GESTIÓN DEL RIESGO EN SISTEMAS DE INFORMACIÓN GEOGRÁFICA

Vanegas Ardila Cristian Camilo
Universidad Piloto de Colombia
Bogotá D.C., Colombia

***Resumen*—** Este documento pretende presentar los componentes de gestión del riesgo y determinar los pasos para la identificación de amenazas y vulnerabilidades en sistemas de información geográfica. Se definirán términos y aspectos que componen los sistemas de información geográfica, y a su vez se contextualizarán los términos de riesgo, vulnerabilidad e impacto. Se tomará como base la norma ISO 27001:2013 con el fin de comparar vulnerabilidades contra amenazas realizando un análisis de riesgos, y de esta manera proponer algunos controles de riesgos para los sistemas de información geográfica.

***Abstract*—** This document aims to present the components of risk management and determine the steps for the identification of threats and vulnerabilities in geographic information systems. Terms and aspects that make up geographic information systems will be defined, and the terms of risk, vulnerability and impact will be contextualized. It will be based on the ISO 27001: 2013 standard in order to compare vulnerabilities against threats by performing a risk analysis, and thus propose some risk controls for the geographic information systems.

***Índice de Términos*—** *A*menaza, GIS, impacto, riesgo, SIG, vulnerabilidad.

I. INTRODUCCIÓN

El presente documento tiene como fin dar a conocer las debilidades que presentan los sistemas de información geográfica (SIG) y las amenazas a las que se encuentran expuestos estos sistemas. Los sistemas de información geográfica han ganado popularidad con el paso del tiempo hasta la actualidad, y a su vez han ganado gran importancia en la sociedad, especialmente en los ámbitos donde se requiere el manejo de datos geográficos. Un SIG es definido como el conjunto de hardware, software, datos, recursos humanos y metodologías para el almacenamiento, análisis, transformación y presentación de determinada información geográfica y sus atributos. La implementación de un SIG debe contemplar medidas de seguridad que protejan los datos contra cualquier situación de riesgo. El presente artículo pretende analizar cómo se encuentra el entorno de gestión de riesgo de un SIG hoy en día y que tipos de vulnerabilidades existen frente a estos sistemas.

II. SISTEMAS DE INFORMACIÓN GEOGRÁFICA (SIG)

Un SIG se define como un conjunto de métodos, hardware, software, herramientas y datos geográficos que están diseñados coordinada y lógicamente en la captura, almacenamiento, análisis, manipulación, transformación y presentación de toda la información geográficamente referenciada junto con sus atributos, con el fin de satisfacer múltiples propósitos como por ejemplo, resolver problemas complejos de planificación y de gestión.

Un SIG funciona como una base de datos con información geográfica (datos alfanuméricos) que se encuentra asociada por un identificador común a los objetos gráficos de un mapa digital. De esta forma, señalando un objeto se conocen sus atributos e inversamente, preguntando por un registro de la base de datos se puede saber su localización a nivel cartográfico.

Existen principalmente dos tipos de sistemas de información geográfica:

A. Modelo vectorial

Lleva a cabo la representación de los datos por medio de los elementos bien definidos como son los puntos, las líneas o los polígonos; éstos se encuentran representados en el SIG por medio de coordenadas UTM (Universal Transversal Mercator), tratándose

de estas coordenadas las representadas en un eje cartesiano (x/y).

B. Modelo Raster

Se caracteriza porque la representación de la información no se realiza por medio de puntos, líneas o polígonos, sino por celdillas o píxeles.

III. COMPONENTES DE UN SIG

Un SIG integra cinco componentes principales, los cuales se describen a continuación:

A. Hardware

El hardware es el computador donde opera el SIG. Hoy en día, los SIG se pueden ejecutar en una gran variedad de plataformas, las cuales pueden variar desde servidores (computador central) hasta computadores desktop (escritorio) o laptop (portátil) que se utilizan en las configuraciones de red o sin conexión.

B. Software

Los programas de SIG proveen las funciones y las herramientas que se requieren para almacenar, analizar y desplegar información geográfica. Los componentes más importantes son:

-Herramientas para la entrada y manipulación de la información geográfica.

-Un sistema de administración de base de datos.

-Herramientas que permitan búsquedas geográficas, análisis y visualización.

-Interfaz gráfica de usuario para que pueda acceder fácilmente a las herramientas.

C. Datos

Se puede decir que posiblemente los componentes más importantes de un SIG son los datos. Los datos geográficos y tabulares relacionados pueden ser recolectados en la empresa, en terreno o bien adquirirlos a quien implementa el sistema de información, así como a terceros que ya los tienen disponibles. El SIG integra los datos espaciales con otros recursos de datos y puede incluso utilizar los administradores de base de datos más comunes para organizar, mantener y manejar los datos espaciales y toda la información geográfica.

D. Recurso humano

La tecnología SIG está limitada si no se cuenta con el personal adecuado que opere, desarrolle y administre el sistema, y llevar a cabo los planes de desarrollo para aplicarlos a los problemas del mundo real. Entre los usuarios de SIG se encuentran los especialistas técnicos, que diseñan y mantienen el sistema para aquellos que los utilizan diariamente en sus labores.

E. Metodología y procedimientos

Para que un SIG tenga éxito, este debe operar de acuerdo a un plan bien diseñado, estructurado y acorde con las reglas de la empresa o institución, ya que son los modelos y prácticas operativas características de cada organización.

F. Vulnerabilidades de los SIG

El posicionamiento GPS dependiente, navegación, y procedimientos de sincronización tienen un impacto significativo en la vida cotidiana. Por consiguiente, es un sistema ampliamente usado que se vuelve un blanco atractivo cada vez más para la explotación ilícita por los terroristas y computo maníacos por diferentes varios motivos; los algoritmos del antispoofing se han vuelto un tema de investigación importante dentro de la disciplina GPS. Este papel proporcionará una revisión de reciente investigación en el campo de GPS spoofing/anti-spoofing.

IV. RIESGOS DE LOS SIG

La información obtenida por los sistemas de información geográfica es bastante sensible y de alta confidencialidad, lo que también lleva a implementar altos niveles de seguridad, por medio de políticas (información, firewall, red, infraestructura, etc.). Estos sistemas están presentando diferentes modalidades de ataques y con diferentes fines; sus modalidades de ataques pueden ser Eavesdropping y Packect sniffing, Snooping y downloading, Tampering o Data diddling, Jamming o Flooding, Spoofing DNS y GPS; los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Debido al inmenso alcance e importancia de estos sistemas y a la importancia y

confidencialidad de la información que obtienen, se han comenzado a realizar todo tipo de estudios para poder definir sus vulnerabilidades, riesgos y amenazas.

A. Tipos de ataques a los SIG

-*Jamming*: Es un ataque que bombardea el receptor GPS con el ruido electrónico.

-*Spoofing*: Este método es más difícil de detectar. El objetivo del spoofing es imitar la señal enviada desde el satélite al receptor GPS pero realizando los menores cambios posibles a la señal.

B. Tipos de atacantes

-*Insiders*: Son personas internas dentro de las compañías que se encargan de utilizar sus permisos para alterar archivos o registros.

-*Outsiders*: Son personas externas a las compañías, que por medio de la ingeniería social obtienen información como usuarios y claves para acceder a los sistemas de las compañías.

C. Métodos y herramientas de ataque

-*Sniffers*: Son programas que monitorean los paquetes de la red que están direccionados a la computadora donde están instalados.

-*Eavesdropping y packect sniffing*: Consiste en capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin cifrar) al ingresar a sistemas de acceso remoto.

-*Snooping y downloading*: Consiste en obtener la información sin modificarla; además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

-*Tampering o data diddling*: Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada.

-*Jamming o flooding*: Este tipo de ataque consiste en desactivar o saturar los recursos del sistema.

-*Spoofing*: Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering.

-*GeoDatabase*: Es un modelo que permite el almacenamiento físico de la información geográfica, ya sea en archivos dentro de un sistema de ficheros o en una colección de tablas en un sistema gestor de base de datos (Microsoft Access, Oracle, Microsoft SQL Server, IBM DB2 e Informix).

V. COMPONENTES DE LOS SIG

Para el desarrollo del presente artículo era necesario detectar cómo funcionan los sistemas de información geográfica y cuáles son sus componentes principales. Se determinó que los SIG son encargados de digitalizar y almacenar la información que es recolectada por los GPS y transmitida a través de señales por medio satélites o de forma manual; debido a este funcionamiento se concluyó que los GPS son una de las herramientas principales de los SIG, pero presentan vulnerabilidades, riesgos y amenazas diferentes, lo que lleva a hacer un análisis de cada uno por separado de la siguiente forma:

-El análisis realizado a los SIG, fue con base a la información que manejan, y que tipo de seguridad deben de tener por el nivel de confidencialidad en los datos obtenidos.

-El análisis que se ha realizado a GPS fue con base a la información que recolecta, como por ejemplo como pueden ser capturadas y manipuladas las señales que transmiten esta información.

Se comienzan a analizar los diferentes términos básicos para el proceso de gestión del riesgo, entre los conceptos que se analizaron fueron:

-*Riesgo*: Es la probabilidad de que se produzca un impacto determinado a un activo.

-*Amenaza*: Es el evento que puede desencadenar un incidente de la organización, produciendo daños o pérdidas materiales en sus activos.

-*Impacto*: Es la consecuencia para un activo de la materialización de una amenaza.

-*Vulnerabilidad*: Es la debilidad de un activo que puede ser explotada por una amenaza para materializar un agresión sobre dicho activo, se

clasifica en alta, media y baja.

-*Evaluación de riesgo*: Se identifican las amenazas, vulnerabilidades y riesgos sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de confidencialidad, integridad y disponibilidad. Se consideran los siguientes puntos:

- La probabilidad de una amenaza.
- La magnitud del impacto sobre el sistema.
- *Determinación de la probabilidad*: Se determina la probabilidad que una vulnerabilidad pueda ser explotada por una amenaza, pueden manejar diferentes tipos de clasificación. Se tienen en cuenta los siguientes factores:
- Fuente de la amenaza y su capacidad.
- Naturaleza de la vulnerabilidad.

Análisis de impacto y factor de riesgo: Se determina el impacto adverso para la organización, como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad, se pueden considerar los siguientes aspectos:

- Consecuencias de tipo financiero, es decir pérdidas causadas sobre un activo físico o lógico determinado y las consecuencias que este activo no funcione, y afecte la operación de la compañía.
- La importancia crítica de los datos y el sistema (importancia a la organización).
- Sensibilidad de los datos y el sistema.

VI. ANÁLISIS DE RIESGOS DE LOS SIG

Identificación de riesgos SIG: El proceso de identificación de riesgos estuvo determinado por la realización previa de identificación y clasificación de los activos, la cual contempla todos los elementos necesarios para mantener estable el SIG. Los activos fueron clasificados en 3 categorías:

A. Sistemas

Hace referencia a activos de hardware y software que pertenecen y pueden ser afectados en los SIG.

SISTEMAS	Programas de comunicación
	Programas de Producción de datos
	Portátiles
	Computadores
	Servidores
	Cortafuegos/Firewall
	Equipos de Red Inalámbrica
	Equipos de red cableada

Fig. 1. Riesgos de los SIG: Sistemas

B. Personal

Esta clasificación de activos hace referencia a las labores que realizan usuarios que intervienen en los SIG.

PERSONAL	Informática/soporte Interno
	Soporte Técnico Externo
	Servicio de Limpieza de Planta
	Servicio de Limpieza Externo

Fig. 2. Riesgos de los SIG: Personal

C. Datos e información

Esta clasificación de activos es la más delicada y vulnerable en el nivel de riesgos, ya que es la que almacena y gestiona la información que es obtenida por los GPS y otros medios de información.

DATOS E INFORMACIÓN	Correo electrónico
	Bases de datos internas
	Bases de datos externas
	Páginas Web internas (Intranet)
	Respaldos
	Infraestructura (Planes, Documentación, etc.)
	Informática (Planes, Documentación, etc.)
	Sistemas de autenticación (ActDir., LDAP,etc)
	Sistemas de información no organizacionales
	Navegación en Internet

Fig. 3. Riesgos de los SIG: Datos e información

Identificación y clasificación de las amenazas SIG: Las amenazas se encuentran identificadas y clasificadas de la siguiente manera:

A. Nivel físico

Esta clasificación está enfocada a amenazas que

provienen de desastres ambientales, degradación o fallas físicas en los SIG.

FÍSICO	Incendio
	Inundación
	Sismo
	Polvo
	Ausencia de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla eléctrica (apagón)
	Falla del sistema (hardware)

Fig. 4. Amenazas de los SIG: Nivel físico

B. *Nivel de usuario*

Estas amenazas están enfocadas hacia los errores que pueda causar un usuario sobre los activos del sistema SIG.

USUARIO	Falta de inducción, capacitación y sensibilización sobre riesgos
	Manejo inadecuado de sistemas y herramientas
	Pérdida de datos por errores de usuario

Fig. 5. Amenazas de los SIG: Nivel de usuario

C. *Nivel de hardware*

Estas amenazas están enfocadas a diferentes fallas que puedan presentar los componentes de hardware de los SIG.

HARDWARE	Infección de sistemas a través de unidades USB sin escaneo previo
	Exposición o extravío de equipos, unidades de almacenamientoUSB, etc.
	Pérdida de datos por error de hardware
	Falta de mantenimiento físico (procesos, repuestos e insumos)

Fig. 6. Amenazas de los SIG: Nivel de hardware

D. *Nivel de datos*

Estas amenazas se enfocan en la información y datos del SIG que pueden estar expuestos a un acceso no autorizado, una alteración, entre otros.

DATOS	Manejo inadecuado de datos críticos (codificar, modificar, eliminar, etc.)
	Transmisión de información crítica o delicada sin cifrar

Fig. 7. Amenazas de los SIG: Nivel de datos

E. *Nivel de software*

Dentro de esta clasificación se encuentran amenazas enfocadas a errores de diseño o pruebas e implementación de software de los SIG.

SOFTWARE
Falta de actualización de software, seguimiento de procesos y recursos.

Fig. 8. Amenazas de los SIG: Nivel de software

F. *Nivel de infraestructura*

Dentro de esta clasificación se encuentran amenazas enfocadas a problemas de organización en la parte de infraestructura que puedan ocasionar perjuicios a los SIG.

INFRAESTRUCTURA
Dependencia del servicio técnico externo
Red cableada expuesta ante acceso no autorizado

Fig. 9. Amenazas de los SIG: Nivel de infraestructura

G. *Nivel de políticas*

Estas amenazas están enfocadas en la falta de normas y reglas en la organización, las cuales pueden llegar a tener un gran riesgo e impacto en los activos de los SIG.

POLÍTICAS	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación
	Falta de definición de perfiles, accesos, privilegios y restricciones del personal
	Ausencia de establecimiento de políticas de seguridad corporativa

Fig. 10. Amenazas de los SIG: Nivel de políticas

H. Nivel de redes

Estas amenazas están enfocadas a fallas de seguridad en el acceso y transmisión de datos a través de la red de los SIG.

REDES	Red inalámbrica expuesta al acceso no autorizado y/o con errores de configuración
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos

Fig. 11. Amenazas de los SIG: Nivel de redes

I. Nivel de acceso

Dentro de esta clasificación se presentan amenazas por parte de acceso de personal no autorizado a los SIG.

ACCESO
Manejo inadecuado de contraseñas (inseguras, no cambiarlas, BD centralizada)
Compartir contraseñas o permisos a terceros no autorizados

Fig. 12. Amenazas de los SIG: Nivel de acceso

VII. ANÁLISIS DE RIESGOS DEL SISTEMA GPS

Identificación de riesgos GPS: El proceso de identificación de riesgos estuvo determinado por la realización previa de la identificación y clasificación de los activos. La identificación de los activos contempla todos los elementos necesarios para mantener estable los elementos que componen el sistema GPS. Los activos fueron clasificados en 2 categorías:

A. Personal

En esta clasificación de activos se determinaron todos aquellos elementos que hacen parte del personal que podrían intervenir en el funcionamiento de los sistemas GPS, y donde las amenazas podrían tener un nivel de impacto significativo.

PERSONAL	Informática/soporte Interno
	Soporte Técnico Externo
	Servicio de Limpieza Interno
	Servicio de Limpieza Externo

Fig. 13. Riesgos de los GPS: Personal

B. Sistemas

En esta clasificación de activos se determinaron todos aquellos elementos que hacen parte del correcto funcionamiento de los GPS.

SISTEMAS	Programas de comunicación
	Programas de Producción de datos
	Portátiles
	Computadoras
	Servidores
	Equipos de Red Inalámbrica
	Vehículos
	Satélites
	Equipos de Topografía
	Antenas receptoras
	Equipos de red cableada

Fig. 14. Riesgos de los GPS: Sistemas

Identificación y clasificación de las amenazas GPS: Las amenazas se encuentran identificadas y clasificadas de la siguiente manera:

A. Nivel físico

Las amenazas identificadas para esta clasificación, son aquellas que puedan afectar los activos por elementos de carácter físico ya sea por un evento natural, por degradación o fallas eléctricas.

FÍSICO	Incendio
	Inundación
	Sismo
	Polvo
	Ausencia de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla eléctrica (apagón)
	Falla del sistema (hardware)

Fig. 15. Amenazas de los GPS: Nivel físico

B. Nivel de criminalidad

Las amenazas identificadas para esta clasificación son aquellas que pueden afectar los activos por situaciones como actos vandálicos, sabotaje, infiltraciones y ataques de ciber delincuentes.

ACTOS ORIGINADOS POR CRIMINALIDAD
Allanamiento (legal/ilegal)
Persecución (civil, fiscal, penal)
Sabotaje (ataque físico y electrónico)
Robo / Hurto (físico)
Daños por vandalismo
Robo / Hurto de información electrónica
Intrusión a Red interna
Infiltración
Virus / Ejecución no autorizada de programas

Fig. 16. Amenazas de los GPS: Nivel de criminalidad

C. Nivel de infraestructura

Las amenazas identificadas para esta clasificación son aquellas que pueden afectar los activos por diferentes tipos de incidencias.

INFRAESTRUCTURA
Dependencia del servicio técnico externo
Red cableada expuesta ante acceso no autorizado

Fig. 17. Amenazas de los GPS: Nivel de infraestructura

D. Nivel de políticas

Las amenazas identificadas en esta clasificación se asocian a la mala implementación o administración de normas de seguridad establecidas para los activos.

POLÍTICAS	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación
	Falta de definición de perfiles, accesos, privilegios y restricciones del personal
	Ausencia de establecimiento de políticas de seguridad corporativa

Fig. 18. Amenazas de los GPS: Nivel de políticas

E. Nivel de hardware

Las amenazas identificadas para esta clasificación son aquellas que afectan los activos por errores, fallas o degradación.

HARDWARE	Infección de sistemas a través de unidades USB sin escaneo previo
	Exposición o extravío de equipos, unidades de almacenamientoUSB, etc.
	Pérdida de datos por error de hardware
	Falta de mantenimiento físico (procesos, repuestos e insumos)

Fig. 19. Amenazas de los GPS: Nivel de hardware

F. Nivel de redes

Las amenazas identificadas en esta clasificación son las que pueden afectar los activos en transmisión de datos o redes inalámbricas.

REDES
Transmisión de información crítica o delicada sin cifrar
Red inalámbrica expuesta al acceso no autorizado y/o con errores de configuración
Acceso electrónico no autorizado a sistemas externos
Acceso electrónico no autorizado a sistemas internos

Fig. 20. Amenazas de los GPS: Nivel de redes

G. Nivel de usuario

Las amenazas identificadas para esta clasificación son aquellas que afectan los activos por mal manejo, falta de capacitación o indiscreción de los usuarios.

USUARIO	Manejo inadecuado de contraseñas (inseguras, no cambiarlas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Perdida de datos por errores de usuario

Fig. 21. Amenazas de los GPS: Nivel de usuario

VIII. CONTROLES DE RIESGOS SIG

En base a los datos obtenidos en el análisis de los SIG, se determinan controles de riesgos para cada activo. Estos controles de riesgo sirven como base para poder mitigar, implementar y controlar los riesgos categorizados de mayor impacto. Los riesgos de menor impacto no son analizados, ya que su control es más elemental o puede ser innecesario realizarlo.

A. Portátiles, PCs de escritorio (Activo)

TABLA I
CONTROL DE RIESGOS SIG: PORTÁTILES

RIESGO	AFECTACIÓN	CONTROLES
Propagación de virus en la red.	Integridad.	Configuración de acceso limitado a redes.
		Monitoreo de puertos.
Pérdida del equipo.	Disponibilidad.	Formato de reportes de daño y/o pérdida del equipo.
		Seguro de equipo contra robo.
		Copia de respaldo de documentos.
		Mantener servicios de sincronización en la nube.
		Cifrar información sensible del equipo.
Intromisiones de otros usuarios al equipo.	Confidencialidad.	Educación en medidas de seguridad e informática.
		Configuración de acceso limitado a redes.
		Creación de contraseñas robustas.
Acceso por entidades externas a información sensible o privada.	Confidencialidad.	Monitoreo de conexiones activas.
		Monitoreo de modificación de archivos.
		Respaldos de seguridad.
Uso delictivo de datos.	Confidencialidad. Integridad.	Respaldos de seguridad.

B. Servidores (Activo)

TABLA II
CONTROL DE RIESGOS SIG: SERVIDORES

RIESGO	AFECTACIÓN	CONTROLES
Acceso no autorizado a los servidores.	Confidencialidad. Integridad. Disponibilidad.	Monitoreo de puertos.
		Recuperación del sistema.

C. Soporte técnico interno (Activo)

TABLA III
CONTROL DE RIESGOS SIG: SOPORTE TÉCNICO INTERNO

RIESGO	AFECTACIÓN	CONTROLES
Acceso y manipulación de redes privadas	Confidencialidad Integridad	Monitoreo de puertos.
Acceso y manipulación a información privada.	Confidencialidad. Integridad.	Determinación de niveles de responsabilidad y acceso.
		Planificación y seguimiento de las tareas de soporte técnico interno.

D. Soporte técnico externo (Activo)

TABLA IV
CONTROL DE RIESGOS SIG: SOPORTE TÉCNICO EXTERNO

RIESGO	AFECTACIÓN	CONTROLES
Robo de información.	Confidencialidad Disponibilidad	Monitoreo de puertos.
Alteración y destrucción de la información.	Integridad Disponibilidad	Planificación y seguimiento de las tareas de soporte técnico externo.

E. Bases de datos internas (Activo)

TABLA V
CONTROL DE RIESGOS SIG: BASES DE DATOS INTERNAS

RIESGO	AFECTACIÓN	CONTROLES
Alteración y destrucción de datos.	Integridad. Disponibilidad.	Copias de seguridad.
Acceso por usuarios no autorizados.	Confidencialidad.	Medidas de acceso robustas con 'id_usuario' y contraseña.
Acceso a datos sensibles o privados.	Confidencialidad.	Cifrado de datos.
		Políticas de gestión de la bases de datos.

F. Respaldos (Activo)

TABLA VI
CONTROL DE RIESGOS SIG: RESPALDOS

RIESGO	AFECTACIÓN	CONTROLES
Alteración y destrucción de respaldos.	Integridad. Disponibilidad.	Actualización frecuente de respaldos.
		Almacenamiento interno de respaldos con protección de acceso.
		Almacenamiento externo de respaldos en ubicaciones diferentes a la organización.
		Capacitación a usuarios respectivos en el proceso de restauración de los datos.
Acceso a respaldos por usuarios no autorizados.	Confidencialidad.	Determinación de niveles de acceso.
		Políticas de respaldos de la base de datos.

G. Sistemas de autenticación (Activo)

TABLA VII
CONTROL DE RIESGOS SIG: SISTEMAS DE AUTENTICACIÓN

RIESGO	AFECTACIÓN	CONTROLES

Exposición de datos de autenticación a usuarios no autorizados.	Confidencialidad. Integridad.	Cifrado de datos del sistema de autenticación.

H. Navegación en internet

TABLA VIII
CONTROL DE RIESGOS SIG: NAVEGACIÓN EN INTERNET

Riesgo	Afectación	Controles
Descarga y propagación de virus.	Integridad	Bloqueo de acceso a páginas de internet no seguras.
		Firewall.
		Chequeo del tráfico de red.
		Políticas de acceso a internet.
Divulgación de información de la organización.	Confidencialidad.	Bloqueo de acceso a páginas de internet no seguras.
		Firewall.
		Chequeo del tráfico de red.
		Políticas de acceso a internet.

GPS: Nivel de usuario

IX. CONTROLES DE RIESGOS GPS

En base a los datos obtenidos en el análisis de los GPS, se determinan controles de riesgos para cada activo. Estos controles de riesgo sirven como base para poder mitigar, implementar y controlar los riesgos categorizados de mayor impacto. Los riesgos de menor impacto no son analizados, ya que su control es más elemental o puede ser innecesario realizarlo.

A. Portátiles, PCs de escritorio (Activo)

TABLA IX
CONTROL DE RIESGOS GPS: PORTÁTILES, PCS DE ESCRITORIO

RIESGO	AFECTACIÓN	CONTROLES
Robo de equipo.	Confidencialidad. Integridad. Disponibilidad.	Adquirir póliza contra robo de equipos.
		Restringir la salida de equipos de las instalaciones.
		Mejorar los niveles de seguridad en las instalaciones.
Robo de información.	Confidencialidad. Disponibilidad.	Cifrar información en los discos duros de los equipos.
		Respaldar información automática en servidores.
		Implementar contraseña de arranque en la BIOS de los equipos.
		Implementar contraseña de inicio de sesión en los equipos.
Infiltración de virus.	Confidencialidad. Integridad. Disponibilidad.	Adquirir antivirus con licenciamiento empresarial.
		Mantener antivirus actualizado en los equipos.
		Tener antivirus activo en todos los equipos.
		Bloquear panel de configuración de antivirus para usuarios finales.
Perdida de información por error de Hardware.	Integridad. Disponibilidad.	Respaldar información automática en servidores.
		Adquirir equipos de cómputo de alta calidad con perfil empresarial.
		Realizar pruebas de esfuerzo en los equipos de cómputo antes de hacer renovación tecnológica.
		Hacer renovación tecnología con un mínimo de 3 años.
		Realizar mantenimiento preventivo en los equipos al menos 2 veces al año en equipos de escritorio.
		Realizar mantenimiento preventivo en los equipos al menos 6 veces al año en equipos móviles
Perdida de información por error de Usuario.	Confidencialidad Integridad Disponibilidad.	Respaldar información automática en servidores.
		Brindar capacitaciones periódicas a los usuarios en la importación del manejo de la información.

B. Equipos de topografía (Activo)

TABLA X
CONTROL DE RIESGOS GPS: EQUIPOS DE TOPOGRAFÍA

RIESGO	AFECTACIÓN	CONTROLES
Robo de equipo.	Confidencialidad. Integridad. Disponibilidad.	Adquirir póliza contra robo de equipos.
		Mejorar los niveles de seguridad en las instalaciones.
Infiltración en información transmitida no cifrada.	Confidencialidad. Integridad.	Cifrar información transmitida.
		Cifrar señales de transmisión.
		Implementar señal de contingencia.

		Monitorear señales de transmisión.
Perdida de información por error de Hardware.	Integridad. Disponibilidad.	Realizar mantenimiento preventivo en los equipos al menos 6 veces al año.
		Renovar equipos cada 3 años.

X. CONCLUSIONES

El manejo inadecuado de los recursos en los SIG se presenta en un mayor grado por la falta de capacitación y de sensibilización de riesgos, para lo cual se deben definir políticas de seguridad claras para cada uno de los activos y usuarios que hacen uso de ellos.

Los controles de acceso asignados a usuarios o sistemas, contribuyen en gran medida en la disminución de los riesgos presentados ante los tres pilares de seguridad: confidencialidad, integridad y disponibilidad, la incorporación de estas medidas son eficientes siempre y cuando exista un seguimiento en las tareas de los usuarios y el funcionamiento de los sistemas.

El masivo uso actual de los sistemas GIS y GPS hace primordial conocer que tan vulnerables pueden ser estos sistemas. Es recomendable identificar y valorar los riesgos presentes en los sistemas descritos, pero aún más importante es saber cuáles pueden ser los controles recomendados con el fin de mitigarlos.

Con el uso de tecnologías que apoyan los procesos de negocio en las empresas, vienen inherentes riesgos que deben ser identificados, valorados y tratados antes que estos se manifiesten, de no hacerlo se verán expuestos a daños y pérdidas considerables.

REFERENCIAS

[1] Sistemas de Información Geográfica. [Online] Available: http://langleruben.wordpress.com

[2] Global Navigation Space Systems. [Online] Available: http://www.raeng.org.uk/publications/reports/global-navigation-space-systems

[3] ESRI. What is GIS? [Online] Available: http://www.esri.com/what-is-gis/

[4] ESRI. Geographyc Information System Knowledge Base. [Online] Available: http://support.esri.com/en/knowledge-base

[5] La base de datos GIS del Mapa Geológico de Colombia. [Online] Available: http://www2.sgc.gov.co/Geologia/Mapa-geologico-de-Colombia/La-base-de-datos-GIS-del-MGC.aspx

[6] Ataques Informáticos, Identificando las Amenazas. [Online] Available: https://www.slideshare.net/jmacostarendon/seguridad-redesservidores

[7] Los Sistemas de Información Geográfico, una Herramienta útil para la Gestión del Riesgo y Manejo de las Emergencias y Catástrofes. [Online] Available: https://www.anepe.cl/los-sistemas-de-informacion-geografico-una-herramienta-util-para-la-gestion-del-riesgo-y-manejo-de-las-emergencias-y-catastrofes/

[8] GIS Overview. [Online] Available: http://www.cs.utah.edu/~arul/gis.pdf

[9] Así funciona el GPS. [Online] Available: http://www.asifunciona.com/electronica/af_gps/af_gps_10.htm

[10] Vanegas, C., (2017). Fig. 1. Riesgos de los SIG: Sistemas.

[11] Vanegas, C., (2017). Fig. 2. Riesgos de los SIG: Personal.

[12] Vanegas, C., (2017). Fig. 3. Riesgos de los SIG: Datos e información.

[13] Vanegas, C., (2017). Fig. 4. Amenazas de los SIG: Nivel físico.

[14] Vanegas, C., (2017). Fig. 5. Amenazas de los SIG: Nivel de usuario.

[15] Vanegas, C., (2017). Fig. 6. Amenazas de los SIG: Nivel de hardware.

[16] Vanegas, C., (2017). Fig. 7. Amenazas de los SIG: Nivel de datos.

[17] Vanegas, C., (2017). Fig. 8. Amenazas de los SIG: Nivel de software.

[18] Vanegas, C., (2017). Fig. 9. Amenazas de los SIG: Nivel de infraestructura.

[19] Vanegas, C., (2017). Fig. 10. Amenazas de los SIG: Nivel de políticas.

[20] Vanegas, C., (2017). Fig. 11. Amenazas de los SIG: Nivel de redes.

[21] Vanegas, C., (2017). Fig. 12. Amenazas de los SIG: Nivel de acceso.

[22] Vanegas, C., (2017). Fig. 13. Riesgos de los GPS: Personal.

[23] Vanegas, C., (2017). Fig. 14. Riesgos de los GPS: Sistemas.

[24] Vanegas, C., (2017). Fig. 15. Amenazas de los GPS: Nivel físico.

[25] Vanegas, C., (2017). Fig. 16. Amenazas de los GPS: Nivel de criminalidad.

[26] Vanegas, C., (2017). Fig. 17. Amenazas de los GPS: Nivel de infraestructura.

[27] Vanegas, C., (2017). Fig. 18. Amenazas de los GPS: Nivel de políticas.

[28] Vanegas, C., (2017). Fig. 19. Amenazas de los GPS: Nivel de hardware.

[29] Vanegas, C., (2017). Fig. 20. Amenazas de los GPS: Nivel de redes.

[30] Vanegas, C., (2017). Fig. 21. Amenazas de los GPS: Nivel de usuario.

[31] Vanegas, C., (2017) Control de Riesgos SIG: Portátiles. TABLA I.
[32] Vanegas, C., (2017) Control de Riesgos SIG: Servidores. TABLA II.
[33] Vanegas, C., (2017) Control de Riesgos SIG: Soporte Técnico Interno. TABLA III.
[34] Vanegas, C., (2017) Control de Riesgos SIG: Soporte Técnico Externo. TABLA IV.
[35] Vanegas, C., (2017) Control de Riesgos SIG: Bases de Datos Internas. TABLA V.
[36] Vanegas, C., (2017) Control de Riesgos SIG: Respaldos. TABLA VI.
[37] Vanegas, C., (2017) Control de Riesgos SIG: Sistemas de Autenticación. TABLA VII.
[38] Vanegas, C., (2017) Control de Riesgos SIG: Navegación en Internet. TABLA VIII.
[39] Vanegas, C., (2017) Control de Riesgos GPS: Portátiles, PCs de Escritorio. TABLA IX.
[40] Vanegas, C., (2017) Control de Riesgos GPS: Equipos de Topografía. TABLA X.