Gestión del riesgo en sistemas de información: Análisis, Adaptación y Control

Jorge Arturo López Arias, Hugo del Ángel Delgado, Víctor Manuel Arias Peregrino, Dulce María León de la O, Clemente Hernández Arias

Tecnológico Nacional de México - Campus Villahermosa/Instituto Tecnológico de Villahermosa, División de Estudios de Posgrado e Investigación

Resumen

La seguridad de los sistemas de información se gestiona cada vez más mediante enfoques basados en el riesgo. La evidencia y experiencia de profesionales del tratamiento de riesgos muestra que estos estudios prospectivos reducen significativamente las pérdidas asociadas con las deficiencias en la seguridad de la información de manera significativa. También se observa la transformación y la evolución del cargo de oficial de seguridad de la información (CISO), asemejándose cada vez más a la de un gestor de riesgos.

Abstract

Information systems security is increasingly managed through risk-based approaches. Evidence and experience from risk management professionals shows that these forward-looking studies significantly reduce the losses associated with information security deficiencies. We also see the transformation and evolution of the information security officer (CISO) position, increasingly resembling that of a risk manager.

Palabras Clave: Gestión de riesgos, seguridad de la información, vulnerabilidad, SGSI
Keywords: Risk management, information security, vulnerability, ISMS

1. INTRODUCCIÓN

La Industria 4.0 concepto que gana posición y que se considera como uno de los mayores retos de la actualidad para las áreas de desarrollo de tecnología como son inteligencia artificial, Big Data, internet de las cosas, robótica avanzada, entre otros, están transformando la forma en que las organizaciones obtienen, fabrican, distribuyen y evalúan sus productos, es por esto que la gestión de riesgos se ha convertido en un componente crucial para garantizar el crecimiento y la supervivencia de las empresas actuales.

Esto se aplica especialmente a los sistemas de información (SI), donde los riesgos son constantes y pueden afectar significativamente las operaciones de la organización, razón por la cual debe priorizar la implementación de metodologías sólidas para identificar, analizar y reducir los riesgos de seguridad de la información (ISO/CEI JTC 1/SC 27, 2022).

Mehari (Méthode Harmonisée d'Analyse de Risques) es una de las metodologías más completas desarrolladas específicamente para la gestión de riesgos en seguridad de la información, fue desarrollado por el Club de la Seguridad de la Información Francés (Jouas, 2022) en los años 90, Mehari sugiere un enfoque sistemático y cuantitativo para evaluar y tratar los riesgos de la seguridad de la información.

La versión Mehari-Standard propone una solución integrada combinando una base de conocimientos con herramientas para los diversos pasos del proceso: clasificación de activos, análisis de escenarios de riesgo, diagnóstico de controles de seguridad, selección y planificación de proyectos de mitigación y monitoreo del perfil de riesgos.

Este artículo busca presentar los conceptos y la metodología fundamentales de Mehari-Standard y mostrar detalles de cada paso involucrado en el análisis, adaptación y control de riesgos de sistemas de información para una comprensión de esta herramienta que apoye a las organizaciones a gestionar de manera proactiva y efectiva los riesgos de seguridad de la información.

2. ANALISIS DE RIESGO, EVOLUCIÓN Y NORMAS QUE LO SUSTENTAN

El análisis de riesgo es un proceso sistemático para identificar y evaluar los riesgos a los que está expuesto un proyecto o una organización, su objetivo es definir estrategias de mitigación que reduzcan la probabilidad y/o el impacto de los eventos centrándose en la etiología y prevención y no en la gestión de las catástrofes, Perles Roselló, M. J. (2015).

Es importante reconocer que la historia y la evolución del análisis de riesgos son más complejas y variadas de lo que se puede resumir en una lista cronológica, la evolución y la adopción del análisis de riesgos en otras industrias no siempre siguieron un patrón lineal y cronológico aun así, la siguiente secuencia tiene como fin brindar una visión general de la evolución del análisis de riesgos en diversos campos con el objeto de denotar la participación activa que ha tenido en el paso del tiempo.

- 1930´s - Surge en proyectos de ingeniería.
- 1940´s - Se populariza en proyectos militares y aeroespaciales.
- 1950´s - Es adoptado por grandes corporaciones.
- 1960´s - Se vuelve estándar en la industria de seguros.
- 1970´s - Se aplica en análisis financiero y evaluación de inversiones.
- 1980´s - Se utiliza en proyectos informáticos y de software.
- 1990´s - Se integra en marcos como PMI, Prince2 y metodologías ágiles.
- 2000´s - Se enfoca en riesgos emergentes como ciberseguridad.
- 2010´s - Surgen normas ISO específicas sobre riesgos de SI.
- Actualidad - Se utilizan técnicas cuantitativas y cualitativas. Enfoque en riesgos estratégicos y de reputación. Integración de análisis prospectivos.

Tabla 1. Estándares alineados para la gestión de riesgos

Estándar ISO / Metodología	ENFOQUE	APORTE CLAVE
Mehari	Específica para riesgos de SI	Procesos y técnicas para análisis cuantitativo
ISO/IEC 27001	Requisitos para SGSI	Implementación y operación de SGSI
ISO/IEC 27002	Buenas prácticas de controles de SI	Recomendaciones de controles de seguridad
ISO/IEC 31000	General para gestión de riesgos	Estructura y principios de gestión de riesgos

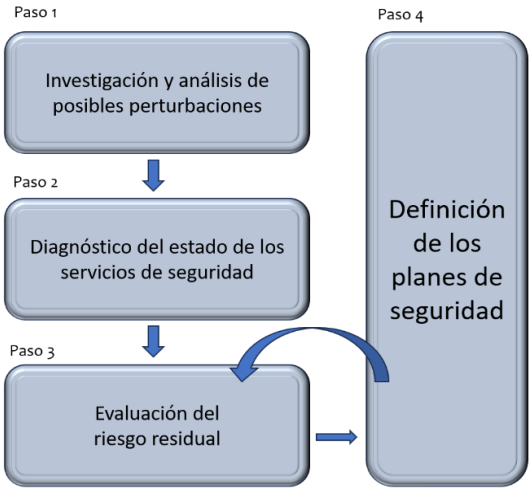

Figura 1. Descripción general del método
Jouas, J. P. (2022). Expedientes Técnicos Mehari—Guía de usuario

CLUSIF

MEHARI™ - Standard-En - 2022 - Versión 2

Mehari base de conocimientos

Worksheet	Contenido	Hide tabs selected below
Intro	Descripción de las hojas de trabajo de la base de conocimientos	
Presentation	Estándar Mehari y presentación de análisis de riesgos	
Stakes analysis and asset classification module.		**Classification tables:** T1, T2 & Classif — Hide ☐
T1 and T2	Tablas de clasificación	
Classif	Clasificación de activos	
Módulo de diagnóstico de servicios de seguridad (o auditoría)		Cuestionarios: de 1 Org a 8 Cex & ISO 27002 puntuación — Hide ☐
Dominio 1 Org to 8 Cex	Cuestionarios relacionados con los dominios de seguridad MEHARI (1 Org to 8 Cex)	
Servicios	Resumen de la calidad de los servicios de seguridad	
ISO 27002	Tabla de puntuación ISO 27002:2013 tras el diagnóstico de los servicios de seguridad	
Módulo de análisis de riesgos (identificación, evaluación y clasificación de riesgos)		Analisis de riesgo: Riesgo por activo o evento — Hide ☐
Scenarios	Cuadro de escenarios de riesgo, incluidas las fórmulas para la evaluación del riesgo	
Risk%Asset	Visualización de seriedad para los escenarios en función del activo involucrado	
Risk%event	Mostrar la gravedad de los escenarios en función del origen o evento considerado	
Tratamiento de riesgos: opciones, planes de reducción de riesgos y seguimiento		**Trtamiento de riesgos :** Action_plans Projects Sel_Projects — Hide ☐
Action_plans	Selección de proyectos de reducción de riesgos, por dominios de riesgo	
Projects	Selección y planificación directa de proyectos	
Sel_Projects	Asistencia en la selección de proyectos de reducción de riesgos	
Tbord	Indicadores y dashboard	
Parámetros y elementos permanentes del método		Matriz de aceptación de riesgos y cuadrículas de evaluación de riesgos I & L — Hide ☐
Supporting_assets	Tabla de activos de apoyo (permite no seleccionar un activo de apoyo)	
Damages	Tabla de daños (permitiendo no seleccionar un daño)	
Expo	Tabla de probabilidad intrínseca de amenazas (o exposición natural)	
Severity	Determinación de la gravedad del riesgo de acuerdo con la probabilidad y el impacto	
IL grids	Cuadrículas para la evaluación de escenarios Impacto y probabilidad	

Fecha	Comunicados y comentarios
2022/01/08	Versión 1-2
2022/02/07	Versión 2 : Alineación con ISO/IEC 27002:2022
MEHARI es un método de gestión de riesgos diseñado y desarrollado por CLUSIF	Club de la Sécurité de l'Information Français http://www.clusif.fr

Figura 2. Módulos y elementos de la herramienta
Jouas, J. P. (2022). Expedientes Técnicos Mehari—Guía de usuario

3. DESARROLLO DE LA METODOLOGÍA MEHARI IDENTIFICACIÓN DE RIESGOS

El primer paso en la gestión de riesgos es comprender las amenazas potenciales que la organización enfrenta, Mehari-Standard facilita esta identificación a través del análisis de las actividades y activos de información importantes del negocio que las soportan; La metodología recomienda comenzar identificando los procesos de misión cruciales de la empresa y para cada proceso, se describirán los resultados potenciales esperados y las interrupciones que se temen que impidan estos resultados. En términos de retrasos, falta de conformidad, exclusión de pasos o pérdida de confidencialidad, estas interrupciones se describen en un nivel funcional.

Posteriormente, se realiza un mapeo entre los activos de información y las interrupciones funcionales que podrían resultar en ellas, Mehari divide los activos en "primarios" (servicios, datos, procesos) y "de soporte" (software, hardware, instalaciones) cada activo principal se examina en función de la disponibilidad, la integridad, la confidencialidad y la eficiencia.

Esta matriz muestra situaciones específicas de riesgo, como la pérdida de la confidencialidad de una base de datos importante o la indisponibilidad de un servidor de aplicaciones. Mehari facilita la clasificación proporcionando listas de activos predefinidos.

Tabla de impacto intrínseco

			D	I	C	E	Selección de activos	Comentarios
Activos de tipo de datos								
Datos e información								
D01	Datos de la aplicación	Datos contenidos en archivos o bases de datos utilizados por las aplicaciones	3	3	3		1	
D02	Datos de oficina	Datos contenidos en archivos personales o compartidos, incluidos archivos de calendario o contactos	3	3	3		1	
D03	Información escrita o impresa	en poder de los usuarios, registros personales, listados impresos e informes de aplicaciones informáticas, y documentación de procesos y otros activos que puedan ser necesarios para el negocio.		3	3		1	
D04	Correo electrónico o correo postal	Correo electrónico, correo postal o faxes	3	3	3		1	
D05	Archivo	archivos patrimoniales, documentales o informáticos					1	
D06	Datos e información publicados	en sitios públicos o internos	3	3			1	
D07	Datos externalizados	en la nube					1	
Activos de tipo de servicio			D	I	C	E		
Servicios de TI								
S01	Servicios de aplicación	Aplicaciones empresariales, servicios de oficina o sistemas comunes	3	3	3		1	
S02	Servicios externalizados	o alojado en la nube					1	
S03	Servicios de publicación de información	en un sitio web interno o público	3	3			1	
Proceso de gestión			D	I	C	E	1	
P01	Proceso de gestión de cumplimiento	requisitos legales o contractuales o de la entidad					1	
P02	Procesos de gobernanza y adopción de decisiones	en la gobernanza de la entidad (que puede dar lugar a una temida disfunción) incluyendo la gobernanza de la seguridad					1	

Nota: Los cuadros sombreados corresponden a casos en los que generalmente no hay clasificación que realizar y para los cuales no hay un escenario de riesgo en la base de datos Mehari.

Leyenda :

D	Disponibilidad
I	Integridad
C	Confidencialidad
E	Eficiencia (de los procesos de gestión, frente al cumplimiento de la legislación o los reglamentos o frente a las normas de gobernanza y toma de decisiones).

Figura 3. Tabla de impacto identificación de riesgo
Jouas, J. P. (2022). Guía de evaluación de servicios de seguridad

ISSN: 2007-4786

4. ANÁLISIS CUANTITATIVO DE RIESGOS

Una vez identificados los escenarios de riesgo, el siguiente paso es realizar un análisis cuantitativo para estimar el nivel de probabilidad e impacto de cada uno, Mehari-Standard propone una metodología estructurada para evaluar estos dos factores de forma inherente, sin tomar en consideración los controles existentes:

Análisis en dos etapas

1. Evaluación inherente: se estima la probabilidad y el impacto máximos, sin considerar aún los controles de seguridad existentes.
   - La probabilidad inherente se mide en una escala del 1 al 4 según la exposición natural de la organización a esa amenaza.
   - El impacto inherente también usa una escala del 1 al 4 que clasifica el daño potencial sobre disponibilidad, integridad, confidencialidad o eficiencia del activo.
2. Evaluación residual: se ajustan la probabilidad y el impacto en base a la eficiencia de los controles de seguridad diagnosticados.
   - Mehari provee cuadrículas de decisión que guían el ajuste de probabilidad e impacto de acuerdo con el tipo de amenaza y controles implementados (CLUSIF, 2022).
   - El resultado es la probabilidad y el impacto residuales, que determinan el nivel final de riesgo.

Con estas estimaciones cuantitativas, Mehari construye una matriz de calor que grafica los escenarios por cuadrantes según su severidad residual, los escenarios en la zona roja son de alto riesgo de igual forma la herramienta también permite la parametrización de la evaluación de riesgos y la comparación de escenarios bajo diferentes supuestos. Para la gestión de riesgos de seguridad de la información, el enfoque cuantitativo de Mehari supera con creces el nivel de análisis cualitativo o subjetivo siendo uno de los valores más importantes de Mehari frente a otras metodologías.

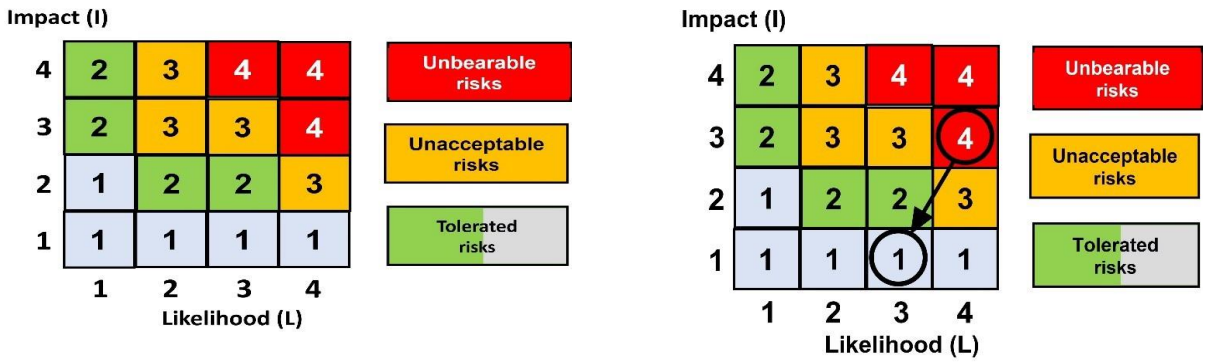

Figura 4. Matriz de aceptación de riesgos – Evaluación de riesgo residual
Jouas, J. P. (2022). MÉHARI Guía de análisis de riesgos y tratamiento

5. TRATAMIENTO DE RIESGOS

Una vez que se obtiene el perfil cuantitativo de riesgos residuales, el siguiente paso en la metodología Mehari es definir el tratamiento apropiado para aquellos que queden por encima de los niveles aceptables, Mehari se enfoca en reducir los riesgos mejorando los controles de seguridad y para esto propone trabajar con

"proyectos de seguridad" que agrupan varios controles relacionados, la base de conocimientos de Mehari contiene una biblioteca de aproximadamente 50 proyectos predefinidos, como por ejemplo:

- Implementación de firewalls y DMZ
- Refuerzo de controles de acceso físico
- Desarrollo de sitio alterno y plan de continuidad
- Capacitación en seguridad para usuarios

Cada proyecto especifica los controles que se utilizan y los nuevos niveles objetivo, el usuario selecciona los proyectos para reducir los riesgos inaceptables en cada dominio o de forma general, se deben planificar los proyectos con fechas de inicio y finalización. Mehari simula la evolución del perfil de riesgos a lo largo del tiempo en función de la implementación prevista. Si los proyectos no producen el resultado deseado, también se pueden modificar.

A través de la selección, planificación y monitoreo de proyectos de seguridad específicos, Mehari proporciona una solución integral para el tratamiento de riesgos es así como la elección de invertir en controles se basa en su enfoque cuantitativo.

Selección de proyectos

Dominios de escenarios	Número de escenarios						Proyectos	*Estado del proyecto*	Selección
	Se 1	Se 2	Se 3	Se 4	Total				
DAPD	Indisponibilidad de datos de aplicación								
	0				19	CALO	Control de acceso a locales sensibles	*Decidido*	
		5	14	0		CASA	Control de acceso a sistemas y aplicaciones	*Seleccionado*	1
						CERD CODI COMA	Control de la transmisión y recepción de datos y mensajes Comprobaciones de datos de incidentes Control de las operaciones de mantenimiento		
						GMAF SADC	Gestión de los medios de acceso a ficheros de datos o archivos de programa Copias de seguridad de datos y configuración (no subcontratadas)		
						SMED SUAI	Seguridad física de los medios de comunicación Monitoreo interno de la actividad	*Decidido*	
						SULO	Supervisión de locales sensibles		

Figura 5. Selección de proyectos
Jouas, J. P. (2022). MÉHARI Guía de análisis de riesgos y tratamiento

6. MONITOREO DE RIESGOS

Una vez definido e implementado el tratamiento de riesgo a través de algún proyecto de seguridad, es crucial llevar a cabo un monitoreo continuo para garantizar que los controles implementados estén logrando y manteniendo la reducción del riesgo deseado.

Mehari facilita el monitoreo a través de indicadores y uso de dashboards que resumen la evolución del perfil de riesgos con base a métricas como:

ISSN: 2007-4786

- Número de escenarios por nivel de riesgo (1 a 4).
- Escenarios mapeados por tipo de activo y criterio afectado.
- Participación de los diferentes tipos de amenazas.

Los tableros permiten incluir los cambios en la probabilidad y el efecto previsto por la implementación de los planes de tratamiento, demostrando si alguno de ellos no está teniendo el efecto contemplado o si han surgido nuevos riesgos.

Dashboard

Refresh

Número de escenarios de riesgo, por nivel

	Level 1	Level 2	Level 3	Level 4
Riesgos intrínsecos	0	0	138	3
Riesgos actuales	1	0	137	3
Reducción de riesgos, al final de todos los planes seleccionados	31	98	12	0
Riesgos aceptados	0	2	1	0
Evasión del riesgo	1	0	1	0
Riesgos transferidos	1	0	1	0

Figura 6. Dashboard – Riesgos evitados, transferidos o aceptados
Jouas, J. P. (2022). Guía de evaluación de servicios de seguridad

El monitoreo efectivo requiere de actualizar periódicamente los análisis para incorporar:

- Modificaciones en el entorno de amenazas (CLUSIF, 2022)
- Nuevos activos y procesos del negocio
- Cambios en la eficiencia de controles existentes
- Riesgos emergentes

Evolution of risks per year

In function of planned projects

	21/04/2022	01/01/2023	01/01/2024	01/01/2025	01/01/2026	01/01/2027	01/01/2028	01/01/2029	01/01/2030	01/01/2031	01/01/2032
Number of level 4 risks	3	0	0	0	0	0	0	0	0	0	0
Number of level 3 risks	137	133	74	60	39	26	16	16	16	16	16

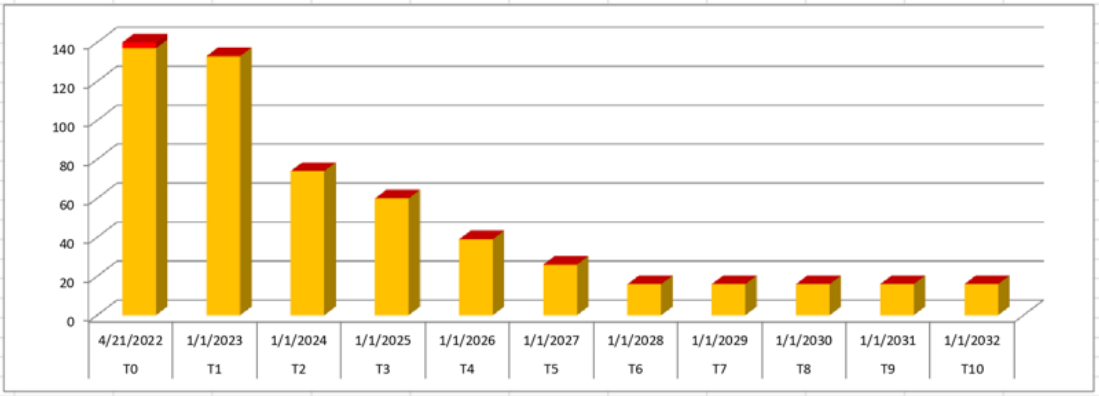

Figura 7. Dashboard – evolución número de riesgos por nivel de gravedad al paso del tiempo
Jouas, J. P. (2022). Guía de evaluación de servicios de seguridad

Es de esta manera, como los dashboards de Mehari-Standard facilitan el seguimiento del perfil de riesgos de forma continua y proactiva del estado actual como del proyectado, con el fin de que los usuarios puedan monitorear el estado y la evolución de los riesgos de seguridad de la información, proporcionando una visión completa para una gestión de riesgos eficaz.

7. CONCLUSIÓN

La gestión de riesgos de seguridad de la información es un proceso sistemático que involucra múltiples etapas, desde la identificación de amenazas hasta el monitoreo de controles, realizar este proceso de manera integral y cuantitativa puede representar un desafío, a continuación, presento algunas recomendaciones que a criterio propio pueden ayudar a conducir a una gestión de riesgos correcta, que no agregue estrés al equipo implementador de un SGSI.

- Utilizar una metodología que brinde procesos, técnicas y herramientas probadas, evitando la improvisación.
- Aprovechar las bases de conocimiento de amenazas y escenarios de riesgo ya considerados por expertos.
- No analizar los riesgos de toda la organización simultáneamente, iniciar con las áreas con riesgos de alto impacto.
- Tener claro quiénes son los dueños de cada riesgo.
- Capacitar al personal de la organización en conceptos básicos de análisis de riesgos.
- Comunicar resultados del análisis en forma simple y focalizada para cada tipo de público. (ejecutivos, técnicos, etc.)
- Monitorear cambios en el entorno que puedan variar el nivel de los riesgos.
- Reevaluar periódicamente.

Una metodología experta como Mehari demuestra su potencial, proveyendo un conjunto de herramientas consistentes para cada paso en la gestión de riesgos de un sistema de información. Su enfoque cuantitativo con base en el análisis detallado de probabilidad e impacto brinda métricas objetivas para la toma de decisiones y la posibilidad de parametrizar los análisis, simular diferentes escenarios y comparar resultados, otorga una gran adaptabilidad al incluir las bibliotecas de amenazas, activos y proyectos de seguridad que aceleran su aplicación con el uso de sus tableros e indicadores Mehari facilita el monitoreo para mantener los riesgos bajo control.

Es definitivo considerar que Mehari representa una solución integral que se posiciona como una de las metodologías más robustas disponibles actualmente para la gestión cuantitativa de riesgos de seguridad de la información tanto para organizaciones que recién inician como para aquellas con programas de seguridad maduros, adoptar un enfoque experto y reproducible como el que ofrece Mehari puede marcar una diferencia significativa en la efectividad de la gestión. Se trata sin duda de una metodología que todo CISO y responsable de un sistema de información debería considerar y evaluar cuidadosamente.

ISSN: 2007-4786

REFERENCIAS

[1] (ISO/CEI JTC 1/SC 27, 2022) ISO/IEC 27001 Sistemas de gestión de seguridad de la información. https://www.iso.org/standard/27001

[2] Jouas, J. P. (2022). Expedientes Técnicos Mehari—Guía de usuario. CLUSIF. https://clusif.fr/services/management-des-risques/les-fondamentaux-de-mehari/

[3] Jouas, J. P. (2022). Guía de evaluación de servicios de seguridad. Mehari: Conceptos fundamentales y especificaciones funcionales. CLUSIF. https://clusif.fr

[4] Jouas, J. P. (2022). MÉHARI Guía de análisis de riesgos y tratamiento. CLUSIF. https://clusif.fr

[5] Besterfield, (2009) Control de calidad (Octava, 1–978-607-442-121–7). Pearson Prentice Hall.Perles

[6] Roselló, M. J. (2015). Evolución histórica de los estudios sobre riesgos. Propuestas temáticas y metodológicas para la mejora del análisis y gestión del riesgo desde una perspectiva geográfica. BAETICA. Estudios De Historia Moderna Y Contemporánea, (26), 103–127. https://doi.org/10.24310/BAETICA.2004.v0i26.342

Correo de autor de correspondencia: ***jalopezarias78@gmail.com***