ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
CARRERA DE TECNOLOGÍA SUPERIOR EN REDES Y TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR, PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGA SUPERIOR EN REDES Y TELECOMUNICACIONES

Elaboración de un plan de contingencia para la auditoría de los sistemas informáticos del Departamento de TICs del Gobierno Autónomo Descentralizado Municipal Intercultural del cantón Saquisilí (GADMICS)

AUTORA: Rivera Reisancho, Jessica Anabel

DIRECTOR: ING. VITERI ARIAS, CRISTIAN SANTIAGO.

LATACUNGA

2024

ÌNDICE

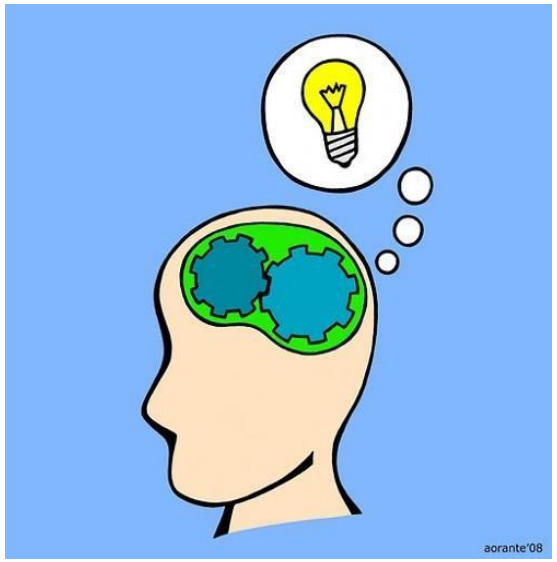
- Antecedentes y planteamiento del problema
- Justificación
- Objetivos generales, específicos
- Alcance
- Marco teórico
- Conclusiones y recomendaciones

Antecedentes

- En los últimos años el aumento significativo en los ataques cibernéticos y las vulnerabilidades de seguridad informática ha puesto en riesgo la información y los sistemas informáticos de las organizaciones.
- La elaboración de un plan de contingencia para la auditoría de los sistemas informáticos del departamento de TICs es fundamental ya que asegura la protección y la continuidad de las operaciones en caso de sufrir incidentes de seguridad informática, además de cumplir con los requisitos de auditoría y regulación de seguridad de la información.

Planteamiento del Problema

- En el 2018 el departamento de TICs del GADMIC Saquisilí ha experimentado una pérdida de información a gran escala debido a la falta de medidas de seguridad adecuadas, lo que resultó en la detención temporal de las actividades de la institución y la insatisfacción entre los usuarios que dependen de los servicios proporcionados por la entidad, a pesar del incidente, en la actualidad no disponen de un plan de contingencia especifico para reducir el riesgo.



Necesidad: Elaboración de un plan de contingencia para la auditoria de los sistemas informáticos del departamento de TICs del Gobierno Autónomo Descentralizado Municipal Intercultural del Cantón Saquisilí (GADMICS)

Justificación

- El GADMICS es una institución que cumple funciones importantes de la planificación y ejecución de proyectos de desarrollo local, lo que la perdida o inaccesibilidad de la información por problemas en los sistemas informáticos pueden afectar el cumplimiento de sus responsabilidades. Por tanto, garantizar la protección de los sistemas informáticos resulta esencial para la continuidad de las operaciones de la institución y la satisfacción de los usuarios.

- Un plan de contingencia para la auditoria de los sistemas informáticos no solo permite afrontar situaciones de emergencia sino también contribuye a mejorar la gestión del riesgo en la organización y a garantizar el cumplimiento de las normativas y reglamentos en materia de seguridad de la información.

OBJETIVOS

GENERAL

Elaborar un plan de contingencia para la auditoria de los sistemas informáticos del departamento de TICs del Gobierno Autónomo Descentralizado Municipal Intercultural del Cantón Saquisilí (GADMICS) con la finalidad de precautelar la información del mismo

ESPECÍFICO

- Identificar y comparar las metodologías de análisis y gestión de riesgos disponibles en el mercado, con el fin de seleccionar la que mejor se adapte a las necesidades del departamento de TICs del GADMICS, para garantizar la protección de su información.
- Identificar los activos críticos del departamento de TICs del GADMICS utilizando la metodología seleccionada para evaluar las amenazas y los riesgos asociados a cada activo.
- Elaboración y entrega del plan de contingencia al departamento de Tics del GADMICS.

Alcance

- El presente proyecto incluye el análisis de las metodologías de gestión de riesgos existentes en el mercado y la selección de la más adecuada para proteger la información del departamento de TIC. Además, se llevará a cabo la identificación de los activos críticos del departamento para una gestión adecuada de las amenazas y riesgos a los que se enfrenta

- La elaboración del plan de contingencia será el resultado final del trabajo, el cual producirá la definición de las acciones y los procedimientos a seguir en situaciones de emergencia o contingencia que puedan surgir en los sistemas informáticos. Dicho plan se entregará en el departamento de TICs para su implementación y seguimiento

- Es importante destacar que este trabajo no abarcara la implementación del plan de contingencia, ni la ejecución de la auditoría de los sistemas informáticos del departamento de TICs

MARCO TEÓRICO

ACTIVOS **AMENAZAS**

Análisis de riesgo

- Es una evaluación sistemática y metodológica de los posibles riesgos asociados con una actividad, proyecto o situación.
- Esta evaluación se realiza mediante la identificación de amenazas potenciales, la estimación de la probabilidad de que ocurran y la evaluación de las posibles consecuencias.

Gestión de riesgo

- Es un proceso integral que abarca la identificación, evaluación, mitigación y monitoreo constante de los riesgos que enfrenta una organización.
- Implica la aplicación de políticas, procedimientos y prácticas diseñadas para minimizar la probabilidad de que ocurran eventos adversos y reducir su impacto en caso de que sucedan

METODOLOGÍA DE ANÁLISIS DE RIESGO

Magerit

- Es una metodología de análisis y gestión de riesgos específicamente diseñada para el ámbito de la seguridad de la información. Se centra en la identificación, evaluación y tratamiento de los riesgos asociados con los activos de información, considerando aspectos de confidencialidad, integridad y disponibilidad.

Octave

- Es una metodología de evaluación de riesgos de seguridad de la información, se enfoca en identificar y mitigar riesgos mediante la evaluación de activos críticos, amenazas y vulnerabilidades, así como en el desarrollo de estrategias de mitigación y gestión de riesgos adaptadas a las necesidades específicas de la organización

Ebios

- Es una metodología francesa para la evaluación y gestión de riesgos de seguridad de la información. Se centra en la identificación de necesidades y objetivos de seguridad, así como en la evaluación de amenazas y vulnerabilidades, para desarrollar medidas de seguridad adaptadas a las particularidades de cada organización.

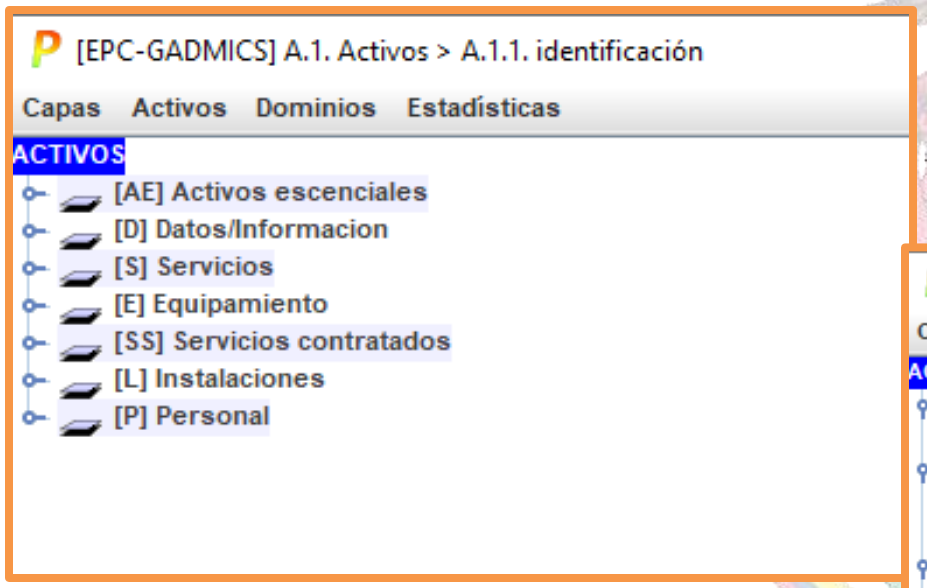
CRITERIO DE SELECCIÓN DE METODOLOGÍA

PARÁMETROS DE EVALUACIÓN	METODOLOGÍAS		
	Magerit	Octave	Ebios
Identificación de activos	✓	✓	✓
Identificación de amenazas	✓	✓	✓
Identificar salvaguardas	✓		
Determinación de la probabilidad	✓	✓	✓
Análisis del impacto	✓	✓	✓
Establecimiento de parámetros	✓		✓
Determinación de riesgo	✓	✓	✓
Estudio cuantitativo	✓		
Estudio cualitativo	✓		

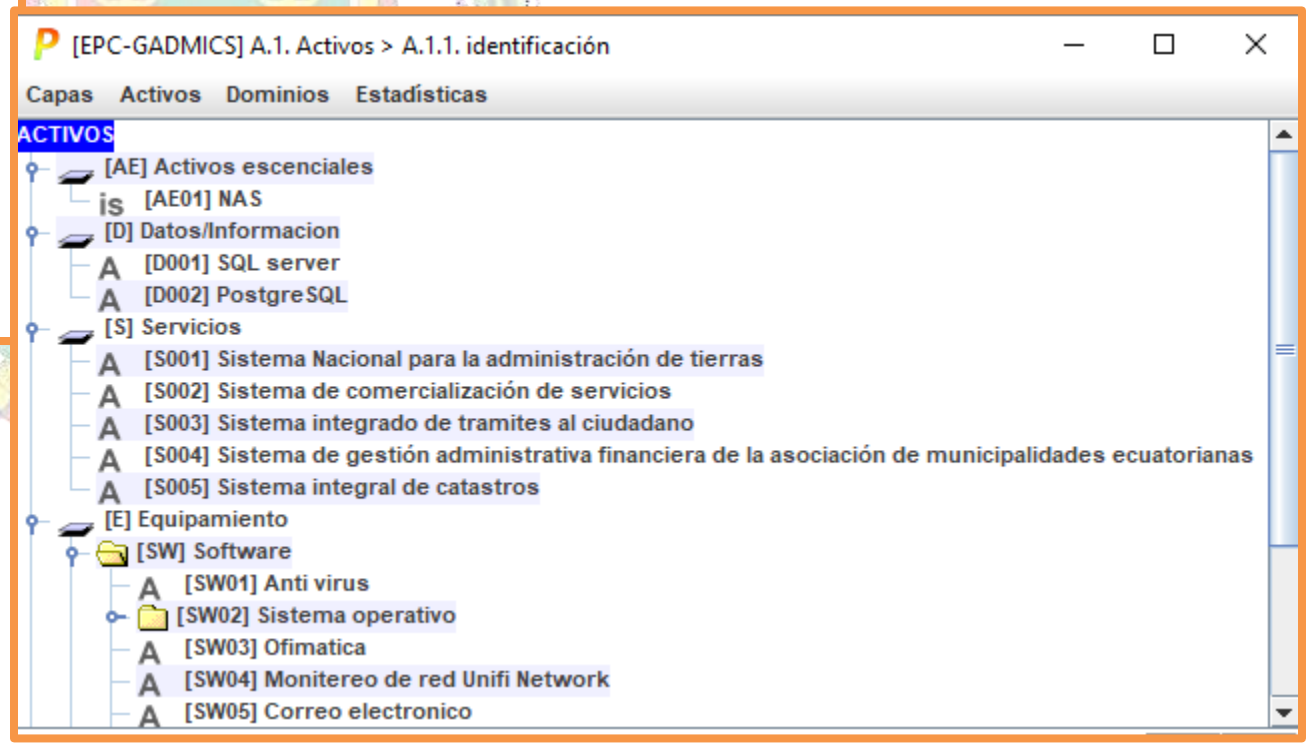
DESARROLLO DEL TEMA

El trabajo de tesis se realizó en el departamento de tecnologías de la información y comunicación (TIC) que depende directamente del Gobierno Autónomo Descentralizado Municipal Intercultural del Cantón Saquisilí (GADMICS) el cual es una institución pública cuyo objetivo principal es el desarrollo social, económico y ambiental de dicho cantón; con tal finalidad ejerce una labor eficiente, transparente y confiable que están sujetas a políticas, estrategias u objetivos de un plan de desarrollo de participación; contribuyendo así a la satisfacción de las necesidades de la comunidad

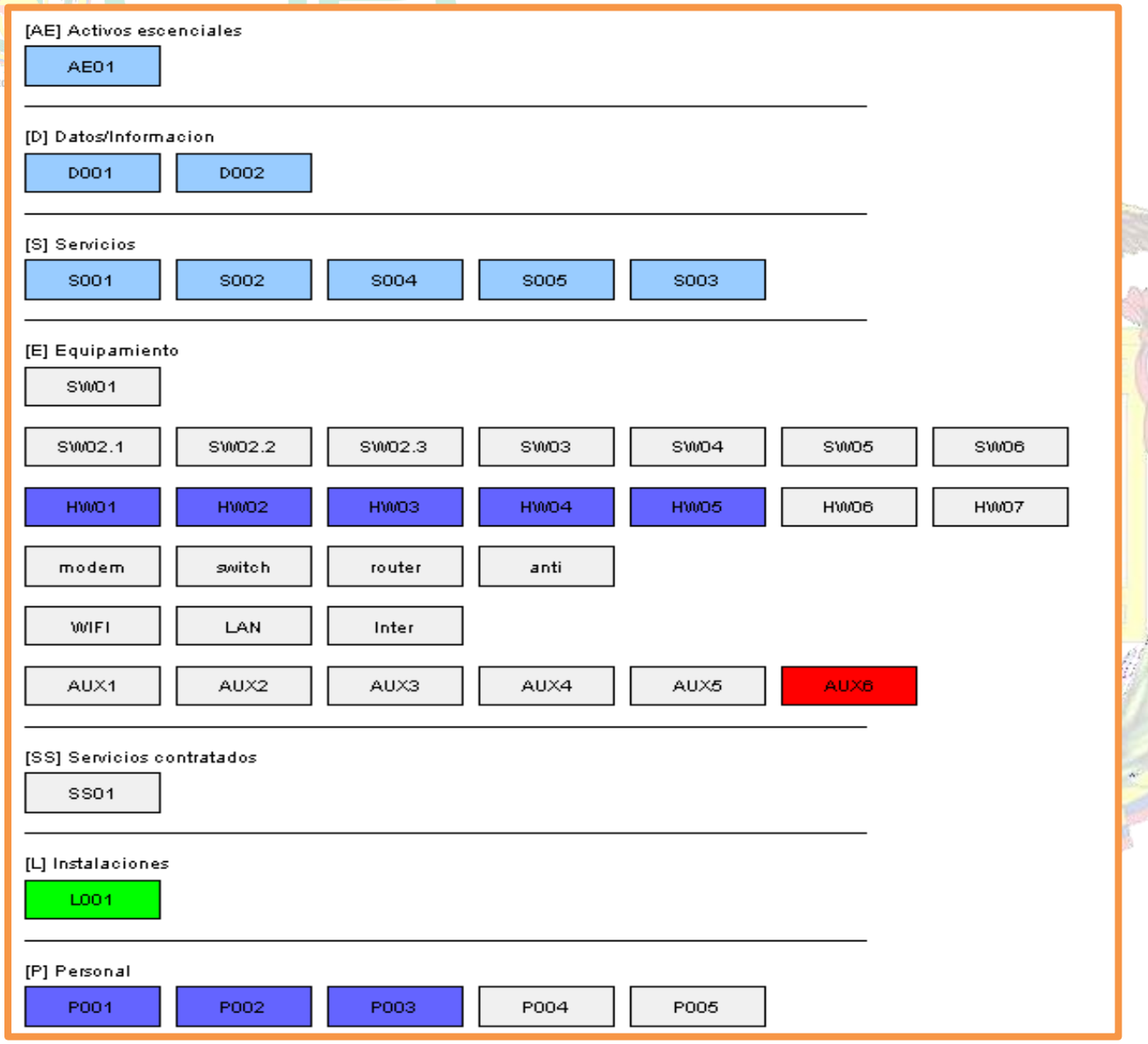
IDENTIFICACIÓN DE LOS ACTIVOS

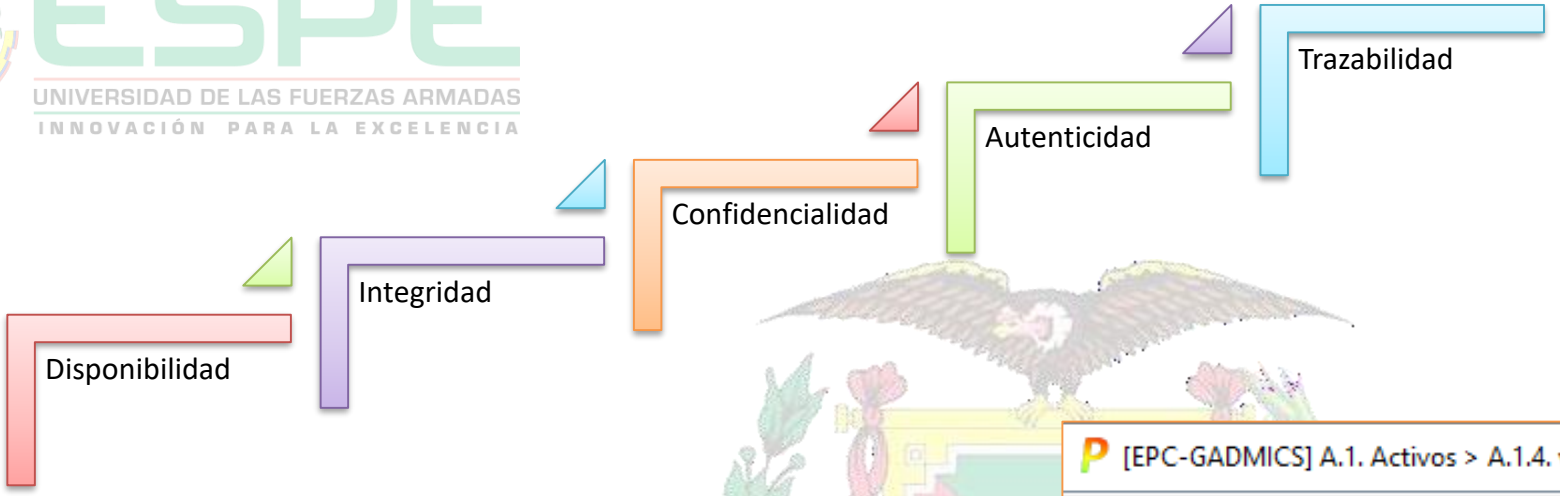


Metodología Magerit clasifica a los activos en las siguientes categorías:



DEPENDENCIA DE LOS ACTIVOS





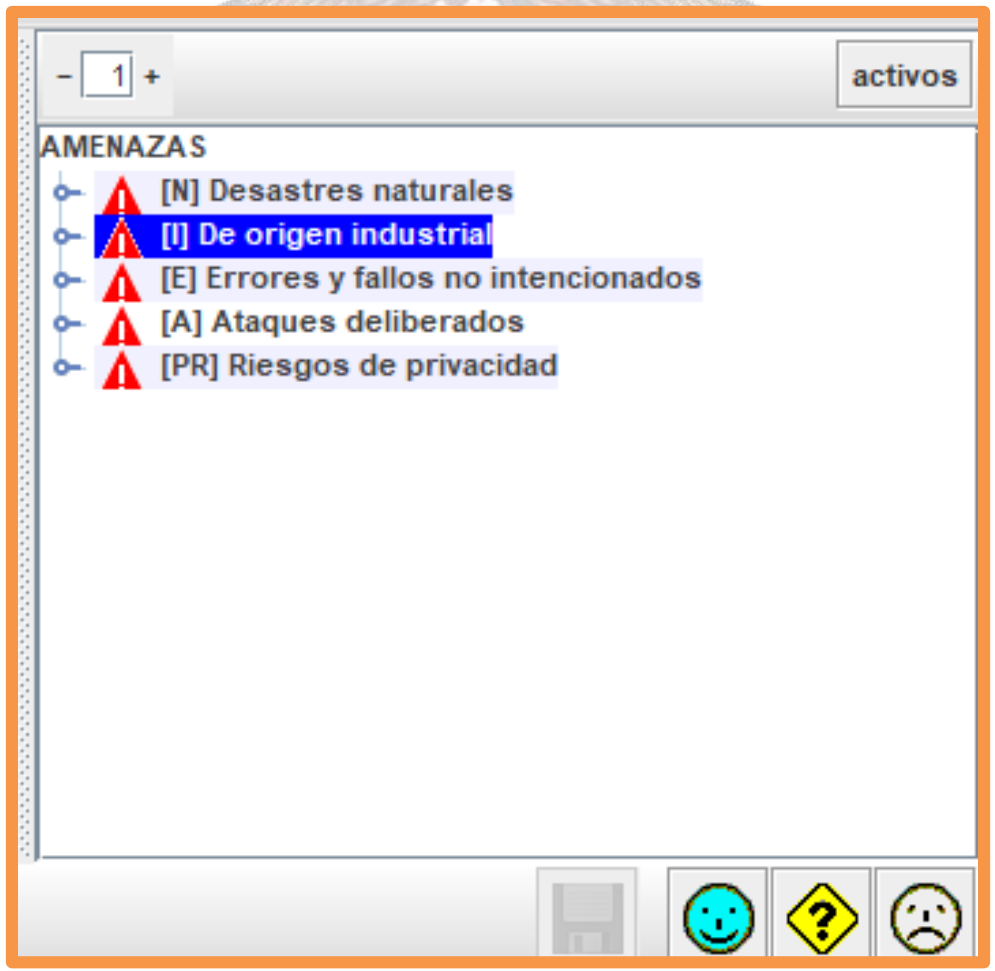
VALORACIÓN DE ACTIVOS

VALOR		CRITERIO
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
8-6	Alto	Daño grave
5-3	Medio	Daño importante
2-1	Bajo	Daño menor
0	Despreciable	Irrelevante

[EPC-GADMICS] A.1. Activos > A.1.4. valoración de los activos

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[AE] Activos escenciales					
[AE01] NAS	[2]	[9]	[7]	[9]	[9]
[D] Datos/Informacion					
[D001] SQL server	[9]	[9]	[9]	[8]	[8]
[D002] PostgreSQL	[9]	[9]	[9]	[9]	[9]
[S] Servicios					
[S001] Sistema Nacional para la administración	[9]	[9]	[9]	[9]	[9]
[S002] Sistema de comercialización de servicios	[9]	[9]	[9]	[9]	[9]
[S003] Sistema integrado de tramites al ciudada	[9]	[9]	[9]	[9]	[9]
[S004] Sistema de gestión administrativa financ	[9]	[9]	[9]	[9]	[9]
[S005] Sistema integral de catastros	[9]	[9]	[9]	[9]	[8]
[E] Equipamiento					
[SW] Software					
[HW] Hardware					
[COM] Comunicaciones					
[AUX] Equipamiento auxiliar					
[SS] Servicios contratados					
[L] Instalaciones					

AMENAZAS


1
activos
AMENAZAS
[N] Desastres naturales
[I] De origen industrial
[E] Errores y fallos no intencionados
[A] Ataques deliberados
[PR] Riesgos de privacidad

Nivel	Criterio
CS	Casi seguro
MA	Muy alta
P	Posible
PP	Poco posible
MR	Muy rara

Nivel		Porcentaje
T	Total	100%
MA	Muy alta	90%
A	Alta	50%
M	Media	10%
B	Baja	1%

VALORACIÓN DE LAS AMENAZAS

activo		co...	prob...	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS										
[AE] Activos escenciales										
[AE01] NAS				A	A	A	T			
[I.5] Avería de origen físico o lóg			P	A						
[E.1] Errores de los usuarios			PP	M	M	M				
[E.2] Errores del administrador (			PP	M	M	M				
[E.15] Alteración de la informaci			MR		M					
[E.18] Destrucción de la informa			P	M						
[E.19] Fugas de información			P			M				
[A.5] Suplantación de la identida			P		A	A	T			
[A.6] Abuso de privilegios de ac			P	B	M	M	T			
[A.7] Uso no previsto			PP	M	M	M				
[A.11] Acceso no autorizado			PP		M	A	T			
[A.15] Modificación de la informa			MR		A					
[A.18] Destrucción de la informa			P	A						
[A.19] Revelación de informació			P			A				
[D] Datos/Informacion										
[D001] SQL server				T	T	T				

ESTADO DE RIESGO

IMPACTO POTENCIAL

Es una medida de la gravedad de las consecuencias que podrían derivarse de la materialización de una amenaza sobre un activo

RIESGO POTENCIAL

El riesgo se calcula al multiplicar la probabilidad de una amenaza por el impacto potencial en el activo afectado, mientras más alto el impacto y la probabilidad el riesgo es mayor

SALVAGUARDAS

Tipos de protección
Prevención
Disuasión
Eliminación
Minimización del impacto
Corrección
Recuperación
Administrativa
Concienciación
Detección
Monitorización

Factor	Nivel	Significado
0%	L0	Inexistente
10%	L1	Iniciado
30%	L2	Reproducible, pero no intuitivo
50%	L3	Proceso definido
75%	L4	Gestionado y medible
100%	L5	Optimizado

IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS

- [G] Gestión de la seguridad
- [T] Naturaleza técnica
- [F] Aspectos físicos de seguridad
- [P] Gestión del factor humano

[base] Base | Fuentes de información

	asp...	tdp	rec...		salvaguarda	dudas	fuente	aplica	com...	curr...	target	PILAR
					SALVAGUARDAS					L3-L4	L3-L5	L2-L5
	G	EL	8		[IA] Identificación y autenticación					L4	L5	L2-L5
	T	EL	7		[AC] Control de acceso lógico					L3	L4	L2-L4
	G	PR	6		[D] Protección de la Información					L3	L4	L2-L4
	G	EL			[K] Protección de claves criptográficas					n.a.	n.a.	n.a.
	G	PR	6		[S] Protección de los Servicios					L3	L4	L2-L4
	G	PR	7		[SW] Protección de las Aplicaciones Informáticas (SW)					L3	L4	L2-L4
	G	PR	7		[HW] Protección de los Equipos Informáticos (HW)					L3	L4	L2-L4
	G	PR	8		[COM] Protección de las Comunicaciones					L4	L5	L2-L5
	G	PR			[IP] Sistema de protección de frontera lógica					n.a.	n.a.	n.a.
	G	PR			[MP] Protección de los Soportes de Información					n.a.	n.a.	n.a.
	G	PR	6		[AUX] Elementos Auxiliares					L3	L4	L2-L4
	F	EL	6		[PPE] Protección física de los equipos					L4	L4	L4
	F	PR	7		[L] Protección de las Instalaciones					L3	L4	L2-L4
	F	EL			[PPS] Protección del perímetro físico					n.a.	n.a.	n.a.
	P	PR	6		[PS] Gestión del Personal					L4	L4	L2-L4
	G	PR			[PDS] Servicios potencialmente peligrosos					n.a.	n.a.	n.a.
	G	CR	6		[IR] Gestión de incidentes					L3	L4	L2-L4

GESTIÓN DE RIESGO

Los riesgos críticos son aquellos que aún representan un alto nivel de riesgo después de haber aplicado todas las medidas de seguridad posibles


1922

Conclusiones

- Se ha realizado una investigación exhaustiva para identificar y comparar las metodologías de análisis y gestión de riesgos disponibles en el mercado. Como resultado, se ha seleccionado la metodología MAGERIT que se adapta a las necesidades específicas del departamento de TICs del GADMICS, lo que garantizará una adecuada protección de su información.

- Mediante la aplicación de PILAR de la metodología MAGERIT, se ha logrado identificar de manera precisa y detallada los activos críticos del departamento de TICs del GADMICS, así como las amenazas y riesgos asociados a cada uno de ellos. Esto proporciona una visión clara de los posibles escenarios de riesgo que pueden afectar la seguridad de la información.

- Se ha elaborado un plan de contingencia completo y detallado que incluye estrategias y controles para mitigar los riesgos identificados. El plan de contingencia proporciona un marco sólido para responder eficazmente a incidentes de seguridad informática y garantizar la continuidad de las operaciones del departamento de TICs del GADMICS en caso de emergencias.

Recomendaciones

- Mantenimiento y Actualización Continua: Es fundamental que el plan de contingencia se mantenga actualizado y se revise de manera periódica para asegurar que refleje los cambios en la infraestructura tecnológica y las nuevas amenazas de seguridad. Asignar responsabilidades claras para la revisión y actualización del plan garantizará su efectividad a lo largo del tiempo.

- Capacitación y Concientización: Es importante llevar a cabo programas de capacitación y concientización periódicos para el personal del departamento de TICs, así como para otros usuarios de los sistemas informáticos. Esto asegurará que todos estén familiarizados con el plan de contingencia y sepan cómo actuar en caso de un incidente de seguridad.

- Respuesta a Incidentes: Establecer un equipo de respuesta a incidentes bien entrenado y coordinado para asegurar una acción rápida y efectiva en caso de que ocurra algún incidente. Definir roles y responsabilidades claras para cada miembro del equipo facilitará una respuesta eficiente.

Gracias por su atención