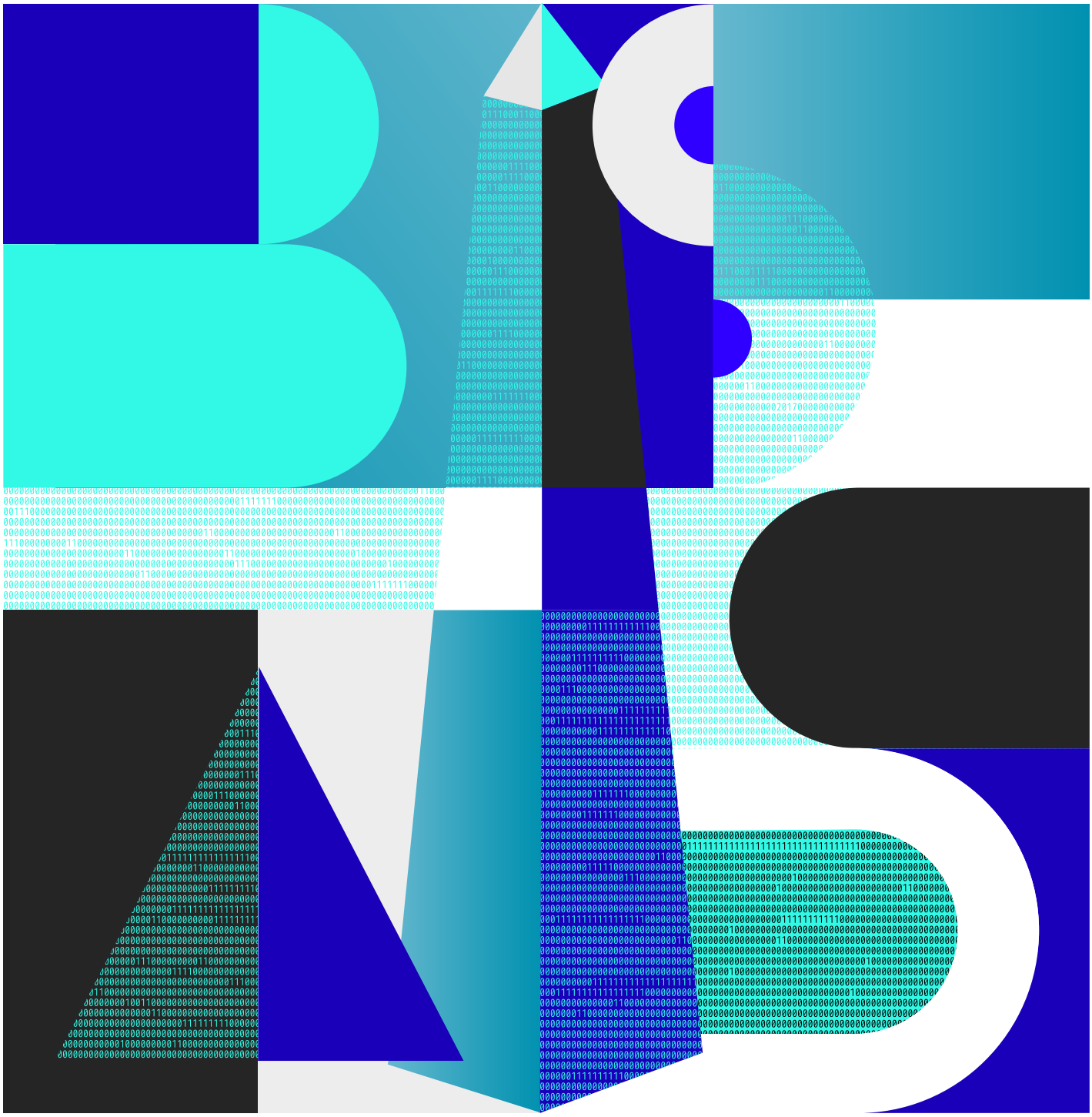
CIBSI

EU DE BA

PSI
POSGRADO EN SEGURIDAD INFORMATICA

CRIPTORED

Libro de Actas



Actas del IX Congreso Iberoamericano de Seguridad Informática
CIBSI2017, Buenos Aires, Argentina, 1 al 3 de Noviembre de 2017

Editores
Alberto E. Dams
Hugo A. Pagola
Luis E. Sánchez Crespo
Jorge Ramió Aguirre

Diseño de Tapas
Federico Dams

ISBN: en trámite

Prefacio

Del 1 al 3 de Noviembre se celebrará en la Universidad de Buenos Aires el IX Congreso Iberoamericano de Seguridad Informática - CIBSI 2017. El congreso está organizado por la Maestría en Seguridad Informática de la UBA en colaboración con la Red Temática Iberoamericana de Criptografía y Seguridad de la Información Criptored.

Este espacio permitirá a las empresas, entidades públicas, entornos militares, de defensa, centros académicos y de investigación exponer sus avances y servicios vinculados con la seguridad, facilitando el intercambio de conocimientos y la formación de redes de colaboración en este ámbito.

El congreso contará con la presencia de especialistas de Latinoamérica y de Europa entre otros de Argentina, Brasil, Colombia, Ecuador, México, Perú, Uruguay, España y Francia. Estamos muy satisfechos por el nivel de los artículos que se presentarán y el de los invitados especiales que tendremos. En esta novena edición del CIBSI, se destacan las presencias de referentes internacionales en la materia como Hugo Scolnik director de la Maestría en seguridad Informática de la UBA y Hugo Krawczyk Distinguished Research Staff Member with the Cryptography Group at the IBM T.J. Watson Research Center.

Organización de la Conferencia

Comité Organizador

Hugo Pagola, Facultad de Ingeniería Universidad de Buenos Aires, Argentina
Alberto Dams, Facultad de Ingeniería Universidad de Buenos Aires, Argentina
Jorge Ramió Aguirre, Universidad Politécnica de Madrid, España
Luis E. Sánchez Crespo, Universidad de Castilla La Mancha, España

Comité Local

Facundo Caram, FIUBA, Argentina
Luis Catanzariti, UTNfrba, Argentina
Marcia Maggiore, MUBA, Argentina
Patricia Prandini, MUBA, Argentina

Comisión de Posgrado Maestría en Seguridad Informática UBA

Mg Ing Alberto Dams, Maestria en Seguridad Informatica UBA, FIUBA, Argentina
Dr Pedro Hecht, Maestria en Seguridad Informatica UBA, Argentina
Ing Hugo Pagola, Maestria en Seguridad Informatica UBA, FIUBA, Argentina
Dr Ricardo Rivas, Maestria en Seguridad Informatica UBA, FCE-UBA Argentina
Dr Raul Saroka, Maestria en Seguridad Informatica UBA, FCE-UBA Argentina
Dr Hugo Scolnik, Maestria en Seguridad Informatica UBA, FCEN-UBA Argentina

Comité del Programa

Marco Aurélio Amaral Henriques	State University of Campinas - Unicamp, Brasil
Javier Areitio	Universidad de Deusto, España
Rodolfo Baader	Universidad de Buenos Aires, Argentina
Gustavo Betarte	Facultad de Ingeniería, Universidad de la República, Uruguay
Carlos Blanco Bueno	Universidad de Cantabria, España
Joan Borrell	Universitat Autònoma de Barcelona, España
Pino Caballero-Gil	DEIOC, Universidad de La Laguna, España
Jeimy Cano	Universidad de los Andes, Colombia
Eduardo Carozo	Universidad de Montevideo, Uruguay
Joan-Josep Climent	Universitat d'Alacant, España
Roger Clotet	Universidad Simón Bolívar, Venezuela
Alberto Dams	Universidad de Buenos Aires, Argentina
José María De Fuentes	Universidad Carlos III de Madrid, España
Josep Domingo-Ferrer	Universitat Rovira i Virgili, España
Jose-Luis Ferrer-Gomila	University of the Balearic Islands, España
Angelica Florez Abril	Universidad Pontificia Bolivariana, Colombia
Walter Fuertes	Universidad de las Fuerzas Armadas ESPE, Ecuador
Amparo Fuster-Sabater	Institute of Applied Physics, Madrid, España
Giovana Garrido	Universidad Tecnologica de Panama
Lorena González Manzano	Universidad Carlos III de Madrid, España
Juan Pedro Hecht	Universidad de Buenos Aires, Argentina

Luis Hernandez Encinas	Institute of Physical and Information Tecnologies, España
Emilio Hernández	Universidad Simón Bolívar, Venezuela
Leobardo Hernández	Universidad Nacional Autónoma de México
Jordi Herrera	Universitat Autònoma de Barcelona, España
Monica Karel Huerta	Universidad Politécnica Salesiana, Ecuador
Angel Martin Del Rey	Universidad de Salamanca, España
Maria Vanina Martinez	Universidad Nacional del Sur in Bahia Blanca, Argentina
Vincenzo Mendillo	Universidad Central de Venezuela
Gaspar Modelo-Howard	Universidad Tecnológica de Panamá
Raul Monge	Universidad Técnica Federico Santa María, Chile
Karel Huerta Monica	Universidad Politécnica Salesiana, Ecuador
Guillermo Morales-Luna	Centro de Investigación y Estudios Avanzados, Mexico
Alfonso Muñoz	Criptored, España
Hugo Pagola	UBA - Facultad de Ingenieria, Argentina
Graciela Pataro	Universidad de Buenos Aires, Argentina
Alberto Peinado	Universidad de Malaga, España
Jose Pirrone	Universidad Catolica Andres Bello, Venezuela
Gustavo Presman	Universidad de Buenos Aires, Argentina
Jorge Ramio	Universidad Politécnica de Madrid, España
Ricardo Rivas	Universidad de Buenos Aires, Argentina
David Rosado	University of Castilla-La Mancha, España
Luis Enrique Sanchez Crespo	Universidad de Castilla La Mancha, España
Antonio Santos-Olmo Parra	Sicaman Nuevas Tecnologías
Raul Saroka	Universidad de Buenos Aires, Argentina
Hugo Scolnik	Universidad de Buenos Aires, Argentina
Pablo Silberfich	Universidad de Buenos Aires, Argentina
Jenny Torres	Escuela Politécnica Nacional, Ecuador
Urko Zurutuza	Mondragon University, España

Proceso para Mantenimiento Dinámico de un Análisis de Riesgos Utilizando MARISMA

L. E. Sánchez, A. Santos-Olmo, S. Camacho, D.G Rosado, E. Fernandez-Medina

***Abstract* – The information society is increasingly dependent on Information Systems Security Management (ISMS) and knowledge of the security risks associated with the value of its assets. However, very few risk analysis methodologies have been produced so as to create systems with which to analyze risks in a rapid and economical manner and which can, in turn, leave this system dynamically updated. This paper presents the "dynamic maintenance of a risk analysis" process of the MARISMA methodology. This process allows a reusable and low cost risk analysis to be obtained. The objective of MARISMA is to carry out a simplified and dynamic risk analysis that will be valid for all companies, including SMEs, and to provide solutions to the problems identified during the application of the "Action Research" scientific method. This methodology is being directly applied to real cases, thus allowing a constant improvement to be made to its processes.**

***Index Terms* — Cibersecurity, *Information Systems Security Management, ISMS*, Risk Analysis, SME, ISO27001, ISO27005, Magerit.**

I. Introducción

Estudios realizados han demostrado que para que las empresas puedan utilizar las tecnologías de la información y las comunicaciones con garantías es necesario disponer de guías, métricas y herramientas que les permitan conocer en cada momento su nivel de seguridad y las vulnerabilidades que aún no han sido cubiertas [1-4]. El problema de conocer los riesgos a los que están sometidos sus principales activos se acentúa especialmente en el caso de las pequeñas y medianas empresas, que cuentan con la limitación adicional de no tener recursos humanos y económicos suficientes para realizar una adecuada gestión [5, 6].

Pero con la llegada de Internet, para las empresas es cada vez más crítico implantar controles de seguridad que les permitan conocer y controlar los riesgos a los que pueden estar sometidas [7, 8]. Algunos autores [9, 10] sugieren la realización de un análisis de riesgos como parte fundamental en la PYME, ya que deben tener en cuenta que el valor y la sanción de los datos robados o filtrados en una pequeña organización es el mismo que para una grande, y por tanto debe tener controlado el valor y los riesgos a los que esos activos están sometidos [11]. Otros autores [12] proponen la necesidad de desarrollar un nuevo modelo de análisis de riesgos (AR) pero orientándolo directamente a las PYMES, considerando que el uso de técnicas de análisis y gestión de riesgos, así como el papel de terceros, es necesario para poder garantizar la seguridad del sistema de información de las PYMES [13]. Aunque la investigación realizada se centra inicialmente en las PYMES los resultados podrían aplicarse en otros sectores como el de salud [14-16], o nuevas tecnologías como el cloud computing [17, 18].

Algunos autores sugieren que no es suficiente con aplicar un enfoque basado en análisis y gestión de riesgos [19] sino que, además de identificar y eliminar riesgos, también este proceso se ha de realizar de manera eficiente, ahorrando dinero, consecuencia directa de una correcta gestión de la seguridad [20]. Otro de los aspectos críticos, es el control de los costes asociados a la gestión de la seguridad, de esta forma, Mercuri [21] se propone asociar como parte fundamental del desarrollo de los SGSI (Sistema de Gestión de Seguridad de la Información) los análisis de coste–beneficio (CBA) en la fase del análisis de riesgos.

Como tal, una de las cuestiones derivadas de las conclusiones es la necesidad de obtener nuevas metodologías y modelos de análisis y gestión del riesgo que permitan adaptarse a las PYMES, con el objetivo de eliminar (o al menos reducir) los inconvenientes y ayudar a estas sociedades a evaluar los riesgos a los que sus activos están expuestos y a establecer los controles de seguridad adecuados [22].

Muchos autores consideran que el punto central de los SGSI debe ser el análisis de riesgos. Entre ellas se puede destacar la propuesta de Barrientos [23] y UE CORAS (IST–2000–25031) [24, 25]. La propuesta de Barrientos [23] está basada en llevar a cabo un análisis relativo a la seguridad informática para identificar el grado de vulnerabilidad y determinar los aspectos de mejora a ser llevados a cabo en la organización con el objeto de reducir el riesgo. Por otro lado, UE CORAS (IST–2000–25031) [24, 25] está desarrollando un marco para el análisis de riesgos de seguridad que utiliza UML2, AS/NZS 4360, ISO/IEC27001, RM–ODP6 y UP7.

Siegel [19] señala que los modelos de seguridad informática que se centran exclusivamente en modelos de eliminación de riesgos no son suficientes, y por otro lado Garigue [20] remarca que actualmente los gerentes no desean saber sólo qué se ha realizado para mitigar los riesgos, también se debe poder dar a conocer eficazmente que se ha realizado esta tarea y si se ha conseguido ahorrar dinero.

Uno de los aspectos cruciales que se extrae de las investigaciones, es que el análisis de riesgos es un proceso

A. Santos-Olmo, Departamento I+D+i, Sicaman Nuevas Tecnologías, Tomelloso (Ciudad Real), España, Asolmo@sicaman-nt.com

L. E. Sánchez, Universidad de Castilla-la Mancha (UCLM), España y Universidad de las Fuerzas Armadas (ESPE), Proyecto Prometeo de la SENESCYT, Ecuador, Luisenrique@sanchezcrespo.org

S. Camacho, Universidad Técnica Ambato, Ecuador, saracamachoestrada1@yahoo.es

D.G. Rosado, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, David.Grosado@uclm.es

E. Fernandez-Medina, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, Eduardo.FdezMedina@uclm.es

costoso que no se puede repetir cada vez que se realiza una modificación. Por eso es importante desarrollar metodologías específicas que permitan mantener los resultados del análisis de riesgos, es decir, procesos que permitan un análisis de riesgos dinámico. El proyecto de la UE Coras [24, 25] hace de este mantenimiento el punto principal de su modelo.

Las principales conclusiones obtenidas es que los modelos de análisis y gestión del riesgo son fundamentales para los SGSIs, pero no existen metodologías que se adecuen al caso de las PYMES, y las existentes se muestran ineficientes para este tipo de compañía.

Por lo tanto, y considerando que las PYMES representan una gran mayoría de empresas tanto a nivel nacional como internacional y son muy importantes para el tejido empresarial de cualquier país, creemos que avanzar en la investigación para mejorar los procesos de análisis y gestión del riesgo para este tipo de empresas puede generar importantes aportaciones. Esto puede contribuir a mejorar no sólo la seguridad de las PYMES, sino también su nivel de competitividad. Por este motivo, a los largo de los últimos años hemos trabajado en elaborar un proceso simplificado que permita analizar y gestionar el riesgo de seguridad en las PYMES [26-28], y además hemos construido una herramienta que automatiza completamente la metodología [29], y lo hemos aplicado en casos reales [30], lo que nos ha permitido validar tanto la metodología como la herramienta.

Toda la metodología de Análisis de Riesgos desarrollada, y en especial las partes relacionadas con los controles, han sido aplicadas sobre la norma ISO/IEC27001 y en especial sobre el Anexo A de ésta, que define los controles que deben cumplirse. Por lo tanto, y aunque esta metodología nace para poder extenderse a otros estándares internacionales, actualmente sólo se ha validado su funcionamiento sobre el estándar internacional de la ISO/IEC27001.

El artículo continúa en la Sección 2 describiendo brevemente las metodologías y modelos para el análisis y la gestión del riesgo de la seguridad y su tendencia actual. En la Sección 3 se introduce nuestra propuesta para el proceso de mantenimiento de un análisis de riesgos dinámico utilizando MARISMA. Finalmente, en la Sección 4 concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

II. ESTADO DEL ARTE

Con el propósito de reducir las carencias mostradas en el apartado anterior y reducir las pérdidas que éstas ocasionan, han aparecido un gran número de procesos, marcos de trabajo y métodos para la gestión del riesgo cuya necesidad de uso para proteger de forma eficaz los activos de una compañía está siendo cada vez más reconocida y considerada por las organizaciones, pero son ineficientes para las PYMES.

En relación con los estándares más destacados se ha podido constatar que la mayor parte de ellos han intentado incorporar procesos para el análisis y la gestión del riesgo, pero que son muy difíciles de implementar y requieren una inversión demasiado alta que la mayoría de las PYMES no pueden asumir [31].

Entre las principales propuestas para el análisis y gestión del riesgo podemos destacar MAGERIT [32], OCTAVE [33] o CRAMM [34]. A pesar de ello, la gestión de la seguridad no puede limitarse al análisis y la gestión del riesgo [19], sino que además de identificar y eliminar riesgos se ha de realizar de manera eficiente, obteniendo la compañía grandes ahorros de costes como consecuencia directa de una mejor gestión de la seguridad [20]. Gracias al análisis de riesgos se podrán identificar los activos y conocer el nivel de seguridad que se debe aplicar. Los expertos también han propuesto recientemente realizar un análisis de riesgos para poder alinear las estrategias de la empresa y de la seguridad [35], ya que esto hace que la empresa pase de tomar una posición reactiva ante la seguridad a una proactiva.

Por otro lado, algunos de los principales estándares de gestión de la seguridad, han intentado incorporar dentro de sus procesos el análisis y la gestión del riesgo:

- *ISO/IEC27005 [36]:* Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC27001 [37] y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- *ISO/IEC21827/SSE–CMM [38, 39]:* El modelo de capacidad y madurez en la ingeniería de seguridad de sistemas describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad.
- *ISO/IEC 15443 [40, 41]:* Clasifica los métodos existentes dependiendo del nivel de seguridad y de la fase del aseguramiento.
- *ISO/IEC2000/ITIL [42, 43]:* ITIL ofrece un elemento para una correcta gestión de riesgos: el conocimiento actualizado y detallado de todos los activos de la organización y de las relaciones, pesos y dependencias entre ellos.
- *COBIT [44]:* Es una metodología para el adecuado control de los proyectos de tecnología, los flujos de información y los riesgos que implica la falta de controles adecuados.

El principal problema de estos procesos es su complejidad para aplicarlos en el caso de las PYMES, ya que han sido concebidos para grandes empresas [45-48]. Se justifica en repetidas ocasiones que la aplicación de este tipo de procesos para las PYMES es difícil y costosa. Además, las organizaciones, incluso las grandes, tienden más a adoptar grupos de procesos relacionados como un conjunto que a tratar los procesos de forma independiente [49].

Por lo tanto, y como conclusión de este apartado, se puede decir que es pertinente y oportuno abordar el problema de desarrollar un nuevo proceso para el análisis y gestión del riesgo de la seguridad para los sistemas de información en las PYMES, así como una herramienta que soporte este proceso, tomando como base la problemática a que este tipo de compañías se enfrenta y que ha llevado a continuos fracasos en los intentos de implantación hasta el momento.

III. METODOLOGÍA MARISMA

Para solucionar los problemas detectados en el análisis y gestión del riesgo, se ha realizado un proceso orientado a las PYMES y enfocado a reducir los costes de mantenimiento del proceso de análisis y gestión del riesgo denominado MDAR. Este proceso se ha obtenido mediante la aplicación del método de investigación en acción y se ha enmarcado dentro de una metodología (MARISMA) que acomete todos los aspectos relacionados con la gestión de la seguridad [14, 50], y bajo la premisa de que cualquier sistemas de Análisis de Riesgos valido para las PYMES también será extrapolable a grandes compañías. El objetivo de este proceso es el de generar un análisis de riesgos de bajo coste mediante la utilización de patrones reutilizables.

Mediante la metodología MARISMA, podemos asociar el análisis y la gestión del riesgo a los controles necesarios para la gestión de la seguridad y consta de tres procesos muy importantes:

- *Proceso 1 – Generación de Esquemas para el Análisis de Riesgos (GEAR -o GEGS: Generación de Esquemas para Gestión de Seguridad-):* Se establece una estructura de relaciones entre los diferentes elementos involucrados en el análisis del riesgo y los controles necesarios para gestionar la seguridad. Estas relaciones se establecen mediante el conocimiento adquirido en las diferentes implantaciones, que es almacenado en una estructura denominada esquema para ser reutilizado con posterioridad, reduciendo los costes de generación de este proceso [51].
- *Proceso 2 – Generación del Análisis y Gestión del Riesgo (GAGR -o GSGS: Generación del Sistema de Gestión de Seguridad-):* Mediante la selección del esquema más adecuado y la identificación de un pequeño conjunto de los principales activos se obtiene un detallado mapa de la situación actual (análisis del riesgo) y un plan de recomendaciones de cómo mejorarlo (gestión del riesgo).
- *Proceso 3 – Mantenimiento Dinámico del Análisis de Riesgos (MDAR -o MSGS: Mantenimiento del Sistema de Gestión de Seguridad-):* Mediante la utilización de las matrices generadas, las cuáles interconectan los diferentes artefactos, el sistema irá recalculando el análisis de riesgos según se produzcan incidentes de seguridad, fallen las métricas definidas o los auditores detecten "no conformidades" en los controles.

En este artículo nos centramos en el tercero de los procesos que tiene por objetivo el mantenimiento del análisis de riesgos de forma que se evite tenerlo que repetir cada vez que se produzca una modificación, permitiendo reducir los costes y hacerlo viable en el tiempo.

IV. MDAR. MANTENIMIENTO DINÁMICO DEL ANÁLISIS DE RIESGOS CON MARISMA

El principal objetivo de este subproceso es permitir y dar soporte a la compañía para que pueda gestionar la seguridad del sistema de información, utilizando para ello los entregables generados en el subproceso GAGR y los elementos que componen el SGSI.

Este subproceso ha sido desarrollado para que sea muy fácil y cómodo para los usuarios del sistema de información su cumplimiento, simplificando las tareas que lo componen.

En la Figura 1 se puede ver el esquema básico de entradas, actividades y salidas que componen este subproceso:

- Entradas: Como entradas se recibirá un conjunto de elementos (reglamentos, procedimientos, controles y su nivel de cumplimiento actual) que componen el SGSI.
- Actividades: El subproceso estará formado por tres actividades. Las actividades A3.2 y A3.3 siempre requerirán de haber realizado primero la actividad A3.1 para poder ejecutarse, y podrán hacerlo tantas veces como sea necesario durante el ciclo de vida (representado por un reloj en el esquema).
- Salidas: La salida producida por este subproceso consistirá en: i) un conjunto de entregables (certificado de cultura de la seguridad, instancias de ejecución de los procedimientos generales, instancias de ejecución del procedimiento de denuncia, cambios de estados en los niveles de cumplimiento de los controles que componen el cuadro de mandos) que servirán de apoyo al auditor de seguridad (AuS) y al responsable de seguridad (Cl/RS) para tomar medidas que mejoren la gestión de la seguridad; ii) datos e información estadística obtenida durante el funcionamiento diario del SGSI que se almacenará en el repositorio de información del SGSI para mantener actualizado el cuadro de mandos del sistema; y iii) conocimiento útil para que el grupo de expertos del dominio puedan mejorar los esquemas existentes y crear nuevos esquemas.

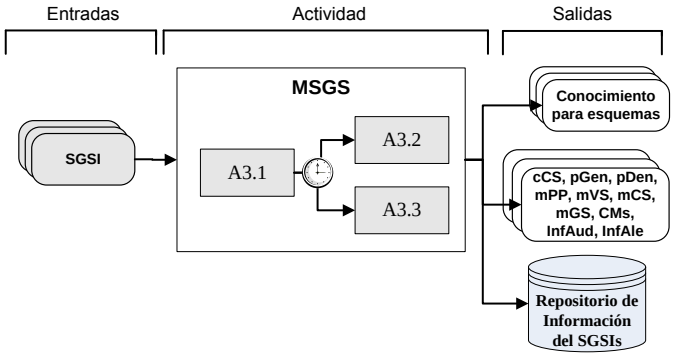


Figura 1. Esquema simplificado a nivel de actividad del subproceso MDAR.

En la Figura 2 se muestran las actividades del subproceso de forma mucho más detallada, viendo cómo interactúan éstas con el repositorio de SGSIs encargado de contener los elementos que conforman los diferentes SGSIs generados.

Los principales objetivos de las actividades de este subproceso son:

- A3.1 – Obtener o renovar el certificado de cultura de seguridad: Esta actividad se ocupa de introducir de

forma progresiva la cultura de seguridad entre los usuarios del sistema, recomendándoles la realización de forma periódica de exámenes de verificación de sus conocimientos con respecto a los reglamentos que componen el sistema de información de la compañía, y limitando la entrada al sistema de información mientras no demuestren que poseen un mínimo conocimiento de dichos reglamentos.

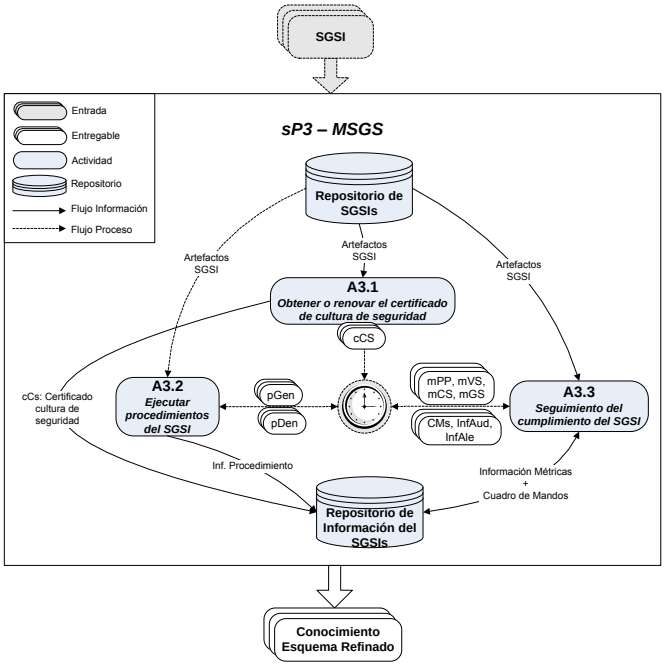


Figura 2. Esquema detallado a nivel de actividad del subproceso MDAR.

- A3.2 – Ejecutar procedimientos del SGSI: Esta actividad permite a los usuarios del sistema de información realizar de forma organizada procesos que afectan a la seguridad del sistema de información y que, por tanto, requieren un cierto grado de gestión. Estos procedimientos se han dividido en dos tipos: i) Procedimientos generales: Contienen las operaciones que deben realizar los usuarios para poder interactuar con el sistema de información de la empresa, manteniendo una adecuada gestión del mismo y el cumplimiento de los controles de seguridad. Es decir, permitirán a los usuarios del sistema de información interactuar con éste de una forma organizada y segura; y ii) Procedimiento de denuncia: Este procedimiento especial permite a los usuarios del sistema de información notificar fallos y violaciones en la seguridad del sistema de información, ayudando a tomar medidas correctivas.
- A2.3 – Seguimiento del cumplimiento del SGSI: Esta actividad se ocupa de mantener actualizado el nivel de madurez y el nivel de cumplimiento de los controles que componen el SGSI de la compañía, con el objetivo de permitir que tanto el responsable de seguridad (Cl/RS) como el auditor de seguridad (AuS) tengan conocimiento lo antes posible de pérdidas de seguridad del sistema de información y puedan tomar medidas correctoras. Las tareas incluidas en esta actividad son: i) la gestión del cuadro de mandos de seguridad; ii) la gestión de la periodicidad de los objetivos; iii) la gestión de las violaciones en los reglamentos de seguridad; iv) la gestión de los certificados de seguridad; v) la realización de auditorías periódicas; vi) la gestión de las métricas generales; y vii) la gestión del sistema de alertas.

Debido a que el subproceso MDAR no tiene un final determinado para las tareas, éstas podrán ejecutarse siempre que sea necesario para mantener la correcta gestión de la seguridad del sistema de información. Esto se ha representado en la Figura 2 mediante la imagen de un reloj.

La información generada en este subproceso se almacenará en el repositorio de información del SGSI, y los entregables se generarán para que el auditor de seguridad (AuS) y el responsable de seguridad (Cl/RS) puedan analizarlos y tomar medidas las medidas correctoras pertinentes para solucionarlos.

A. Objetivos.

Los principios básicos considerados durante el desarrollo de las actividades que conforman este subproceso son:

- Aportar a los usuarios del sistema de información los elementos necesarios para poder trabajar con él, manteniendo una adecuada gestión de la seguridad y con un coste de recursos reducido y adecuado a las PYMES.
- Permitir al responsable de seguridad (Cl/RS) conocer en todo momento el nivel de madurez de la gestión de seguridad del sistema de información de la compañía y el nivel de cumplimiento de cada uno de los controles o salvaguardas que lo componen, permitiéndole tomar en el menor plazo posible medidas correctoras.
- Incorporar la gestión de la seguridad como una pieza más de la compañía, creando una cultura de seguridad alrededor de ella.

B. Entrada y salida.

El mantenimiento del SGSI es un subproceso cuyas entradas se componen de:

- Un Plan de mejora (PM) y una Matriz de riesgos (MR) que servirán al auditor de seguridad (AuS) y al responsable de seguridad (Cl/RS) para poder acometer mejoras en la seguridad del sistema de información.
- Un conjunto de elementos seleccionados del esquema del SGSI, que componen la base del SGSI propiamente dicho: i) reglamentos seleccionados; ii) procedimientos activos; iii) roles del SGSI asociados a los procedimientos; iv) controles de seguridad con su nivel de cumplimiento actual que servirán para inicializar los valores del cuadro de mandos de

seguridad (CMs) del sistema de información; v) conjunto de métricas.

Mediante estas entradas y la ayuda del auditor de seguridad (AuS) y del responsable de seguridad (Cl/RS), se pondrá en funcionamiento el SGSI de la compañía, que estará formado por una serie de salidas que realimentarán y mantendrán actualizado el SGSI:

- Certificados de cultura de la seguridad (cCS): Es el certificado que se entrega a los usuarios del sistema de información y que les autoriza a poder acceder al mismo.
- Procedimientos generales (proGen): Cuando se ejecuta uno de los procedimientos que se incluyó en el esquema del subproceso GEAR y se seleccionó durante el subproceso GAGR, se crea una instancia del mismo que es el conjunto de datos generados para esa ejecución en concreto.
- Procedimiento de denuncia (proDen): Esta salida consiste en la instancia de ejecución del procedimiento de denuncia, y está formada por los datos recogidos a lo largo de todo el proceso de ejecución del mismo.
- Cuadro de mandos de seguridad (CMs): Esta salida contiene el nivel de cumplimiento de los controles de seguridad que componen el cuadro de mandos al finalizar la tarea T3.3.1.
- Métricas de periodicidad de los procedimientos (mPP): Esta salida contiene el estado de la periodicidad de los procedimientos del SGSI al finalizar la tarea T3.3.2.
- Métricas de violaciones de seguridad (mVS): Esta salida contiene el estado de las violaciones de seguridad activas en el sistema al finalizar la tarea T3.3.3.
- Métricas de cultura de seguridad (mCS): Esta salida contiene el estado de la cultura de seguridad para cada usuario que forma parte del SGSI al finalizar la tarea T3.3.4.
- Informe de auditorías (InfAud): Informe de las diferencias existentes entre los niveles de cumplimiento de los controles que componen el cuadro de mandos de seguridad y los medidos por el auditor de seguridad (AuS).
- Métricas generales de seguridad (mGS): Esta salida contiene las medidas de diferentes parámetros del SGSI que aportan las métricas generales activas en el sistema.
- Informe de alertas (InfAle): Esta salida contiene el informe de las últimas alertas de seguridad que se han producido en el SGSI.

Las salidas de este subproceso se almacenarán en el repositorio de SGSIs para ir actualizando los valores del cuadro de mandos y, por otra parte, se generarán entregables para que puedan ser analizados por el auditor de seguridad (AuS), el responsable de seguridad (Cl/RS) y para que el grupo de expertos del dominio (GED) puedan refinar los esquemas existentes o crear nuevos esquemas mediante el subproceso GEAR.

C. Actores.

En la Tabla 1 se muestra en qué actividades y tareas tendrá que intervenir cada uno de los tipos de actores definidos en la metodología.

En la actividad actual participarán los siguientes tipos de actores: el cliente (Cl), con todos los roles asociados al mismo, y el auditor de seguridad (AuS).

Todos los usuarios del departamento de sistemas tendrán como mínimo el perfil de usuario del sistema de información (Cl/US), y adicionalmente podrán tener asignados otros perfiles de los presentes en la lista. Por ello, para simplificar la Tabla 1, se ha puesto sólo el perfil de usuario del sistema de información (Cl/US) en lugar de todos los perfiles posibles del cliente (Cl).

Tabla 1. Intervención de los actores en el proceso MDAR

MARISMA						
MDAR						
A3.1: Obtener certificado de cultura de seguridad.						
T3.1.1						
Cl/US						
A3.2: Renovar el certificado de cultura de seguridad.						
T3.2.1						
Cl/US						
A3.3: Ejecutar procedimientos del SGSI.						
T3.3.1						
Cl/US						
A3.4: Activar procedimiento de denuncia.						
T3.4.1						
Cl/US						
A3.5: Seguimiento del cumplimiento del SGSI.						
T3.5.1	T3.5.2	T3.5.3	T3.5.4	T3.5.5	T3.5.6	T3.5.7
Cl/RS	Cl/RS	Cl/RS	AuS	Cl/RS	Cl/RS	Cl/RS

D. Actividades.

A continuación se describirán en detalle las entradas, salidas, relaciones y objetivos de cada una de las diferentes actividades y tareas que componen el subproceso MDAR de la metodología MGSM–PYME.

D.1. Actividad A3.1: Obtener o renovar el certificado de CS

El principal objetivo de esta actividad es establecer una cultura de seguridad básica en los usuarios que tendrán que trabajar con el sistema de información de la compañía, sin la cual no podrán acceder al mismo.

Durante el desarrollo de la investigación se han probado diversos métodos para establecer una cultura de la seguridad

en la compañía. Finalmente, el procedimiento que se ha determinado implantar consiste en la realización de una serie de cuestionarios de seguridad asociados al reglamento del SGSI, con el objetivo de mantener y mejorar la cultura de la seguridad de la compañía sin que tenga un coste alto de mantenimiento.

La idea principal es requerir un "certificado de nivel cultural" con respecto al sistema de la información a los usuarios del mismo, certificado que puede ser retirado y que debe ser renovado periódicamente para garantizar que se sigue manteniendo dicho nivel de cultura de seguridad.

La actividad ha demostrado que, por su sencillez y el poco tiempo que requiere, va creando de forma progresiva una cultura de la seguridad en los usuarios. La automatización de la misma evita costes adicionales de mantenimiento y planificación, y hace que la cultura de seguridad se mantenga como algo inherente al propio sistema de información.

En la **¡Error! No se encuentra el origen de la referencia.** se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

- Entradas: Como entradas se recibirán las respuestas de los usuarios al cuestionario de preguntas sobre el reglamento generado por el sistema.
- Tareas: El subproceso estará formado por una sola tarea que se ocupará de la emisión de los certificados de seguridad.
- Salidas: La salida producida por este subproceso consistirá en el certificado de cultura de seguridad en el caso de que la nota obtenida en el cuestionario sea superior a cinco o la denegación del certificado en caso contrario. Si se suspende el examen, se recomendará al usuario el estudio del manual de seguridad incluido en el SGSI o bien la asistencia a un curso de gestión de seguridad para aumentar los conocimientos en la materia.

En la Figura 3 muestra la tarea de la actividad de forma mucho más detallada, viendo cómo interactúa ésta con el repositorio de información de SGSIs encargado de contener los certificados de seguridad concedidos y la nota obtenida.

A continuación describimos el objetivo de cada una de las tareas:

- Tarea T3.1.1 – Realización del test de cultura de seguridad: El objetivo de la tarea T.3.1.1 es realizar una evaluación de los conocimiento que un usuario que desea acceder al sistema de información de la compañía tiene con respecto al reglamento que compone el SGSI, determinando si está preparado o no para acceder al mismo. El limitar el acceso al sistema de información a los usuarios, hasta que consigan demostrar que tienen unos conocimientos básicos de cómo deben actuar con él, es un control que ayuda a mitigar los riesgos a los que está sometido el sistema, obligando a los usuarios a incrementar su cultura de seguridad de forma progresiva y con un bajo coste. En el caso de que un usuario suspenda un examen, deberá volver a estudiar la información del SGSI o asistir a un curso de gestión de seguridad para adquirir el nivel de conocimientos adecuados para acceder al sistema. Dentro de esta tarea existen dos procesos diferenciados: i) Obtención del certificado de cultura de la seguridad.; ii) Renovación del certificado de cultura de la seguridad.

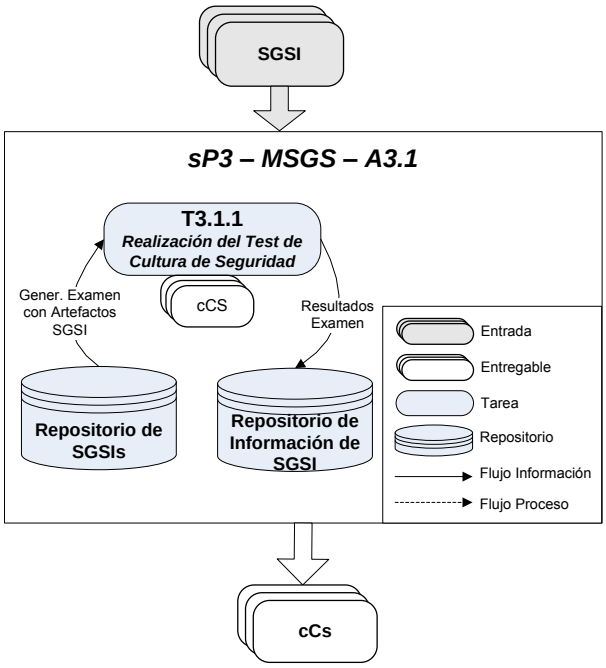


Figura 3. Esquema detallado a nivel de tarea de la actividad A3.1.

En la Figura 4 se puede ver en detalle el diagrama de flujo de los diferentes pasos que conforman el primero de estos procesos (obtención del certificado de cultura de la seguridad). La primera vez que el usuario accede al sistema de información, deberá aceptar la política de seguridad de la empresa. De esta forma se garantiza que el usuario lea, aunque sea de forma rápida, la política de la empresa (mejorando la cultura de seguridad). Después, el usuario deberá pasar un test inicial compuesto por unas veinte preguntas extraídas al azar a partir del SGSI de la compañía.

Mientras el usuario no consiga obtener más del 50% de respuestas correctas en el test se considera que su "cultura de seguridad" para el sistema de información de la compañía no es adecuada y deberá realizar otro examen hasta conseguir una calificación superior o igual a cinco. El usuario no podrá acceder al sistema de información de la compañía hasta que no alcance un nivel adecuado de "cultura de seguridad". De esta forma se garantiza implantar la cultura de una forma eficiente. Una vez que el usuario consiga el aprobado su nota se guardará en un registro, se le concederá un certificado de "cultura de seguridad" y se le dará acceso al sistema de información. La nota obtenida será importante para poder mantener el certificado obtenido en el tiempo, ya que ésta se verá modificada

por otras tareas del sistema.

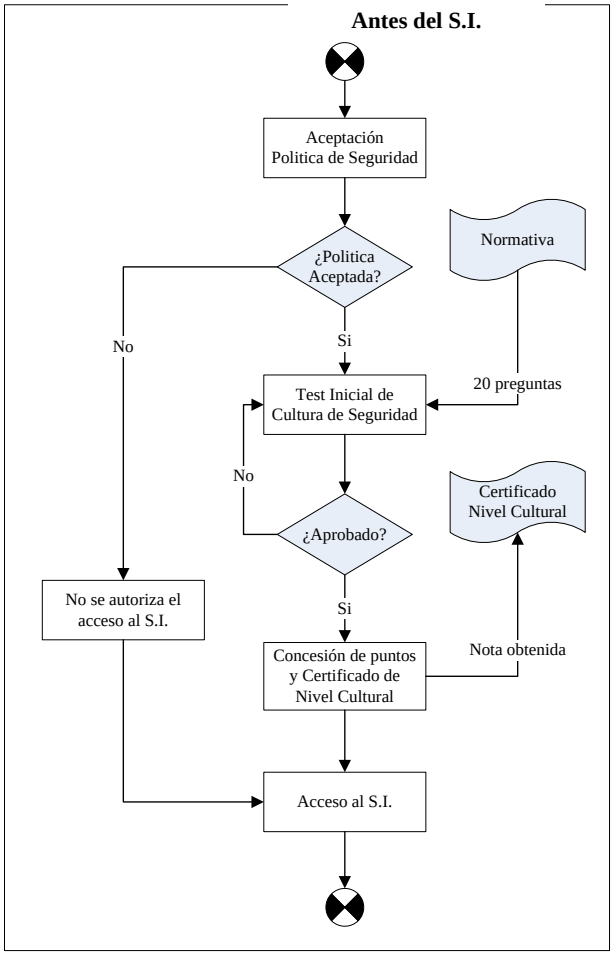


Figura 4. Obtención inicial de un certificado de "cultura de seguridad".

El segundo de los procesos que componen la tarea de "realización del test de cultura de seguridad" es la renovación del certificado de cultura de la seguridad (CS), ya sea por la caducidad del mismo o por la pérdida de puntos de la calificación. Los pasos de este proceso se pueden ver en detalle en el diagrama de flujo de la Figura 5.

Se ha establecido un periodo de renovación del certificado de cultura de la seguridad de 1 año, aunque esta cifra podría reducirse a 6 meses para acelerar el establecimiento de la cultura de la seguridad de la información. Debido a la sencillez del procedimiento no es aconsejable relajar más el tiempo de la renovación de los certificados, porque podría degradarse la cultura de seguridad (ej.: se considera que un tiempo de 2 años sería contraproducente), ni forzarlo demasiado porque podría producir rechazo entre los usuarios (Ej.: se considera que un tiempo inferior a 6 meses crearía rechazo entre los usuarios).

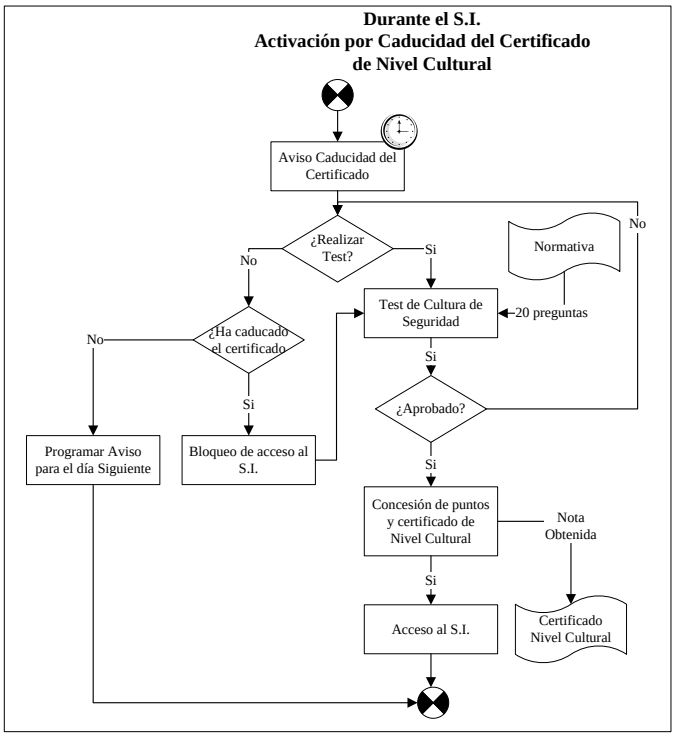


Figura 5. Esquema de renovación de un certificado de la CS.

Para evitar interferir en el trabajo diario de los usuarios, la notificación de caducidad del certificado se produce desde 1 mes antes de ser efectiva, de forma que el usuario puede postergar la realización de los test al momento que desee dentro de ese periodo. El sistema diariamente le irá recordando el tiempo que resta para que caduque su certificado. Llegada la fecha de caducidad, si el usuario no ha realizado y aprobado el test se bloqueará su acceso al sistema de información hasta que consiga renovar el certificado.

Dado que el tiempo consumido por recurso (TcR) es uno de los factores principales de éxito para la metodología (en particular en el caso de las PYMES), se han realizado estimaciones del tiempo que podría costar la implantación de la cultura de seguridad, llegando a la conclusión de que la sencillez del proceso lo hace totalmente aceptable para las PYMES (se ha estimado que la obtención inicial del certificado podría llevar entre 1 y 2 horas, en torno a 90 minutos para la lectura de la política de seguridad y el entendimiento de los elementos del SGSI, y unos 30 minutos para la realización y aprobación de test). Esta inversión de tiempo se realizaría sólo inicialmente ya que, aunque el certificado se debe renovar de forma periódica, la política de seguridad sólo se debe leer y aprobar inicialmente.

La experiencia obtenida a partir de los casos de prueba demuestra que los usuarios del sistema de información consideran esta inversión de tiempo razonable, a su vez la necesidad de obtener el certificado para poder acceder al sistema de información, hace que no sea cuestionada por ellos.

Por último, merece la pena destacar que los usuarios que intentaron saltarse la lectura de la política de seguridad para ahorrar tiempo tuvieron que repetir varias veces los test, invirtiendo finalmente el mismo tiempo que si hubieran leído la política. Cualquiera de los dos caminos se puede considerar correcto, ya que ambos conducen al objetivo de introducir en los usuarios la semilla inicial de la "cultura de seguridad".

Con esta sencilla tarea los usuarios nunca pierden conciencia de la importancia de mantener actualizado su nivel de cultura de la seguridad. Así mismo, dado que los test se realizan al azar mediante combinación de preguntas de los reglamentos de seguridad activados en la compañía, los usuarios van tomando conciencia cada vez mayor de estos reglamentos, de una forma intuitiva y con un coste mínimo.

D.2.Actividad A3.2: Ejecutar procedimientos del SGSI

Esta actividad tiene como principal objetivo permitir a los usuarios del sistema de información la ejecución de los procedimientos que contienen los procesos necesarios para mantener el SGSI de la compañía.

La ejecución de uno de los procedimientos pertenecientes al SGSI producirá una instancia del procedimiento, que será el conjunto de datos únicos introducidos durante la ejecución de ese procedimiento.

En la Figura 6 se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

- Entradas: Como entradas se recibirán: i) el certificado de cultura de seguridad, ya que sin él no se puede acceder al sistema de información de la empresa; ii) los datos de entrada de los usuarios de la empresa para la fase del procedimiento que se esté ejecutando; iii) del repositorio de información del SGSI se obtendrán los datos de la fase anterior de la instancia del procedimiento que se está ejecutando.
- Tareas: El subproceso estará formado por dos tareas que son independientes y que se corresponden con los dos tipos de procedimientos existentes en el sistema (generales y de denuncia).
- Salidas: La salida producida por este subproceso consistirá en un informe que contenga toda la información generada en la instancia de cada fase del procedimiento durante la ejecución del mismo, con el objetivo de que el auditor de seguridad (AuS) y el responsable de seguridad (Cl/RS) puedan analizarla y determinar mejoras en los procedimientos.

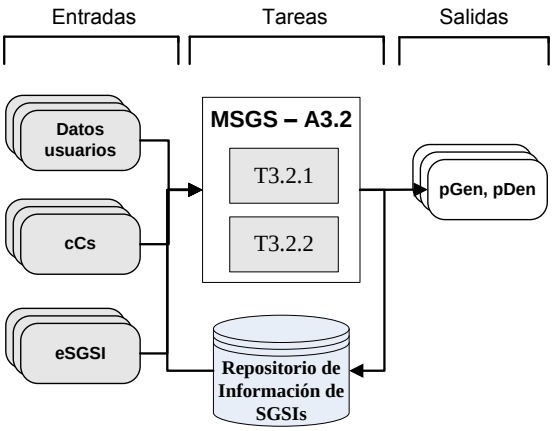


Figura 6. Esquema simplificado a nivel de tarea de la actividad A3.2.

En la Figura 7 se muestran las actividades del subproceso de forma mucho más detallada, viendo cómo interactúan éstas con el repositorio de SGSIs encargado de contener las estadísticas y los datos introducidos por los usuarios del sistema de información durante el trabajo diario con el SGSI.

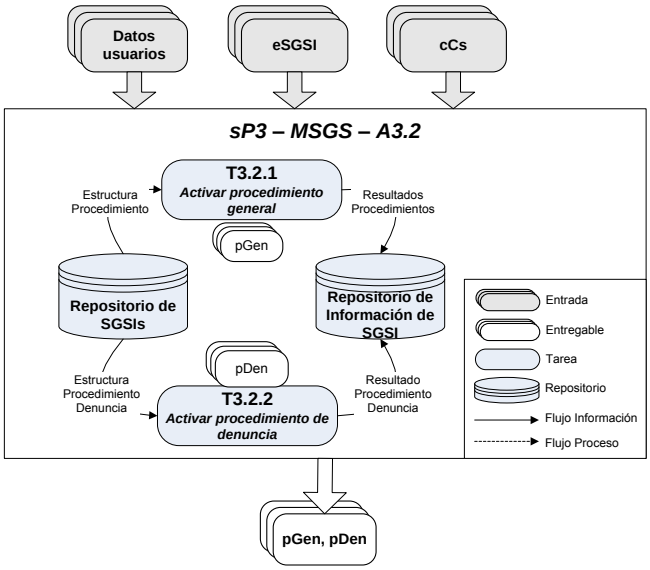


Figura 7. Esquema detallado a nivel de tarea de la actividad A3.2.

Los procedimientos se encuentran divididos en fases. Cada fase de un procedimiento puede ser ejecutada por un usuario diferente.

A continuación describimos el objetivo de cada una de las tareas:

- Tarea T3.2.1 – Activar procedimiento general: Mediante la tarea T3.2.1 se puede iniciar una instancia de unos de los procedimientos generales que forman parte del SGSI de la compañía. El objetivo de estos procedimientos es permitir a los usuarios del sistema de información realizar las operaciones que afectan a la seguridad de éste de una forma organizada. Los procedimientos tienen asignada una política de

seguridad a nivel de fase, de tal forma que sólo aquellos roles que tengan acceso a las fases podrán participar en el proceso. Sólo aquellos roles que tengan acceso a la fase inicial de un procedimiento podrán iniciar una instancia del mismo, y sólo los que tengan acceso a la fase final podrán finalizar dicha instancia. Las fases intermedias podrán ser ejecutadas por aquellas personas que tengan los roles adecuados y hayan sido designados como receptores de dicha fase por el usuario responsable de la fase anterior (Figura 8). Cuando un usuario inicia un procedimiento, el sistema irá de forma automática activando las fases y solicitando las operaciones necesarias para pasar a la siguiente fase a cada uno de los usuarios involucrados, como se puede ver en la Figura 8. De esta forma, hasta que el usuario responsable de una fase no dé la aprobación de la misma, el procedimiento quedará pendiente y el sistema almacenará los retrasos ocasionados para un posterior análisis. Durante la ejecución de los procedimientos se genera información estadística de los tiempos de ejecución de cada fase y el origen de los retrasos producidos, con el objetivo de poder tomar decisiones que los hagan más eficientes.

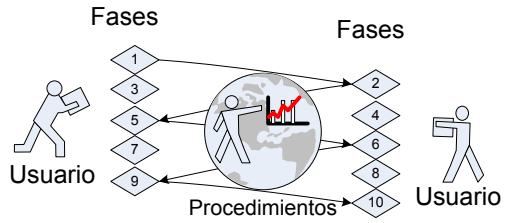


Figura 8. Flujo de actividad en procedimientos.

- Tarea T3.2.2 – Activar procedimiento de denuncia: El objetivo de la tarea T3.2.2 es gestionar y evaluar las violaciones de seguridad y mantener actualizado el nivel de seguridad de los controles. El perfil más importante en este procedimiento es el responsable de seguridad (Cl/RS). El esquema general de este procedimiento se puede ver en la Figura 9, y es el encargado de gestionar las denuncias por parte de un usuario del sistema sobre el incumplimiento de una regla de un reglamento.

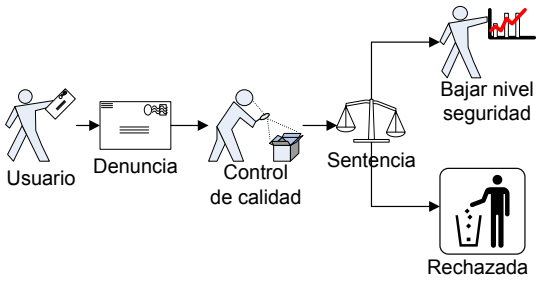


Figura 9. Esquema del procedimiento de denuncia.

La tarea se inicia cuando un usuario del sistema de información detecta una violación de seguridad o un incumplimiento de una regla del reglamento aprobado para el SGSI de la compañía y decide poner en conocimiento del responsable de seguridad (Cl/RS) dicha violación. Éste recibe la denuncia y determina si está justificada o no. En el caso de considerarla justificada aprobará la misma, lo que causará una disminución del nivel de seguridad de los controles asociados a esa regla (mediante la matriz definida en la T1.4.8).

Este procedimiento posibilita que las violaciones en el reglamento del SGSI afecten de forma directa e inmediata al cuadro de mando, sin necesidad de esperar que un auditor venga a revisar el sistema. Así mismo se ven afectados todos los niveles del cuadro de mandos, alertando a la gerencia de forma sencilla cuando algo va mal, sin necesidad de esperar a la auditoría anual o bi–anual que realiza un auditor externo para poder tomar decisiones. Al poder tomarse decisiones cuando los problemas aparecen, sin necesidad de esperar un periodo largo de tiempo, se evita el efecto dominó que se produce al empezar a degradarse controles de seguridad y carecer de la información necesaria para aplicar las medidas correctivas antes de que afecten a otros controles. Por último, se evita el efecto de desorientación que produce al responsable de seguridad (Cl/RS) conocer la existencia de fallos en el sistema, pero no su origen.

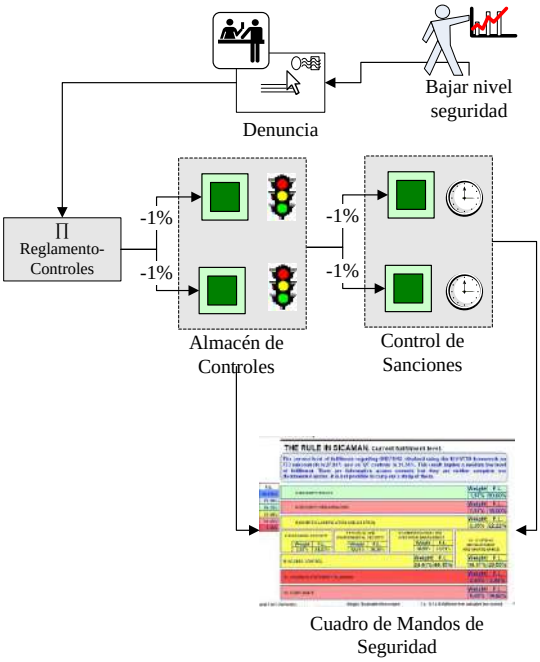


Figura 10. Esquema de activación de un procedimiento de denuncia.

En la Figura 10 se puede ver un esquema del funcionamiento de este procedimiento internamente. Utilizando la matriz de reglamentos–controles determina qué controles tienen que recibir la sanción.

Estos controles se sancionan con un –1% de nivel de cumplimiento, pero esta sanción sólo durará un periodo de tiempo (normalmente 1 año), por lo que se almacenará en un deposito denominado "control de sanciones". El valor del nivel del cumplimiento del control se actualizará en el cuadro de mandos, tanto al aprobarse la sanción como al caducar la misma.

D.3.Actividad A3.3: Seguimiento del cumplimiento del SGSI

Esta actividad tiene como principal objetivo mantener actualizado el nivel de madurez del SGSI y conocer en todo momento el nivel de cumplimiento de los controles de seguridad que forman parte del SGSI de la compañía.

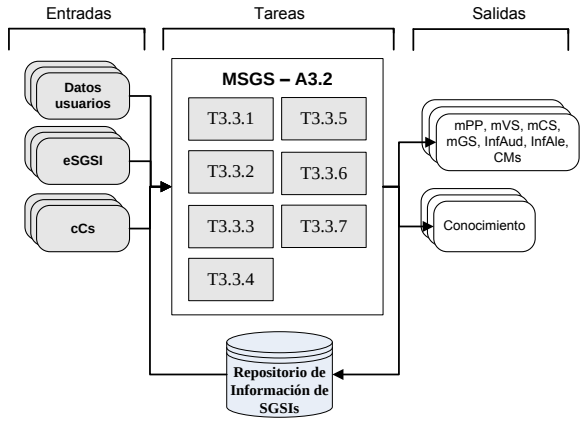


Figura 11. Esquema simplificado a nivel de tarea de la actividad A3.3.

En la Figura 11 se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

- Entradas: Como entradas se recibirán: i) el certificado de cultura de seguridad ya, que sin él no se puede acceder al sistema de información de la empresa; ii) datos de entrada de los usuarios (ej.: mediciones de los niveles de cumplimiento de los controles por parte del auditor de seguridad como parte del proceso de recalibrado); iii) del repositorio de información del SGSI se obtendrá información de cambios en el nivel de cumplimiento de los controles de seguridad.
- Tareas: El subproceso estará formado por siete tareas que son independientes y que se irán ejecutando cuando sea necesario, sin una limitación temporal (representada por un reloj en el esquema). Estas tareas son: i) gestión del cuadro de mandos de seguridad; ii) gestión de la periodicidad de los procedimientos; iii) gestión de las violaciones de seguridad; iv) gestión de los certificados de cultura de la seguridad; v) realización de las auditorías periódicas; vi) realización de métricas generales; vii) gestión del sistema de alertas.
- Salidas: La salida producida por este subproceso consistirá en una serie de informes asociados a cambios en los niveles de cumplimiento de los controles de seguridad y a violaciones de los reglamentos, con el objetivo de que el auditor de seguridad (AuS) y el responsable de seguridad (Cl/RS) puedan analizarla y determinar mejoras en los mismos.

En la Figura 12 se muestran las actividades del subproceso de forma mucho más detallada, viendo cómo interactúan éstas con el repositorio de SGSIs encargado de contener las estadísticas y los datos introducidos por los usuarios del sistema de información durante el trabajo diario con el SGSI.

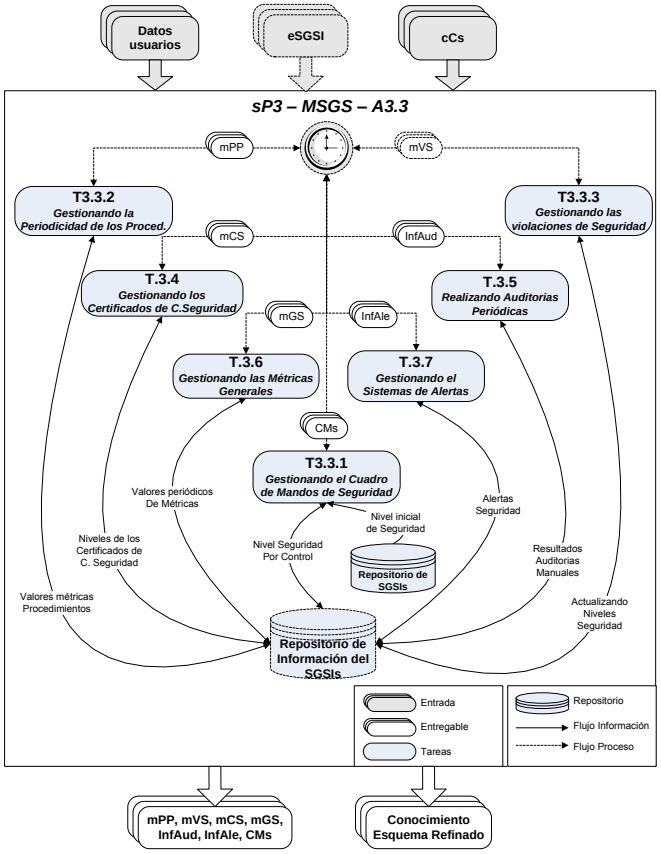


Figura 12. Esquema detallado a nivel de tarea de la actividad A3.3.

Cada una de las tareas definidas en esta actividad tiene un objetivo claramente definido para mantener actualizado el sistema, que es:

- T3.3.1 – Gestionando el cuadro de mandos de seguridad: Permite al responsable de seguridad (Cl/RS) tener conocimiento en todo momento del nivel de la gestión de la seguridad del sistema de información sin tener que esperar a costosas y tardías auditorías externas.
- T3.3.2 – Gestionar la periodicidad de los procedimientos: Permite medir el impacto de incumplir la ejecución de un procedimiento sobre el sistema.
- T3.3.3 – Gestionar las violaciones de seguridad: Permite medir el impacto que tendrá el incumplimiento de una regla de seguridad de uno de los reglamentos aprobados en el SGSI sobre el resto

de artefactos que conforman el sistema.

- T3.3.4 – Gestionar los certificados de cultura de la seguridad: Permite medir el nivel de los usuarios con respecto a la cultura de seguridad de la compañía, para tomar medidas correctoras (Ej. cursos de concienciación o seguridad).
- T3.3.5 – Realización de auditorías periódicas: Los realizará de forma periódica un auditor externo como mecanismo de recalibración del CMs.
- T3.3.6 – Realización de métricas generales: Permite medir otros factores específicos del SGSI asociados al funcionamiento de los procedimientos y controles (ej.: tiempo de respuesta a incidentes de seguridad).
- T3.3.7 – Gestionar el sistema de alertas: Facilita que el responsable de seguridad (RS) tenga constancia de fallos o distorsiones en la gestión de la seguridad del S.I. sin tener que estar supervisándolo de forma constante.

Dentro de estas tareas, las T3.3.2, T3.3.3, T3.3.4, T3.3.5 y T3.3.6 generan valores que alteran el nivel de seguridad de la compañía representado en el cuadro de mandos (T3.3.1), lo que puede producir alertas en el sistema (T3.3.7). En la Tabla 2 se puede ver el efecto que tiene sobre los controles de seguridad la activación de cada una de esas tareas.

Tabla 2. Cuadro de métricas de autorregulación del nivel de seguridad

Tarea	Efecto sobre controles	Condiciones de activación
T3.3.2: Periodicidad de los proced.	Sube y baja el nivel	Cada ejecución de procedimientos, cada mes y cada tres meses. Penalización de –1% ó +1% de los controles asociados.
T3.3.3: Denuncias	Baja el nivel	Cuando el responsable de seguridad aprueba una denuncia, el usuario denunciado es sancionado con: –1 punto del certificado de cultura de seguridad. –1% de los controles asociados al reglamento incumplido.
T3.3.5: Auditorías	Sube y baja el nivel	Anual y bi–anualmente. Actualiza todos los controles con los nuevos valores.
T3.3.6: Métricas generales	Sube y baja el nivel	De forma constante cuando un procedimiento lo requiera.
T3.3.4: Certificados de cultura de seguridad	Sube y baja el nivel	Al entrar en el S.I., al llegar al nivel mínimo de puntos permitidos, anualmente. Cada pregunta del examen: • Fallada –0,1% de los controles asociados. • Acertada +0,1% de los controles asociados.

Esta actividad se ha diseñado para que permita al SGSI evolucionar el nivel de cumplimiento de los controles de seguridad de forma dinámica sin que sea obligatoria, aunque sí aconsejable, la intervención de auditores externos. De esta forma, la compañía no tiene que esperar a la llegada de auditores externos para conocer cómo está evolucionando la seguridad del sistema de información, sino que el sistema la actualiza constantemente cambiando el nivel de seguridad de los controles y reajustando todos los objetos del sistema.

El resultado de cada cambio se ve reflejado en el nivel de cumplimiento de los controles del cuadro de mandos de seguridad, que se convierte en el centro de control del responsable de seguridad (Cl/RS) de la empresa para analizar la evolución del sistema y tomar medidas correctivas.

A continuación describimos el objetivo de cada una de las tareas:

- Tarea T3.3.1 – Gestionar el cuadro de mandos de controles de seguridad: La tarea T3.3.1 tiene como objetivo realizar actualizaciones en los controles de seguridad que componen el cuadro de mandos. La ausencia de este cuadro de mandos de seguridad en las compañías hace que no tengan capacidad de tomar decisiones en materia de seguridad a corto plazo, ya que dependen de la visita de los auditores periódicamente (aproximadamente cada dos años) para poder determinar qué controles se han ido degenerando con el tiempo. Sin embargo en la metodología MGSM–PYME la existencia de un cuadro de mandos de seguridad dinámico hace que el responsable de seguridad (Cl/RS) tenga en todo momento conocimiento de aquellos controles de seguridad que requieren mayor supervisión y sobre los que se deben tomar medidas correctoras.
- Tarea T3.3.2 – Gestionar la periodicidad de los procedimientos: La tarea T3.3.2 muestra una de las métricas específicas de la metodología, cuyo objetivo es dotar a cada procedimiento de una periodicidad de ejecución (tiempo mínimo en que el procedimiento debe ser ejecutado). De esta forma, cuando uno de los procedimientos del SGSI pasa más del periodo mínimo que tiene definido sin ejecutarse, lanza una alerta cuyo objetivo es reducir el nivel de seguridad de los controles asociados a ese procedimiento del SGSI y a los elementos asociados al mismo. El responsable de seguridad (Cl/RS) determina en última instancia si tiene sentido o no disminuir la seguridad. Por el contrario, cuando un procedimiento se ejecuta antes de cumplirse la periodicidad establecida, hace que se incremente el nivel de cumplimiento de los controles asociados. El sistema de periodicidad de los objetos ha sido planificado para que se vaya autorregulando anualmente, por lo que inicialmente se establece que todos los objetos tienen una periodicidad mensual (ej.: si el primer año un procedimiento se ejecuta 50 veces, el año siguiente la periodicidad de dicho procedimiento pasara a ser 365/50, es decir, semanalmente; el siguiente año se realizará la media con toda la información de la base de datos relativa a

la periodicidad del objeto, hasta que se consiga la periodicidad más cercana a la realidad. Por el contrario, si un procedimiento se debe ejecutar sólo 2 veces al año, inicialmente se disparará cada mes, y el responsable de seguridad determinará si realmente se está incumpliendo el procedimiento, en cuyo caso aprobará la penalización (–1%), o por el contrario no ha sido necesario ejecutarlo, en cuyo caso anulará la penalización). De esta forma, cada procedimiento periódicamente intenta recordar su existencia al responsable de seguridad (Cl/RS) regulando el nivel de cumplimiento (NC) de los controles asociados.

- Tarea T3.3.3 – Gestionar las violaciones de seguridad: El objetivo de la tarea T3.3.3 es aportar otro mecanismo de medición que permita mantener actualizado el nivel de la gestión de la seguridad en la compañía. Esta tarea permite controlar las violaciones del reglamento de seguridad del SGSI de la compañía, penalizando los controles asociados a las reglas que se han violado en el caso de que el responsable de seguridad (Cl/RS) considere que realmente ha existido una violación. Al contrario que en los mecanismos de autorregulación incluidos en otras tareas, el porcentaje de la penalización en el sistema de denuncias es alta dado que existe una evidencia de la violación del reglamento de seguridad. En la metodología se ha establecido una penalización del 1% de valor total de los controles de seguridad que estén relacionados con la regla incumplida y un 1 punto menos en el certificado de cultura de la seguridad del usuario del sistema de información que ha ocasionado la violación. Esta tarea sólo tiene carácter sancionador, no existiendo mecanismo en la misma que permita aumentar el nivel de cumplimiento de los controles o del certificado de cultura de la seguridad. Por último, se ha determinado no premiar al usuario que efectúa la denuncia para evitar que ésta quede invalidada por ello.
- Tarea T3.3.4 – Gestionar los certificados de cultura de seguridad: El objetivo de la tarea T3.3.4 es actualizar la puntuación de los certificados de cultura de seguridad y de los controles de seguridad asociados a estos cuando se producen ciertas acciones: i) violaciones del reglamento de seguridad; y ii) cuando se pierde el certificado de cultura de la seguridad por tener menos puntos de los requeridos. A lo largo de la investigación se ha determinado que cuanto mayor es la cultura de seguridad de la compañía, mayor es el número de denuncias que llegan de parte de los usuarios, máxime cuando dichas denuncias no implican actualmente sanciones graves contra los denunciados. Cuando se realiza una denuncia de un incidente de seguridad y el responsable de seguridad considera que está justificada y, por lo tanto la aprueba, además de verse afectado el nivel de seguridad global de la compañía se ve afectada la puntuación del certificado de cultura de la seguridad del usuario que cometió la violación de seguridad. Cada violación implica la pérdida de un 1 punto del certificado de cultura de la seguridad (NCS) que el usuario tenía hasta el momento, y que era el resultado de la nota obtenida en el test de cultura de seguridad, menos los puntos que ya hubiera perdido durante el periodo de validez de ese certificado por violaciones de la normativa activa en la compañía. Si la pérdida de puntos debida a violaciones de seguridad hace que la puntuación del certificado de cultura de la seguridad baje de los 5 puntos, se le quitará al usuario el certificado, y con ello el acceso al sistema de información de la compañía, hasta que vuelva a aprobar el examen y así obtenga un nuevo certificado de seguridad. Todo este proceso se puede ver en la Figura 13. Este proceso sirve como control preventivo para que los usuarios del sistema de información sean conscientes de que las violaciones de las normativas tienen un coste. Así mismo, la medida no es excesivamente grave y por tanto los usuarios no la ven con rechazo. Este control no tiene un coste de gestión representativo, ni en tiempo ni en recursos para la compañía, pero supone un importante refuerzo para establecer una correcta cultura de seguridad en la compañía.

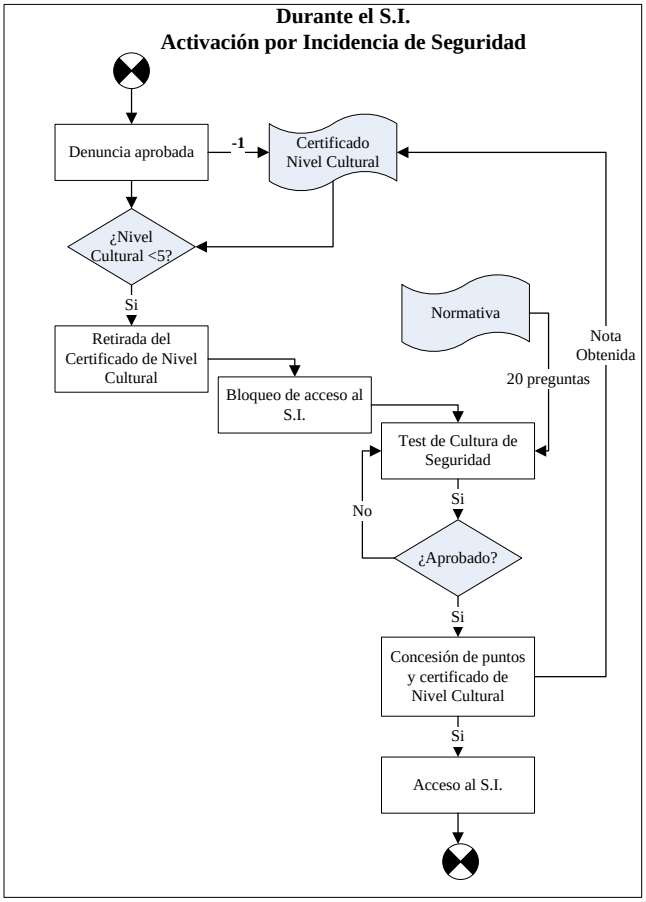


Figura 13. Alteración del NCS por una violación de la normativa.

- Tarea T3.3.5 – Realización de auditorías periódicas: El objetivo de la tarea T3.3.5 es la realización de auditorías externas, que servirán para recalibrar los niveles de cumplimiento de los controles de seguridad que componen el cuadro de mandos del SGSI. Esta tarea consiste en la realización de una lista de verificación (que podría ser la realizada en la tarea T1.2.2) por parte del auditor de seguridad (AuS) y comparar el resultado del nivel de cumplimiento obtenido para cada control de seguridad del SGSI en la evaluación del auditor externo de seguridad (AuS) con el nivel de cumplimiento actual del cuadro de mandos, con el objetivo de: i) determinar las variaciones existentes entre los controles y determinar las causas de las mismas y qué métricas han funcionado de forma incorrecta; y ii) recalibrar el cuadro de mandos, actualizando de nuevo el nivel de cumplimiento de los controles de seguridad. La metodología se ha planteado para reducir la necesidad de las auditorías periódicas, por dos motivos: i) el primero es que suponen un elevado coste para la empresa; y ii) el segundo es que al realizarse en periodos de tiempo largos (ej.: cada dos años), no sirven para tomar medidas a corto plazo, que son las que realmente suponen un ahorro de coste a la empresa al mantener el nivel de la seguridad. A lo largo de la investigación se ha llegado a la conclusión de que si el responsable de seguridad detecta en una fase temprana la degeneración de un control de seguridad es muy fácil determinar y aplicar medidas correctivas, ya que el control tan sólo está sufriendo una degeneración, pero sigue teniendo los pilares sobre los que aplicar las medidas correctivas. Por el contrario, si un nivel empieza a degenerar y este procedimiento se alarga en el tiempo sin tomar medidas correctoras, finalmente el control pierde toda su consistencia, requiriendo de un esfuerzo enorme para volver a cumplirlo. Esto es debido a que cuando un control se degrada durante un largo espacio de tiempo termina afectando negativamente a la cultura de seguridad de la compañía. Por lo tanto, la metodología evita depender sólo de las auditorias periódicas (ej.: bi–anuales), dejando éstas como un mero mecanismo de auto–regulación para determinar pequeñas desviaciones que se han podido producir. Los resultados de la auditoría a nivel de cumplimiento de los controles de seguridad no deberían diferir en más de un 5% del nivel de cumplimiento que actualmente tiene el cuadro de mandos de seguridad del SGSI. En caso contrario, se deberían determinar las causas de la desviación: i) mal funcionamiento de las métricas definidas; ii) falta de métricas; iii) utilización incorrecta del SGSI por parte de los usuarios; iv) falta de supervisión del responsable de seguridad (Cl/RS), v) etc.
- Tarea T3.3.6 – Gestionar las métricas generales: El objetivo de la tarea T3.3.6 es aportar nueva información del estado de la seguridad del SGSI mediante el uso de una serie de métricas generales. Estas métricas no afectan de forma directa al nivel de cumplimiento de los controles del SGSI, pero aportan información al responsable de seguridad (Cl/RS) sobre medidas que debe tomar para mejorar la gestión de la seguridad del sistema de información. El responsable de seguridad (Cl/RS) puede determinar alterar el valor de los niveles de cumplimiento de los controles de seguridad de forma manual, a partir de la información aportada por estas métricas, en caso de que lo considere conveniente.
- Tarea T3.3.7 – Gestionar el sistema de alertas: El objetivo de la tarea T3.3.7 es evitar que el responsable de seguridad (Cl/RS) tenga que estar continuamente analizando todos los controles del cuadro de mandos de seguridad para determinar si se está produciendo degeneración del sistema. Esta tarea envía una alerta al responsable de seguridad (Cl/RS) cuando el nivel de cumplimiento de un control supera uno de los límites establecidos (ej.: 0–10%, 10–25%, 25–50%, 50–75%, 75–90%, 90–100%), indicándole que se ha producido un cambio desde el limite X al Y, y las causas que lo han motivado. De esa forma el responsable de seguridad (Cl/RS) puede determinar si las causas han sido objetivas o se trata de una mala interpretación del sistema y, por tanto, puede volver a regular el nivel del control. En la Figura 14 se puede ver gráficamente el flujo seguido por la tarea.

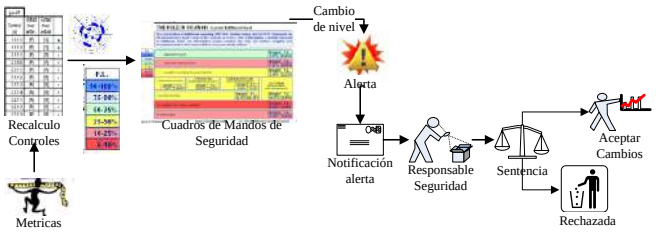


Figura 14. Sistema de alertas para control de niveles de seguridad

V. CONCLUSIONES.

En este artículo se ha presentado el proceso que permite el mantenimiento dinámico de un análisis de riesgos a lo largo del tiempo, el cual permite soportar los resultados generados durante la investigación y que cumple con los objetivos perseguidos, especialmente la capacidad de generarse y mantenerse actualizado a lo largo del tiempo con un bajo coste en recursos humanos y económicos, lo que suponía dos de los grandes problemas de este tipo de sistemas para todas las compañías en la que se realizó la investigación.

El análisis de riesgos para las PYMES deberá tener un coste de generación y mantenimiento muy reducido, aún a costa de sacrificar precisión en el mismo, pero siempre manteniendo unos resultados con la calidad suficiente.

Se ha definido cómo se puede utilizar este proceso y las mejoras que ofrece con respecto a otros modelos que afrontan el problema de una forma más precisa y detallada, pero

también más costosa, lo que no las hace válidas para el caso de las PYMES.

El proceso ha sido validado con más de 20 compañías de España y Colombia, facilitadas por la empresa Sicaman nuevas Tecnologías S.L. Las características ofrecidas por el proceso y su orientación a las PYMES ha sido muy bien recibida, y su aplicación está resultando muy positiva ya que permite a este tipo de empresas realizar una adecuada gestión del riesgo al que están sometidos los activos de su sistema de información, haciéndola sostenible a lo largo del tiempo, y permitiéndole conocer en tiempo real como este riesgo se ve alterado. Además, con este proceso se obtienen resultados a corto plazo y se reducen los costes que supone el uso de otros procesos, consiguiendo un mayor grado de satisfacción de la empresa.

El proceso MDAR de MARISMA cumple con los objetivos propuestos, así como con los principios que según la OCDE [52] debe seguir todo proceso de evaluación del riesgo, según el cual el sistema debe tener la capacidad de autoevaluar su riesgo de forma continuada en el tiempo, proponiendo medidas.

Finalmente, se considera que el trabajo realizado debe ser ampliado con nuevas especificaciones, nuevos esquemas, mejorando los algoritmos de análisis y gestión del riesgo de forma que puedan ofrecer planes más detallados y profundizando en el proceso con nuevos casos de estudio.

La mayor parte de las futuras mejoras del proceso se están orientando a mejorar la precisión del mismo, pero siempre respetando el principio de coste de recursos, es decir, se busca mejorar el proceso sin incurrir en costes de generación y mantenimiento del análisis de riesgos.

AGRADECIMIENTOS

Esta investigación ha sido co-financiada por los proyectos *SEQUOIA – Security and Quality in Processes with Big Data and Analytics* (TIN2015-63502-C3-1-R) financiados por el *"*Ministerio de Economía y Competitividad y Fondo Europeo de Desarrollo Regional FEDER", del proyecto ERAVAC ISO25000 (13/16/IN/4/014) financiados por la "Consejería de Economía, Empresas y Empleo" y del proyecto "Plataformas Computacionales de Entrenamiento, Experimentación, Gestión y Mitigación de Ataques a la Ciberseguridad - Código: ESPE-2015-PIC-019" financiado por la ESPE y CEDIA (Ecuador), y ha contado con la participación de la empresa Sicaman Nuevas Tecnologías (www.sicaman-nt.com) que ha permitido validar los resultados.

Referencias

[1] Wiander, T. *Implementing the ISO/IEC 17799 standard in practice – experiences on audit phases.* in *AISC '08: Proceedings of the sixth Australasian conference on Information security*. 2008. Wollongong, Australia.

[2] Johnson, M., Cybercrime: Threats and Solutions, 2014.

[3] Von Solms, R., Information security management: processes and metrics, 2014.

[4] Pinheiro, F.S. and W.R. Júnior, INFORMATION SECURITY AND ISO 27001. Revista de Gestão & Tecnologia, 2016. 3(3).

[5] Wiander, T. and J. Holappa, Theoretical Framework of ISO 17799 Compliant. Information Security Management System Using Novel ASD Method., in Technical Report, V.T.R.C.o. Finland, Editor 2006.

[6] Whitman, M. and H. Mattord, Principles of information security2011: Cengage Learning.

[7] Kluge, D. Formal Information Security Standards in German Medium Enterprises. in CONISAR: The Conference on Information Systems Applied Research. 2008.

[8] Dhillon, G. and J. Backhouse, Information System Security Management in the New Millennium. Communications of the ACM, 2000. 43(7): p. 125-128.

[9] Volonino, L. and S. Robinson. Principles and Practice of Information Security. in 1 edition, Anderson, Natalie E. 2004. New Jersey, EEUU.

[10] Michalson, L., Information security and the law: threats and how to manage them. Convergence, 2003. 4(3): p. 34-38.

[11] Cholez, H. and F. Girard, Maturity assessment and process improvement for information security management in small and medium enterprises. Journal of Software: Evolution and Process, 2014. 26(5): p. 496-503.

[12] Spinellis, D. and D. Gritzalis. Information Security Best Practise Dissemination: The ISA-EUNET Approach. in WISE 1:First World Conference on Information Security Education. 1999.

[13] Candiwan, C. Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia. in The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014). 2014. The Society of Digital Information and Wireless Communication.

[14] Sánchez, L.E., et al., Managing Security and its Maturity in Small and Medium-sized Enterprises. J. UCS, 2009. 15(15): p. 3038-3058.

[15] Vivas, T., A. Zambrano, and M. Huerta. Mechanisms of security based on digital certificates applied in a telemedicine network. in Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE. 2008.

[16] Vivas, T., et al., Aplicación de Mecanismos de Seguridad en una Red de Telemedicina Basados en Certificados Digitales, in IV Latin American Congress on Biomedical Engineering 2007, Bioengineering Solutions for Latin America Health, C. Müller-Karger, S. Wong, and A. La Cruz, Editors. 2008, Springer Berlin Heidelberg. p. 971-974.

[17] Alebrahim, A., D. Hatebur, and L. Goeke. Pattern-based and ISO 27001 compliant risk analysis for cloud systems. in Evolving Security and Privacy Requirements Engineering (ESPRE), 2014 IEEE 1st Workshop on. 2014.

[18] Tariq, M.I. and V. Santarcangelo. Analysis of ISO 27001: 2013 Controls Effectiveness for Cloud Computing. in ICISSP. 2016.

[19] Siegel, C.A., T.R. Sagalow, and P. Serritella, Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. Security Management Practices, 2002. sept/oct: p. 33-49.

[20] Garigue, R. and M. Stefaniu, Information Security Governance Reporting. Information Systems Security, 2003. sept/oct: p. 36-40.

[21] Mercuri, R.T., Analyzing security costs. Communication of the ACM, 2003. 46: p. 15-18.

[22] Bugdol, M. and P. Jedynak, Integration of Standardized Management Systems, in Integrated Management Systems2015, Springer International Publishing. p. 129-160.

[23] Barrientos, A.M. and K.A. Areiza, Integration of a safety management system withan information quality management system., in Master's thesis2005, Universidad EAFIT.

[24] Lund, M.S., F.d. Braber, and K. Stolen, Proceedings of the Seventh European Conference On Software Maintenance And Reengineering (CSMR'03). IEEE, 2003.

[25] Fredriksen, R., et al. The CORAS framework for a model-based risk management process. in 21st International Conference on Computer Safety, Reliability and Security (Safecomp 2002). 2002. Springer: LNCS 2434.

[26] Sánchez, L.E., et al. Security Management in corporative IT systems using maturity models, taking as base ISO/IEC 17799. in International Symposium on Frontiers in Availability, Reliability and Security (FARES'06) in conjunction with ARES. 2006. Viena (Austria).

[27] Sánchez, L.E., et al. MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs. in 9th International Conference on Enterprise Information Systems (WOSIS'07). 2007b. Funchal, Madeira (Portugal). June.
[28] Sánchez, L.E., et al. Developing a model and a tool to manage the information security in Small and Medium Enterprises. in International Conference on Security and Cryptography (SECRYPT'07). 2007a. Barcelona. Spain.: Junio.
[29] Sánchez, L.E., et al. SCMM-TOOL: Tool for computer automation of the Information Security Management Systems. in 2nd International conference on Software and Data Technologies (ICSOFT'07). . 2007c. Barcelona-España Septiembre.
[30] Sánchez, L.E., et al. Practical Application of a Security Management Maturity Model for SMEs Based on Predefined Schemas. in International Conference on Security and Cryptography (SECRYPT'08). 2008. Porto–Portugal.
[31] Gupta, A. and R. Hammond, Information systems security issues and decisions for small businesses. Information Management & Computer Security, 2005. 13(4): p. 297-310.
[32] V3, M., Methodology for Information Systems Risk Analysis and Management (MAGERIT version 3), 2012, Ministerio de Administraciones Públicas (Spain).
[33] Alberts, C.J. and A.J. Dorofee, Managing Information Security Risks: The OCTAVE Approach., ed. A.-W.P. Co.2002.
[34] CRAMMv5.0, CRAMM v5.0, CCTA Risk Analysis and Management Method., 2003.
[35] Gerber, M. and R. Von Solms, Management of risk in the information age. Computers & Security, 2005. 24(1): p. 16-30.
[36] ISO/IEC27005, ISO/IEC 27005:2011, Information Technology - Security Techniques - Information Security Risk Management Standard (under development). 2011.
[37] ISO/IEC27001, ISO/IEC 27001:2013, Information Technology - Security Techniques Information security management systemys - Requirements., 2013.
[38] SSE-CMM, Systems Security Engineering Capability Maturity Model (SSE-CMM), Version 3.0. Department of Defense. Arlington VA. 326., 2003.
[39] ISO/IEC21827, ISO/IEC 21827:2008, Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM), 2008, ISO/IEC. p. 123.
[40] ISO/IEC15443-1, ISO/IEC TR 15443-1:2012, Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework., 2012.
[41] ISO/IEC15443-2, ISO/IEC TR 15443-2:2012, Information technology -- Security techniques -- A framework for IT security assurance -- Part 2: Assurance methods., 2012.
[42] ISO/IEC20000-1, ISO/IEC 20000-1:2011, Information technology - Service management - Part 1: Specification., 2011.
[43] ISO/IEC20000-2, ISO/IEC 20000-2:2012, Information technology - Service management - Part 2: Code of practice., 2012.
[44] COBITv5.0, Cobit Guidelines, Information Security Audit and Control Association, ISACA, Editor 2013.
[45] Batista, J. and A. Figueiredo, SPI in very small team: a case with CMM. Software Process Improvement and Practice, 2000. 5(4): p. 243-250.
[46] Hareton, L. and Y. Terence, A Process Framework for Small Projects. Software Process Improvement and Practice, 2001. 6: p. 67-83.
[47] Tuffley, A., B. Grove, and M. G, SPICE For Small Organisations. Software Process Improvement and Practice, 2004. 9: p. 23-31.
[48] Calvo-Manzano, J.A., et al., Experiences in the Application of Software Process Improvement in SMES. Software Quality Journal., 2004. 10(3): p. 261-273.
[49] Mekelburg, D., Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes. Software Quality Professional, 2005. 7(3): p. 4-13.
[50] Santos-Olmo, A., et al., A Systematic Review of Methodologies and Models for the Analysis and Management of Associative and Hierarchical Risk in SMEs, in 9th International Workshop on Security in Information Systems (WOSIS12) In conjunction with 11th International Conference on Enterprise Information Systems (ICEIS12).2012: Wroclaw, Poland. p. 117 -124.
[51] Sanchez, L.E., et al., ISMS Building for SMEs through the Reuse of Knowledge. Small and Medium Enterprises: Concepts, Methodologies, Tools, and Applications, 2013: p. 394.
[52] OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security., O.f.E.C.-o.a.D. (OECD). Editor 2002: Paris.

Luis Enrique Sánchez is PhD and MsC in Computer Science and is a Professor at the University of Castilla-la Mancha (Ciudad Real, Spain), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Professional Services and R&D departments of the company Sicaman Nuevas Tecnologías S.L. COIICLM board or committee member and responsible for the professional services committee. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha, in Ciudad Real (Spain).

Antonio Santos-Olmo is MsC in in Computer Science and is an Assistant Professor at the Escuela Superior de Informática of the Universidad de Castilla- La Mancha in Ciudad Real (Spain) (Computer Science Department, University of Castilla La Mancha, Ciudad Real, Spain), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Software Factory departments of the company Sicaman Nuevas Tecnologías S.L. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha, in Ciudad Real (Spain).

Sara Camacho Estrada is a Juris Doctor, Master in Information Technology and Multimedia Education, Master in Higher Education, Teaching and Administration. Director of the Languages Center for two periods at the Universidad Técnica de Ambato in Ecuador. Vice-dean of the Education Faculty at the Universidad Técnica de Ambato in Ecuador. Author and director of the TEFL Master´s program at the Universidad Técnica de Ambato in Ecuador. Author of a wide variety of programs like interactive software for learning English, international accreditations, and language learning programs.

David G. Rosado has an MSc and PhD. in Computer Science from the University of Málaga (Spain) and from the University of Castilla-La Mancha (Spain), respectively. His research activities are focused on security for Information Systems and Cloud Computing. He has published several papers in national and international conferences on these subjects, and he is co-editor of a book and chapter books. Author of several manuscripts in national and international journals (Information Software Technology, System Architecture, Network and Computer Applications, etc.). He is member of Program Committee of several conferences and workshops nationals and internationals such as ICEIS, ICCGI, CISIS, SBP, IAS, SDM, SECRYPT, COSE and international journals such as Internet Research, JNCA, KNOSYS, JKSU, and so on. He is a member of the GSyA research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain.

Eduardo Fernández-Medina holds a PhD. and an MSc. in Computer Science from the University of Sevilla. He is associate Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha at Ciudad Real (Spain), his research activity being in the field of security in databases, datawarehouses, web services and information systems, and also in security metrics. Fernández-Medina is co-editor of several books and chapter books on these subjects, and has several dozens of papers in national and international conferences (DEXA, CAISE, UML, ER, etc.). Author of several manuscripts in national and international journals (Information Software Technology, Computers And Security, Information Systems Security, etc.), he is director of the GSyA research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain.