FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

Evaluación y gestión de riesgos en ciberseguridad institucional, implementando inteligencia artificial

Fernando Nicolas
Alomoto Quintanilla
fernando.alomoto@udla.edu.ec

Brandon Sebastian
Villacis Salazar
brandon.villacis@udla.edu.ec

Ingeniería en Tecnologías de la Información

DESCRIPCIÓN Y ALCANCE

La institución de educación superior enfrenta un incremento sostenido de riesgos en ciberseguridad debido a la dependencia de activos tecnológicos críticos y a la ausencia de procesos estandarizados y automatizados para la evaluación de riesgos. En muchos casos, el análisis se realiza de forma manual, con alta dependencia del criterio del evaluador, lo que dificulta la priorización de riesgos y la toma de decisiones oportunas.

Frente a esta problemática, el proyecto propone el diseño e implementación de un sistema institucional de evaluación y gestión de riesgos, basado en la metodología MAGERIT v3, apoyado por controles ISO/IEC 27002 e inteligencia artificial aplicada a la fase de evaluación, permitiendo un análisis más consistente y ágil.

OBJETIVO GENERAL

Desarrollar un sistema institucional para la evaluación y gestión de riesgos en ciberseguridad, basado en la metodología MAGERIT v3, incorporando inteligencia artificial para la evaluación automatizada de riesgos y Power BI como herramienta de visualización, con el fin de apoyar la toma de decisiones estratégicas en seguridad de la información.

METODOLOGÍA

El proyecto es basado en los marcos MAGERIT v3 e ISO/IEC 27002:2022, aplicado a activos críticos. La metodología contempla la identificación e inventario de activos, su valoración en Disponibilidad, Integridad y Confidencialidad (D/I/C) mediante cuestionarios estructurados, la identificación de amenazas y vulnerabilidades usando el catálogo MAGERIT y el apoyo de inteligencia artificial local, el cálculo de impacto y riesgo, la visualización mediante matrices de riesgo y la recomendación de salvaguardas alineadas a ISO 27002, permitiendo además la reevaluación periódica para medir la efectividad de las acciones de mitigación.

ANÁLISIS Y DISCUSIÓN DE RESULTADOS

Valoraciones

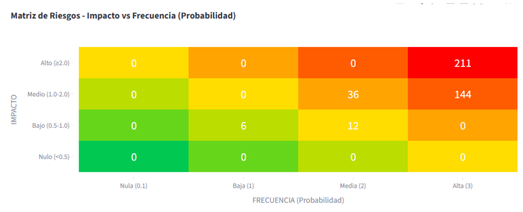
Nombre_Activo	D	Valor_D	I	Valor_I	C	Valor_C	Criticidad	Criticidad_Nivel	RTO_Tiempo	RTO_Nivel	RPO_Tiempo
SNAPP12	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
SNAPI01N2	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
SNAPI01N1	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
SNAPI01N3	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
SNAPP12_02	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
OCREG04	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
OCREG03	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
OCSSB01	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
BASTION_PROD	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
OCJCOG01	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)

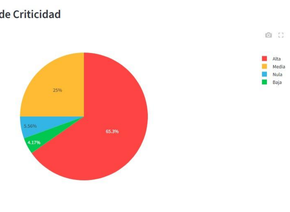
Nombre_Activo	Criticidad	Cod_Amenaza	Cod_Vuln	Deg_D	Deg_I	Deg_C	Impacto
Servidor Físico Dell PowerEdge R750	Alta	A.24	HW-V01	100%	13%	8%	3.00
Servidor Físico Dell PowerEdge R750	Alta	E.2	HW-V06	76%	63%	24%	2.28
Servidor Físico Dell PowerEdge R750	Alta	A.11	HW-V02	65%	72%	72%	2.16
Servidor Físico Dell PowerEdge R750	Alta	A.5	HW-V03	43%	72%	72%	2.16
Servidor Físico Dell PowerEdge R750	Alta	A.8	HW-V04	70%	59%	32%	2.10
Servidor Físico Dell PowerEdge R750	Alta	E.1	HW-V05	65%	59%	32%	1.95
VM-DB-ORACLE-PROD-01	Baja	A.24	HW-V01	74%	12%	8%	0.74
VM-DB-ORACLE-PROD-01	Baja	A.11	HW-V02	47%	66%	70%	0.70
VM-DB-ORACLE-PROD-01	Baja	A.5	HW-V03	31%	66%	70%	0.70
VM-DB-ORACLE-PROD-01	Baja	E.2	HW-V06	55%	57%	23%	0.57
VM-DB-ORACLE-PROD-01	Baja	A.8	HW-V04	51%	55%	31%	0.55

Salvaguardas

Id	ID_Evaluacion	ID_Activo	Nombre_Activo	Riesgo_	Vulnerabilidad	Amen
49	EVA-001	ACT-EVA-001-016	BASTION_PROD		Firmware desactualizado: BIOS/UEFI sin actualizaciones de seguridad	Deneg
147	EVA-001	ACT-EVA-001-016	BASTION_PROD		Hardware obsoleto: Equipos sin soporte del fabricante	Errore
169	EVA-001	ACT-EVA-001-016	BASTION_PROD		Puertos USB habilitados: Acceso físico a puertos sin control	Acces
213	EVA-001	ACT-EVA-001-016	BASTION_PROD		Discos sin cifrar: Almacenamiento local sin encriptación	Difusi
310	EVA-001	ACT-EVA-001-016	BASTION_PROD		BIOS sin contraseña: Configuración de hardware accesible	Errore
50	EVA-001	ACT-EVA-001-034	OCADP01		Firmware desactualizado: BIOS/UEFI sin actualizaciones de seguridad	Deneg
148	EVA-001	ACT-EVA-001-034	OCADP01		Hardware obsoleto: Equipos sin soporte del fabricante	Errore
171	EVA-001	ACT-EVA-001-034	OCADP01		Puertos USB habilitados: Acceso físico a puertos sin control	Acces
172	EVA-001	ACT-EVA-001-034	OCADP01		Falta de TPM: Sin módulo de plataforma segura para cifrado	Supla

Mapa radar con el mapa de calor





Nivel de madurez

CONCLUSIONES Y RECOMENDACIONES

- **Conclusiones**

La aplicación de MAGERIT v3 facilitó la identificación de activos relevantes, amenazas y niveles de riesgo inherente y residual, considerando los criterios de Disponibilidad, Integridad y Confidencialidad, lo que permitió obtener una visión clara y coherente del estado de los riesgos dentro del contexto institucional.

La integración de inteligencia artificial ejecutada de forma local apoyó el proceso de evaluación mediante la generación de valoraciones consistentes y alineadas a los criterios definidos por la metodología, manteniendo la confidencialidad de la información y sin reemplazar el criterio del analista humano.

Recomendaciones:

Se recomienda mantener la actualización periódica del sistema automatizado, fortalecer la capacitación del personal y ampliar el sistema para futuras evaluaciones de madurez y monitoreo continuo.

IMPLICACIONES ETICAS

El proyecto considera principios éticos fundamentales como la confidencialidad, integridad y uso responsable de la información institucional. Los datos analizados son anonimizados y utilizados exclusivamente con fines académicos y de mejora en la gestión de riesgos, garantizando la privacidad de la institución y el cumplimiento de buenas prácticas en ciberseguridad.

PRINCIPALES REFERENCIAS

MAGERIT v3 – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
ISO/IEC 27002:2022 – Controles de seguridad de la información.
Microsoft Power BI – Visualización y análisis de datos.
Literatura académica sobre gestión de riesgos e inteligencia artificial aplicada a ciberseguridad.

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

Risk assessment and management in institutional cybersecurity, implementing artificial intelligence

Fernando Nicolas
Alomoto Quintanilla
fernando.alomoto@udla.edu.ec

Brandon Sebastian
Villacis Salazar
brandon.villacis@udla.edu.ec

Ingeniería en Tecnologías de la Información

DESCRIPTION AND SCOPE

Higher education institutions face a sustained increase in cybersecurity risks due to their dependence on critical technological assets and the absence of standardized and automated processes for risk assessment. In many cases, analysis is performed manually, with a high degree of dependence on the evaluator's criteria, which makes it difficult to prioritize risks and make timely decisions.

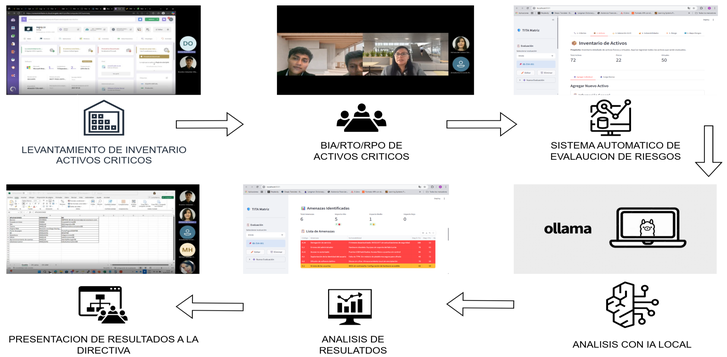
In response to this problem, the project proposes the design and implementation of an institutional risk assessment and management system based on the MAGERIT v3 methodology, supported by ISO/IEC 27002 controls and artificial intelligence applied to the assessment phase, allowing for a more consistent and agile analysis.

GENERAL OBJECTIVE

Develop an institutional system for cybersecurity risk assessment and management, based on the MAGERIT v3 methodology, incorporating artificial intelligence for automated risk assessment and Power BI as a visualization tool, in order to support strategic decision-making in information security.

METHODOLOGY

The project is based on the MAGERIT v3 and ISO/IEC 27002:2022 frameworks, applied to critical assets. The methodology includes the identification and inventory of assets, their assessment in terms of Availability, Integrity, and Confidentiality (A/I/C) using structured questionnaires, the identification of threats and vulnerabilities using the MAGERIT catalog and local artificial intelligence support, the calculation of impact and risk, visualization using risk matrices, and the recommendation of safeguards aligned with ISO 27002, also allowing for periodic reassessment to measure the effectiveness of mitigation actions.



ANALYSIS AND DISCUSSION OF RESULTS

Assessments

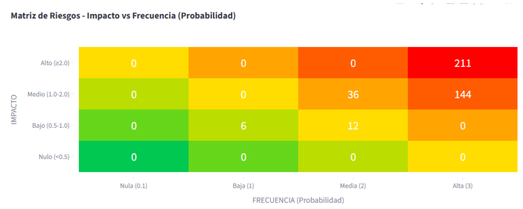
Nombre_Activo	D	Valor_D	I	Valor_I	C	Valor_C	Criticidad	Criticidad_Nivel	RTO_Tiempo	RTO_Nivel	RPO_Tiempo
SNAPP12	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
SNAPI01N2	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
SNAPI01N1	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
SNAPI01N3	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
SNAPP12_02	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
OCREG04	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
OCREG03	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
OCSSB01	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
BASTION_PROD	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)
OCJCOG01	A	3	A	3	A	3	3	Alta	< 1 hora	Alto	0 (cero pérdida)

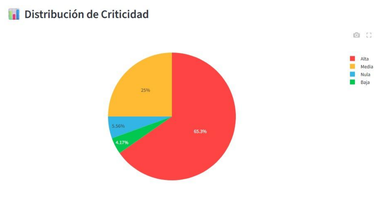
Nombre_Activo	Criticidad	Cod_Amenaza	Cod_Vuln	Deg_D	Deg_I	Deg_C	Impacto
Servidor Físico Dell PowerEdge R750	Alta	A.24	HW-V01	100%	13%	8%	3.00
Servidor Físico Dell PowerEdge R750	Alta	E.2	HW-V06	76%	63%	24%	2.28
Servidor Físico Dell PowerEdge R750	Alta	A.11	HW-V02	65%	72%	72%	2.16
Servidor Físico Dell PowerEdge R750	Alta	A.5	HW-V03	43%	72%	72%	2.16
Servidor Físico Dell PowerEdge R750	Alta	A.8	HW-V04	70%	59%	32%	2.10
Servidor Físico Dell PowerEdge R750	Alta	E.1	HW-V05	65%	59%	32%	1.95
VM-DB-ORACLE-PROD-01	Baja	A.24	HW-V01	74%	12%	8%	0.74
VM-DB-ORACLE-PROD-01	Baja	A.11	HW-V02	47%	66%	70%	0.70
VM-DB-ORACLE-PROD-01	Baja	A.5	HW-V03	31%	66%	70%	0.70
VM-DB-ORACLE-PROD-01	Baja	E.2	HW-V06	55%	57%	23%	0.57
VM-DB-ORACLE-PROD-01	Baja	A.8	HW-V04	51%	55%	31%	0.55

Safeguards

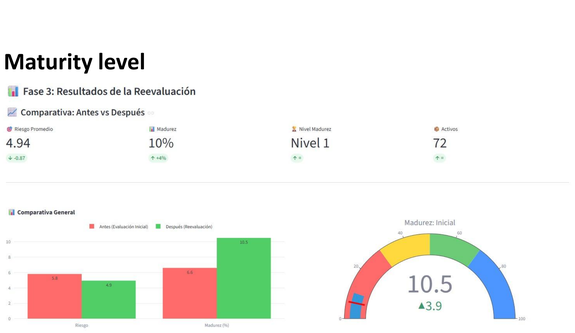
Id	ID_Evaluacion	ID_Activo	Nombre_Activo	Riesgo_	Vulnerabilidad	Ame
49	EVA-001	ACT-EVA-001-016	BASTION_PROD		Firmware desactualizado: BIOS/UEFI sin actualizaciones de seguridad	Deneg
147	EVA-001	ACT-EVA-001-016	BASTION_PROD		Hardware obsoleto: Equipos sin soporte del fabricante	Errore
169	EVA-001	ACT-EVA-001-016	BASTION_PROD		Puertos USB habilitados: Acceso físico a puertos sin control	Acces
170	EVA-001	ACT-EVA-001-016	BASTION_PROD		Falta de TPM: Sin módulo de plataforma segura para cifrado	Supla
213	EVA-001	ACT-EVA-001-016	BASTION_PROD		Discos sin cifrar: Almacenamiento local sin encriptación	Difusi
310	EVA-001	ACT-EVA-001-016	BASTION_PROD		BIOS sin contraseña: Configuración de hardware accesible	Errore
50	EVA-001	ACT-EVA-001-034	OCADP01		Firmware desactualizado: BIOS/UEFI sin actualizaciones de seguridad	Deneg
148	EVA-001	ACT-EVA-001-034	OCADP01		Hardware obsoleto: Equipos sin soporte del fabricante	Errore
171	EVA-001	ACT-EVA-001-034	OCADP01		Puertos USB habilitados: Acceso físico a puertos sin control	Acces
172	EVA-001	ACT-EVA-001-034	OCADP01		Falta de TPM: Sin módulo de plataforma segura para cifrado	Supla

Radar map with heat map





Maturity level



CONCLUSIONS AND RECOMMENDATIONS

Conclusions:

The application of MAGERIT v3 facilitated the identification of relevant assets, threats, and inherent and residual risk levels, considering the criteria of Availability, Integrity, and Confidentiality, which provided a clear and consistent view of the status of risks within the institutional context.

The integration of locally executed artificial intelligence supported the evaluation process by generating consistent assessments aligned with the criteria defined by the methodology, maintaining the confidentiality of the information and without replacing the judgment of the human analyst.

Recommendations:

It is recommended to maintain regular updates of the automated system, strengthen staff training, and expand the system for future maturity assessments and continuous monitoring.

ETHICAL IMPLICATIONS

The project considers fundamental ethical principles such as confidentiality, integrity, and responsible use of institutional information. The data analyzed is anonymized and used exclusively for academic purposes and to improve risk management, ensuring the institution's privacy and compliance with good cybersecurity practices.

MAIN REFERENCES

MAGERIT v3 – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

ISO/IEC 27002:2022 – Controles de seguridad de la información.

Microsoft Power BI – Visualización y análisis de datos.

Literatura académica sobre gestión de riesgos e inteligencia artificial aplicada a ciberseguridad.