

Análisis de riesgos y amenazas de ciberseguridad en el estado ecuatoriano, utilizando la metodología Magerit

Analysis of cybersecurity risks and threats in the Ecuadorian state, using the Magerit methodology.

Manuel Guamán

jose.guaman@est.ucacue.edu.ec

Universidad Católica de Cuenca, Ecuador

José Antonio Carrillo

jacarrilloz@ucacue.edu.ec

Universidad Católica de Cuenca, Ecuador

Cristhian Flores Urgilés

chfloresu@ucacue.edu.ec

Universidad Católica de Cuenca, Ecuador

Cristina Flores Urgilés

cmfloresu@ucacue.edu.ec

Universidad Católica de Cuenca, Ecuador

Mario Ron Egas

mbron@espe.edu.ec

Universidad Católica de Cuenca, Ecuador

**Pro Sciences: Revista de Producción,
Ciencias e Investigación**

CIDEPRO, Ecuador

e-ISSN: 2588-1000

Periodicidad: Trimestral

Vol. 7, No. 49, 2023

editor@journalprosciences.com

Recepción: 14 julio 2023

Aprobación: 29 agosto 2023

DOI: <https://doi.org/10.29018/issn.2588-1000vol7iss49.2023pp139-165>

Resumen: El estado ecuatoriano, debido a su tamaño, relevancia económica y vasta cantidad de información confidencial, se ha convertido en un objetivo atractivo para los atacantes cibernéticos. Esto ha llevado a la realización de un estudio enfocado en el análisis de riesgos y amenazas de ciberseguridad de los activos del país. En donde los objetivos planteados fueron: a) Realizar un análisis de riesgos y amenazas de ciberseguridad en el estado ecuatoriano, para determinar las vulnerabilidades a las que se encuentra expuesto el país, b) Realizar un estudio teórico sobre las metodologías de análisis y gestión de riesgos que se puedan aplicar para países, c) Realizar un levantamiento de activos críticos de información pertenecientes al Estado ecuatoriano, d) Analizar los riesgos, determinar vulnerabilidades y amenazas de ciberseguridad; para los activos críticos del estado ecuatoriano utilizando la metodología Magerit. Se aplicó la metodología MAGERIT para identificar y categorizar las amenazas, vulnerabilidades y riesgos, clasificando los activos críticos en áreas como gobierno, salud y energía, y las amenazas según su origen, como errores de usuarios, fallos técnicos, ataques deliberados y desastres naturales. El estudio evaluó el impacto potencial de cada amenaza en términos de confidencialidad, integridad y disponibilidad, y estimó la probabilidad de ocurrencia, calculando así el nivel de riesgo para priorizar acciones de mitigación. Los resultados revelaron que los activos con mayores riesgos son los datos personales y financieros de los ciudadanos, historias clínicas e información gubernamental confidencial.

Palabras Clave: ciberseguridad, metodología Magerit, infraestructura crítica, Ecuador

Como citar: Guamán , M., Carrillo Zenteno, J. A., Flores Urgilés , C., Flores Urgilés , C., & Ron Egas , M. (2023). Análisis de riesgos y amenazas de ciberseguridad en el estado ecuatoriano, utilizando la metodología Magerit. Pro Sciences: Revista De Producción, Ciencias E Investigación, 7(49). Recuperado a partir de <https://journalprosciences.com/index.php/ps/article/view/676>

Abstract: The Ecuadorian state, due to its size, economic relevance, and vast amount of confidential information, has become an attractive target for cyber attackers. This has led to the conduct of a study focused on the analysis of cybersecurity risks and threats to the country's assets. The proposed objectives were: a) To carry out an analysis of risks and threats of cybersecurity in the Ecuadorian state, to determine the vulnerabilities to which the country is exposed, b) To conduct a theoretical study on the methodologies of analysis and risk management that can be applied to countries, c) To carry out a survey of critical information assets belonging to the Ecuadorian State, d) To analyze the risks, determine vulnerabilities, and threats of cybersecurity for the critical assets of the Ecuadorian state using the Magerit methodology.

The MAGERIT methodology was applied to identify and categorize threats, vulnerabilities, and risks, classifying critical assets into areas such as government, health, and energy, and threats according to their origin, such as user errors, technical failures, deliberate attacks, and natural disasters. The study evaluated the potential impact of each threat in terms of confidentiality, integrity, and availability, and estimated the likelihood of occurrence, thus calculating the risk level to prioritize mitigation actions.

The results revealed that the assets with the highest risks are the personal and financial data of citizens, medical records, and confidential governmental information.

Key words: cybersecurity, Magerit methodology, critical infrastructure, Ecuador

INTRODUCCIÓN

En un entorno global progresivamente interconectado y digitalizado, la ciberseguridad se ha establecido como un pilar indispensable para garantizar la integridad, confidencialidad y accesibilidad de los datos (Astrillón, 2021). Los retos que encara la ciberseguridad son variados y en constante evolución, abarcando desde la alteración de información y salvaguarda de infraestructuras esenciales, hasta la lucha contra el delito informático y el espionaje cibernético.

La interconexión ha permitido que los países enfrenten una variedad de riesgos y amenazas de ciberseguridad; bajo este contexto, este escenario plantea la necesidad de un enfoque sistemático y metódico para identificar, evaluar y manejar tales amenazas. Centrándose en analizar los riesgos que existen debido a las vulnerabilidades de las infraestructuras digitales, las amenazas potenciales que pueden explotar estas vulnerabilidades y el impacto que estos eventos podrían tener en la seguridad y estabilidad del Ecuador. Esto incluye, pero no se limita a, ataques a la infraestructura crítica, espionaje cibernético, robos de identidad, fraude en línea y ataques de denegación de servicio.

El tema del análisis de riesgos y amenazas de ciberseguridad en países es amplio y multifacético, que abarca diversas disciplinas, desde la ciencia de la computación y la ingeniería de sistemas hasta la política y la economía. Para navegar eficazmente en este campo, es importante comprender tanto las dimensiones técnicas como las socioeconómicas y políticas de la ciberseguridad, y cómo se interceptan y se afectan mutuamente.

Ciberseguridad

La ciberseguridad es la práctica de proteger los sistemas informáticos y la información de los ataques cibernéticos. La ciberseguridad es una tarea compleja y en constante evolución. Al tomar medidas para protegerse de los ciberataques, las personas, las empresas y los gobiernos pueden ayudar a proteger sus sistemas informáticos y la información (Mendivil Caldentey, Sanz Urquijo, & Gutiérrez Almazor, 2022).

Amenazas cibernéticas

De acuerdo con Carvajal (2022), las amenazas cibernéticas se refieren a los posibles ataques maliciosos o intentos de acceso no autorizado a sistemas de información, con el propósito de robar, alterar, destruir o interrumpir los datos. Estos ataques son realizados por ciberdelincuentes, que pueden ser individuos o grupos, con motivos que varían desde el crimen financiero, el espionaje, la interrupción de servicios, hasta la guerra cibernética.

- **Malware:** Software malicioso que daña o toma el control de sistemas informáticos sin permiso. Incluye virus, gusanos y ransomware
- **Pishing:** Técnica de engaño en la que los ciberdelincuentes se hacen pasar por entidades legítimas para robar información confidencial.
- **Ataques de denegación de servicio (DoS):** Sobrecarga intencional de un sistema con tráfico malicioso para dejarlo inaccesible a usuarios legítimos.
- **Ataques de denegación de servicio distribuido (DDoS):** Variante del ataque DoS, que utiliza múltiples dispositivos para coordinar un ataque masivo y dificultar la mitigación:
- **Espionaje cibernético:** Infiltración en sistemas informáticos o redes para obtener información confidencial o secretos empresariales.
- **Ataques de día cero:** Aprovechamiento de vulnerabilidades desconocidas previamente en software o sistemas operativos.
- **Ataques de fuerza bruta:** Método de prueba de todas las combinaciones posibles para descifrar contraseñas o claves encriptadas (Castro, y otros, 2018)

Vulnerabilidades cibernéticas

Las vulnerabilidades cibernéticas se refieren a las debilidades o fallos en un sistema informático, red o software que pueden ser explotados para llevar a cabo actividades malintencionadas. Estas pueden ser utilizadas por actores maliciosos, como hackers o ciberdelincuentes, para penetrar en un sistema, alterar su funcionamiento, robar datos o causar daño de otras maneras (Anaya Moreno, 2021).

Las vulnerabilidades cibernéticas en un país son aquellas debilidades o fallos en los sistemas de información que ponen en riesgo la seguridad de la misma, permitiendo que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la información (Mamoona Humayun, Alshayeb, & Mahmood, 2020)

Gestión de riesgos

La gestión de riesgos es un enfoque sistemático para identificar, evaluar y controlar los riesgos. Es un proceso que ayuda a las organizaciones a tomar decisiones informadas sobre cómo lidiar con el riesgo. El objetivo de la gestión de riesgos es reducir la probabilidad y/o el impacto de eventos negativos, esta se puede aplicar a una amplia gama de actividades, incluidas las operaciones comerciales, la planificación financiera y la gestión de proyectos (ACCID, 2019).

Metodologías para la gestión de riesgos

Magerit

Menéndez (2022) “Es la metodología de análisis y gestión de riesgos de los Sistemas de Información, se encarga de analizar el impacto que puede tener una empresa en un incidente de seguridad, tratando de identificar las amenazas que pueden llegar a afectar a la empresa y las vulnerabilidades explotadas por estas amenazas teniendo así una idea de las medidas preventivas y correctivas adecuadas para cada caso” (pág. 43).

Magerit está compuesta de seis fases tales como:

- Definición del alcance: Se refiere a definir las áreas estratégicas en las que se va a revisar.
- Establecer los activos importantes de la organización con el objetivo de darles valor
- Determinar las vulnerabilidades y amenazas
- Conocer el impacto de los activos ante las amenazas
- Tratar el riesgo de probabilidad de ocurrencia de esa amenaza (Hurtado, 2018, pág. 9).

Octave

Esta metodología permite identificar y administrar los riesgos de seguridad de la información, se enfoca en tres aspectos fundamentales:

- Activo: Identifica los activos críticos de la organización, tales como la información que es crucial para la operación y supervivencia del negocio
- Amenaza: Identifica y evalúa las amenazas a estos activos, que pueden ser tanto internas (por ejemplo, empleados descontentos o errores de operación) como externas (por ejemplo, hackers o competidores)
- Vulnerabilidad: Evalúa las vulnerabilidades o debilidades que podrían ser explotadas por las amenazas para dañar los activos (Llauce Valdera, 2022).

Almagro (2019) manifiesta que:

El marco NIST CSF está diseñado para ayudar a las organizaciones a mejorar su postura de seguridad identificando, evaluando y mitigando los riesgos para sus sistemas de información. Incluye una serie de pasos, como la identificación de activos, la identificación de amenazas, la evaluación de vulnerabilidades y el desarrollo de controles de seguridad.

Entre las funciones del marco NIST CSF se encuentran:

- Identificar: Esta fase ayuda a desarrollar un entendimiento organizacional con el fin de determinar el riesgo de ciberseguridad de sistemas, personas, activos, datos y capacidades
- Proteger: Describe las medidas de ciberseguridad adecuadas para garantizar la entrega de servicios de infraestructuras críticas.
- Detectar: Establece las actividades de ciberseguridad para identificar la ocurrencia de un evento de ciberseguridad.
- Responder: Incluye actividades para tomar medidas ante un evento de ciberseguridad
- Recuperar: Identifica las actividades requeridas para mantener los planes de resiliencia y para restaurar cualquier capacidad (Luis Almagro, 2019, págs. 5-6).

Proceso de gestión de riesgos del Project Management Institute (PMI)

Este proceso está diseñado para ayudar a los gerentes de proyectos a identificar, evaluar y mitigar los riesgos que podrían afectar sus proyectos. Incluye una serie de pasos, como la identificación de riesgos, la evaluación de riesgos y el desarrollo de planes de respuesta a los riesgos (Project Management Institute, 2008).

De las metodologías analizadas anteriormente, se puede determinar al marco NIST CSF para aplicarlo a nivel nacional ya que es un marco adaptable y flexible que permite a las organizaciones y a los países a identificar y priorizar los riesgos de forma efectiva. Además, que se enfoca directamente en la ciberseguridad; mientras que la metodología Magerit proporciona una metodología sistemática para identificar, analizar y evaluar los riesgos que amenazan los sistemas de información.

Estado del Arte

La ciberseguridad se ha convertido en una preocupación esencial en todo el mundo, y el Ecuador no es la excepción. En la era de la digitalización, las amenazas y riesgos de ciberseguridad son cada vez más frecuentes y sofisticados, lo que hace imprescindible un análisis detallado y actualizado en el contexto del estado ecuatoriano. Las siguientes investigaciones permiten la identificación de las áreas en las que la ciberseguridad es más vulnerables, las principales amenazas existentes, las estrategias y medidas que se están tomando para mitigar estos riesgos, así como las brechas y desafíos que aún quedan por abordar.

Alvarado (2020) presenta en su artículo un estudio de los ataques cibernéticos en el Ecuador desde el año 2013, a través de una investigación descriptiva-analítica. En el que determina los servicios automatizados que tiene el país, políticas, regulaciones y estrategias. Estudiando en primera instancia el caso de Julián Assange, considerando leyes y acuerdos organizacionales. El autor concluye que el Estado ecuatoriano no cuenta con estrategias adecuadas para combatir ataques cibernéticos, es por ello que considera importante la creación de entidades que se enfoquen en la protección de infraestructuras críticas, así como un activo importante como es la información.

Por otro lado, Leyva en el año (2021), realiza un análisis de las políticas públicas del estado ecuatoriano a través de una revisión documental de fuentes certificadas. El autor analiza el régimen político en el ámbito estructural, sectorial y territorial; determinando aspectos para la construcción de estrategias nacionales, entre las que se encuentran la alineación para trabajar de manera armoniosa, la coordinación de sectores tanto públicos como privados, directivas, tareas, responsabilidades entre las partes interesadas. Concluye que el Ecuador debe adquirir políticas públicas conjuntamente con un modelo de gobernanza en seguridad cibernética.

Carvajal (2022) en su documento presenta un análisis del modelo de ciberseguridad del Estado ecuatoriano mediante una investigación analítica-conceptual, determinando amenazas en este ámbito en instituciones pertenecientes al Ecuador. La autora propone que el cuidado de amenazas, riesgos y daños se debe realizar para el mundo real y virtual, definiendo políticas públicas que puedan demostrar efectividad.

Dichas investigaciones permiten comprender las estrategias de ciberseguridad nacional ecuatorianas, analizar los activos importantes del país con el fin de realizar un análisis de riesgos y vulnerabilidades

Metodología

El presente estudio se lleva a cabo mediante la aplicación de la metodología MAGERIT, la cual consta de cinco fases: Identificación de activos, determinación de amenazas, determinación de medidas preventivas, medición del impacto residual y estimación del riesgo residual, cada una de ellas cumpliendo con un proceso específico; ya que este marco ofrece una estructura sólida para la gestión de la ciberseguridad y puede ser adaptado para su uso a nivel nacional.

La investigación se realizará a través de un enfoque estratégico, mismo que permite considerar tendencias emergentes en ciberseguridad, capacidades y recursos del país.

El método utilizado para el desarrollo de la investigación es inductivo, puesto que se realiza una investigación, y calificación para determinar los activos que se encuentran en riesgo.

Resultados

Al aplicar la metodología Magerit, es fundamental realizar la comprensión y el análisis de los activos de información del Ecuador, con la finalidad de determinar cómo puede verse afectado y que riesgos están presentes en las infraestructuras críticas del país.

Identificación de activos

Resulta crucial identificar todos los activos de información e infraestructura crítica del Ecuador para llevar a cabo la gestión de riesgos de los mismos. En la siguiente matriz se enumeran distintos tipos de activos que fueron tomados de la estrategia nacional de ciberseguridad del Ecuador; se identifican las infraestructuras relacionadas con cada sector. En la columna "Activos de Información", se identifican los activos de información relevantes asociados con cada infraestructura crítica o sector en el contexto del Ecuador. Estos se asocian con los tipos de activos que propone la metodología Magerit.

Tipo de Infraestructura Tipo de Procesos	Sector Macro proceso	Infraestructura Proceso	ID	Activos de Información Subproceso	Tipo de Activo MAGERIT
Infraestructura estratégica	Comunicaciones	Redes	Ac-001	Sistemas de enrutamiento	[COM] Redes de comunicaciones
		Instalaciones	Ac-002		
		Sistemas	Ac-003	Datos tributarios de los ciudadanos	[D] Datos / Información
	Tecnologías de ciberseguridad	Equipos físicos y de TI	Ac-004	Infraestructura de red	[COM] Redes de comunicaciones
		Firewalls	Ac-005	Firewalls	[AUX] equipamiento auxiliar
		Herramientas de gestión de identidad y acceso	Ac-006	Sistemas de gestión de identidad y acceso	[SW] aplicaciones (software)

Infraestructura crítica	Energía	Centrales eléctricas	Ac-007	Sistemas SCADA	[SW] aplicaciones (software)	
		Plantas de energía alternativas	Ac-008	Redes de distribución	[L] instalaciones	
	Transporte	Aeropuertos	Ac-009	Sistemas de control de tráfico aéreo y marítimo	[COM] Redes de comunicaciones	
		Puertos	Ac-010			
		Redes de carreteras y ferrocarriles	Ac-011	Datos de transporte		[D] Datos / Información
	Agua	Plantas de tratamiento de agua potable	Ac-012	Sistemas de control de tratamiento y distribución	[L] instalaciones	
	Petróleo y gas	Refinerías	Ac-013	Sistemas de control de producción	[L] instalaciones	
		Terminales de almacenamiento y distribución	Ac-014	Información sobre reservas y operaciones	[D] Datos / Información	
		Oleoductos y gasoductos	Ac-015			
	Salud	Hospitales	Ac-016	Historias clínicas de pacientes (IESS, Hospitales)		[D] Datos / Información
		Centros de atención primaria	Ac-017		Datos de pacientes	
	Militar	Bases militares	Ac-018	Datos sobre reservas y operaciones	[D] Datos / Información	
		Centros de operaciones	Ac-019	Sistemas de mando y control militar	[SW] aplicaciones (software)	
			Sistemas de información del	Ac-020	Datos gubernamentales	

Datos personales	Gobierno	gobierno central			[D] Datos / Información
		Instituciones financieras	Ac-021	Información Financiera de los ciudadanos	
		Sistemas de información de entidades gubernamentales	Ac-022	Información confidencial Registro único del ciudadano	

Escala de calificación de los activos de información e infraestructura crítica

Para evaluar los activos y la infraestructura crítica estatal, se utilizó una combinación de factores cuantitativos y cualitativos. Los factores cuantitativos se expresaron en términos numéricos, lo que permitió el análisis comparando los riesgos asumidos con los costos de las posibles soluciones. Los factores cualitativos se describieron utilizando una serie de criterios, que permitieron evaluar la gravedad de los posibles desenlaces y la probabilidad de su ocurrencia.

Tabla 1. Evaluación cuantitativa de los activos de información e infraestructura crítica.

Fuente: Autoría Propia

Valor		Criterio
9-10	Extremo	Daño extremadamente grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Insignificante	Irrelevante

El valor del activo e infraestructura crítica, se determinará utilizando la siguiente fórmula:

$$\text{Valor Activo} = C + I + D$$

En donde:

$C = \text{Confidencialidad}$

$I = \text{Integridad}$

$D = \text{Disponibilidad}$

Determinada la escala de valor, se procede a la realización de la evaluación de los activos de información e infraestructura estatal del Ecuador, basado en las dimensiones críticas (confidencialidad, integridad, disponibilidad).

Tabla 2. Escala de valor para calificación de activos de información. Fuente: (Gómez & Candau, 2012)

Rango	Calificación
1-3	Bajo
4-6	Medio
7-9	Alto
10-12	Muy Alto
13-15	Extremo

Tabla 3. Evaluación de los activos de ciberseguridad del estado ecuatoriano. Fuente: Autoría Propia.

Código activo	Tipo de Activo	Activo	Confidencialidad	Integridad	Disponibilidad	Total
Ac - 001	[D] Datos / Información	Datos tributarios de los ciudadanos	5	5	5	15
Ac - 002		Información sobre reservas y operaciones	4	4	3	11
Ac - 003		Historias clínicas de pacientes (IESS, Hospitales, centros de salud)	5	5	4	14
Ac - 004		Datos gubernamentales	5	5	5	15
Ac - 005		Información financiera de los ciudadanos	5	5	5	15
Ac - 006		Registro único del ciudadano	5	4	5	14
Ac - 003	[SW] Software - Aplicaciones informáticas	Sistemas de gestión de identidad y acceso	5	5	5	15
Ac - 004		Sistemas SCADA	5	4	4	13

Ac - 005		Sistemas de mando y control militar	5	3	4	12
Ac - 007	[COM] Redes de comunicaciones	Sistemas de enrutamiento	5	5	5	15
Ac - 008		Infraestructura de red	5	4	5	14
Ac - 009		Sistemas de control de tráfico aéreo y marítimo	5	5	5	15
Ac - 008	[HW]Equipamiento informático (hardware)	Firewall	5	5	5	15
Ac - 010	[L] Instalaciones	Redes de distribución (energía)	5	4	5	14
Ac - 011		Sistemas de control de tratamiento y distribución (agua)	5	5	5	15
Ac - 012		Sistemas de control de producción (petróleo y gas)	5	5	5	15

Identificación de las amenazas

Según el método Magerit, tras determinar los activos críticos (aquellos que se encuentran en el rango extremo), se avanza hacia la clasificación de las amenazas. Esta clasificación se realiza en base a la probabilidad de que dichas amenazas se materialicen y el daño potencial que podrían ocasionar. En la matriz que se presenta a continuación, se muestra el código correspondiente a cada amenaza, la categoría a la que pertenece el activo y las dimensiones que se evalúan (confidencialidad, integridad, disponibilidad).

Tabla 4. Clasificación de amenazas de los activos de información del estado ecuatoriano. Fuente: Autoría Propia.

CÓDIGO	ACTIVO	COD. A.	AMENAZA
Ac - 001	Datos tributarios de los ciudadanos	[E.15]	Alteración accidental de la información
		[E.19]	Fuga de Información
		[A.25]	Robo
		[A.30]	Ingeniería Social
Ac - 003	Historias clínicas de pacientes (IESS, hospitales)	[E.15]	Alteración accidental de la información
		[E.18]	Destrucción de información
		[E.19]	Fugas de información
Ac - 004	Datos gubernamentales	[E.2]	Errores del administrador
		[E.15]	Alteración accidental de la información
		[A.19]	Divulgación de información
		[E.19]	Fugas de información
		[A.11]	Acceso no autorizado
Ac - 005	Información Financiera de los ciudadanos	[E.15]	Alteración accidental de la información
		[A.25]	Robo
		[A.30]	Ingeniería Social
Ac - 006	Registro único del ciudadano	[E.15]	Alteración accidental de la información
		[E.19]	Fugas de información
Ac - 007	Sistemas de gestión de identidad y acceso	[E.2]	Errores del administrador
		[E.8]	Difusión de software dañino

		[A.5]	Suplantación de la identidad del usuario
		[A.11]	Acceso no autorizado
		[E.21]	Errores de mantenimiento / actualización de programas (software)
Ac - 008	Sistemas SCADA	[E.2]	Errores del administrador
		[E.21]	Errores de mantenimiento / actualización de programas (software)
		[A.11]	Acceso no autorizado
Ac - 010	Sistemas de enrutamiento	[A.9]	[Re-]encaminamiento de mensajes
		[A.12]	Análisis del tráfico
		[COM]	redes de comunicaciones
Ac - 011	Infraestructura de red	[E.2]	Errores del administrador
		[I.8]	Avería de origen físico o lógico
		[A.24]	Denegación de servicio
Ac - 012	Sistemas de control de tráfico aéreo y marítimo	[I.8]	Fallo de servicios de comunicaciones
		[E.2]	Errores del administrador
		[A.6]	Abuso de privilegios de acceso
Ac - 013	Firewall	[A.11]	Acceso no autorizado
		[I.5]	Avería de origen físico o lógico
		[E.23]	Errores de mantenimiento
Ac - 014	Redes de distribución (energía)	[N.1]	Fuego
		[N.*]	Desastres naturales
		[A.11]	Acceso no autorizado
		[E.15]	Alteración accidental de la información
Ac - 015	Sistemas de control de tratamiento y distribución (agua)	[N.2]	Daños por agua
		[N.*]	Desastres naturales
Ac - 016	Sistemas de control de producción (petróleo y gas)	[I.*]	Desastres industriales
		[N.*]	Desastres naturales
		[A.18]	Destrucción de información

Análisis y gestión de riesgos

Para el análisis y gestión de riesgos de acuerdo a la metodología Magerit, se debe evaluar los activos de información e infraestructura crítica de Ecuador. En el que se sitúan los activos críticos conjuntamente con sus amenazas y con la probabilidad y el impacto para calcular el riesgo.

Para realizar el cálculo de probabilidad se utilizarán los siguientes valores:

Tabla 5. Escala de probabilidad. Fuente: Autoría Propia

Nivel de probabilidad	Descripción	Valor
Muy bajo	La amenaza es probable que se materialice en el entorno actual o futuro previsible	1
Bajo	Existen circunstancias en las cuales la amenaza podría materializarse, pero no son raras	2
Medio	Existen circunstancias razonablemente posibles en las que las amenazas podrían materializarse	3
Alto	La amenaza es probable que se materialice en circunstancias normales	4
Muy alto	La amenaza es casi segura que se materializarán en el futuro previsible, a menos que se tomen medidas para prevenirla	5

Tabla 6. Escala de impacto. Fuente: Autoría Propia.

Nivel de impacto	Descripción	Valor
Insignificante	El daño a los activos, operaciones o reputación de la organización sería mínimo y manejable sin medidas correctivas especiales	1
Menor	El daño causaría inconvenientes menores y retrasos, pero no afectaría de manera significativa a las operaciones o a la reputación de la organización	2
Moderado	El daño causaría una interrupción notable y tendría un efecto moderado en las operaciones o la reputación de la organización	3
Mayor	El daño causaría una interrupción significativa en las operaciones o tendría un efecto grande en la reputación de la organización	4
Catastrófico	El daño causaría una interrupción grave en las operaciones o tendría un efecto devastador en la reputación de la organización	5

Para calcular el riesgo de los diferentes activos, se realiza una multiplicación de la probabilidad por el impacto. La siguiente tabla contiene el valor de los riesgos dependiendo de su nivel:

Tabla 7. Escala de valoración de los riesgos. Fuente: Autoría Propia.

Riesgo	Descripción	Rango
Bajo	Riesgo aceptable	1-6
Medio	Riesgo tolerable	7-14
Alto	Riesgo inadmisible	15-25

Tabla 8. Análisis de riesgos de los activos de información críticos del estado ecuatoriano.

Fuente: Autoría Propia.

ACTIVO	COD. A.	AMENA ZA	Impacto	Probabilidad	Riesgo
Datos tributarios de los ciudadanos	[E.15]	Alteración accidental de la información	5	3	15
	[E.19]	Fuga de Información	4	2	8
	[A.25]	Robo	4	4	16
	[A.30]	Ingeniería Social	4	3	12
Historias clínicas de pacientes (IESS, hospitales)	[E.15]	Alteración accidental de la información	5	2	10
	[E.18]	Destrucción de información	5	1	5
	[E.19]	Fugas de información	4	2	8
Datos gubernamentales	[E.2]	Errores del administrador	5	1	5
	[E.15]	Alteración accidental de la información	5	3	15
	[A.19]	Divulgación de información	5	4	20
	[E.19]	Fugas de información	5	5	25
	[A.11]	Acceso no autorizado	5	3	15
Información Financiera de los ciudadanos	[E.15]	Alteración accidental de la información	5	4	20
	[A.30]	Ingeniería Social	5	3	15

Registro único del ciudadano	[E.15]	Alteración accidental de la información	4	1	4
	[E.19]	Fugas de información	3	5	15
Sistemas de gestión de identidad y acceso	[E.2]	Errores del administrador	4	2	8
	[E.8]	Difusión de software dañino	5	2	10
	[A.5]	Suplantación de la identidad del usuario	5	1	5
	[A.11]	Acceso no autorizado	5	2	10
	[E.21]	Errores de mantenimiento / actualización de programas (software)	4	2	8
Sistemas SCADA	[E.2]	Errores del administrador	5	3	15
	[E.21]	Errores de mantenimiento / actualización de programas (software)	4	3	12
	[A.11]	Acceso no autorizado	5	2	10
Sistemas de enrutamiento	[A.9]	[Re-]encaminamiento de mensajes	4	2	8
	[A.12]	Análisis del tráfico	4	4	16
	[COM]	redes de comunicaciones	4	3	12
Infraestructura de red	[E.2]	Errores del administrador	5	2	10
	[I.8]	Avería de origen físico o lógico	5	3	15
	[A.24]	Denegación de servicio	5	4	20
Sistemas de control de tráfico aéreo y marítimo	[I.8]	Fallo de servicios de comunicaciones	5	2	10
	[E.2]	Errores del administrador	5	3	15
	[A.6]	Abuso de privilegios de acceso	4	2	8
Firewall	[A.11]	Acceso no autorizado	5	3	15
	[I.5]	Avería de origen físico o lógico	5	2	10
	[E.23]	Errores de mantenimiento	4	3	12
Redes de distribución (energía)	[N.1]	Fuego	5	1	5
	[N.*]	Desastres naturales	5	2	10
	[A.11]	Acceso no autorizado	5	2	10

	[E.15]	Alteración accidental de la información	4	3	12
Sistemas de control de tratamiento y distribución (agua)	[N.2]	Daños por agua	5	3	15
	[N.*]	Desastres naturales	5	2	10
Sistemas de control de producción (petróleo y gas)	[I.*]	Desastres industriales	5	3	15
	[N.*]	Desastres naturales	5	2	10
	[A.18]	Destrucción de información	5	2	10

CONTROLES

Analizado el riesgo de cada amenaza de los activos más críticos, es necesario implementar salvaguardas a aquellos riesgos medios y altos. El propósito primordial de este análisis es promover la instauración de sistemas de controles robustos y proporcionados a los riesgos identificados en las infraestructuras críticas del Ecuador. Así, si se concretan sucesos nocivos, las entidades encargadas de cada activo poseen la aptitud de reaccionar de una forma ágil y pertinente, disminuyendo la probabilidad de afectación a sus funciones y, por ende, mitigando el impacto en la sostenibilidad de sus operaciones.

Tabla 9. Selección de controles a los activos de información del estado ecuatoriano. Fuente: Autoría Propia.

ACTIVO	CO D.	AMENAZA	RIESG	CONTROL
Datos tributarios de los ciudadanos	[E.15]	Alteración accidental de la información	15	Cifrado de la información
	[E.19]	Fuga de Información	8	Aseguramiento de la integridad
	[A.25]	Robo	16	Copias de seguridad de los datos (backup)
	[A.30]	Ingeniería Social	12	
Historias clínicas de pacientes (IESS, hospitales)	[E.15]	Alteración accidental de la información	10	Formación y concienciación
	[E.19]	Fugas de información	8	Identificación y autenticación
	[E.15]	Alteración accidental de la información	15	Copias de seguridad de los datos (backup)
	[A.19]	Divulgación de información	20	Formación y concienciación
	[E.19]	Fugas de información	25	Identificación y autenticación
	[A.11]	Acceso no autorizado	15	Control de acceso lógico
Información Financiera de los ciudadanos	[E.15]	Alteración accidental de la información	20	Copias de seguridad de los datos (backup)
	[A.30]	Ingeniería Social	15	Formación y concienciación
	[E.19]	Fugas de información	15	Identificación y autenticación
Sistemas de gestión de identidad y acceso	[E.2]	Errores del administrador	8	Copias de seguridad (backup)

	[E.8]	Difusión de software dañino	10	Protección de las Aplicaciones Informáticas
	[A.11]	Acceso no autorizado	10	Control de acceso lógico
	[E.21]	Errores de mantenimiento / actualización de programas (software)	8	Cambios (actualizaciones y mantenimiento)
Sistemas SCADA	[E.2]	Errores del administrador	15	Copias de seguridad (backup)
	[E.21]	Errores de mantenimiento / actualización de programas (software).	12	Registro y auditoría
	[A.11]	Acceso no autorizado	10	Gestión de claves criptográficas Sistema de protección perimetral
Sistemas de enrutamiento	[A.9]	[Re-]encaminamiento de mensajes	8	Protección del servidor de nombres de dominio (DNS)
	[A.12]	Análisis del tráfico	16	Autenticación del canal
	[COM]	redes de comunicaciones	12	Seguridad Wireless (WiFi)
Infraestructura de red	[E.2]	Errores del administrador	10	Registro y auditoría
	[I.8]	Avería de origen físico o lógico	15	Protección del cableado
	[A.24]	Denegación de servicio	20	Segregación de las redes en dominios
Sistemas de control de tráfico aéreo y marítimo	[I.8]	Fallo de servicios de comunicaciones	10	Herramienta de monitorización de tráfico

	[E.2]	Errores del administrador	15	Formación y concienciación
	[A.6]	Abuso de privilegios de acceso	8	Aseguramiento de la disponibilidad
Firewall	[A.11]	Acceso no autorizado	15	Control de acceso lógico
	[I.5]	Avería de origen físico o lógico	10	Continuidad del negocio
	[E.23]	Errores de mantenimiento	12	Gestión de riesgos
	[N.*]	Desastres naturales	10	Protección de las Instalaciones Plan de Recuperación de Desastres (DRP)
	[A.11]	Acceso no autorizado	10	Control de acceso lógico
	[E.15]	Alteración accidental de la información	12	Control de los accesos físicos
Sistemas de control de tratamiento y distribución (agua)	[N.2]	Daños por agua	15	Plan de Recuperación de Desastres (DRP)
	[N.*]	Desastres naturales	10	Protección de las Instalaciones
Sistemas de control de producción (petróleo y gas)	[I.*]	Desastres industriales	15	Protección de las Instalaciones
	[N.*]	Desastres naturales	10	Plan de Recuperación de Desastres (DRP)
	[A.18]	Destrucción de información	10	Control de los accesos físicos Protección criptográfica del contenido

DISCUSIÓN

El análisis de riesgos mediante la metodología Magerit ha permitido determinar vulnerabilidades significativas en la ciberseguridad de Ecuador. Puntos sensibles incluyen activos informativos esenciales, como datos tributarios y financieros de ciudadanos, así como historias clínicas del sector salud. Estos están expuestos a amenazas, como fugas, alteraciones de datos y accesos no autorizados.

Para asegurar la confidencialidad e integridad de esta información, es imprescindible implementar controles tecnológicos. El cifrado de información, la realización de copias de seguridad y sistemas robustos de identificación y autenticación de usuarios destacan entre las medidas primordiales.

La infraestructura de Tecnologías de Información y Comunicación (TIC) es esencial para el Estado. Un fallo en este sector podría desencadenar repercusiones en servicios públicos y en la seguridad nacional. Así, garantizar la disponibilidad mediante planes de recuperación ante desastres, inversiones estratégicas en ciberseguridad y programas educativos para el personal es vital.

Por ello se requiere un énfasis de amenazas, tanto internas como externas. Internamente, la ingeniería social y errores por parte de los administradores se catalogan entre los riesgos más altos. Esto resalta la imperiosa necesidad de formar y capacitar al personal en ciberseguridad. Externamente, enfrentamos ataques deliberados que demandan una colaboración interinstitucional y regional. Estrategias integrales serán esenciales para combatir estas amenazas. Las evaluaciones periódicas de riesgo son herramientas valiosas. Estas guían las inversiones en ciberseguridad, garantizando que los recursos se dirijan hacia los puntos más vulnerables. En Ecuador, la ciberseguridad debe ser abordada integralmente, considerando tecnología, formación de personal y alianzas entre instituciones, tanto públicas como privadas.

En síntesis, este análisis determina prioridades en ciberseguridad, estableciendo un camino claro para la inversión en controles, políticas y formación de personal. La periodicidad en estas evaluaciones es crucial para una estrategia adaptativa y proactiva ante las amenazas cibernéticas.

CONCLUSIONES

El estado ecuatoriano es un objetivo atractivo para los atacantes debido a su tamaño, su importancia económica y su riqueza en información confidencial. En este contexto, se enfatizó la necesidad de llevar a cabo un análisis exhaustivo de los riesgos y amenazas de ciberseguridad, con el objetivo de robustecer las infraestructuras vitales y garantizar la integridad de la información reservada, contribuyendo así a la consolidación de una gestión gubernamental segura y minimizando posibles vulnerabilidades.

La aplicación del análisis de riesgos mediante la metodología Magerit ha facilitado la categorización y priorización de los riesgos asociados, optimizando la distribución de recursos en los puntos de mayor necesidad, y resultando en una administración más efectiva y económica de los riesgos vinculados a la ciberseguridad.

En consecuencia, se hace imperativo que el Estado ecuatoriano ponga en marcha estrategias concretas para atenuar dichos riesgos y amenazas, incorporando la adopción de soluciones tecnológicas de seguridad, la formación especializada del personal, y la elevación del nivel de consciencia en materia de ciberseguridad.

REFERENCIAS BIBLIOGRÁFICAS

- ACCID. (2019). *Prevención y gestión de riesgos*. Profit Editorial.
- Anaya Moreno, J. A. (01 de 01 de 2021). *repository.unad.edu.co*. Obtenido de [repository.unad.edu.co](https://repository.unad.edu.co/bitstream/handle/10596/41343/jaamayam.pdf?sequence=3&isAllowed=y):
<https://repository.unad.edu.co/bitstream/handle/10596/41343/jaamayam.pdf?sequence=3&isAllowed=y>
- ARTIEDA, V. E. (01 de 05 de 2022). *repositorio.puce.edu.ec*. Obtenido de [repositorio.puce.edu.ec](http://repositorio.puce.edu.ec/bitstream/handle/22000/20370/Hacktivismo%20de%20Anon%20en%20el%20Ecuador.pdf?sequence=1&isAllowed=y):
<http://repositorio.puce.edu.ec/bitstream/handle/22000/20370/Hacktivismo%20de%20Anon%20en%20el%20Ecuador.pdf?sequence=1&isAllowed=y>

- Astrillón, C. O. (2021). PROTECCIÓN DE DATOS EN LA ECONOMÍA DIGITAL UNA APROXIMACIÓN DESDE LA REGULACIÓN DEL COMERCIO INTERNACIONAL. *UCM*, 33-76.
- Carvajal Artieda, V. E. (01 de 05 de 2022). *repositorio.puce.edu.ec*. Obtenido de repositorio.puce.edu.ec:
<http://repositorio.puce.edu.ec/bitstream/handle/22000/20370/Hacktivismo%20de%20Anonymous%20en%20el%20Ecuador.pdf?sequence=1&isAllowed=y>
- Castro, M. I., Morán, G. L., Navarrete, D. S., Cruzatty, J. E., Anzúles, G. R., Mero, C. J., . . . Merino, M. A. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*. Editorial Área de Innovación y Desarrollo, S.L.
- Chang, J. E. (2020). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. *Revista Científica Aristas*, 18-27.
- Gómez, M. A., & Candau, J. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. España: Ministerio de Hacienda y Administraciones Públicas. Obtenido de pilar.ccn-cert.cni.es: <https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file>
- Hurtado, M. (2018). GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT. *Universidad Piloto de Colombia. Hurtado. Metodología de Análisis de Riesgo. 1*, 1-12.
- Llauce Valdera, L. (01 de 01 de 2022). *repositorio.unprg.edu.pe*. Obtenido de repositorio.unprg.edu.pe:
https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/10411/Llauce_Valdera_Luciano.pdf?sequence=1&isAllowed=y
- Luis Almagro. (01 de 01 de 2019). *www.oas.org*. Obtenido de *www.oas.org*:
<https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf>
- Mamoona Humayun, M. N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Revista árabe de ciencia e ingeniería*, 3171-3189.

- Méndez, A. E. (2021). Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano. *Polo del Conocimiento* , 1229-1250.
- Mendivil Caldentey, J., Sanz Urquijo, B., & Gutiérrez Almazor, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. *Revista de Medios y Educación*, 197-225.
- Menéndez Arantes , S. C. (2022). *Auditoría de la Seguridad Informática*. Madrid: RA-MA.
- Project Management Institute. (01 de 01 de 2008). *www.sadamweb.com.ar*. Obtenido de www.sadamweb.com.ar:
https://www.sadamweb.com.ar/news/2016_08Agosto/Guia_Fundamentos_para_la_Direccion_de_Proyectos-4ta_Edicion.pdf?PMBOX=http://www.sadamweb.com.ar/news/2016_08Agosto/Guia_Fundam
dam