UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Seguridad informática aplicada a la ingeniería geomática

TESIS

Que para obtener el título de

Ingeniero Geomático

P R E S E N T A

Daniel Macouzet Iturbe

DIRECTOR DE TESINA

M. en I. Adolfo Reyes Pizano

Ciudad Universitaria, Cd. Mx., 2019

Dedicatoria

A Winny Lorelei Meza Martínez, eres tú.

Agradecimientos

A mi madre, quien fue la primera en ver crecer mi trabajo.

A Ana María Escalante Gonzalbo por haberme dado una oportunidad invaluable para poder aprender más.

A Francisco Pérez Eugenio por compartir sus conocimientos desinteresadamente.

A Adolfo Reyes Pizano por ayudarme desde los primeros pasos hasta los últimos de la carrera.

A María Elena Osorio Tai por ayudarme a perfeccionar el trabajo con el cual termino la carrera.

A mis sinodales Roberto Ascencio Villagómez, Ana Lilia Salas Alvarado y Luis Bruno Garduño Castro.

A quienes me han influenciado para ser quien ahora soy, como son mi padre, mi familia, mis amigos y mis profesores que me han instruido.

TABLA DE CONTENIDO

I. INTRODUCCIÓN

I.1 PLANTEAMIENTO DEL PROBLEMA Y JUSTIFICACIÓN

Los ingenieros geomáticos han tenido la necesidad de procesar y almacenar mayores cantidades de información hasta el punto de no poder realizarse por métodos antes habituales, que se mencionarán en el capítulo 3, debido a la cantidad de tiempo requerido para ello. El uso de computadoras para el procesamiento, almacenamiento y transporte de datos es una práctica cada vez más común en un creciente número de áreas tanto personales como profesionales, incluyendo en la Ingeniería Geomática, lo que nos facilita en gran medida las labores. Pero al igual que casi todo, tiene sus ventajas y sus desventajas, las cuales no siempre se conocen.

La Universidad Nacional Autónoma de México (UNAM) define la carrera en Ingeniería Geomática de la siguiente manera: "*En la carrera de Ingeniería Geomática se llevan a cabo actividades relacionadas con la adquisición, proceso y almacenamiento de elementos topográficos y geográficos que son la base para la producción de mapas, planos, cartas e imágenes que se utilizan en forma digital para realizar estudios y análisis, con fines multidisciplinarios.*

Esta profesión sirve de apoyo a otras geociencias como: geografía, geofísica, oceanografía, ecología, que dependen de dichos estudios. En ella se emplean sistemas modernos para la medición, captura, análisis y almacenamiento de la información referente a la superficie de la tierra.

Los ingenieros geomáticos aplican sus conocimientos de cartografía, fotogrametría, sistemas de información, geodesia, topografía, percepción remota, informática y computación, con lo que resuelven problemas y abren nuevas oportunidades en áreas como: desarrollo, operación y mantenimiento de sistemas de información geográfica y construcción de obras civiles" (UNAM, 2018).

Y los objetivos educacionales del programa son los siguientes:

1. *Los egresados aplican los conocimientos de su disciplina, para resolver proyectos de Ingeniería Geomática, respetando la normatividad técnica vigente.*
2. *Los egresados contribuyen por medio de sus habilidades, conocimientos y actitudes al desarrollo de proyectos de su disciplina, haciendo uso adecuado de los recursos y de las TIC, para lograr soluciones funcionales.*
3. *Los egresados trabajan en instituciones públicas, privadas o de manera independiente.*
4. *Los egresados trabajan en grupos inter y multidisciplinarios, en un entorno de responsabilidad social y conducta ética.*
5. *Los egresados tienen la capacidad para continuar su formación en un área específica, realizando estudios de posgrado y educación continua*. (Facultad de Ingeniría, 2018)

En el primer objetivo del programa se menciona el respeto de la normatividad técnica vigente, el cual incluye la correcta protección de la información. En el segundo

objetivo se menciona el uso adecuado de los recursos y de las Tecnologías de Información y Comunicación (TIC) las cuales adquieren, procesan y almacenan información fundamental para la Ingeniería Geomática. Y el quinto objetivo menciona la capacidad del egresado para continuar su formación en un área específica, entre las cuales se encuentran la informática y la computación, antes mencionadas en la definición de Ingeniería Geomática.

En este trabajo se hablará acerca de la adquisición, el proceso y el almacenamiento de los elementos geográficos que se utilizan en forma digital, sobre los sistemas modernos para la medición, captura, análisis y almacenamiento de la información, y sobre algunos conocimientos necesarios, pero generalmente desconocidos, de informática y computación.

I.2 OBJETIVO GENERAL

Exponer la importancia de los conocimientos en seguridad de la información aplicados en los sistemas modernos usados en la Ingeniería Geomática para la medición, captura, análisis y almacenamiento de la información referente a la superficie de la Tierra, ya que para poder identificar con mayor facilidad las posibles amenazas en un conjunto de procesos y procedimientos es necesario estar familiarizado con ellos.

II. LA INGENIERÍA GEOMÁTICA Y LOS ORDENADORES

II.1 EVOLUCIÓN DE LA INGENIERÍA GEOMÁTICA

De acuerdo a la Real Academia Española el término “Geomática” proviene “del francés *géomatique,* de *géo-* 'geo-' y la t. de *informatique* 'informática'” (Real Academia Española), surge recién en el siglo XXI como resultado del uso de las nuevas tecnologías de la información junto con algunas ciencias de la tierra, algunas de las cuales se mencionarán como antecedentes de la Geomática.

- **Topografía**

  La topografía es el *arte de describir y delinear detalladamente la superficie de un terreno* (Real Academia Española), su uso es tan antiguo que resulta imposible determinar con exactitud su origen, se encuentra relacionado con la astronomía, la astrología y las matemáticas. De no ser por la topografía no se habrían podido edificar la inmensa cantidad de monumentos y construcciones que se han hecho. La topografía ha evolucionado como muchas otras ciencias, desde el uso de cuerdas con marcas a intervalos definidos usadas desde hace siglos, pasando por el odómetro, la cinta y llegando a las estaciones totales y escáneres que se ocupan hoy en día, que ahorran varias horas de trabajo en campo y se obtienen cada vez más mediciones más precisas y exactas conforme los instrumentos de medición evolucionan (McCormac, 2007).

- **Geodesia**

  La geodesia *es la ciencia que desarrolla y estudia los métodos, tecnologías y procedimientos dirigidos a determinar con exactitud el tamaño y la forma de la Tierra o parte de ella, incluyendo su campo gravitacional externo, como una función del tiempo* (Instituto Nacional de Estadística y Geografía). La geodesia también se encuentra en una estrecha relación con otras áreas del conocimiento, que han ido evolucionando y así se han podido conseguir mediciones más cercanas al valor real de la Tierra, avances entre los cuales figuran una considerable cantidad relativa a la física. En la era moderna el uso de computadoras ha permitido procesar grandes volúmenes de datos que no sería posible realizar sin la tecnología, además de tener la capacidad de hacer el trabajo de forma más rápida, fácil y eficiente. Además, la geodesia amplía sus horizontes llegando hasta la medición del relieve del fondo marino, tanto para objetos estáticos como móviles. La geodesia hace uso de tecnologías emergentes, añadiendo nuevos elementos y herramientas a su creciente catálogo de recursos (Vaníček, y otros, 1986).

- **Cartografía**

  La antigüedad de la cartografía se remonta hace casi tanto como la topografía, ambas acompañando a la humanidad por más tiempo que la misma escritura. La creación de mapas se ha desarrollado en todo el planeta, cuya fidelidad ha ido aumentando con el paso del tiempo, ha permitido representar extensiones más grandes de terreno. Gran parte de la cartografía moderna depende de la medición

correcta del terreno, otra gran parte depende de la habilidad de plasmar esas mediciones en un plano, cosa que con el paso del tiempo hace uso de nuevas técnicas y herramientas que facilitan el proceso. Hoy en día resulta imposible trabajar con la precisión del 15% obtenida por Eratóstenes un par de siglos antes de Cristo al estimar la longitud de los meridianos (Raisz, 1985), que para ese entonces era impresionante y suficiente.

- **Percepción Remota**

  La Percepción Remota *es la ciencia (para algunos, arte o técnica) que permite observar y obtener información de nuestro planeta -desde el espacio-, sin estar en contacto con ella* (Instituto Nacional de Estadística y Geografía). Al hablar de la medición del terreno haciendo uso de imágenes tomadas desde el aire estamos hablando de técnicas relativamente nuevas, teniendo en cuenta algunas de las ciencias prehistóricas que han existido por milenios. Tanto la fotografía como la capacidad del hombre de volar tienen apenas menos de un par de siglos. Las primeras imágenes útiles para propósitos científicos fueron tomadas en 1858 por G. Tournachon desde un globo (Kazansev, 2017), los avances posteriores en la fotogrametría fueron realizados más sistémicamente por parte de la milicia. El costo de realizar un vuelo fotogramétrico era elevado e implicaba necesariamente el uso de una aeronave tripulada, ahora un vuelo fotogramétrico puede realizarse con aeronaves no tripuladas de diferentes clases, desde un avión que requiere una pista de aterrizaje hasta multirrotores más prácticos, pero menos estables en el vuelo que

los anteriores. También se obtienen imágenes capturadas desde satélites con sensores que captan frecuencias del espectro electromagnético no visibles para el ojo humano y que se han aprendido a interpretar, ampliando aún más las fronteras de la teledetección y de la Ingeniería Geomática (Kazansev, 2017).

- **GNSS GPS**

  Un Sistema Global de Navegación por Satélites (*Global Navigation Satellite System,* **GNSS**) es una constelación de satélites que emite señales que son usadas para calcular la ubicación de un receptor de esas señales en cualquier parte de la Tierra (Berné Valero, y otros, 2014), uno de esos sistemas que es usado en la Ingeniería Geomática es el Sistema de Posicionamiento Global (*Global Position System*, **GPS**). Todo el proyecto del Sistema de Posicionamiento Global fue el resultado de la colaboración de varias partes interesadas. El lanzamiento del primer satélite de GPS se realizó apenas en 1978, en 1982 se confirmó una precisión entre las estaciones de 1 a 2 partes por millón (Leick, 2004), y rápidamente conforme pasaba el tiempo había más interés en las posibles aplicaciones de esta nueva tecnología. La tecnología GPS ha ido mejorando rápidamente desde entonces, su precisión y velocidad han aumentado, y su uso se ha extendido. Los satélites GPS transmiten en un código accesible por civiles y también transmiten en código encriptado anti falsificación para uso militar (Leick, 2004), por lo que se puede deducir que las señales de GPS que se ocupan normalmente están expuestas a ser alteradas o falsificadas.

II.2 PROCESAMIENTO DE DATOS ASISTIDO POR COMPUTADORA

Desde hace miles de años que se saben realizar los cálculos manualmente, sin embargo, existe una probabilidad relativamente alta de cometer equivocaciones y obtener resultados falsos. Una forma de reducir la probabilidad de errores al realizarse cálculos es minimizar la interacción humana al realizarse los cálculos, delegando esa labor a instrumentos de cálculo o máquinas que deberían arrojar los mismos resultados a los cálculos cuando se usen correctamente, además de reducir el tiempo necesario y poder realizar cálculos cada vez más complejos con una mayor facilidad. Algunos ejemplos de instrumentos mecánicos de cálculo son los huesos de Napier, la regla de cálculo y el ábaco.

El cálculo ha evolucionado junto con la tecnología aprovechando todos los recursos que ésta le ha brindado y se creó la primera calculadora en 1623 llamada *reloj calculador*, la cual funcionaba mecánicamente. No fue sino hasta 1972 que se inventó la primera calculadora electrónica de bolsillo, la cual representa un hito en la historia de la informática y los procesos por los cuales realizamos cálculos tal cual se conocen hoy en día (Torra, 2010).

En 1943 se puso en funcionamiento el considerado como el primer ordenador electrónico programable digital, llamado *Colossus*, cuyas funciones lógicas fueron diseñadas por Alan Turing. Después, en 1945 se finalizó otra máquina conocida como *ENIAC*, la cual tenía un tiempo de cálculo de 0.2 milisegundos para una suma. Posteriormente fue superada en 1951 por la *UNIVAC*, acrónimo de *Universal Automatic*

Computer, que fue creada como una computadora multipropósito, tardaba 0.5 microsegundos para hacer una suma y ya usaba cintas en vez de tarjetas perforadas lo cual mejoraba la automatización (Torra, 2010).

Un principal problema de las máquinas en ese entonces era que no tenían un programa en su memoria para controlarla, es por eso que para poder reprogramarla se tenían que hacer cambios en las conexiones de sus circuitos.

Posteriormente surgieron los lenguajes de programación, con los cuales se puede instruir a un ordenador cómo debe comportarse para que hagan lo que les solicitemos sin la necesidad de manipular directamente el *hardware* de la máquina. En 1954 IBM comenzó a desarrollar el lenguaje de programación *FORTRAN* (*FORmula TRANslation*), cuyos resultados en su implementación sorprendieron hasta a los participantes en su desarrollo. Con FORTRAN, el programador podía usar un lenguaje preciso para especificar al ordenador los procedimientos matemáticos y podía ser traducido a diferentes máquinas ya que permitía cierto nivel de abstracción, algo que adoptaron otros lenguajes posteriores como el COBOL y el LISP (Torra, 2010).

Para tener un punto de comparación del poder de cálculo de las computadoras se puede usar el número máximo de decimales que se han podido calcular del número Pi (π). Antes del uso de las computadoras, el máximo número de decimales calculados de π fue realizado por el inglés D. F. Ferguson usando la ayuda de calculadoras: en 1946 consiguió calcular 620 decimales, en 1947 llegó a los 808 decimales, y en 1949 alcanzó los 1120 decimales con la colaboración de John Wrench. Posteriormente John hizo la primera

aproximación de π usando una computadora, usó el ENIAC y luego de tan solo 70 horas de cálculo se obtuvo una aproximación de 2037 decimales. Con la tecnología disponible en el año 2011 la aproximación tenía más de 2.7 billones de dígitos (2.7×10^{12}) (Torra, 2010).

III. PROCESOS Y PROCEDIMIENTOS DE LA INGENIERÍA GEOMÁTICA EN ORDENADORES

La Ingeniería Geomática hace uso de sistemas modernos para la medición, captura, análisis y almacenamiento de la información necesaria para desempeñar sus tareas. A continuación se analizarán algunos de los sistemas involucrados en los diferentes aspectos mencionados (considerando que la medición y captura son la adquisición, el análisis es el proceso de la información, y el almacenamiento) para posteriormente analizar los posibles riesgos relacionados a cada uno y cómo reducirlos.

III.1 ADQUISICIÓN

Entre las diferentes formas en que los ingenieros geomáticos obtienen la información referente a la superficie de la Tierra se encuentran métodos tan sencillos y antiguos como la medición con el uso de la cinta, como métodos más modernos y complejos que en muchos casos involucran el uso de tecnologías electrónicas, las cuales al ser empleadas correctamente reducen considerablemente la probabilidad de cometer errores y la desviación estándar de los errores de resultados obtenidos, sobre los cuales vamos a centrar nuestra atención.

Estando en el campo se puede obtener la información que se necesite mediante el uso de dispositivos electrónicos como los distanciómetros, las estaciones totales, escáneres, dispositivos GPS, cámaras fotográficas y aeronaves no tripuladas.

También obtenemos los datos que se necesiten por medios indirectos al no capturar la información en persona directamente del entorno, como es el caso de imágenes satelitales que se descargan a través de una aplicación web usando una conexión a internet. Otro ejemplo es cuando entre colegas se proporcionan la información que necesiten al transmitirla por diferentes medios, como una unidad flash, correo electrónico o tal vez brindando una liga para descargar la información de la nube.

III.2 PROCESO

El análisis de la información obtenida puede realizarse por diferentes medios, en los cuales invariablemente se encuentra la necesidad de la intervención humana. Debido al gran volumen de información que se maneja en la Ingeniería Geomática, y que sigue aumentando con el paso del tiempo, no es raro que el procesamiento de los datos obtenidos se base en el empleo de artefactos electrónicos, desde el uso de una calculadora con solamente operaciones básicas, hasta estaciones de trabajo con procesadores múltiples y capacidad de procesamiento simultáneo usando varias unidades de procesamiento gráfico en paralelo.

Típicamente se hace uso de programas y aplicaciones (*software*), diseñados para cubrir necesidades específicas, que facilitan la interacción y uso de los recursos con los que cuente una máquina física (*hardware*). Como ejemplo de *software* se pueden mencionar los editores de texto, hojas de cálculo, visualizadores de archivos, navegadores de internet, complementos e incluso el mismo sistema operativo. También se encuentra *software* más especializado en procesos geomáticos, como *software* para trabajar con

imágenes satelitales, con Sistemas de Información Geográfica (SIG), para dibujo asistido por computadora (CAD) y otros, que también son ejecutados sobre un sistema operativo.

III.3 ALMACENAMIENTO

Toda la información que se maneja mediante diferentes dispositivos electrónicos tiene que estar almacenada en algún lugar. Independientemente del medio en el que se encuentre almacenada, ya sea desde tarjetas perforadas hasta almacenamiento experimental en ADN, se trata de la misma información que puede ser cualquier conjunto de datos que pueden ser procesados por diferentes computadoras.

Entre de los diferentes medios de almacenamiento que pueden usar comúnmente los ordenadores algunos de los que se pueden mencionar son:

- Unidad de disco duro (HDD)
- Unidad de estado sólido (SSD)
- Compact Disk (CD)
- Digital Versatile Disc (DVD)
- Blu-ray Disk (BD)
- Cintas electromagnéticas
- Unidades flash
- Tarjetas de memoria
- Códigos de barras
- Códigos QR

Sin importar qué medio de almacenamiento se ocupe siempre existen riesgos como flujo no deseado de información, *malware*, daño o robo a la unidad de almacenamiento, pérdida de información, etc.

III.4 MANEJO DE GRANDES VOLÚMENES DE INFORMACIÓN

La creciente capacidad de las máquinas para el procesamiento de datos se relaciona directamente con la necesidad de mayores capacidades de almacenamiento de los mismos. Un ejemplo puede ser las imágenes, ya sea que se hable de fotografías que son tomadas recreativamente con familia y amigos, o ya sean imágenes aéreas o satelitales que cuya resolución espacial aumenta con cada generación de satélites que ponen en órbita, dependiendo su objetivo, el espacio de almacenamiento digital que requieren va en aumento. Hoy en día puede resultar imposible guardar toda la información que se una persona maneja diariamente ocupando menos de 1 MB que ofrecían los primeros disquetes que antes se usaban (TECHNOLOGICAL TRENDS IN THE DEVELOPMENT OF THE FLOPPY DISK., 2004) (International Business Machines Corporation, 1971), en cambio ahora se suelen usar las unidades flash con entrada USB con capacidades superiores a los 8192 MB, que son 8 GB. De igual forma la velocidad de transferencia de datos ha ido aumentando en diferentes componentes, como las conexiones inalámbricas con protocolos más rápidos, cables de mayor categoría, puertos con mayor velocidad de transferencia, etc.

No es raro que, al manejar tanta información, una pequeña parte de toda ella sea alterada, es por ello que se toman diferentes contramedidas para evitar que se vea

comprometida su integridad, pero siendo tanta información ¿Cómo saber si ha sido o no alterada? Algunas de las soluciones que han ido surgiendo a tal necesidad se encuentran las siguientes:

- **Hash**: Son funciones o algoritmos que resultan en un conjunto de caracteres de una longitud determinada y es de un solo sentido, es decir que no se puede obtener la entrada original a partir del resultado, por lo que se usan para almacenar contraseñas de forma segura, si una pequeña parte del mensaje es alterada entonces el resultado cambia radicalmente. Son también usadas para saber si los datos se transmitieron correctamente. La probabilidad que 2 conjuntos de datos tengan como resultado el mismo resultado hash es prácticamente nula (Gómez Urgellés, 2010).
- **Arreglos redundantes de discos independientes**: Mejor conocido por su acrónimo RAID (*Redundant Array of Independent Disks*). Como el nombre sugiere es un conjunto de discos en el cual hay redundancia de datos, de esta forma al estar repetida la información hay garantía de poder recuperar la información que se haya podido ver comprometida dentro del arreglo en caso que alguno de los discos falle. Hay algunas ventajas y desventajas en los diferentes tipos de arreglos RAID, entre las principales desventajas se encuentra que no se puede aprovechar al máximo la capacidad de almacenamiento de todos los discos del arreglo, menos en RAID 0 que no tiene redundancia. Entre las ventajas se encuentra que para que haya pérdida de información tienen que fallar más de un disco duro al mismo tiempo, dependiendo

del arreglo puede que para que haya pérdida tengan que fallar al menos tres unidades de almacenamiento simultáneamente como en el caso de RAID 6(cita).

- **Protocolos**: Otra de las contramedidas que se han implementado para prevenir la alteración y pérdida total o parcial de información, y así mantener su integridad y disponibilidad, es el funcionamiento de ciertos protocolos de transporte que verifican que los datos hayan llegado a su destino y que no hayan sido alterados en su trayecto.

Al implementar correctamente algunas de las soluciones antes mencionadas se puede asegurar que la información se encuentra inalterada y que se puede trabajar correctamente con ella sin preocupación.

IV. NECESIDAD GLOBAL DE LA SEGURIDAD INFORMÁTICA

Los riesgos relacionados a la información se pueden clasificar como accidentales o intencionales. Los crímenes computacionales son los intencionales, los cuales consisten en cualquier actividad criminal en donde sistemas computacionales o redes son usados como herramientas para el crimen, es decir, la violación de una ley o regulación siempre que involucre al menos una computadora como medio en todo o parte del proceso. Algunos tipos de crímenes computacionales son:

- Empresariales: Aquí se encuentran acciones como espionaje corporativo y el robo de propiedad intelectual.
- Por diversión: Hay personas que realizan crímenes sin fines lucrativos ni por una causa, solamente por diversión o pasatiempo.
- Molestar o descontentar empleados: Cuando se busca atacar a una empresa pero el ataque no se realiza directamente contra ella, sino a sus empleados con el fin de desestabilizarla.
- Ciberterrorismo: Son crímenes realizados por una causa, enviar un mensaje y/o causar terror por diferentes motivos. Varios actos de *hacktivismo* entran en esta categoría.
- Financieros: Son los crímenes enfocados hacia tarjetas de crédito y entidades financieras principalmente, como bancos y casas de cambio monetario.

- Personales: Cuando los crímenes tienen por objetivo atacar a una persona en específico por diversas razones, como el robo de identidad o campañas de desprestigio.

Cualquiera que sea el término empleado, ya sea *Gobernanza de la seguridad*, *Seguridad Cibernética* o *Seguridad de la información*, se refieren a todas las acciones destinadas a minimizar el riesgo al que es expuesta la información. Siempre hay riesgos, es prácticamente imposible estar completamente seguro contra las amenazas, hay que minimizarlos lo más que se pueda, siempre y cuando resulte conveniente. No es conveniente realizar una inversión en seguridad mayor al valor del activo que queremos proteger.

La seguridad de la información se basa en el modelo "Triada CIA", siendo el acrónimo en inglés de "Confidencialidad, Integridad y Disponibilidad" (*Confidentiality, Integrity and Availability*) (F. DeFranco, 2014).

- **Confidencialidad**: Se refiere a quién o qué tiene acceso a un material en específico y se puede ver claramente con la clasificación de la información. Con los datos personales se suele relacionar más fácilmente con la palabra *privacidad*. Una buena práctica para mantener la confidencialidad es la política del *Privilegio Mínimo*, en la cual solamente se puede acceder a los recursos necesarios para cumplir con las funciones que tiene que realizar además de un nivel de autorización. Un buen ejemplo de confidencialidad es el encriptado, ya que aunque la información sea robada no puede ser leída.

- **Integridad**: Hace referencia a la confiabilidad de los datos mismos, o de la máquina que los almacene y/o procese, ya que la integridad tanto de la máquina como de los datos puede ser comprometida. Hay diferentes métodos para verificar si los datos han cambiado, uno de ellos es el uso de “hashes”, y otro método puede ser verificar que se obtengan los mismos resultados usando los mismos procesos con los mismos insumos.
- **Disponibilidad**: Hace referencia a que los recursos o servicios se encuentren en condición de ser accedidos o usados. Tener un 100% de disponibilidad es imposible, así como eliminar el riesgo, por lo que muchas veces se dice que un recurso tiene por ejemplo “cuatro nueves” de disponibilidad o confiabilidad cuando se puede garantizar que estará disponible el 99.99% del tiempo (Latency analysis of systems with multiple interfaces for ultra-reliable M2M communication, 2016).

La clasificación de la información es más comúnmente referida cuando se discute sobre información militar o gubernamental, sin embargo, hay varias organizaciones que pueden usar sistemas de clasificación similares. El sistema de clasificación sirve para asegurar que la información es marcada de cierta forma que solo aquellos con el nivel apropiado de autorización pueden tener acceso a la información, adicionalmente en algunos casos junto con la necesidad de saber. La norma ISO 27001, que trata sistemas de gestión de la seguridad de la información, no define niveles de clasificación sino que cada empresa o persona define los niveles que le resulten convenientes con base en las necesidades específicas de cada caso (International Organization for Standardization,

International Electrotechnical Commission, 2013). Un ejemplo de una clasificación es el siguiente:

- **Ultra secreto**: Su divulgación puede resultar en daño excepcionalmente grave a la seguridad nacional o internacional. Ejemplos incluyen datos de inteligencia militar vital, llaves criptográficas usadas para proteger comunicaciones y diseños detallados de armas.
- **Secreto**: Su divulgación puede dañar seriamente la seguridad nacional. Ejemplos incluyen inteligencia significante, planos militares, desarrollo técnico y estrategias diplomáticas.
- **Confidencial**: Su divulgación puede causar daños a la seguridad nacional. Ejemplos incluyen pruebas de fuerza militar, datos de rendimiento, entrenamiento técnico y documentos de operaciones.
- **Sensible pero no clasificada**: Información que no es clasificada como ultra secreta, secreta o confidencial pero su divulgación es aún restringida para proteger intereses nacionales.
- **No clasificada**: Esta información está en general disponible públicamente como resultado de la estrategia de la *Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura* (UNESCO, 2007), a pesar de que clasificaciones especiales, como *no clasificado solo para fuerzas de la ley*, puedan ser asignadas para restringir divulgación a ciertas organizaciones con la necesidad de saber.

IV.1 PERSONALES

La privacidad puede ser definida como los derechos y obligaciones de los individuos y organizaciones con respecto a la recolección, uso, retención y revelación de información personal, aunque la información personal es un concepto genérico y engloba cualquier información que sea acerca de un individuo identificable.

La privacidad es un asunto serio ya que mucha información puede ser revelada si no se protege correctamente, principalmente si no se le otorga la importancia debida. Accidentalmente se puede revelar información identificable personalmente como nombres, direcciones, números telefónicos, ingresos, familiares, trabajo actual, trabajos anteriores, relaciones personales, números de seguridad social, cuentas bancarias y muchas cosas más que pueden ser usadas con fines maliciosos.

La política de privacidad dice qué pueden hacer con la información personal, por eso es importante que se preste atención a los términos y condiciones que se aceptan al realizar diferentes actividades como por ejemplo crear una cuenta y llenar un formulario en una página en internet.

Para reducir los riesgos contra la privacidad como usuarios se puede tener en cuenta algunos puntos importantes, como son las buenas costumbres, que son acciones que se hacen o evitan hacer para no comprometer la seguridad. Unos ejemplos de buenas costumbres son: No revelar contraseñas, revisar las políticas de privacidad, verificar la autenticidad de las páginas de internet que se visitan, no instalar cualquier programa desconocido en nuestros dispositivos, usar redes virtuales privadas, revisar y configurar

los parámetros de privacidad de las cuentas de redes sociales a conveniencia, tener respaldada la información, y tener encriptados los archivos y dispositivos. Cada individuo decide qué costumbres adoptar y seguir para proteger su privacidad.

IV.2 EMPRESARIALES

Cuando se habla de la protección de información empresarial la complejidad de las contramedidas a los posibles riesgos y amenazas aumenta considerablemente, sobre todo por los ataques directos que sufren contra su información con malas intenciones. Las necesidades de cada organización pueden diferir mucho entre ellas, pero en general casi siempre se pueden encontrar las siguientes:

- **Políticas**: Las políticas son documentos que indican qué se debe hacer bajo diferentes circunstancias. Varía mucho dependiendo de las necesidades de la organización y cómo se haya decidido su estructura. Pueden ser tan sencillas y reducidas que no alcancen a llenar una página, también pueden ser tan complejas y exhaustivas que sobrepasen las 100 páginas. En ellas se pueden encontrar por ejemplo la periodicidad y el método usado para obtener respaldos de información específica que se maneje. También se puede encontrar si un individuo ajeno a la organización puede entrar en las instalaciones, bajo qué condiciones, si debe llevar un gafete, escolta y demás.
- **Buenas costumbres y capacitación**: Las acciones de cada individuo afectan a toda la organización, por lo que hay que tener la seguridad que los riesgos relacionados con cada uno de los empleados sea el mínimo posible, es por ello que no siempre se

puede confiar en las buenas costumbres de cada uno y hay que capacitar al personal, desde simples pláticas de concientización hasta cursos sobre el manejo de software necesario para mantener segura la información, como pueden ser aplicaciones de encriptado de archivos.

- **Software antimalware**: Una organización debe tener la seguridad que la información que maneja y almacena no se vea comprometida en confidencialidad, integridad ni en disponibilidad, algo que puede resultar de alguna pieza de software malicioso. Una empresa maneja diferentes tipos de información dependiendo de sus actividades, en muchos casos manejan información identificable personalmente tanto de sus empleados como de sus clientes, independientemente de la información relacionada a su giro de negocio.
- **Hardware especializado**: En empresas en donde la seguridad por software resulte insuficiente para conseguir el nivel de seguridad deseado, es necesario la implementación de dispositivos diseñados específicamente para la protección de la información por medios computacionales.
- **Personal especializado**: Son personas con un conocimiento profundo sobre las amenazas y vulnerabilidades de las empresas que buscan mejorar continuamente la seguridad al evaluar los bienes de la empresa, analizar y calificar los riesgos posibles, asignar y aceptar los riesgos residuales y aceptables mediante la implementación de diferentes contramedidas de diferentes tipos, la evaluación de esas contramedidas,

el monitoreo y medición de los procesos empresariales, y la mejora continua de la seguridad.

V. FUENTES DE AMENAZA PARA UN SISTEMA DE INFORMACIÓN GEOGRÁFICA

En todo sistema de información se encuentran diferentes orígenes potenciales de una gran cantidad de amenazas diferentes que en cualquier momento que se analice tienen la posibilidad de poner en riesgo la confidencialidad, la integridad y/o la disponibilidad de la información, ya sea que tengan una probabilidad muy alta de afectarla o una extremadamente baja.

V.1 TIPOS DE AMENAZAS

Las amenazas pueden ser de diferentes naturalezas, y no necesariamente implican que alguien esté realizando acciones con intenciones maliciosas. Las fuentes de amenaza pueden ser de tipo humano, natural, fallas en los sistemas de información y actividades maliciosas (AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN, 2007).

- **Humanas**: Dentro de las fuentes humanas se encuentra la gente, ya sea que busquen intencionalmente causar daño o que terminen representando una amenaza por los errores que puedan cometer. Dentro de las personas se puede encontrar gente maliciosa tanto interna como externa a la empresa, terroristas, saboteadores, factores políticos o competitivos, pérdida de personal clave, manifestaciones violentas, errores cometidos por intervención humana y problemas culturales, entre otros.

- **Naturales**: Aquí se encuentra la posibilidad que un fenómeno de la naturaleza pueda afectar a la infraestructura informática. Dependiendo de las condiciones del lugar en que se encuentre, aquí se pueden mencionar fenómenos como incendios, inundaciones, tornados, huracanes, ciclones, tormentas de nieve, tormentas eléctricas, sismos e inclusive la posibilidad que caiga un meteorito. Puede que a algunos les suene absurdo contemplar la posibilidad que un cuerpo del espacio destruya las instalaciones, y la información dentro, al caer en la Tierra, pero es un claro ejemplo de un riesgo que en la mayoría de las ocasiones se decidirá aceptar, o puede que sea solucionado junto con otros peligros al hacer respaldos y almacenarlos en otro sitio.

- **Fallas en los sistemas de información**: Cualquier cosa en el sistema que pueda dejar de funcionar correctamente se encuentra aquí, como por ejemplo las fallas de hardware, fallas de software, una cámara rota del sistema de circuito cerrado de televisión, una pieza mal atornillada, un candado o una cerradura que no sea del nivel de seguridad que se necesite, una puerta que no sea lo suficientemente resistente o que se encuentre abierta, falla en el sistema de respaldos.

- **Actividades maliciosas**: se encuentra aquí el código malicioso, el cual tiene una amplia variedad de tipos y consecuencias, algunos ejemplos pueden ser la disminución del rendimiento de una máquina, robo de información tanto

empresarial como personalmente identificable, pérdida de información y la indisponibilidad temporal o permanente de varios componentes computacionales de una infraestructura empresarial.

V.2 CRÍMENES

Hay diferentes crímenes de los cuales se puede ser objetivo, algunos de ellos existen desde hace casi 4000 años, actualmente aún son motivo de cuidado y pueden ser mitigados mediante controles administrativos, técnicos y físicos. Entre estos crímenes se pueden encontrar los siguientes: Robo, fraude, sabotaje, chantaje, espionaje industrial, revelación no autorizada, ataques remotos por conductos cibernéticos, pérdida de credibilidad (campañas de desprestigio), pérdida de información propietaria, y repercusiones legales (O'Hara, y otros, 2016).

V.3 PERPETRADORES

Cuando una persona es responsable de alguna ofensa contra la seguridad de los bienes de una organización o individuo. Hackers, crackers, *script kiddies*, traición de empleados, error de hacker ético, terceros, ignorancia. A grandes rasgos se pueden definir de la siguiente forma (O'Hara, y otros, 2016):

- ***Hackers***: Un *hacker* puede ser tanto un programador computacional que puede crear programas computacionales que antes no existían, o un

individuo que desea entrar en una red, tomar control de ella y dañar o desacreditar procesos computacionales legítimos. En el caso de la segunda definición su primer objetivo es exceder el nivel autorizado de los privilegios en el sistema, pueden ser individuos internos o externos a la organización.

- ***Crackers***: Este término es en ocasiones usado para diferenciar a los *hackers* mal intencionados de los que no lo son, aunque muchas veces se usan los términos indiscriminadamente. Un *cracker* busca irrumpir en un sistema sin previa autorización de forma ilegal y no ética.
- ***Script kiddies***: Son individuos que buscan hackear usando programas y herramientas programadas por otros. No necesariamente tienen conocimientos avanzados de seguridad.
- **Traición de empleados**: Son individuos de adentro de la organización y tienen más acceso y oportunidad que alguien de fuera, por lo que es importante monitorear la satisfacción interna de los empleados.
- **Error de hacker ético**: Un hacker ético es aquel autorizado a probar la seguridad de los equipos con el fin de identificar las fallas en la seguridad. Es posible que en este proceso se termine comprometiendo la seguridad de la organización o los bienes de la misma.
- **Terceros**: Son personas externas a la organización, incluye visitantes, proveedores, consultores, personal de mantenimiento y demás. Estos

individuos pueden obtener información del interior de la organización. Lo mínimo recomendable es supervisión directa de los terceros por parte de un empleado de confianza.

- **Ignorancia**: Un individuo con falta de conocimiento puede resultar ser parte de un crimen o de un incidente sin siquiera conocer los resultados de sus acciones. La ignorancia puede ser combatida mediante la capacitación en diferentes áreas internas de la organización y de esta forma reducir el riesgo en general.

V.4 MÉTODOS DE ATAQUE

Básicamente hay dos tipos de ataques: activos o pasivos (O'Hara, y otros, 2016).

- **Ataques pasivos:** Son ataques que se caracterizan por ser técnicas de observación. Lo que buscan es obtener más información acerca de la red. Algunos ejemplos son análisis de la red, análisis del tráfico de una sola máquina y el espionaje de los datos transmitidos.
- **Ataques activos:** Los ataques pasivos son más fáciles de detectar que los ataques pasivos, ya que implican realizar una acción que causa una alteración en el procesamiento normal de la información. Algunos ejemplos de tipos de ataques pasivos incluyen: Pruebas de penetración, ingeniería social, *phishing* y revisar la basura.

VI. NECESIDADES DE LA SEGURIDAD INFORMÁTICA EN LA INGENIERÍA GEOMÁTICA

La Ingeniería Geomática está basada principalmente en la información, en los procesos a los cuales es sometida esa información, las herramientas con las cuales es procesada y la aplicación correcta de los resultados Para poder identificar con mayor facilidad las posibles amenazas en un conjunto de procesos y procedimientos es necesario estar familiarizado con ellos, y de esta forma poder implementar contramedidas para minimizar la probabilidad que sucedan incidentes, o en su defecto mitigar las consecuencias. Tratar de implementar contramedidas en procesos y procedimientos que nos resultan desconocidos puede resultar ser algo escabroso.

VI.1 POSIBLES AMENAZAS Y RIESGOS A LA INFORMACIÓN EN LA INGENIERÍA GEOMÁTICA

Toda pieza de información se encuentra en un riesgo constante tanto en su confidencialidad como en su integridad y su disponibilidad, y la información que es ocupada en la Ingeniería Geomática no se encuentra exenta a los riesgos, ya sea que pertenezcan a una o varias categorías de la clasificación de los riesgos antes mencionada. Es prácticamente imposible estar completamente seguro ante todas las posibles amenazas, y menos aún el poderlas exponer en este documento, por lo que solamente se mencionarán un par de casos con el fin de exponer algunos de los escenarios.

Casos:

Se presentan a continuación dos casos los cuales se escriben al texto tal y fueron presentados.

1. En varias ocasiones he visto consecuencias bastante desagradables, como pérdida de información, resultante de una pieza de software malicioso, ya sea un virus, gusano, troyano y/o *ransomware*. Una de esas ocasiones fue estudiando en la carrera realizando un trabajo en equipo con dos compañeros de la clase. En esa ocasión el proyecto era bastante importante y tuvimos la precaución de haber respaldado nuestro proyecto, que estábamos haciendo en computadora, en cuatro dispositivos diferentes, de los cuales dos eran ordenadores portátiles y dos eran unidades flash USB. Al trabajar en una computadora de la sala de cómputo de la División de Ingeniería Civil y Geomática se infectó una de las memorias con un malware, la cual posteriormente infectó a una de nuestras computadoras portátiles cuando íbamos a actualizar el resto de las copias a la versión más reciente y la computadora infectó a la otra memoria. La última de nuestras copias en la otra computadora afortunadamente no se vio afectada gracias a que la computadora contaba con un buen antimalware que detuvo la propagación. De cuatro copias de nuestros archivos se perdieron tres.

2. Otro caso que he visto en repetidas ocasiones es el uso de software de licencia sin contar con una licencia válida y el uso de programas diseñados para prevenir la detección del uso ilegal del software, lo cual conocemos más familiarmente por el nombre de *piratería de software*. Lo que gran parte de la gente desconoce

es que el uso de software sin licencia puede implicar un riesgo para la seguridad del usuario, ya que dentro de los programas empleados para prevenir la detección del uso ilegal del software se puede encontrar código malicioso, el cual en varias ocasiones el usuario decide ignorar pese a las alertas de su software antivirus, en caso que sea lo suficientemente bueno como para haberlo detectado, con tal de poder hacer uso de un software cuya licencia no puede o no quiere pagar por la razón que sea. Un ejemplo en concreto sobre el problema de usar *software* pirata lo podemos encontrar en el software ENVI 5.3 de *Harris Geospatial*, que he visto ser usado sin licencia un gran número de ocasiones, ya que al no contar con una licencia no recibe las actualizaciones de seguridad contra las vulnerabilidades que han sido descubiertas, como es el caso de la vulnerabilidad CVE-2015-8277 (National Institute of Standards and Technology, 2016), presente en la tecnología de *Flexera FlexNet Publisher* usada en los productos de software IDL y ENVI (HARRIS GEOSPATIAL SOLUTIONS), la cual tiene la calificación más alta en severidad obteniendo un 10.0 de un máximo de 10.0 en algunas bases de datos sobre vulnerabilidades ya que implica un impacto completo a la confidencialidad, a la integridad y a la disponibilidad de los archivos en el sistema y toda la información que contengan, la explotación de esta vulnerabilidad tiene una complejidad baja ya que no necesita condiciones específicas ni conocimientos y habilidades avanzadas para explotar esta vulnerabilidad, solamente que se encuentre el software ENVI en su versión 5.3 o

IDL sin haber recibido la actualización de seguridad como sucede con el *software* pirateado. Tampoco se necesita ningún método de autenticación como podría ser el tener que iniciar sesión con usuario y contraseña, y además esta vulnerabilidad puede ser explotada a través de la red sin tener acceso físico directo a la máquina objetivo (CVE Details, 2016).

VI.2 NECESIDAD DE CAPACITACIÓN EN SEGURIDAD

Ya sea en el ámbito profesional como en el personal todos necesitan tener cierta conciencia acerca de las buenas prácticas de seguridad, de las cuales una gran parte pueden ser deducidas por sentido común al analizar con suficiente escrutinio los diferentes elementos involucrados en el activo o en el proceso que se quiera proteger, algo que normalmente no es realizado por la falta de costumbre o conciencia. Otra parte de las buenas prácticas de seguridad puede ser no tan evidente por diferentes razones, ya sea porque para ello se ocupan herramientas especializadas que son generalmente desconocidas para la población en general, o porque necesitan tener un punto de vista diferente.

Para poder prevenir y detectar las amenazas que puedan comprometer la información, archivos, procesos y demás, es necesario saber qué es normal y qué no lo es dentro de lo que se desea proteger. Entre los diferentes puntos a los que se pueden prestar atención se encuentran los tipos de archivos que se usen en el medio en que se labore (como dwg, csv, xlsx, docx), cuánto almacenamiento deben consumir, el tráfico de datos en la red (IP, HTTP, HTTPS, SMTP, FTP, SNMP), los puertos usados por las

aplicaciones y programas que ocupemos (80, 443, 123, etc.), qué programas son usados y necesitados, la cantidad de recursos que consumen los programas, qué procesos y servicios usan los programas, y los equipos que estén conectados en la red local (direcciones MAC, IP).

Una vez identificado qué es normal en nuestra red se puede restringir más fácilmente de antemano, o al menos detectar más rápidamente, cualquier actividad anómala. Al evitar las actividades anómalas se está reduciendo considerablemente los riesgos, ya que solamente sucederán cosas que se sabe que no resultan perjudiciales a los bienes de la empresa, en el caso de no poder evitar de antemano las anomalías, pero se puedan detectar rápidamente entonces se pueden comenzar a realizar las medidas necesarias para poder detener la actividad potencialmente peligrosa y detener cualquier incidente antes que llegue a afectar de forma severa.

Las vulnerabilidades no siempre son las mismas, algunas dejan de ser un riesgo potencial con el paso del tiempo, como son las correcciones en actualizaciones. Algunas otras amenazas están siempre presentes, como la ingeniería social y robos de identidad, y siempre habrá nuevos peligros. Con cada elemento que se agregue a la infraestructura se añaden posibles fallas y vulnerabilidades, las cuales pueden ser conocidas de antemano pero hay algunas que no las conocen ni los mismos desarrolladores, quienes conforme las vayan conociendo las corrigen en las posteriores actualizaciones. Habrá vulnerabilidades que no puedan ser corregidas mediante una actualización, en esos casos se tendrán que

implementar contramedidas adicionales para que esa vulnerabilidad no pueda ser explotada, y de esa forma dejar de ser un riesgo.

VII. SOLUCIONES ANTE POSIBLES AMENAZAS A LA INFORMACIÓN

Existen diferentes controles de acceso que pueden ser aplicados en 3 aspectos diferentes: administrativo, físico o lógico/técnico, también conocidos como controles técnicos de acceso. Los controles de acceso defensivos se pueden clasificar en: Preventivos, detectivos, correctivos, disuasorios, directivos, recuperativos y compensativos (Conrad, y otros, 2012). Algunos controles de acceso pueden entrar en varias categorías dentro de esta clasificación, y son aplicados dependiendo de la naturaleza del incidente ya que algunos controles pueden resultar inefectivos contra ciertos incidentes mientras que resuelvan completamente otros con una naturaleza completamente diferente.

VII.1 PREVENCIÓN

Los controles de acceso preventivos son desplegados para evitar o detener actividad no deseada o no autorizada desde antes que llegue a suceder y así evitar el tener que lidiar con el problema y todo lo que conlleve. Algunos ejemplos de este tipo de control de acceso son: rejas, candados, biométricas, puertas dobles, iluminación, sistemas de alarma, separación de deberes, rotación de trabajos, clasificación de datos, pruebas de penetración, encriptado, auditorías, instalar cámaras de vigilancia, tarjetas de proximidad, políticas de seguridad, procedimientos de marcar de vuelta a ciertas llamadas telefónicas,

capacitación de conciencia de seguridad, software antimalware, cortafuegos y sistemas de prevención de intrusos.

VII.2 DETECCIÓN

Los controles de acceso detectivos son puestos para descubrir y detectar actividad no deseada o no autorizada una vez que sucedieron o en el momento que están sucediendo, una vez identificada la actividad es más fácil tomar medidas al respecto. Unos ejemplos son guardias de seguridad, detectores de movimiento, el monitoreo en vivo mediante cámaras de seguridad, la revisión de las grabaciones de cámaras de seguridad, rotación de trabajo, vacaciones obligatorias para que cierto personal potencialmente malicioso no obstruya ciertas revisiones, auditorías, *honeypots* y *honeynets*, sistemas de detección de intrusos, reportes, supervisión y revisión de usuarios, e investigación de incidentes.

VII.3 CORRECCIÓN

Los controles de acceso correctivos suceden una vez que una actividad no deseada o no autorizada fue realizada, lo que hacen los controles correctivos es modificar la situación resultante del incidente a un estado deseado nuevamente, resolver los problemas que haya causado y que el ambiente regrese a la normalidad. Algunos ejemplos de controles correctivos pueden ser terminar la actividad no deseada o no autorizada, remover un elemento malicioso, reiniciar un servidor que se comporta anormalmente, cargar de nuevo la configuración desde un archivo, suspensión de labores de un empleado

problemático, y sistemas de detección de intrusos que al momento de detección detengan el ataque en proceso.

VII.4 DISUACIÓN

Los controles de acceso disuasorios están pensados para que al ser desplegados desanimen las intenciones de realizar una actividad no deseada o no autorizada. Puede que no representen en sí un verdadero obstáculo a hacerlo, en ello radica la diferencia con los controles de acceso preventivos ya que los preventivos al tratar de bloquear la actividad representan un obstáculo real, aunque algunos controles preventivos pueden ser a su vez disuadir las intenciones de realizar una actividad. Un ejemplo de un control preventivo que no disuada es una puerta oculta ya que previene el acceso no deseado o no autorizado sin tener que disuadir las intenciones de abrirla, mientras que un ejemplo de un control completamente disuasorio puede ser poner alambres a forma de una cerca con un letrero que diga *Precaución: 200'000 Volts*, dando la impresión que es una cerca electrificada, al inducir corriente a los alambres pasa a ser un control preventivo y disuasorio. Otros ejemplos pueden ser guardias, candados, letreros, puertas dobles, cámaras de vigilancia funcionales o no funcionales, y dispositivos que prenden y apagan la luz a ciertas horas en lugares sin gente para dar la impresión que hay gente dentro.

VII.5 RECUPERACIÓN

Los controles recuperativos buscan reparar y restablecer actividades, funciones y/o recursos de diferente naturaleza, como pueden ser recursos humanos, recursos informáticos, recursos financieros, etc., a su estado normal luego de un incidente de

seguridad. Los controles de recuperación son una extensión de los controles correctivos ya que un control recuperativo está recobrando algo consecuente a un incidente, mientras que un control correctivo no necesariamente está siendo recuperativo. Algunos ejemplos de controles recuperativos son rescatar información de un disco dañado mediante trabajo forense, restablecer documentos borrados en un ordenador, conseguir información de un respaldo, volver a cargar una máquina virtual a partir de una copia de respaldo, y la sustitución de un disco duro defectuoso en un arreglo redundante de discos independientes.

VII.6 COMPENSACIÓN

Los controles compensativos son los últimos en ser utilizados ya que al necesitarlos significa que todos los demás tipos de controles han fallado en alguna manera. Pueden ser usados en adición o en lugar de otros controles. Un ejemplo típico de este tipo de controles es contratar los servicios de una empresa aseguradora que cubra los gastos en caso de ser víctimas de robo, desastre natural, accidentes laborales, siniestros, etc. Otro ejemplo puede ser que los clientes queden insatisfechos al adquirir un producto o servicio y se les ofrezca cambiar el producto por otro, aunque represente una pérdida cuantitativa al costar dinero se evita una pérdida cualitativa al mantener la reputación de la empresa gracias a la consecuente satisfacción del cliente.

VIII. LEGISLACIÓN

VIII.1 NORMATIVA INFORMÁTICA VIGENTE EN MÉXICO

Los datos personales, como números de teléfono, correo electrónico y dirección del domicilio, son un bien valioso para las personas propietarias de los mismos. Dentro de las empresas el tratamiento de la información, y los datos personales de los empleados y clientes tiene que realizarse de acuerdo a la *Ley Federal de Protección de Datos Personales en posesión de los particulares*, ya que toda empresa está obligada a proteger la información que tenga en posesión. En dicho documento se encuentra que un gran número de puntos mencionados en el presente documento están contemplados y tienen que ser cumplidos, de lo contrario hay riesgo de acusación por no proteger adecuadamente los datos personales, ir a juicio, pagar multa, compensaciones y posiblemente llegar al encarcelamiento (CALDERÓN HINOJOSA, 2010).

Otro documento oficial que trata sobre no intentar obtener información que no sea correspondiente a uno y la importancia de mantener segura la información, es el *Código Penal Federal Mexicano*, que trata el tema de la información, su obtención y divulgación, y sanciones en sus artículos 210 y 211 (CÁMARA DE DIPUTADOS DEL H.CONGRESO DE LA UNIÓN, 1931).

VIII.2 ESTÁNDARES INTERNACIONALES

Hay ciertos estándares que en principio no son obligatorios para un gran número de actividades. Algunas certificaciones tienen como requisito que se cumplan ciertos estándares para poder acreditar a una persona, empresa o proceso.

Una entidad respetada que cabe mencionar en cuanto a estándares es la *International Standard Organization* (ISO) cuyos estándares son reconocidos internacionalmente como una línea base para todo aquello que tengan contemplado en su amplia lista de estándares. Otras entidades enfocadas en seguridad de la información es la *Information Systems Audit and Control Association* (ISACA) y El Consejo Internacional de Consultores de Comercio Electrónico (EC-COUNCIL) quienes proporcionan diferentes certificaciones.

Los estándares y certificaciones son una garantía de la calidad del trabajo, otorga cierto prestigio a las empresas y los clientes seguridad en los productos o servicios certificados.

VIII.3 CONSECUENCIAS POR DIVULGACIÓN INDEBIDA

Como se mencionó anteriormente, los datos personales y la información son un activo importante en cualquier industria. Hay consecuencias si la información que se custodia es divulgada indebidamente por diferentes motivos, no solamente consecuencias legales, es muy probable que la reputación se vea afectada y la confianza que se haya tenido se pierda parcial o totalmente.

Lo primero que hay que hacer en caso de una fuga de información es buscar el problema, encontrarlo, corregirlo y aprender de ello para asegurar que no se vuelva a repetir.

Una forma de mitigar alguna fuga de información es compensar a los afectados de alguna forma para reducir su descontento. Entre las compensaciones que se pueden implementar está asegurar a los afectados por un tiempo determinado en caso que se haga mal uso de los datos que se hayan filtrado, compensación económica y uso gratuito de los servicios que la empresa proporcione.

IX. EJEMPLO PRÁCTICO

Se supone una empresa llamada *GeomáticEjemplo* desempeña varias labores de Ingeniería Geomática, ha crecido desde un pequeño grupo de personas hasta ser una organización de un tamaño considerable, y ahora necesita mejorar su infraestructura informática. Hay que tener en cuenta que entre más grande sea una empresa corre un mayor riesgo, tanto de una falla accidental como de ser el objetivo de un ataque dirigido, por lo que habrá ciertas cosas que tendrán que cambiar en cuanto a su forma de trabajar lo más pronto posible para que la transición sea lo más fácil posible. También es importante mencionar que procedimientos, circunstancias y líneas base tendrán que establecerse y registrarse formalmente dentro de políticas y manuales, mientras que habrá otras que puedan dejarse sin especificar permitiendo cierta libertad de decisión, al menos de momento, y puede que algunas de ellas posteriormente se tengan que formalizar si es que las necesidades de la empresa lo requieren conforme vaya evolucionando.

IX.1 SEGURIDAD ADMINISTRATIVA

La seguridad administrativa se refiere a las políticas de seguridad que guiarán dentro del proceso de seguridad, por lo que dentro de la empresa es lo primero que se comenzará a construir dependiendo de las necesidades específicas de *GeomáticEjemplo* y dentro de las políticas se plasmará todo lo contemplado dentro de la seguridad administrativa, seguridad física y seguridad lógica.

Para comenzar con las políticas se puede considerar que la empresa *GeomáticEjemplo* permite que los empleados traigan sus propios dispositivos a la empresa y los ocupen para sus labores profesionales. Entre los dispositivos que normalmente traen los empleados se encuentran teléfonos inteligentes, tabletas y ordenadores portátiles. Estos dispositivos están sujetos a diferentes riesgos incluyendo *malware*, robo y malfuncionamiento, poniendo en riesgo los recursos de la empresa que almacenen, es por ello que es recomendable que los recursos y actividades de la empresa estén y se realicen únicamente en equipos administrados por la misma, de esta forma se tiene un control centralizado sobre los dispositivos y se puede proteger la información de formas que no se implementarían de lo contrario. Los dispositivos de la empresa contarían con sistemas de encriptado usando contraseñas cuya resistencia a diferentes ataques sea elevada para proteger los bienes informáticos. También se pueden rastrear los dispositivos en caso de robo o extravío, y para cuando se crea necesario se pueden equipar con capacidades de eliminación remota para los casos en que se crea que el dispositivo no se puede recuperar, de esta manera se evita que la información sea accedida por gente ajena a la empresa y que no esté autorizada.

La información solamente debería ser accedida por quienes tengan la necesidad de usarla en sus actividades laborales mientras exista esa necesidad. Es completamente comprensible que el contador de la empresa necesite ver los libros de contaduría, mientras que sería sospechoso que el conserje quiera ver dichos libros en un aparente intento de espionaje corporativo, o que el cartógrafo quiera obtener los expedientes

correspondientes al personal femenino de la empresa. Para evitar el mal uso de la información se aplican los siguientes:

- **Necesidad de saber**: Proceso mediante el cual se identifica quiénes necesitan poder acceder a qué recursos y áreas de la empresa. Así se pueden crear diferentes grupos con los privilegios y las restricciones que se requieran.
- **Principio del privilegio mínimo**: Establece que las personas no deben tener más permisos de los necesarios para acceder a más de la información y recursos que necesitan para poder cumplir con sus tareas laborales, son permisos asignados individualmente. El privilegio mínimo es más granular que la *necesidad de saber*.
- **Separación de deberes**: nadie debería ser la única persona encargada de cumplir una tarea desde su principio hasta el final, esto con el fin de evitar la oportunidad de realizar fraudes dentro de la empresa.

Para no tener que estar asignando y revocando permisos a cada uno de los miembros del personal de forma individual dentro de la infraestructura lo que se hace es crear grupos dentro de los cuales se encuentra todo el personal. Un individuo puede pertenecer a uno o más grupos dependiendo de lo que necesite para desempeñar sus tareas. Puede que la empresa *GeomáticEjemplo* aún no sea lo suficientemente grande como para tener un gran número de grupos, pero sus expectativas de seguir creciendo son grandes, por lo que es recomendable comenzar a llevar este control ya que implementarlo luego que haya crecido puede llegar a ser complicado por el número de

empleados. Los permisos de acceso que puede comenzar a gestionar de una manera formal pueden ser los siguientes:

- 01 Áreas comunes
- 02 Artículos de limpieza
- 03 Salas de cómputo para el procesamiento de datos
- 04 Almacén (hojas, cartuchos de impresión, engrapadoras, cuadernos, etc.)
- 05 Bodega con equipo de campo
- 06 Llaves de entrada a las instalaciones
- 07 Sala de servidores
- 08 Archivos de recursos humanos
- 09 Archivos de los clientes
- 10 Libros de registros y contaduría
- 11 Oficinas de los directivos

En la tabla 1 se muestran los grupos con los que la empresa puede comenzar a gestionar los permisos del personal pueden ser los siguientes:

	PERMISOS										
RUPO	01	02	03	04	05	06	07	08	09	10	11
Directivos	X	X	X	X	X	X	X	X	X	X	X
Ing. Jefe	X	X	X	X	X	X					
Sistemas	X		X				X				
Contaduría	X								X	X	
RH	X							X			
Ingenieros	X		X								
Conserje	X	X									
Visitantes	X										

Tabla 1

La ausencia de algunos permisos de la tabla 1 no significa que el personal de conserjería únicamente podrá hacer el aseo en las áreas comunes, sino que realizará el aseo en áreas normalmente restringidas mientras haya al menos una persona correspondiente al área presente, por mencionar un ejemplo. Restringir los derechos no es por menospreciar al personal, el hecho de no poder acceder a un lugar o recurso lo libra de la responsabilidad o sospecha en caso que algo no deseado suceda en ese lugar o con ese recurso.

La seguridad de la información tiene que estar presente en todos los procesos para que funcione correctamente, ya que la información al final de cuentas se encuentra tan vulnerable como el momento en que se encuentre menos protegida a lo largo de todo su recorrido. A menudo se llega a olvidar que las mismas personas son parte de los procesos por los que pasan los datos con los que trabajamos, un aspecto fundamental para poder mantener seguros dichos datos es que todos los empleados de la empresa tengan conciencia sobre la seguridad de la información, ya que las personas como parte del proceso son igual de importantes que cualquier otro elemento involucrado, además que hablamos de vidas. Las personas deben ser vistas como el activo más valioso de la empresa, y al igual que otros activos se tienen que implementar medidas para protegerlas en caso de diferentes contingencias como pueden ser: incendios, temblores, asaltos y demás. Se deben verificar periódicamente los mecanismos contra incendios, las rutas de

evacuación, las condiciones de las instalaciones, que haya material de seguridad y prevención en los sitios adecuados y tratar de tener contemplado todo lo que pueda salir mal. En adición se tienen que hacer simulacros para corregir las fallas en este tipo de contingencias y realizar las modificaciones pertinentes en el plan de emergencia para que la vida de los empleados no sea comprometida por algún descuido.

IX.1.1 Conciencia y capacitación del personal

El primer paso es concientizar a todos los empleados involucrados a seguir las políticas establecidas y no saltase las políticas ni los procedimientos. Una falla en el proceso puede comprometer la seguridad y poner en riesgo toda la información dentro de la infraestructura, por mencionar un ejemplo puede estar el caso del empleado que use el equipo del trabajo para acceder a páginas de internet de dudosa reputación que puedan contener *ransomware*, y de un momento a otro su computadora se encuentre bloqueada, toda la información almacenada en ella esté encriptada y en el monitor haya un mensaje que diga algo similar a:

"Tu información está encriptada. Si quieres recibir la clave para poder revertir el proceso deposita $10'000ºº en bitcoins a la cartera […] antes de ser eliminados dentro de 72 horas y envía una captura de pantalla de la transacción a la dirección de correo […]. Una vez que hayamos confirmado la transacción te enviaremos la clave.

Te quedan 71 h 59 m 43 s

Ingrese su clave aquí: _____"

Si era el único lugar en donde se almacenaban los datos de un trabajo entonces toda la operación se detiene en lo que se resuelve ese problema bajo la amenaza de perder todo cuando el contador de la pantalla llegue a cero.

Otro ejemplo puede ser que en las políticas de seguridad de la información se establezca que al pasar los datos actualizados desde un disco duro portátil a una estación de trabajo se deba verificar la integridad de los mismos una vez copiados, un empleado decida ignorar ese paso teniendo en mente que no es necesario, borre la información del disco duro para tener más espacio para algo más y resulte que los progresos de varios días de trabajo no se copiaron correctamente, resultando en un retraso en el progreso del proyecto.

Todos los miembros de la empresa deberán recibir capacitación adecuada a sus responsabilidades laborales dentro de la empresa para proteger a la misma de las posibles amenazas ya sea por malicia, como en el primer ejemplo, ya sea por accidente, como en el segundo ejemplo; ya sea una amenaza interna o externa. Los empleados también deberían recibir capacitación relativa al trabajo de sus compañeros para evitar que en caso que alguno de los miembros de un equipo de trabajo tenga que ausentarse por un breve periodo de tiempo, entonces las labores no se vean necesariamente detenidas. Es decir, que ningún empleado sea completamente indispensable ya que si es el único que sabe realizar alguno de los pasos del proceso entonces el proyecto se encontraría detenido si ese individuo se encuentra indispuesto.

Dentro de las políticas que se desarrollan para la empresa *GeomáticEjemplo* se deben establecer lapsos de tiempo en los cuales se llevarán a cabo programas de conciencia y las capacitaciones pertinentes. Se debe asegurar que todos los miembros de la empresa estén familiarizados con las políticas y que las sigan correctamente.

IX.1.2 Revisiones y auditorías

La seguridad no es un producto sino un proceso, ya que para poder mantener segura una organización hay que revisar constantemente que no haya vulnerabilidades que puedan ser explotadas. Puede que en un momento las instalaciones de *GeomáticEjemplo* puedan ser consideradas seguras, y al siguiente día se haya vuelto pública una vulnerabilidad en un modelo de cerraduras que permite abrirlas usando algún ataque que requiera poca habilidad y que la empresa tiene instalada en un gran número de sus puertas. Además, que los mismos empleados internos encargados de la seguridad busquen periódicamente puntos débiles y posibles mejoras es necesario que se realicen auditorías hechas por una empresa externa, por lo que se llamará al menos una vez al año a los expertos auditores en seguridad miembros de la empresa *AuditoresEjemplo*. Esto con el fin de contar con un punto de vista diferente y experto al que le resulte más fácil encontrar cosas que nosotros como parte de la empresa auditada no veamos por diferentes razones. Puede que los empleados internos estén acostumbrados que al entrar al edificio se deje pasar a la persona que viene justo detrás de nosotros con el fin de ser amables, los auditores pueden encontrar que esa práctica es un riesgo de dejar entrar a un desconocido ajeno a la empresa mientras que los demás lo vean perfectamente

normal. También una empresa de auditoría externa como *AuditoresEjemplo* ayuda a la empresa al darle seguimiento a las fallas de seguridad por corregir y posibles mejoras que se puedan implementar.

Muchas personas al saber que la empresa o el área en que trabajan serán auditadas tienden a asustarse debido a una idea equivocada de lo que puede tratar la auditoría. Los auditores no son gente con malas intenciones cuyo fin sea el de dejarnos sin trabajo, sino que su trabajo consiste en comunicar las fallas en los procesos y procedimientos que se desempeñan en lo que se va a auditar y de esta forma se pueda hacer algo al respecto para corregirlos y así poder desempeñar mejor las labores de la empresa. Puede que los auditores encuentren ciertos indicios de actividades fraudulentas dentro de la empresa que sean realizadas por un pequeño número de los empleados buscando conseguir de forma ilegal más dinero para ellos. Puede que los empleados ya estén familiarizados con cómo revisan sus supervisores y por eso hayan sabido esconder sus actos criminales. Si un auditor, o equipo de auditoría, encuentra algo que deba ser notificado lo incluirá en su reporte que le entregará al encargado de nuestra empresa y la siguiente vez que regresen a hacer una nueva auditoría hagan seguimiento de los puntos encontrados en la auditoría pasada y den su visto bueno a las correcciones realizadas o sugerir alguna otra solución.

IX.2 SEGURIDAD FÍSICA

Para mantener segura la información hay que tener en cuenta el aspecto físico, que las personas solamente puedan acceder a los recursos o entrar a las habitaciones que tengan que entrar únicamente en el horario en el que tengan que entrar, no solamente

empleados sino también clientes y visitantes. Unas de las áreas que la empresa considera que no requiere prácticamente ninguna restricción de acceso es a los baños, el comedor y tal vez alguna sala de espera que estarían consideradas en las áreas comunes, mientras que unas de las áreas que no deberían poder ser accedidas fácilmente sin autorización son las oficinas de los directivos mientras ellos no se encuentren presentes, la sala de servidores, los archiveros de recursos humanos con la información personalmente identificable de todos los empleados, el cuarto con equipo de campo (como estaciones totales, teodolitos, antenas GPS, drones, tripiés y el resto del equipo con el que cuenta la empresa), y las máquinas con información de los proyectos y de los clientes. Dependiendo de lo que se quiera proteger será el nivel de seguridad que se implemente. Ya que no se necesita alta seguridad para mantener guardados los artículos de limpieza ni la papelería que se guarda en el almacén se pueden usar cerraduras de seguridad baja, ya que protegen artículos que no son demasiado valiosos y se tiene cierta confianza en el personal de la empresa que no va a intentar robarlos. En cambio las puertas que resguarden equipo valioso, como la sala de servidores, el equipo de campo y la puerta principal puede que cuenten con alguna cerradura resistente a ataques físicos de fuerza bruta, y cuyo mecanismo de apertura sea de alta seguridad.

IX.3 SEGURIDAD LÓGICA

La parte de seguridad lógica se refiere a la parte abstracta e impalpable de un sistema computacional. Dentro de esta seguridad se encuentra la arquitectura de la red, cortafuegos, antivirus, sistemas de detección de intrusos, contraseñas, certificados ssl,

arreglos RAID, respaldos periódicos automatizados y demás elementos que permiten mantener la información confidencial, íntegra y disponible contra diferentes amenazas, como pueden ser virus, gusanos, troyanos, *spyware*, *ransomware*, malfuncionamiento de las unidades de almacenamiento, eliminación accidental de archivos, intentos de acceso remoto no autorizado, y una larga lista que aumenta con el paso del tiempo.

En principio se diseña una arquitectura de red que proporcione una base estable sobre la cual se puede implementar correctamente diferentes medidas en la empresa actual y con la flexibilidad de adaptarse ante la posibilidad de un posterior crecimiento de la organización. Una arquitectura de red que cuente con una *Zona Desmilitarizada* (DMZ) permite un mayor control sobre la red contando con suficiente protección sobre las máquinas de la *Red de Área Local* (LAN) para evitar accesos desde Internet, los cuales no son necesarios, y dentro de la DMZ se colocan los servidores que necesitan ser accedidos desde Internet. Al tener ambas redes separadas, LAN y DMZ, se puede contener con mayor facilidad una posible infección y realizar las acciones necesarias para restablecer el control sobre la red con mayor facilidad teniendo que lidiar con un menor número de computadoras comprometidas.

Dentro de la DMZ se encuentran servidores que necesitan ser accedidos desde Internet. Algunos servicios que requieren de lo anterior son:

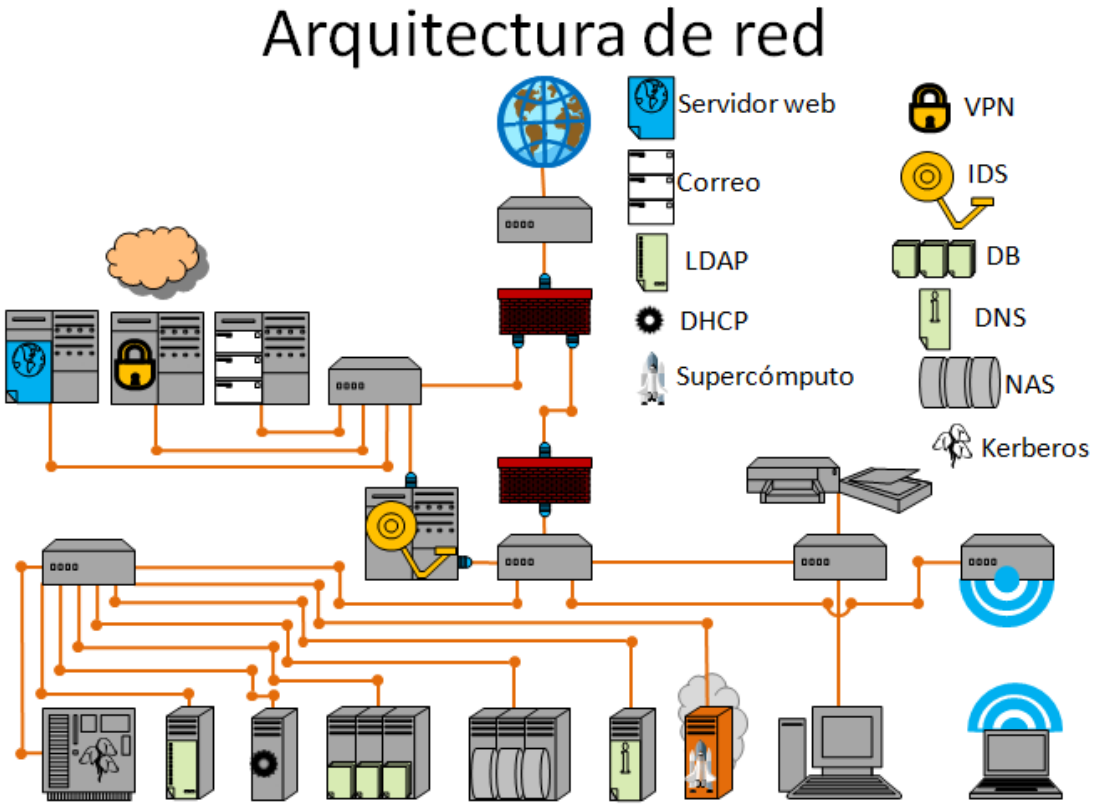
- Páginas web
- Red Privada Virtual (VPN)
- Correo electrónico

En la LAN se encuentran algunos otros elementos, como son:

- Servidor de autenticación de red Kerberos
- Servidor de Protocolo Ligero de Acceso a Directorios (LDAP)
- Servidor de Protocolo de Configuración Dinámica de Host (DHCP)
- Bases de datos
- Almacenamiento Conectado en Red (NAS)
- Servidor de Sistema de Nombres de Dominio (DNS)
- Unidades de supercómputo o de cómputo de alto rendimiento
- Computadoras de escritorio
- Puntos de Acceso (AP)
- Escáneres e impresoras conectadas a la red
- Otros dispositivos de red (teléfonos, tabletas, laptops, etc.)

Un caso especial que en esta propuesta se encuentra conectado tanto a la DMZ como a la LAN es el Sistema de Detección de Intrusos (IDS). En este caso el IDS se encontrará conectado a los conmutadores (mejor conocidos por su nombre en inglés *Switch*) en un puerto *espejo* de cada uno que se encargue de mandar una copia de todo el tráfico de la red al puerto que cada uno tenga asociado al IDS, ambas tarjetas de red del IDS no contarán con una dirección IP sino que se encontrarán únicamente en modo monitor, de esta forma solamente reciben sin poder transmitir y sin contar con la capacidad de ser detectadas por ningún otro dispositivo tanto en la DMZ como en la LAN. El IDS incluirá en sus registros cualquier actividad que pueda parecer sospechosa para su

posterior revisión periódica, la cual puede ser incluso en tiempo real, semanal, diario, etc. Pero para este caso será al iniciar las actividades los días lunes, miércoles y viernes para revisar los registros desde la última revisión hasta el último registro que haya en el momento de la revisión.



Todas las computadoras de escritorio y estaciones de trabajo que se encuentren en la red deberán contar con cuentas de usuario no administrativo para su uso regular, dichas cuentas y las cuentas de administrador, necesarias para cualquier cambio en la configuración del equipo e instalación de nuevo software, contarán con contraseñas resistentes a ataques, y además de las contraseñas contarán con certificados instalados

para su autenticación con otros equipos en la red con los cuales tengan que establecer alguna conexión. Es importante y recomendable que cada usuario conozca su contraseña, no la tenga anotada, no sea reciclada (usada para alguna otra cuenta o equipo) y que no la comparta con nadie. Otro elemento con el que contarán las computadoras de escritorio y estaciones de trabajo es con programas *antimalware*, el cual deberá ser usado para analizar al momento cualquier dispositivo que sea conectado, para analizar los sitios web a los que se acceda y los archivos descargados.

Hay puertos específicos que deberán estar abiertos en los cortafuegos para que se pueda acceder a ciertos servicios necesarios desde alguna de las redes hacia las otras (LAN, DMZ e Internet), y especificar para qué máquinas estarán abiertos, el resto de los puertos deberán estar cerrados para evitar tener una mayor superficie de la red expuesta. Para identificar qué puertos deberán estar abiertos hay que estar familiarizado con los programas y los servicios que estén corriendo en las redes.

Al tener un servidor de páginas web en la DMZ normalmente se tendría que permitir el paso del tráfico de datos desde Internet y desde la LAN hacia el servidor de páginas web, y las respuestas del servidor al cliente solicitante, en el puerto 80 para el protocolo HTTP y 443 para el tráfico HTTPS, a no ser que se configure el servidor para que los servicios sean accesibles usando otros puertos. Si se desea que ese mismo servidor de páginas web pueda ser administrado desde otra máquina dentro de la misma red local entonces se debe permitir el acceso al servidor en su puerto 22 para SSH, pero no se debe poder acceder desde el resto de Internet, por lo que se puede limitar el acceso a máquinas

con direcciones IP públicas que estén dentro de la misma administración y que correspondan a la misma tarjeta de red del cortafuegos correspondiente a la DMZ, y también a direcciones IP privadas que se ocupen en la red local, que podrían acceder usando la otra tarjeta de red que maneja el tráfico correspondiente a la red local.

Para Los otros servicios que se estén ejecutando en los servidores se tendrá que hacer lo mismo que con el servidor de páginas web pero usando los puertos correspondientes a los servicios que proporcionen. En el caso del servidor de correo electrónico se requieren más servicios disponibles, por lo que se necesitan tener más puertos abiertos. Para poder recibir los correos electrónicos desde internet necesita tener abierto el puerto de SMTP que es el puerto 25, para que los usuarios puedan acceder a los correos que les han llegado a sus cuentas de correo electrónico tiene que tener abierto el acceso a IMAP y/o POP3, que son los puertos 143 y 110 respectivamente. Si cuenta con interfaz web entonces también el acceso a HTTP y HTTPS. Siempre es preferible usar las versiones encriptadas de los protocolos que son SMTPS (puerto 465), IMAPS (puerto 993) y POP3S (puerto 995). En el caso del servidor de VPN que use el protocolo IPsec se tienen que tener abiertos los puertos 1293, 500 y 4500.

Los servidores también necesitan iniciar conexiones con otros servidores, como son NTP (puerto 123), DNS (puerto 53) y SQL (puerto 156), los cuales se deben permitir siempre y cuando la solicitud provenga de la DMZ hacia servidores confiables de Internet o de la LAN. Si en la DMZ no se tiene ningún servidor de NTP o de DNS disponible para el

público en general entonces cualquier solicitud a los puertos 123 o 53 proveniente de Internet hacia nuestra red debe ser bloqueada.

Las interacciones entre la red local y la zona desmilitarizada tendrán en el cortafuegos una configuración bastante similar a la que haya entre la zona desmilitarizada e Internet, salvo las conexiones para administración de los servidores. Sin embargo hay que considerar las conexiones entre los dispositivos en la misma red local, ya que dentro de la misma hay servidores (como Kerberos, DHCP, LDAP y DNS) y otros dispositivos a los cuales los usuarios se conectarán desde otras máquinas (como NAS y posiblemente a máquinas de alto rendimiento). Estas regulaciones estarán aplicadas por el cortafuegos que se encuentra entre la red local y el cortafuegos que se conecta a Internet. Para empezar todas las conexiones con Internet deberían iniciar en la red local, por lo que cualquier intento de conexión que inicie desde Internet deberá ser bloqueado. En principio solamente debería haber interacciones entre las estaciones de trabajo y máquinas específicas, todos los demás intentos de conexión deberán ser detenidos.

Además de regular las interacciones entre dispositivos de la red local, se puede implementar un control de aplicaciones, el cual impide el paso de los paquetes de datos cuando se detecte que es generado por alguna aplicación cuyo uso se desea restringir por diferentes motivos, incluyendo la posibilidad que resulte en una distracción para los empleados de la organización, como pueden ser juegos de video que dependan de interacciones en internet, páginas web de entretenimiento y aplicaciones de redes sociales.

Antes de iniciar actividades normales en la empresa se tendrá que poner a prueba la red para probar que no se puedan realizar actividades maliciosas y también para verificar que las actividades autorizadas puedan realizarse sin que la seguridad implementada represente un obstáculo, si hay alguna actividad que no se pueda realizar como debiera entonces se deberán revisar los registros de los dispositivos de seguridad para encontrar en dónde están siendo filtrados los paquetes de datos y por qué. Puede que se esté intentando hacer uso de algún servicio que no se haya contemplado inicialmente y el puerto esté cerrado, que se necesite algún protocolo que no se sabía que se necesitaba, que alguna aplicación haga uso de algún servicio de una página que se haya restringido en el control de aplicaciones, o que se deba a muchas otras causas que se descubrirán al revisar los registros. Al identificar por qué las cosas no funcionan normalmente se podrán agregar, quitar o modificar reglas del cortafuegos, añadir excepciones al filtro de contenido, crear listas blancas de dispositivos, o lo que sea necesario realizar para no obstaculizar las actividades organizacionales.

IX.4 POLÍTICAS DE SEGURIDAD

Una vez planteadas las necesidades específicas en cuanto a la seguridad administrativa, la física y la lógica sólo queda plasmarlas formal y ordenadamente en un documento de políticas. Estas políticas iniciales resultantes no son definitivas y tendrán que irse modificando para acoplarse a las necesidades de seguridad de la empresa sin obstruir el trabajo ni entrar en conflicto con los objetivos de la empresa.

Las políticas de seguridad iniciales resultantes de este ejemplo son:

- Toda persona que trabaje en la empresa deberá ser fácilmente identificable.
- Toda persona que no trabaje en las instalaciones deberá estar en todo momento pertinente acompañado por personal de la empresa.
- No se permitirá el acceso a las instalaciones a personal desconocido si existe la menor duda de su identidad. Se deberá identificar como empleado de la empresa antes de permitirle el paso.
- Los activos de la empresa (incluyendo equipo, documentos e información) serán únicamente accedidos por el personal con la autoridad y necesidad de hacerlo.
- Todo el personal contará con las llaves correspondientes a las áreas que están autorizados a entrar, y bajo ninguna circunstancia ordinaria compartirá sus llaves con personal no autorizado a entrar a las mismas áreas.
- En caso que un juego de llaves sea extraviado o haya sospecha que ha sido comprometido se procederá a cambiar la combinación de todas las cerraduras que puedan estar comprometidas. Una vez realizado el cambio se verificará que todos los juegos de llaves puedan abrir correctamente las puertas que les corresponden.
- El personal participará en programas de capacitación y concientización sobre seguridad al ingresar a la empresa. Posteriormente se revisarán sus conocimientos respecto al tema cada 6 meses para mantener sus capacidades.
- Se realizarán simulacros de evacuación de las instalaciones cada 3 meses y se verificarán los tiempos de evacuación, el correcto funcionamiento de las salidas de emergencia y las condiciones de los extintores de incendios.

- Las puertas correspondientes a la entrada principal y a las habitaciones en donde se guarden activos valiosos (equipo costoso e información personal) deberán ser sólidas y resistentes a ataques físicos al igual que sus cerraduras. Las cerraduras además deberán ser resistentes a ganzuado u otro tipo de violación.
- La estructura de la red contará con 2 dispositivos cortafuegos en serie, una zona desmilitarizada en la que se encuentren los equipos accesibles desde Internet y una red de área local en la que se encontrará el equipo que no sea accesible desde internet.
- Los equipos cuyo software no cuente con funciones de actualización automática, y dicha función no pueda ser implementada, se actualizarán manualmente una vez por mes o antes de ser necesario, como en el caso que exista una actualización importante.
- Los registros del sistema de detección de intrusos se examinarán, desde el registro más antiguo sin revisar, en búsqueda de actividad sospechosa los días lunes, miércoles y viernes, al momento de iniciar actividades laborales en los días mencionados.
- Los datos y archivos sobre los trabajos que no requieran estar almacenados localmente en las computadoras y estaciones de trabajo serán almacenados en el servidor de almacenamiento conectado en red para su resguardo.

- Toda actividad relativa al trabajo se realizará en equipo de la empresa mientras sea posible. En caso que se necesite acceder remotamente se hará uso de la red privada virtual para asegurar la confidencialidad de la comunicación.
- Todo archivo y unidad de almacenamiento que sea conectado a equipo de la empresa deberá ser analizado con software antimalware antes de ser usado.

Como se puede apreciar, en las políticas resultantes no se contemplan todos y cada uno de los escenarios que pueden ocurrir y habrá momentos en los que haya que tomar decisiones con base en los diferentes factores que puedan estar involucrados en cada caso específico. Las políticas anteriores son el primer modelo de políticas para una empresa que las irá modificando con base en las necesidades que vayan surgiendo.

En cuanto a las actividades de seguridad de la información al hacer mediciones de campo, las podemos considerar dentro de las buenas costumbres, y por ello no es necesario incluirlas explícitamente en las políticas, a no ser que por ciertas circunstancias futuras se considere oportuno incluirlas.

X. CONSLUSIONES

La seguridad es un elemento muy importante en diferentes aspectos dentro de la vida cotidiana tanto personal como laboralmente. A pesar de su importancia no todas las personas tienen conciencia de ella y gran parte de sus tareas son realizadas sin tener en cuenta qué puede salir mal, siendo eso un riesgo desde su vida personal hasta llegar a las empresas en que laboren. Mantener el bienestar de una organización es un trabajo de todos, y aunque hay ciertas cosas que cada individuo debe tener en cuenta y llevar a cabo para lograrlo hay temas que no están obligados a saber, sino que es trabajo de un especialista ir más allá y guiar a los demás miembros de la compañía adecuadamente sin obstaculizar los objetivos principales de la misma.

Para que alguien dedicado a la seguridad pueda implementar contramedidas a los riesgos potenciales en un área de trabajo es importante que cuente con conocimientos acerca del área. Es necesario conocer lo que se quiere proteger y cómo funciona para no terminar obstaculizando los procesos que necesita en un intento de mantenerlo seguro.

Bibliografía

AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN. **Tarazona T., César H. 2007.** 84, Colombia : Universidad Externado de Colombia, 04 de 08 de 2007, Vol. 28. https://revistas.uexternado.edu.co/index.php/derpen/article/view/965.

B. Galindo, Aldon Cris. 2017. *Information Security: Principles and Practices.* New York : Delve Publishing LLC, 2017.

Berné Valero, José Luis, Anquela Julián, Ana Belén y Garrido Villén, Natalia. 2014. *GNSS. GPS: fundamentos y aplicaciones en Geomática.* Primera. Valencia : Universitat Politècnica de València, 2014. Vol. I.

CALDERÓN HINOJOSA, FELIPE DE JESÚS. 2010. *LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES.* México : s.n., 2010. http://stcs.senado.gob.mx/docs/08.pdf.

CÁMARA DE DIPUTADOS DEL H.CONGRESO DE LA UNIÓN. 1931. *CÓDIGO PENAL FEDERAL.* DOF 17-06-2016. México : s.n., 1931. http://www.ssp.df.gob.mx/TransparenciaSSP/sitio_sspdf/art_14/fraccion_i/normatividad_aplicable/54.pdf.

Conrad, Eric, Misenar, Seth y Feldman, Joshua. 2012. *CISSP Study Guide.* Segunda edición. Waltham : Syngress, 2012. págs. 27-29. https://books.google.com.mx/books?id=8DvPN8FKQbkC&printsec=frontcover&hl=es#v=onepage&q&f=false. ISBN: 978-1-59749-961-3.

CVE Details. 2016. CVE Details. [En línea] 23 de 02 de 2016. [Citado el: 17 de 04 de 2018.] https://web.archive.org/web/20180417150406/https:/www.cvedetails.com/cve/CVE-2015-8277/. https://www.cvedetails.com/cve/CVE-2015-8277/.

F. DeFranco, Joanna. 2014. *What Every Engineer Should Know About Cyber Security and Digital Forensics.* NW : Taylor & Francis Group, 2014.

Facultad de Ingeniría. 2018. Facultad de Ingeniría / Ingeniría Geomática. [En línea] 2018. [Citado el: 16 de Marzo de 2018.] https://web.archive.org/web/20180316054018/http://www.ingenieria.unam.mx:80/programas_academicos/licenciatura/geomatica.php. http://www.ingenieria.unam.mx:80/programas_academicos/licenciatura/geomatica.php.

Gómez Urgellés, Joan. 2010. *Matemáticos, espías y piratas informáticos: Codificación y criptografía.* Barcelona : RBA Editores, 2010.

HARRIS GEOSPATIAL SOLUTIONS. Harris Geospatial Solutions: Geospatial Data and Analytics. [En línea] [Citado el: 17 de 04 de 2018.] https://web.archive.org/web/20180417145938/http:/www.harrisgeospatial.com/Support/SelfHelpTools/HelpArticles/HelpArticles-Detail/TabId/2718/ArtMID/10220/ArticleID/15316/Workaround-and-best-practices-to-mitigate-risk-for-FlexNet-Publisher-security-vulnerab. https://www.harrisgeospatial.com/Support/Self-Help-Tools/Help-Articles/Help-Articles-Detail/ArtMID/10220/ArticleID/15316/Workaround-and-best-practices-to-mitigate-risk-for-FlexNet-Publisher-security-vulnerability-CVE-2015-8277.

Instituto Nacional de Estadística y Geografía. ¿Qué es la Geodesia? *INEGI.* [En línea] [Citado el: 21 de Noviembre de 2017.] https://web.archive.org/web/20171121184953/http://www.inegi.org.mx/geo/contenidos/geodesia/geodesia_descripcion.aspx. http://www.inegi.org.mx/geo/contenidos/geodesia/geodesia_descripcion.aspx.

—. Elementos de la percepción remota. *INEGI.* [En línea] [Citado el: 22 de Noviembre de 2017.] https://web.archive.org/web/20171122102206/http://www.inegi.org.mx/geo/contenidos/imgpercepcion/imgsatelite/elementos.aspx. http://www.inegi.org.mx/geo/contenidos/imgpercepcion/imgsatelite/elementos.aspx.

International Business Machines Corporation. 1971. IBM Archives: Diskette. [En línea] 1971. [Citado el: 22 de 11 de 2018.] https://web.archive.org/web/20181122174227/https://www.ibm.com/ibm/history/exhibits/vintage/vintage_4506VV2132.html. https://www.ibm.com/ibm/history/exhibits/vintage/vintage_4506VV2132.html.

International Organization for Standardization, International Electrotechnical Commission. 2013. ISO/IEC 27001:2013. Londres : ISO, 2013. 27001.

Kazansev, Taras. 2017. *Introduction to Remote Sensing.* New York : Delve Publishing, 2017.

Latency analysis of systems with multiple interfaces for ultra-reliable M2M communication. **Nielsen, Jimmy J. y Popovski, Petar. 2016.** Edinburgo : Institute of Electrical and Electronics Engineers Inc., 2016. 2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). ISBN 978-1-5090-1749-2.

Leick, Alfred. 2004. *GPS satellite surveying.* New Jersey : John Wiley & Sons, Inc., 2004.

McCormac, Jack. 2007. *TOPOGRAFÍA.* México : Limusa, 2007.

Miguel Pérez, Julio César. 2015. *Protección de datos y seguridad de la información.* Cuarta. Madrid : RA-MA Editorial, 2015.

National Institute of Standards and Technology. 2016. NVD - CVE-2015-8277. *NATIONAL VULNERABILITY DATABASE.* [En línea] 23 de 02 de 2016. [Citado el: 17 de 04 de 2018.] https://web.archive.org/web/20180417151153/https:/nvd.nist.gov/vuln/detail/CVE-2015-8277. https://nvd.nist.gov/vuln/detail/CVE-2015-8277.

O'Hara, Brian T. y Keele, Allen. 2016. *CISA: Certiied Information System Auditor Study Guide.* Fourth Edition. Indianapolis : John Wiley & Sons, Inc., 2016. ISBN: 978-1-119-05624-9.

Raisz, Erwin. 1985. *CARTOGRAFÍA GENERAL.* Barcelona : OMEGA, 1985.

Real Academia Española. geomática | Definición de geomática - Diccionario de la lengua española - Edición del Tricentenario. [En línea] [Citado el: 6 de 11 de 2018.] http://dle.rae.es/?id=J7c4kXU.

—. topografía | Definicióon de topografía - Diccionario de la lengua española - Edición del Tricentenario. [En línea] [Citado el: 7 de Noviembre de 2018.] http://dle.rae.es/?id=a34RotT.

TECHNOLOGICAL TRENDS IN THE DEVELOPMENT OF THE FLOPPY DISK. **Kawamata, Toshio y Morita, Kazuhiko. 2004.** 32, Japón : Elsevier B.V., 2004, Fuji Shashin Fuirumu kenkyu hokoku, págs. 12-22. 03673189.

Torra, Vicenç. 2010. *Del ábaco a la revolución digital: Algoritmos y computación.* Barcelona : RBA Editores, 2010.

Towards practical, high-capacity, low-maintenance information storage in synthesized DNA. **Goldman, Nick, y otros. 2013.** s.l. : Nature Publishing Group, 23 de 1 de 2013, Nature, Vol. 494, págs. 77–80. https://www.nature.com/articles/nature11875.

UNAM. 2018. Oferta Académica UNAM | Ingeniería Geomática. [En línea] 2 de Abril de 2018. [Citado el: 3 de Abril de 2018.] https://web.archive.org/web/20180403031346/http://oferta.unam.mx/carreras/33/ingenieria-geomatica. http://oferta.unam.mx/carreras/33/ingenieria-geomatica.

UNESCO. 2007. Estrategia a Plazo Medio 2008-2013. *34 C/4.* París : UNESCO, 2007. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

Vaníček, Petr y Krakiwsky, Edward. 1986. *GEODESY: THE CONCEPTS.* Segunda. Ámsterdam : Elsevier Science B.V., 1986.

XI. APÉNDICES

XI.1 GLOSARIO

Activo: Cualquier cosa de valor que esté bajo posesión de una organización. Los bienes incluyen tanto artículos tangibles como sistemas de información y propiedad física y bienes intangibles como propiedad intelectual. Incluye al personal.

Amenaza: El potencial para una fuente de amenaza para ejercitar (detonar accidentalmente o explotar intencionalmente) una vulnerabilidad específica.

Ataque: Un ataque es la explotación de una vulnerabilidad por un agente de amenaza. En otras palabras, un ataque es cualquier intento intencional de explotar una vulnerabilidad de la infraestructura en la seguridad de una organización para causar daño, pérdida o divulgación de bienes. Un ataque puede también ser visto como cualquier violación o falla en la adherencia a la política de seguridad de una organización.

Brecha: Una brecha es la ocurrencia de un mecanismo de seguridad siendo desviado/puenteado o frustrado por un agente de amenaza. Cuando una brecha es combinada con un ataque puede resultar en una penetración o una intrusión.

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Honeypot: Máquina intencionalmente vulnerada que busca ser atractiva para los ataques computacionales con el fin de estudiarlos, también puede ser solamente una distracción para los atacantes.

Honeynet: Red intencionalmente vulnerada que busca ser atractiva para los ataques computacionales con el fin de estudiarlos, también puede ser solamente una distracción para los atacantes.

Impacto: La magnitud del daño que pueda ser causado por el ejercicio de una amenaza de una vulnerabilidad.

Malware: Software malicioso.

Penetración: Es la condición en que un agente de amenaza ha ganado acceso a la infraestructura de una organización a través de la burla de controles de seguridad y es capaz de arriesgar bienes directamente.

Probabilidad: Qué tan probable es que una vulnerabilidad potencial pueda ser ejercitada dentro de la construcción de un entorno de amenaza asociado.

Riesgo: Es una función de la probabilidad de una amenaza dada a raíz de una vulnerabilidad potencial, y el impacto resultante de ese evento adverso en la organización.

Salvaguardias: Un salvaguardia, o contramedida, es cualquier cosa que remueva o reduzca una vulnerabilidad o proteja contra una o más amenazas específicas.

Software: Conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Vulnerabilidad: Una falla o debilidad en los procedimientos de seguridad del sistema, en el diseño, implementación o controles internos que puedan ser ejercitados

(detonados accidentalmente o explotados intencionalmente) y resulta en una brecha de seguridad o una violación de las políticas de seguridad del sistema.