La Infraestructura de Datos Espaciales (IDE) de la Dirección General Marítima

CC Eduardo Fabre Cujar
My Luis Latorre Jacome
My Dolman López Zapata

Escuela Superior de Guerra “General Rafael Reyes Prieto”
Curso de Estado Mayor - CEM 2025
Gestión de Riesgos Cibernéticos
Jaider Ospina Navas
28 de febrero de 2025

La Infraestructura de Datos Espaciales (IDE) de Dimar

La Infraestructura de Datos Espaciales (IDE) de Dimar es un sistema que integra información y productos temáticos de la actividad marítima de Colombia.

Características de la IDE de Dimar

- Integra información y productos temáticos de la actividad marítima del país
- Pone a disposición de la comunidad aplicaciones web geográficas de fácil consulta
- Facilita la consulta y conocimiento sobre las actividades, recursos y servicios de los mares y costas
- Apoya la investigación científica marina y la protección de la vida humana en el mar

Qué es una IDE

Una IDE es un sistema virtual que integra datos, metadatos, tecnologías, políticas, estándares, recursos humanos y usuarios. Su objetivo es compartir información geográfica en la red.

Componentes de una IDE

Los componentes de una IDE son: Datos espaciales, Servicios, Metadatos.

Estos componentes se ordenan y estructuran mediante estándares, reglas y un marco normativo.

Descripción del escenario

La IDE de DIMAR integra información y productos temáticos sobre la actividad marítima en Colombia, facilitando aplicaciones web geográficas para la consulta de datos sobre mares y costas. Los componentes clave de la IDE incluyen datos espaciales, servicios y metadatos, organizados bajo estándares y políticas. El sistema Zabbix, que supervisa esta infraestructura, consta de un servidor central, agentes, una base de datos y un frontend web, con acceso diferenciado para administradores y usuarios limitados.

La IDE de DIMAR es un sistema integral que permite:

- **Integración de Datos:** Combina datos geoespaciales, metadatos y servicios de la actividad marítima.
- **Accesibilidad:** Proporciona aplicaciones web geográficas para la consulta de información, facilitando el acceso a la comunidad, investigadores y autoridades.
- **Soporte a la Investigación:** Fomenta la investigación científica en el ámbito marino y contribuye a la protección de la vida humana en el mar.

Componentes Clave de la IDE

1. **Datos Espaciales:** Información geográfica que se utiliza para mapear y analizar la actividad marítima.
2. **Servicios:** Aplicaciones y APIs que permiten la interacción con los datos espaciales.
3. **Metadatos:** Información descriptiva sobre los datos, que facilita su búsqueda y utilización.

Sistema Zabbix

El sistema Zabbix se encarga de la supervisión de la infraestructura de la IDE. Sus componentes son:

- **Servidor Central:** Responsable de almacenar datos y realizar el procesamiento.
- **Agentes:** Instalados en diferentes dispositivos para recoger y enviar información al servidor.
- **Base de Datos:** Donde se almacenan las métricas recolectadas y la configuración del sistema.
- **Frontend Web:** Interfaz mediante la cual los usuarios interactúan con el sistema.

Análisis de riesgos

El análisis de riesgos es un componente crítico en la ciberseguridad, ya que permite identificar, evaluar y priorizar las amenazas que pueden afectar la Infraestructura de Datos Espaciales (IDE) de DIMAR. A continuación, se presenta un análisis detallado de cada amenaza identificada en el contexto del modelo STRIDE, junto con su probabilidad de ocurrencia, impacto potencial y medidas de mitigación específicas.

A continuación, se detallan las amenazas potenciales clasificadas según el modelo STRIDE:

1. **Spoofing:**

- **Descripción:** Suplantación de identidad de usuarios administradores o de servicios esenciales.
- **Ejemplo de Amenaza:** Un atacante envía correos electrónicos de phishing para obtener credenciales de acceso de un administrador de la IDE.

2. **Tampering:**

- **Descripción:** Manipulación de datos o configuraciones que puede afectar la integridad del sistema.
- **Ejemplo de Amenaza:** Un atacante accede al servidor Zabbix y modifica configuraciones críticas, afectando la supervisión de la infraestructura.

3. **Repudiation:**

- **Descripción:** Un usuario puede negar haber realizado ciertas acciones en el sistema.
- **Ejemplo de Amenaza:** Un empleado modifica datos y luego niega haberlo hecho, dificultando la investigación de incidentes.

4. **Information Disclosure:**

- **Descripción:** Fugas de información confidencial o sensible.
- **Ejemplo de Amenaza:** Un atacante explota una vulnerabilidad en el frontend web para acceder a metadatos sensibles de la IDE.

5. **Denial of Service (DoS):**

- **Descripción:** Ataques que buscan hacer que los servicios sean indisponibles.
- **Ejemplo de Amenaza:** Un ataque DDoS que colapsa el servidor Zabbix, impidiendo la monitorización de la infraestructura.

6. **Elevation of Privilege:**

- **Descripción:** Un usuario con acceso restringido logra obtener mayores privilegios.
- **Ejemplo de Amenaza:** Un usuario con permisos limitados explota una vulnerabilidad en el sistema para obtener acceso administrativo.

Para la evaluación de amenazas se tomaron los 6 componentes de la Infraestructura de Datos Espaciales de DIMAR: 1. Marina Mercante, 2. Investigación Científica Marina, 3. Señalización Marítima, 4. Litorales y Áreas Marítimas, 5. Servicio Meteorológico marino, 6. Servicio Hidrográfico.

Área de Servicio	Amenaza	Probabilidad (%)	Impacto	Justificación de la Evaluación
1. Marina Mercante	Spoofing	70	8	Alta exposición a ataques de phishing dirigidos a usuarios.
	Tampering	60	7	Posibilidad de modificación de datos críticos como registros.
	Repudiation	50	6	Riesgo de negación de acciones en la gestión de datos.

	Information Disclosure	80	9	Datos sensibles sobre operaciones comerciales pueden ser expuestos.
	Denial of Service (DoS)	75	8	Ataques DDoS pueden afectar la disponibilidad del servicio.
	Elevation of Privilege	50	7	Vulnerabilidades pueden ser explotadas para escalar privilegios.
2. Investigación Científica Marina	Spoofing	60	7	Riesgo de suplantación en el acceso a datos de investigación.
	Tampering	50	7	Manipulación de datos de investigación podría afectar resultados.
	Repudiation	40	5	Dificultad para rastrear cambios en datos de investigaciones.
	Information Disclosure	70	8	Fuga de información confidencial sobre investigaciones.
	Denial of Service (DoS)	65	7	Interrupciones pueden afectar proyectos en curso.
	Elevation of Privilege	40	6	Posibilidad de acceso no autorizado a datos críticos.
3. Señalización Marítima	Spoofing	65	8	Ataques de phishing pueden comprometer sistemas de señalización.
	Tampering	55	7	Alteraciones en la señalización pueden causar accidentes.
	Repudiation	45	5	Dificultad para rastrear cambios en el sistema de señalización.
	Information Disclosure	60	7	Exposición de información sobre puntos críticos de señalización.
	Denial of Service (DoS)	70	8	Ataques DDoS pueden afectar la operación de sistemas de señalización.
	Elevation of Privilege	45	6	Posibilidad de escalada en acceso a sistemas de señalización.

4. Litorales y Áreas Marítimas	Spoofing	60	7	Riesgo de suplantación en acceso a datos sobre litorales.
	Tampering	50	6	Manipulación de datos sobre áreas marítimas puede ser crítica.
	Repudiation	40	5	Dificultad para rastrear acciones en la gestión de litorales.
	Information Disclosure	65	7	Fugas de información sobre recursos marinos pueden ocurrir.
	Denial of Service (DoS)	60	8	Interrupciones pueden afectar la gestión de recursos.
	Elevation of Privilege	40	6	Vulnerabilidades pueden ser explotadas en el acceso a datos.
5. Servicio Meteorológico Marino	Spoofing	70	7	Alta exposición a phishing dirigido a usuarios de datos meteorológicos.
	Tampering	60	8	Alteraciones en reportes meteorológicos pueden tener graves consecuencias.
	Repudiation	50	5	Dificultad para rastrear cambios en datos meteorológicos.
	Information Disclosure	75	8	Fuga de información meteorológica sensible puede ser crítica.
	Denial of Service (DoS)	70	8	Ataques DDoS pueden afectar la disponibilidad de servicios críticos.
	Elevation of Privilege	45	7	Posibilidad de acceso no autorizado a información meteorológica.
6. Servicio Hidrográfico	Spoofing	65	8	Riesgo de suplantación en acceso a datos hidrográficos.
	Tampering	55	7	Manipulación de datos hidrográficos puede afectar la navegación.
	Repudiation	45	5	Dificultad para rastrear cambios en datos hidrográficos.

	Information Disclosure	70	8	Fuga de información sensible sobre recursos hidrográficos.
	Denial of Service (DoS)	65	8	Interrupciones pueden afectar la navegación y operaciones.
	Elevation of Privilege	40	6	Vulnerabilidades pueden ser explotadas en acceso a datos hidrológicos.

MATRIZ DE RIESGO

La Infraestructura de Datos Espaciales (IDE) de Dimar usando STRIDE

Área de Servicio	**Probabilidad General (%)**	**Impacto Promedio (1-10)**	**Nivel de Riesgo (1-100)**	**Justificación de la Evaluación**
1. Marina Mercante	70	7.5	52.5	Alta exposición a amenazas cibernéticas, especialmente spoofing e información sensible.
2. Investigación Científica Marina	60	7	42	Riesgo moderado de suplantación y divulgación de información confidencial.
3. Señalización Marítima	65	7	45.5	Riesgo de spoofing y DoS que pueden comprometer la seguridad de la navegación.
4. Litorales y Áreas Marítimas	60	7	42	Amenazas de spoofing e información sensible sobre recursos marinos.
5. Servicio Meteorológico Marino	70	7.5	52.5	Alta probabilidad de divulgación de información sensible y ataques DDoS.
6. Servicio Hidrográfico	65	7	45.5	Riesgo de suplantación y manipulación de datos que afectan la navegación.

Selección y análisis para determinar las medidas de mitigación:

Amenaza	Descripción	Ejemplo de Amenaza	Probabilidad	Impacto	Medidas de Mitigación
Spoofing	Suplantación de identidad mediante engaño de credenciales.	Ataque de phishing para obtener credenciales de un administrador.	Alta	Alto	Autenticación de dos factores (2FA). - Capacitación sobre identificación de phishing. - Uso de autenticación robusta.
Tampering	Manipulación no autorizada de datos o configuraciones.	Modificación de configuraciones en el servidor Zabbix.	Media	Alto	- Controles de acceso estrictos. - Auditorías de configuración. - Monitoreo de integridad de archivos.
Repudiation	Negación de acciones realizadas en el sistema por el usuario.	Un empleado niega haber modificado datos críticos.	Media	Medio	- Implementar auditorías de acciones. - Políticas claras sobre el uso del sistema. - Formación sobre la integridad de datos.

Amenaza	Descripción	Ejemplo de Amenaza	Probabilidad	Impacto	Medidas de Mitigación
Information Disclosure	Fugas de información confidencial o sensible.	Acceso a metadatos sensibles a través de una vulnerabilidad.	Alta	Alto	- Cifrado de datos en reposo y en tránsito. - Pruebas de penetración regulares. - Políticas de acceso restringido.
Denial of Service (DoS)	Ataques que buscan hacer un servicio inaccesible.	Ataque DDoS que afecta el servidor Zabbix.	Alta	Alto	- Soluciones de mitigación de DDoS. - Plan de respuesta ante incidentes. - Uso de CDN para absorber tráfico.
Elevation of Privilege	Escalada de privilegios de un usuario restringido a uno con mayores permisos.	Un usuario explota una vulnerabilidad para obtener acceso administrativo.	Media	Alto	- Revisión periódica de privilegios. - Pruebas de seguridad de aplicaciones. - Principio de privilegio mínimo.

Aplicación modelo DREAD con el fin de prevenir posibles errores derivados de prejuicios o simplificaciones. Se propone utilizar el modelado DREAD, que se centra en cuantificar las categorías de Daño, Reproducibilidad, Explotabilidad, Usuarios Afectados y Descubrimiento, utilizando parámetros de calificación establecidos.

Área de Servicio	Daño (Promedio)	Reproducibilidad (Promedio)	Explotabilidad (Promedio)	Usuarios Afectados (Promedio)	Descubrimiento (Promedio)	Puntaje Total Promedio (DREAD)
1.Marina Mercante	7.33	6.33	5.67	6.67	5.67	31.67
2.Investigación Científica Marina	6.33	5.33	4.67	5.00	4.67	26.00
3. Señalización Marítima	7.00	6.00	5.33	6.00	5.50	29.17
4. Litorales y Áreas Marítimas	6.00	5.00	4.67	5.00	4.67	25.33
5. Servicio Meteorológico Marino	8.33	6.00	6.00	7.50	5.33	33.17
6. Servicio Hidrográfico	6.67	5.50	5.00	6.00	5.00	28.17

Diseño de controles de seguridad

Controles Técnicos

- **Firewall:** Configurar firewalls para restringir el acceso a los componentes críticos de la IDE y Zabbix. Esto incluye reglas específicas para limitar el acceso a direcciones IP autorizadas.
- **IDS/IPS:** Implementar un sistema de detección y prevención de intrusiones para monitorear el tráfico de red y detectar actividades sospechosas en tiempo real.
- **Autenticación de Dos Factores (2FA):** Implementar 2FA para accesos administrativos, añadiendo una capa adicional de seguridad que requiere un segundo método de verificación.
- **Cifrado de Datos:** Utilizar cifrado para proteger datos sensibles, tanto en reposo como en tránsito, asegurando que la información no sea accesible en caso de interceptación.

Controles Administrativos

- **Políticas de Seguridad:** Definir y documentar políticas de seguridad que incluyan protocolos de acceso, uso de contraseñas y manejo de incidentes.
- **Gestión de Acceso:** Realizar auditorías periódicas de permisos y accesos para asegurar que solo el personal autorizado tenga acceso a información y sistemas críticos.
- **Capacitación del Personal:** Implementar programas de capacitación en ciberseguridad para todos los empleados, enfatizando las mejores prácticas para la protección de datos y la detección de fraudes.

Controles Físicos

- **Seguridad Física:** Asegurar que los servidores y dispositivos de red estén ubicados en áreas con acceso restringido, controladas por sistemas de seguridad física.
- **Control de Acceso Físico:** Utilizar sistemas de control de acceso, como tarjetas magnéticas o biometría, para limitar el acceso a los servidores.

Diseño de Diagrama de Seguridad Multicapa

1. Capa de Perímetro
    - Firewalls: Monitoreo y control del tráfico entrante y saliente.
    - Sistemas de Detección de Intrusos (IDS): Identificación de posibles amenazas y ataques.
2. Capa de Red
    - Segregación de Redes: Dividir la red en segmentos para limitar el acceso.
    - VPNs: Proporcionar acceso seguro a la red para usuarios remotos.
3. Capa de Aplicación
    - Protección de Aplicaciones Web (WAF): Filtrar y monitorear el tráfico HTTP para proteger aplicaciones.
    - Autenticación y Autorización: Implementar controles de acceso robustos.
4. Capa de Datos
    - Cifrado de Datos: Proteger la información tanto en reposo como en tránsito.
    - Clasificación de Datos: Identificar y clasificar datos sensibles para su manejo adecuado.
5. Capa de Monitoreo y Respuesta
    - SIEM (Security Information and Event Management): Recopilación y análisis de registros de seguridad.

- Planes de Respuesta a Incidentes: Establecer procedimientos para responder a incidentes de seguridad.

6. Capa de Concienciación y Formación
    - Capacitación de Empleados: Programas de formación en ciberseguridad para todo el personal.
    - Simulaciones de Ataques: Ejercicios para entrenar a los empleados en la identificación de amenazas.

Matriz RACI para el Análisis de Riesgos Cibernéticos la Infraestructura de Datos Espaciales (IDE) de la Dirección General Marítima (DIMAR)

Actividad / Rol	Equipo de Análisis de Riesgos	Junta Directiva	Personal de TI	Personal de Seguridad	Empleados
Identificación de Riesgos	R	A	C	C	I
Evaluación de Riesgos	R	A	C	C	I
Implementación de Medidas de Seguridad	C	I	R	R	I
Monitoreo de Seguridad	C	I	R	R	I
Capacitación en Ciberseguridad	C	I	C	R	R
Revisión de Políticas de Seguridad	C	A	C	R	I
Respuesta a Incidentes	C	I	R	R	I
Reporte de Incidentes	C	I	R	R	I

Evaluación de las Medidas de Mitigación

Efectividad

Las medidas propuestas están diseñadas para mitigar las amenazas identificadas y mejorar la postura de seguridad general de la IDE de DIMAR. Por ejemplo, la implementación de 2FA puede reducir significativamente el riesgo de suplantación de identidad.

Impacto

Las medidas de mitigación impactan positivamente en la disponibilidad, integridad y confidencialidad de los datos al crear barreras efectivas contra accesos no autorizados y manipulaciones.

Costo

El costo de implementación de estas medidas puede variar, pero la inversión se justifica al considerar el potencial costo de un incidente de seguridad, que puede incluir la pérdida de datos, daños a la reputación y sanciones legales.

Métricas de Evaluación

- **Completitud:** Se han identificado las amenazas más relevantes, pero es crucial realizar revisiones periódicas para abordar nuevas vulnerabilidades.
- **Precisión:** Las amenazas identificadas son pertinentes y reflejan riesgos reales para la IDE y el sistema Zabbix.
- **Viabilidad:** Las medidas de mitigación son viables y factibles, considerando los recursos disponibles.
- **Costo-beneficio:** Las medidas proporcionan un retorno de inversión adecuado al reducir el riesgo de incidentes costosos.
- **Claridad y Organización:** El informe está estructurado de manera clara y lógica, facilitando la comprensión de las amenazas y las soluciones propuestas.

Conclusiones y Recomendaciones

La implementación del modelo STRIDE ha permitido identificar amenazas significativas para la Infraestructura de Datos Espaciales de DIMAR. Se recomienda:

1. **Implementar las Medidas Propuestas:** Adoptar las medidas de mitigación identificadas, priorizando aquellas con mayor impacto y probabilidad.
2. **Auditorías y Revisión Continua:** Realizar auditorías de seguridad periódicas para evaluar la efectividad de las medidas y ajustar las políticas según sea necesario.
3. **Capacitación Continua:** Mantener programas de capacitación en ciberseguridad para todo el personal, asegurando que estén al tanto de las mejores prácticas y amenazas emergentes.
4. **Colaboración con Expertos:** Considerar la colaboración con expertos en ciberseguridad para evaluar la infraestructura y proporcionar asesoramiento adicional.

Bibliografía

- Cisco. (2022). *Mejores prácticas de arquitectura de seguridad de red*. Documentos técnicos de seguridad de Cisco.
- ISO/IEC 27001:2022. *Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos*. Organización Internacional de Normalización.
- Microsoft. (2022). *Modelado de amenazas STRIDE: identificación y mitigación de amenazas de seguridad*. Blog de seguridad de Microsoft. Recuperado de https://www.microsoft.com/security/blog
- MITRE. (s.f.). *MITRE ATT&CK framework*. MITRE. https://attack.mitre.org/
- NIST. (2021). *Marco para mejorar la ciberseguridad de infraestructuras críticas (versión 1.1)*. Instituto Nacional de Estándares y Tecnología (NIST). Recuperado de https://www.nist.gov/cyberframework
- OpenAI. (2025, 18 de febrero). *Respuesta generada por ChatGPT* [Modelo de lenguaje de IA]. OpenAI. Disponible en https://chat.openai.com
- Threat-Modeling.com. (2025). *DREAD Threat Modeling*. https://threat-modeling.com/dread-threat-modeling/