Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

MAESTRÍA EN GESTIÓN ESTRATÉGICA DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN

TRABAJO FINAL DE MAESTRÍA

Seguridad de la información en soluciones de inteligencia de negocios en las Pyme de Argentina

AUTOR: EDUARDO EMANUEL QUINTERO

DIRECTORA: MAG. PATRICIA PRANDINI

MARZO 2023

1. Dedicatoria

El presente trabajo lo dedico a Delmira, por su apoyo y aliento que me permiten avanzar en mi vida. También, a Natalia y Gabriel que con su ejemplo y perseverancia me inspiraron a seguir adelante.

2. Agradecimientos

A los profesores de la Universidad de Buenos Aires, especialmente a Claudio Freijedo, Virginia Chaina, Raul Saroka y Patricia Prandini, por su gran compromiso en la educación y por permitirme aprender de sus valiosos conocimientos.

Al grupo de alumnos de esta maestría con los que he tenido el gusto de trabajar en equipo.

3. Resumen

El presente trabajo busca mostrar a través de un caso en una Pyme de Argentina que provee servicios de marketing digital, la relevancia de considerar la seguridad de la información en soluciones de inteligencia de negocios[1] (en inglés, Business Intelligence o BI).

Se abordan los conceptos de las diferentes tecnologías utilizadas en BI, como motores de bases de datos, repositorios y gestión de los datos, la infraestructura tecnológica en la nube, análisis de datos y otros más actuales como la inteligencia artificial. Luego, se describen los conceptos más importantes sobre seguridad de la información y se analizan los elementos tecnológicos que se utilizan habitualmente en una empresa para proteger los sistemas de información y servidores.

A continuación, se describe el escenario de la solución de inteligencia de negocios actualmente en uso por la Pyme y un breve detalle de la infraestructura tecnológica existente.

Por otra parte, se exponen los beneficios que aportan los estándares existentes en materia de seguridad de la información. Luego se analiza la norma ISO/IEC 27001:2022 y se describen los temas relacionados a la correcta gestión de la seguridad de la información, el contexto de la organización, las políticas de seguridad como marco de referencia, la identificación de riesgos en BI, las campañas de concientización al capital humano de una Pyme y algunas consideraciones para la mejora continua.

Por último, se crea un plan inicial con recomendaciones que pueda servir como base para aplicar seguridad de la información en sistemas de inteligencia de negocios, en el ámbito de pequeñas y medianas empresas de Argentina, con énfasis en el control de acceso y la protección de la información almacenada.

1 El autor entiende por soluciones de inteligencia de negocios a los sistemas de computación modernos que brindan información y apoyan las decisiones gerenciales en una empresa.

Palabras claves: Inteligencia de Negocios, Pyme, Seguridad de la información.

Contenido

4. Justificación

El presente trabajo intenta descubrir un tema tecnológico poco visto y descuidado en el mundo de las pequeñas y medianas empresas de Argentina. La iniciativa de implementar y utilizar soluciones para inteligencia de negocios deja expuesta una de las carencias más clásicas en las Pyme, que es no disponer de un área de sistemas propio. La dependencia de la tercerización de proyectos de tecnología y la delegación de su implementación trae inconvenientes a largo plazo, uno de ellos es el abandono de los proyectos implementados[2], como sucede con las soluciones de BI. Además, es importante destacar que muchos de los trabajos que fueron tercerizados carecen de documentación clara para su correcta administración, ya que estos proyectos fueron implementados rápidamente con criterios acotados al alcance del presupuesto.

En este contexto, la rotación permanente de los grupos tecnológicos tercerizados y la búsqueda constante de la inversión más eficiente en las Pyme complica la perspectiva global de la gestión de las tecnologías en la empresa, ya que los proveedores se limitan solo a la implementación y puesta en marcha del proyecto por el cual fue contratado temporalmente. Por este motivo la seguridad de la información en proyectos de tecnologías de la información se posterga para ser abordado en una fase futura, aunque por falta de conciencia y presupuesto disponible esta fase queda sin abordar, lo que deja al proyecto funcionando sin seguridad informática. En otras palabras, los activos de información, muchas veces críticos para la supervivencia de la empresa, quedan desprotegidos y la entidad, expuesta.

En los últimos años, la pandemia de COVID-19 ha aumentado la ciberdelincuencia y los ataques informáticos a las aplicaciones web desde cualquier parte del mundo y las Pyme hoy son un blanco fácil, incluyendo a las de nuestro país, ya que muchas de ellas no

2 El autor entiende el abandono de los proyectos implementados como aquellos que nunca recibieron revisión o mejora continua.

cuentan con medidas básicas de seguridad implementadas. Asimismo, los ataques informáticos más comunes buscan obtener información de los repositorios de datos, para acceder a información sensible como, datos personales de los usuarios, tarjetas de crédito o algún dato de valor que pueda ser usado por el ciberdelincuente para obtener algún beneficio. Los repositorios de datos pertenecientes a soluciones de inteligencia de negocios, big data o minería de datos se han vuelto objetivos favoritos de los ciberdelincuentes, ya que se puede obtener mucha información útil en un mismo lugar.

La fundación OWASP[3] (en inglés, The OWASP Foundation) con sede principal en Estados Unidos, publica anualmente un informe con el top 10 de vulnerabilidades más relevantes en aplicaciones web de todo el mundo. En el informe publicado para el año 2021 se encuentran entre las primeras, las fallas en el control de acceso y la exposición de datos sensibles, dos cuestiones claves para entender porque se debe considerar la seguridad de la información en soluciones de inteligencia de negocios en las Pyme.

El autor aborda un caso de la realidad presente en una Pyme de Argentina que tiene como actividad principal proveer servicios de marketing digital, oportunamente, propone analizar una solución para inteligencia de negocios implementada hace varios años, en la cual se descuidó o no se consideró implementar medidas básicas de seguridad de información para un funcionamiento adecuado, la cual presenta riesgos para el negocio y su reputación.

3 https://owasp.org

5. Planteamiento del tema

La utilización de sistemas de información en las actividades diarias de las empresas ayuda a automatizar procesos y ordenar las operaciones habituales del negocio. El sector de las Pyme trata de mantenerse actualizado e implementar los sistemas que sean necesarios, a fin de poder agilizar sus operaciones y minimizar la dependencia de las tareas manuales. Como consecuencia de esto, día a día se genera gran cantidad de datos e información que es guardada en unidades de almacenamiento pertenecientes a la empresa.

En muchas ocasiones los sistemas implementados en las Pyme no obedecen a una visión sistémica, sino que dividen a sus diferentes áreas, ya que no se logra unificar y cubrir con una sola solución de software todas las necesidades del negocio, dando como resultado pequeñas islas de información dentro de una misma empresa. En este contexto, cada área de una Pyme deberá ser consciente de la información que genera o que tiene en su poder.

En relación con la generación de datos creciente y las unidades de almacenamiento disponibles, se encuentra la necesidad de disponer de recursos tecnológicos adecuados para una correcta gestión de la información, más aún cuando se trata del almacenamiento de información o datos sensibles de personas.

Una característica común de las Pyme de Argentina es que no se cuenta con un área propia de tecnología o sistemas. En consecuencia, la mayoría de las tareas realizadas en materia de tecnología informática son lideradas y ejecutadas por personal tercerizado o consultores externos, quienes resuelven las necesidades con algún criterio propio y en general, con una perspectiva de corto plazo.

Se debe tener presente que, si bien con la contratación de personal tercerizado se pueden ahorrar importantes costos por la implementación de tecnología o resolver necesidades de soporte técnico puntuales, esto no delega la responsabilidad por el tratamiento de información sensible o la confidencialidad de esta. Así pues, el desafío será entender la necesidad de una correcta administración de la información almacenada en poder

de las Pyme, los estándares existentes en materia de seguridad de la información y los inconvenientes que pueden afectar al negocio por la irresponsabilidad en el cuidado de la información almacenada.

Para poder desarrollar el tema se irán respondiendo las siguientes preguntas:

1. ¿Cuáles son las tecnologías que se usan en inteligencia de negocios?

2. ¿Cómo está instalada la solución de BI en la Pyme argentina del ámbito marketing digital analizada?

3. ¿Qué beneficios aporta la norma ISO/IEC 27001:2022 en materia de seguridad?

4. ¿Cuáles son los riesgos para el negocio cuando no se tiene en cuenta la seguridad de la información en soluciones de BI?

6. Objetivos

Objetivo principal

El objetivo principal es explorar e identificar los beneficios de aplicar seguridad a los sistemas de inteligencia de negocios en las Pyme de Argentina.

Objetivos específicos

• Identificar las tecnologías actuales utilizadas para inteligencia de negocios.

• Describir la situación actual de una implementación de inteligencia de negocios en una Pyme argentina del ámbito marketing digital.

• Exponer los beneficios que aporta el estándar ISO 27001 con relación a la seguridad de la información almacenada.

• Presentar un plan inicial con recomendaciones que permitan aplicar la seguridad de la información en los sistemas de inteligencia de negocios en las Pyme de Argentina.

7. Marco teórico

Primeramente, el autor aborda los conceptos y definiciones más importantes que se utilizan en este trabajo, con relación a la seguridad de la información y las tecnologías para soluciones de inteligencia de negocios.

Seguridad informática

Es el conjunto de tecnología informática y procesos establecidos que tiene como objetivo prevenir el acceso y/o uso no autorizado o indebido de los sistemas informáticos pertenecientes a una organización. Asimismo, estos procesos tienen una relación directa con la información digitalizada o electrónica existente en la organización o empresa y la necesidad de su protección.

La seguridad de la información está estrechamente relacionada con la seguridad informática, ya que sin esta última no sería posible asegurar la información de la empresa. Los tres pilares o principios más importantes de la seguridad de la información son: confidencialidad, integridad y disponibilidad.

Confidencialidad

La confidencialidad es necesaria para garantizar que la información este accesible solo para aquellas personas que estén autorizadas (Instituto Nacional de Ciberseguridad de España, 2021). Con esto, se espera prevenir la divulgación no autorizada de la información.

Integridad

Esta referida a poder garantizar que un archivo no fue modificado desde su creación o durante su transmisión en Internet o la red local de la empresa, incluyendo su creación o destrucción parcial o total. Además, se garantiza poder detectar cualquier modificación o cambio sobre los archivos (Vieites, 2011).

Disponibilidad

Se refiere a que las personas o procesos informáticos autorizados puedan acceder a la información en el momento y de la manera en que lo requieran. Además, se consideran medidas para recuperación de información ante situaciones imprevistas y desastres naturales como terremotos, inundaciones o incendios.

Normalización

Es la actividad que busca identificar, analizar y establecer lineamientos de mejora continua en diversos sectores, como organizaciones, gobierno y consumidores. Aunque la normalización abarca muchos ámbitos de aplicación, el autor destaca la normalización para Tecnología de la información y Seguridad que fueron tratados en la ISO.

Organización Internacional de Normalización

La ISO (en inglés, International Organization for Standardization) es una organización no gubernamental independiente y tiene como objetivo desarrollar estándares internacionales que faciliten el comercio internacional. Agrupa representantes de organismos de diferentes países para el consenso y trabajo conjunto, además de grupos expertos para el apoyo técnico. Los primeros estándares de la ISO se publicaron en 1987 referidos a la dirección de Calidad. Actualmente, la ISO está conformada por 167 países miembros organizados en tres jerarquías de participación.

Norma ISO 27001

La norma internacional ISO/IEC 27001:2022[4] fue elaborada por el Comité Técnico de Tecnología de la Información de la Organización Internacional de Normalización (en

[4] Publicación de la norma ISO/IEC 27001:2022. https://www.iso.org/standard/82875.html

inglés ISO) y la Comisión Electrotécnica Internacional (IEC). Estas dos instituciones conforman el sistema especializado para el desarrollo de normas y estándares a nivel mundial. Concretamente, el documento de la norma ISO/IEC 27001:2022 fue desarrollado por el Comité Técnico conjunto ISO/IEC JTC 1 de Tecnología de la Información y el Subcomité SC 27 Técnicas de seguridad.

La norma ISO/IEC 27001:2022 proporciona los requisitos para poder establecer y mantener un sistema de gestión de la seguridad de la información. Este sistema permite garantizar la confidencialidad, integridad y disponibilidad de la información utilizando las herramientas adecuadas.

A lo largo de este trabajo, el autor utilizará la frase “la norma” en referencia a la norma ISO/IEC 27001:2022.

IRAM

Es el Instituto Argentino de Normalización y Certificación, su sede principal se encuentra en Buenos Aires y fue fundado en el año 1935. Es miembro de la Organización Internacional de Normalización y representante oficial para Argentina. A través de IRAM[5] es posible obtener preparación, auditoria y certificaciones ISO de validez internacional, como la ISO 27001.

Inteligencia de negocios

Los programas de computación que brindan información y apoyan las decisiones gerenciales han evolucionado con el paso del tiempo. Entre los años 1990 y 2000, el desarrollo de sistemas web y la integración de varias tecnologías permitió la posibilidad de explotar nuevas maneras de aprovechar el software. Así, aparecen los sistemas de

[5] https://www.iram.org.ar

planificación de recursos empresariales (en inglés, Enterprise Resource Planning o ERP) que permitieron aumentar la integración de las diferentes áreas de la empresa, lo que ofreció la posibilidad de tener más información disponible para apoyar decisiones gerenciales. La evolución de los sistemas de apoyo a la decisión son lo que hoy se conoce como sistemas para inteligencia de negocios.

Los datos y las necesidades de las empresas cambian continuamente a lo largo del tiempo, en relación con esto, Aguilar (2019) afirma: "La necesidad de añadirle conocimientos (insights) adecuados para ayudar a la toma de decisiones ha ido asentando el concepto de Inteligencia de Negocios como un conjunto de componentes ─infraestructura física, de hardware y software─ que conforman una arquitectura para ayudar a una eficiente toma de decisiones" (pág. 3).

Las consultores internacionales y empresas de soluciones de software coinciden que la inteligencia de negocios llegó para apoyar la toma de decisiones.

Conceptos según Gartner y Microsoft

Según la consultora internacional Gartner Inc. (Gartner, 2019), el análisis e inteligencia empresarial (ABI) es un término que engloba el software y la infraestructura necesaria para el análisis de la información, que permitirá mejorar y optimizar las decisiones.

Para la empresa estadounidense Microsoft Corporation (Microsoft, 2020), la inteligencia empresarial (BI) ayuda a las compañías a analizar datos históricos y actuales, para descubrir conocimientos prácticos y tomar decisiones estratégicas.

Datos

En un contexto informático, un dato es un registro de una transacción, que de manera aislada no tiene relevancia ni representa conocimiento de una situación. Las empresas

registran datos en sus actividades diarias y estos son almacenados en una o más computadoras propias o de terceros contratados a tal fin.

Información

La información es un conjunto de datos procesados que poseen un significado, propósito y contexto. Asimismo, el lector puede apreciar en la información algún nivel de importancia, relevancia y utilidad.

Sousa y Oz (2018) señalan las características que debe tener la información útil:

- Relevante: se relaciona al problema en cuestión.
- Completa: no es parcial.
- Precisa: puede servir para tomar decisiones.
- Actual: se basa en hechos recientes.
- Económica: el costo de la obtención debe considerarse porque impacta al negocio.

Tecnologías utilizadas en inteligencia de negocios

A medida que pasan los años las tecnologías de la información realizan ciclos de actualización constante, optimizaciones y mejoras que permiten su mayor aprovechamiento o su adaptación a diferentes escenarios de la realidad. Un ámbito que ha atravesado varios cambios en las últimas décadas es el de los sistemas de información empresarial y las tecnologías que se utilizan en este. Para poder identificar las tecnologías actuales utilizadas para inteligencia de negocios, el autor propone repasar los conceptos básicos de cada una de ellas, ya que en su mayoría aportan alguna mejora u optimización y están siendo utilizadas en las Pyme de Argentina.

Bases de datos

Una base de datos es un conjunto de datos o información almacenado en una computadora que tienen algún tipo de relación o vínculo entre sí. Estos conjuntos de datos son administrados y controlados por un sistema de gestión de bases de datos (en inglés, DataBase Management System o DBMS). Las bases de datos más utilizadas usan estructuras llamadas tablas, que contienen filas y columnas. Para poder leer y escribir datos o información en las bases de datos se utiliza el lenguaje de consulta estructurada (en inglés, Structured Query Language o SQL).

SQL

SQL[6] es un lenguaje de acceso a bases de datos que permite inserción de datos, consultas y borrado. Asimismo, facilita la creación y modificación de esquemas o estructuras, además del control de acceso a los datos. SQL lleva muchos años de difusión y se convirtió en estándar de la Organización Internacional de Normalización (ISO) desde 1987.

NoSQL

Los sistemas de gestión de bases de datos NoSQL, no utilizan SQL como lenguaje principal de consultas y los datos almacenados no requieren estructuras fijas como las tablas. Las bases de datos NoSQL se clasifican según la forma en que almacenan los datos, siendo las más utilizadas las que comprenden categorías como clave-valor y bases de datos documentales. El sistema de base de datos NoSQL más conocido es MongoDB[7] y se encuentra en la categoría de bases de datos documentales.

6 Publicación del estándar SQL ISO/IEC 9075-1:2016. https://www.iso.org/standard/63555.html
7 https://docs.mongodb.com/manual/introduction/

Bases de datos en memoria

Una base de datos en memoria (en inglés in-memory database o IMDB) almacena los datos en la memoria principal de la computadora, para ofrecer tiempos más rápidos de respuesta. Las bases de datos tradicionales almacenan los datos en el disco rígido de la computadora y las operaciones de entrada y salida son más lentas comparadas con las que se realizan en la memoria principal.

Almacenes de datos

Un almacén de datos (del inglés, data warehouse) permite contener y combinar información de diferentes fuentes o bases de datos en un único almacén de manera centralizada. Con esto se logra almacenar datos de diferentes áreas de la empresa o de sus sistemas aislados de manera centralizada, para ser utilizados por herramientas de inteligencia de negocios. Normalmente son utilizados para almacenar datos de toda la empresa y su tamaño es superior a 100 gigas.

Almacén de datos de área específica

Un data mart es una base de datos que en ocasiones se encuentra aislada de los sistemas de una empresa, se puede considerar como una versión pequeña de un almacén de datos o data warehouse y resulta más económico. El data mart se concentra en un área o departamento específico del negocio, para permitir el análisis de información de dicha unidad organizativa. Normalmente reúne datos estructurados de pocas fuentes y su tamaño es menor a 100 gigas.

Lagos de datos

Un lago de datos (en inglés, data lake) es un repositorio que contiene una gran cantidad de datos en bruto y sin procesar que fueron obtenidos de diversas fuentes, generalmente fuentes externas a la empresa. Se utiliza una arquitectura plana para almacenar los datos, es decir que las estructuras para almacenar no tienen jerarquías y se mantienen los datos solo por el tiempo que se requiera. Para el acceso a un data lake se asignan permisos a usuarios específicos. Los usuarios no tienen acceso a las fuentes de los datos, sino que solo acceden a ellos a través del data lake. Estos datos pueden ser resultados de transacciones externas a la empresa y pueden no estar procesados o estructurados.

Extraer, transformar y cargar

Las operaciones para extraer, transformar y cargar (en inglés Extract, Transform and Load o ETL) son las más importantes en un almacén de datos. ETL consiste en la extracción, que es la lectura de datos de una o más bases de datos, la transformación, que significa poder convertir los datos extraídos de forma que se pueda colocar en un almacén o base de datos. Y por último cargar, que implica poder grabar los datos en un almacén de datos (Ramesh, Dursun y Efraim, 2016).

Procesamiento analítico en línea

El procesamiento analítico en línea (del inglés, On-Line Analytical Processing) es una solución para agilizar las consultas a grandes cantidades de datos. Se utiliza un concepto llamado cubo OLAP, también llamado cubo multidimensional o estructuras multidimensionales, para agrupar varios resúmenes de datos categorizados en áreas de interés. De esta manera, utilizando los cubos se reduce el tiempo de las consultas realizas.

Brito Pinto et al. (2018) señalan que el análisis multidimensional ayuda a las empresas a extraer el máximo valor de sus datos, ya que transforma volúmenes de datos en información, lo que permite realizar un análisis y comparar con factores del negocio.

Analítica de negocios

La analítica de negocios se refiere al conjunto de herramientas tecnológicas que se utilizan para descubrir tendencias a partir de los datos presentes o históricos. En el análisis se utilizan modelos descriptivos y se hacen simulaciones de situaciones para crear predicciones. Asimismo, con esta información se espera poder aprovechar oportunidades en el mercado. No se utilizan métodos estadísticos avanzados y la analítica forma parte de los procesos de inteligencia de negocios.

Análisis de datos

El análisis de datos es un proceso que permite inspeccionar, limpiar y transformar datos, con la intención de obtener información útil que pueda servir de apoyo en la toma de decisiones.

Cuadros de mando y KPI

Los cuadros de mando o visualizaciones son representaciones gráficas de los indicadores clave de rendimiento (en inglés, key performance indicator o KPI) en relación con los procesos de la empresa. Cada negocio crea sus propios indicadores y estos deben ser específicos, medibles, alcanzables, relevantes y oportunos. Los gráficos que pueda visualizar el usuario deben permitir realizar comparaciones y contextualizar datos, con el fin de aportar información útil que ayuden en la toma de decisiones.

Grossmann y Rinderle-Ma (2015) afirman que los KPI permiten medir el desempeño del negocio con respecto a metas en cualquier perspectiva del negocio. Por ejemplo, un indicador puede referirse a la adquisición de nuevos clientes o la mejora de los servicios producidos, medidos con relación a la satisfacción del cliente. Para otra empresa, los KPI pueden ser la deserción de los estudiantes o los costos por título. La identificación de KPI suele basarse en la identificación de procesos y la medición de los resultados del negocio en comparación con los objetivos establecidos.

La nube

Para comprender el concepto de computación en la nube (en inglés, cloud computing o cloud), hay que analizar que ya es posible alquilar recursos de hardware y software a empresas prestadoras del servicio, por ejemplo, Google, Microsoft, Amazon u otras, en cualquier parte del mundo. Estas empresas ofrecen a los consumidores la posibilidad de utilizar recursos informáticos por un determinado tiempo a cambio de un pago o suscripción.

Pardo y Jaén (2014) sostienen que el concepto de computación de nube abarca un modelo que permite acceso remoto a recursos informáticos, según nuestras necesidades y bajo demanda a través de Internet, a un conjunto compartido de recursos que son configurables, como redes, servidores, almacenamiento o software, que pueden ser reservados y liberados de manera rápida.

En resumen, las características principales son:

- Disponibilidad de recursos bajo demanda con modelo de pago por uso.
- Acceso remoto a través de Internet.
- Recursos agrupados y virtualizados.
- Escalamiento y liberación de recursos en tiempo real.
- Servicios con monitoreo, privacidad y políticas de seguridad.

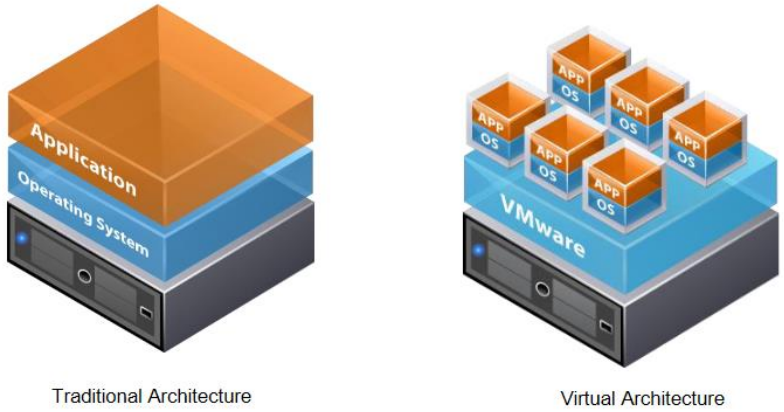
Virtualización

La virtualización sirve para poder utilizar una misma computadora llamada a veces servidor para albergar distintos sistemas separados. Con la evolución de la electrónica las computadoras tienen cada vez más potencia de cómputo y mejor hardware. Esto obligó a los administradores de TI a repartir las capacidades de una computadora para varios sistemas, ya que tener una supercomputadora para un solo sistema es un desperdicio de capacidades de hardware. En la antigüedad, la arquitectura tradicional usaba una sola computadora para un solo sistema operativo (en inglés, OS), hoy con la virtualización es posible repartir partes de una computadora, como el microprocesador, memoria principal, almacenamiento, tarjeta de conexión a la red y otros recursos, a pequeños servidores virtuales dentro de la misma computadora física. Así, se logra separar y aislar recursos físicos de una computadora en nuevos grupos lógicos llamados servidores virtuales o máquinas virtuales (en inglés, virtual machines o VM). En la actualidad, es común alquilar un servidor virtual a un proveedor de la nube como Amazon, Google o Microsoft para no tener que afrontar un costo alto por la compra de una supercomputadora física.

La empresa estadounidense VMware Inc. actualmente propiedad de Dell Inc, proporciona software para virtualización. Su producto más conocido es VMware ESXi[8] y fue lanzado en el año 2001.

A continuación, se presenta una descripción grafica de la arquitectura tradicional y la actual, utilizando la virtualización de VMware:

[8] https://www.vmware.com/ar/products/esxi-and-esx.html



Nota. Arquitectura de virtualización, por VMware Inc., 2009, VMware (https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/Virtualization-for-MySQL-on-VMware.pdf).

Big Data

Big data es un término que describe grandes cantidades de datos estructurados y no estructurados. Para ampliar la definición, De Luna (2021) sostiene que el concepto de big data abarca las estrategias tecnológicas utilizadas para recopilar, organizar y procesar datos, con el objetivo de proporcionar ideas, información o conclusiones a partir de enormes cantidades de datos.

Minería de datos

Con la minería de datos (en inglés, Data Mining) se intenta comprender una gran cantidad de datos y analizar si estos pueden ser utilizados para extraer conclusiones. En relación con este concepto, Tan et al. (2019) señalan que la minería de datos es el proceso para descubrir automáticamente información útil en grandes repositorios de datos de distintas fuentes. Las técnicas que se utilizan rastrean grandes conjuntos de datos para

encontrar patrones útiles, que de otro modo siguen siendo desconocidos. Además, proporcionan la capacidad de predecir el resultado de alguna observación futura.

Inteligencia artificial

La inteligencia artificial es la simulación de inteligencia humana en sistemas de computación o computadoras. Para la empresa estadounidense Oracle Corporation (Oracle, 2021) la inteligencia artificial se refiere a sistemas que intentan imitar a la inteligencia humana para realizar algunas tareas y pueden mejorar iterativamente a partir de la información que recopilan. Algunos ejemplos que utilizan esta tecnología son los chatbots, utilizados para responder a clientes y proporcionar respuestas más eficientes. También, los asistentes inteligentes usados para analizar información crítica, proveniente de grandes conjuntos de datos de texto para mejorar la programación logística o el aprovisionamiento de almacenes en las industrias. Otro ejemplo son los motores de recomendación, que dan recomendaciones automatizadas para programas de TV según los hábitos de visualización de los usuarios.

Criptografía

La criptografía es la ciencia que estudia técnicas para transformar o cifrar información y hacerla irreconocible. El termino proviene del griego "Kriptos" que significa oculto y "Grafos" que significa escritura, el significado conjunto es escritura en modo secreto (Vieites, 2011). Un sistema criptográfico aplica cambios en el texto original a veces llamado texto claro y obtiene un texto cifrado que no puede ser leído por una persona humana, excepto que disponga de las claves y demás elementos necesarios para acceder a él.

Ransomware

El INCIBE (Instituto Nacional de Ciberseguridad de España, 2020) describe al Ransomware como un tipo de software malicioso (en inglés, Malware) que toma el control de la computadora cifrando la información existente. Luego, la persona o grupo a cargo del Ransomware solicita dinero a la víctima a cambio de descifrar los archivos previamente cifrados y permite el acceso a la información, aunque, si se paga el rescate no hay garantías de que el ciberdelincuente devuelva la información original a la víctima.

OWASP Top 10

Es el informe anual de la fundación estadounidense OWASP (acrónimo de Open Web Application Security Project), donde se analizan y priorizan las vulnerabilidades de aplicaciones web de todo el mundo.

A continuación, se presenta el ranking de vulnerabilidades del año 2021.

1	Pérdida de control de acceso
2	Fallas criptográficas
3	Inyección
4	Diseño inseguro
5	Configuración de seguridad incorrecta
6	Componentes vulnerables y desactualizados
7	Fallas de identificación y autenticación
8	Fallas en el software y en la integridad de los datos
9	Fallas en el registro y monitoreo
10	Falsificación de solicitudes del lado del servidor

Nota. Adaptado de OWASP Top 10 - 2021, por OWASP, 2021, OWASP (https://owasp.org/Top10/es).

En el desarrollo de este trabajo el autor expondrá que las dos primeras vulnerabilidades están muy relacionadas a la seguridad de la información en soluciones de inteligencia de negocios, más aún el ámbito de las Pyme argentinas.

Los conceptos de cada vulnerabilidad según la fundación OWASP son los siguientes:

1. Pérdida de control de acceso: El control trata de que los usuarios no puedan actuar fuera de los permisos que le fueron asignados. Las fallas en este control conducen a la divulgación de información no autorizada, la modificación o la destrucción de datos.
2. Fallas criptográficas: Es el control de protección de los datos en tránsito a través de las redes y en reposo, los que se encuentran almacenados. Se controla el uso de criptografía obsoleta o en desuso y la ausencia de cifrado en datos sensibles, como las contraseñas almacenadas.

8. Aspectos metodológicos

Se realizó un estudio de caso que permitió analizar la realidad presente en una Pyme argentina donde el autor ha desempañado su labor. Se aplicó una investigación de tipo exploratoria que permitió identificar la importancia de la seguridad de la información en soluciones de inteligencia de negocios utilizadas en las Pyme de Argentina. Se investigó un problema poco estudiado partiendo de información escasa disponible para lograr la exposición de algunos supuestos. Además, se realizó un trabajo descriptivo y se utilizó un enfoque cualitativo.

La técnica de recolección utilizada fue el análisis de documentos. Se recolectó datos a partir de la lectura de fuentes primarias y secundarias. Se realizó la descripción, análisis, desarrollo e interpretación de los temas para encontrar significados.

Para identificar las tecnologías actuales utilizadas en inteligencia de negocios, describir la situación actual de una implementación de BI en una Pyme argentina del ámbito marketing digital y exponer los beneficios que aporta el estándar ISO 27001 con relación a la seguridad de la información almacenada, se realizó una revisión bibliográfica. Para presentar un plan inicial con recomendaciones que permitan aplicar la seguridad de la información en los sistemas de inteligencia de negocios en las Pyme de Argentina, se realizó una síntesis de la bibliografía y se utilizó los conocimientos adquiridos a lo largo de toda la maestría y otros de la experiencia del autor en diferentes tareas de consultoría.

9. Desarrollo

9.1 Tecnologías actuales utilizadas para inteligencia de negocios

En el mercado internacional existen numerosas soluciones de software dedicadas al ámbito de la inteligencia de negocios. Estas soluciones utilizan diferentes tecnologías de la información para el acceso a los datos, los cuales son uno de los elementos más importantes para su funcionamiento.

En los primeros tiempos en la década de los noventa se utilizaban tecnologías para los sistemas de información ejecutiva (en inglés, Executive Information System o EIS), que podían ofrecer a la gerencia información agrupada y graficada de manera simple. Con el paso del tiempo, las tecnologías y herramientas para inteligencia de negocios fueron evolucionando y atravesaron cambios en cada una de sus partes: almacenamiento, gestión de datos, análisis y reportes. En la actualidad, se sumaron otras innovaciones tecnológicas más avanzadas como big data e inteligencia artificial.

Almacenamiento de datos

Los almacenes de datos o data warehouse en inglés, están siendo muy utilizados en los últimos años por empresas que poseen gran cantidad de datos. Esto se debe en gran parte a que los costos de almacenamiento de información son menores cada año. Los proveedores de servicios de almacenamiento en la nube, como Google, Amazon o Microsoft, permiten utilizar discos en servidores virtuales remotos por un pequeño costo. Aunque existen muchos proveedores de almacenamiento en la nube, la mayoría permite elegir la cantidad de espacio que se pretende utilizar y el tipo de tecnología de disco. Además, ofrecen un servicio de crecimiento por demanda, en donde primero se contrata una cantidad mínima y luego se paga a medida que se ocupa más espacio en disco con información almacenada. Esta opción de almacenamiento resulta más económica que la de tener un servidor propio en alguna oficina

de la empresa, ya que se delega al proveedor la responsabilidad de cuestiones como el suministro de electricidad sin interrupciones, la conexión a Internet, la disponibilidad sin días de espera, recuperación de desastres, la mano de obra especializada, etc.

En resumen, hoy resulta más conveniente contratar la tecnología de almacenamiento en la nube de proveedores como Google, Amazon o Microsoft y centralizar en ella los datos de las distintas fuentes y por ello es la opción más elegida por las empresas.

Gestión de los datos

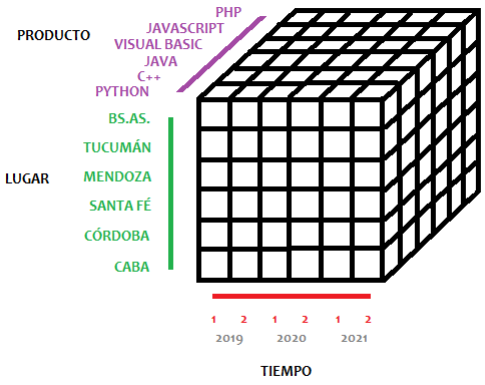
Las nuevas necesidades para manejar datos de manera más ordenada dieron origen a la aparición de sistemas para extraer, transformar y cargar dato (en inglés extract, transform and load o ETL). Estos sistemas facilitan la integración y el almacenamiento de datos de manera más prolija, aunque sean obtenidos de diferentes orígenes, como pueden ser las bases de datos que son externas a la empresa. Entre las soluciones más destacadas de esta última década y que se utilizan en grandes empresas, se encuentra la de la compañía estadounidense llamada Informática[9], con su producto Power Center que es una solución para ETL y análisis de datos. Otra solución robusta es la de IBM con su producto InfoSphere DataStage, utilizada principalmente para la integración de datos de diferentes orígenes y ETL. Existen productos de menor costo para las Pyme, como lo es la propuesta de la empresa Microsoft con su producto Power BI. Además, existen soluciones de código abierto que no requieren afrontar costos de licencias, como el caso de Apache Nifi[10] de la Fundación de software Apache.

[9] https://www.informatica.com

[10] https://nifi.apache.org

Análisis de los datos

El avance de nuevas tecnologías de información y las necesidades de negocio han llevado a los especialistas en todo el mundo a encontrar nuevas soluciones para mejorar el análisis de los datos, la información, el negocio y su contexto. Una de las herramientas de análisis más interesantes es la del análisis multidimensional, que permite relacionar los datos que se tienen a un hecho. Actualmente se analiza usando este modelo multidimensional y para representar la información que se está trabajando se utiliza un cubo. Para poder entender esta herramienta a continuación se muestra un ejemplo de un cubo, representando tres dimensiones: producto, lugar y tiempo. El análisis multidimensional permitiría conocer, por ejemplo, en qué provincia se vendió más un producto o servicio de desarrollo de software y en qué semestre del año. La información obtenida a partir de este cubo, luego podría ser parte de un indicador clave de rendimiento o KPI utilizado por la gerencia.



Dimensiones de un cubo OLAP representando; Producto, lugar y tiempo.

Fuente: Elaboración propia.

Minería de datos

Una característica de la última década es que los datos son generados y distribuidos de forma masiva en diferentes plataformas tecnológicas a través de Internet. Un ejemplo de esto es cómo en una plataforma de comercio electrónico los usuarios generan datos al iniciar su sesión para interactuar con el sistema. Si estos datos fueran utilizados para un análisis, se podría obtener información sobre el horario en el que accede mayor cantidad de usuarios y desde qué provincia ingresan y en base a la información del perfil se podría conocer el sexo y la edad.

Existen empresas que tienen sistemas abiertos para consultas de datos, de los cuales se podría extraer algún tipo de información que pueda resultar interesante para el negocio. Un ejemplo de esto podría ser la empresa Mercadolibre, que permite conocer en su sitio web de comercio electrónico la cantidad de visitas que ha tenido un producto o publicación en un periodo de tiempo. Esto podría resultar atractivo en algunas situaciones, si se consultan estos datos cada hora y por cada producto que se tenga a la venta, se podrá conocer que productos reciben más visitas de posibles clientes y en qué horarios. Además, se podría observar que los productos que reciben una mayor cantidad de visitas puede que no sean los que más se venden y que posiblemente, los usuarios prefieran comprar en otra empresa como la competencia, dado a que no se tiene el producto de la marca que el usuario busca o que el precio no sea el adecuado.

Existen otros sistemas como las redes sociales que también permiten consultas abiertas a datos, que luego pueden ser relacionados con otros para obtener información de interés para el negocio. Cada red social publica sus datos a través de una API[11], que puede consultarse desde un sistema para minería de datos, obteniéndose datos masivos. Por ejemplo, si se estuviera analizando el perfil de la competencia se podrá obtener información sobre todas las interacciones de sus seguidores y filtrando estas, la provincia de la mayor influencia de usuarios y el sexo. Al finalizar el análisis con minería de datos, se podría

11 Interfaz de programación de aplicaciones.

obtener información que antes no se tenía. En este caso, se podría conocer que la mayor cantidad de posibles clientes de la competencia son hombres de la provincia de Santa Fe, Argentina, algo que se debería considerar en las próximas campañas de comercialización de la empresa.

La minería de datos permite buscar datos de valor para el negocio en grandes cantidades de datos, que sueltos o sin relación no tienen ningún valor. Además, la recolección masiva de datos permite descubrir alguna tendencia de interés que pueda tener el público en general y que no esté visible en sistemas propios de la empresa.

Existen varios proveedores de software para minería de datos, siendo algunos de los más conocidos Oracle Data Mining y Microsoft Sql Management Studio, ambos con un costo de licenciamiento. Por el lado del software libre, las soluciones más relevantes son Weka[12], creado por la universidad de Waikato en Nueva Zelanda y RapidMiner studio[13] creado por la Universidad Técnica de Dortmund en Alemania. En todos los programas para minería de datos es posible utilizar algún modelo que consta de varias etapas. Las más utilizadas son: definir el problema, preparar los datos resolviendo cuestiones de formato, explorar datos, crear e implementar los modelos o estructuras en las bases de datos. Estas etapas suelen ser cíclicas y repetitivas en todo el tiempo que se esté realizando la minería de datos. Además, estas herramientas suelen soportar los algoritmos de minería más conocidos, como los de grupos o agrupación en clústeres, árboles de decisión y los de estadística como el Bayes Naive.

Reportes y visualizaciones

Los reportes permiten a los usuarios disponer de un flujo de información actualizada para colaborar con la gerencia. Las diferentes visualizaciones, gráficos o mapas, sirven para representar de manera simplificada un resumen con los valores en los que se tiene interés,

[12] https://waikato.github.io/weka-wiki/documentation/
[13] https://github.com/rapidminer/rapidminer-studio/

que en algunas ocasiones son indicadores claves de rendimiento o KPI. Los sistemas de información atravesaron muchas actualizaciones en cuestiones de representación gráfica, pasando por tablas, gráficos de torta, diagramas, tableros de control, mapas, etc. Actualmente, en todas las soluciones de inteligencia de negocios existen opciones para crear reportes o visualizaciones. Algunos proveedores separan el gestor de reportes en un software aparte, como es el caso de la empresa Microsoft, con su producto Power BI Report Server que permite ampliar los reportes de Microsoft Power BI.

Lo más relevante en la última década, es que los proveedores de software para inteligencia de negocios mejoraron y simplificaron la tarea de creación de reportes. Esto permite a los usuarios que no son especialistas en el tema, crear reportes utilizando asistentes paso a paso o plantillas ya existentes, con lo cual se logra una rápida adaptación para utilizar el programa.

Big Data

Con el uso actual de Internet, los datos masivos son generados por los distintos dispositivos y usuarios en los sistemas de información y comunicaciones. Muchos de los datos provienen de los usuarios de manera inconsciente y expuestos a Internet través de los sistemas web. Para muchas organizaciones esto puede traer un beneficio, ya que se podría estar utilizando estos datos de acceso público en beneficio del negocio. La big data se construye con el uso de los sistemas y cambia día a día, lo que resulta aún más atractivo, ya que, si estos datos se recolectan a diario, existe la posibilidad de que se pueda medir el comportamiento de posibles clientes o del público en general y hacer un análisis para encontrar patrones.

Los sistemas actuales de inteligencia de negocios poseen funciones para hacer un aprovechamiento de big data que circula a diario en Internet. Los datos son capturados a través de pequeños programas que se conectan a redes sociales, sitios web y otras fuentes, donde se extraen datos en distintos formatos para luego ser procesados en un formato y

almacenados en bases de datos para un posterior análisis. Así, estos grandes volúmenes de datos son consumidos por las funciones de análisis de la inteligencia de negocio, la cual debe mirarse como un ejercicio constante necesario para nutrir con datos a las bases de datos y no como algo estático o de una sola vez.

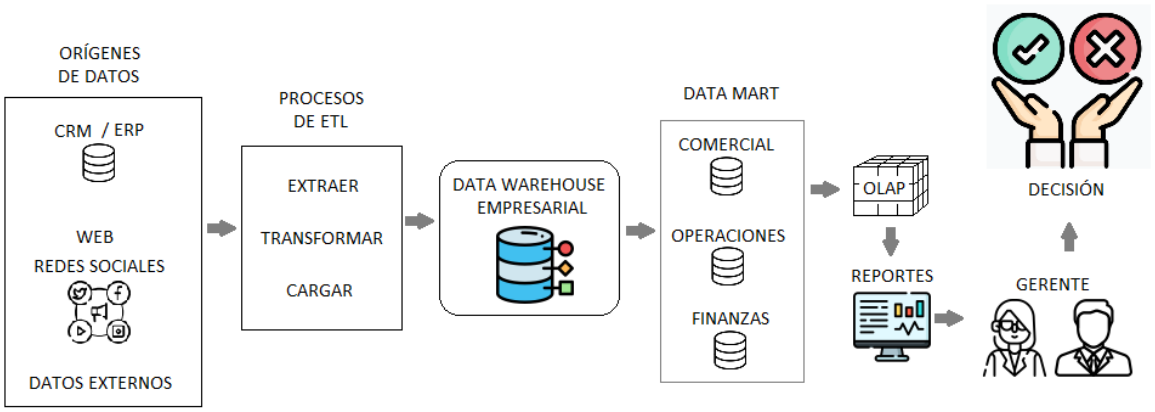
Los proveedores que se han mencionado anteriormente en el apartado sobre gestión de los datos también incluyen características y herramientas para big data. La empresa estadounidense Informática, tiene su producto Power Center edición big data y ya facilita al usuario nuevos conectores para extraer datos de redes sociales, como Facebook, LinkedIn y Twitter. También permiten conexiones a los almacenamientos de la nube como Amazon, Google y Microsoft. En cuanto a las soluciones de código abierto, Apache Nifi posee pequeños programas construidos en java llamados procesadores, que permiten conectar las redes sociales Facebook, Twitter, Instagram, LinkedIn, sitios webs, email y otros orígenes, además de dar la posibilidad para desarrollar conectores propios en el lenguaje de programación java. Todos los proveedores soportan formatos de archivos conocidos, como los archivos de datos con extensión txt, cvs, JSON, etc. y también archivos comprimidos.

Inteligencia artificial

Los sistemas de inteligencia de negocios que están a la vanguardia incorporan nuevas funciones que permiten aprovechar algoritmos de inteligencia artificial. Un ejemplo concreto de esto es el producto Power BI de la empresa Microsoft, que pone a disposición del usuario de manera gratuita una muestra del alcance de su solución. Si se utilizan funciones de inteligencia artificial, se puede lograr resultados para atender necesidades típicas, por ejemplo, análisis predictivo en el crecimiento o caída de ventas, segmentación de clientes, la predicción de comportamientos de clientes, etc. Además, se incluyen modelos de informes y tableros de ejemplo realizados utilizando inteligencia artificial sobre un conjunto datos de muestra, lo cual permite conocer y aprender cómo se implementan los algoritmos.

Desde el año 2020, la empresa Tableau (adquirida a mediados del 2019 por Salesforce) también incorporó en su producto para inteligencia de negocios una función llamada “explique los datos”. Esta función utiliza modelos estadísticos avanzados para intentar extraer y presentar información relevante de los datos, aunque solo está disponible para la versión del producto con licencia.

El siguiente gráfico muestra una arquitectura simplificada de una solución de inteligencia de negocios:



Fuente: Elaboración propia.

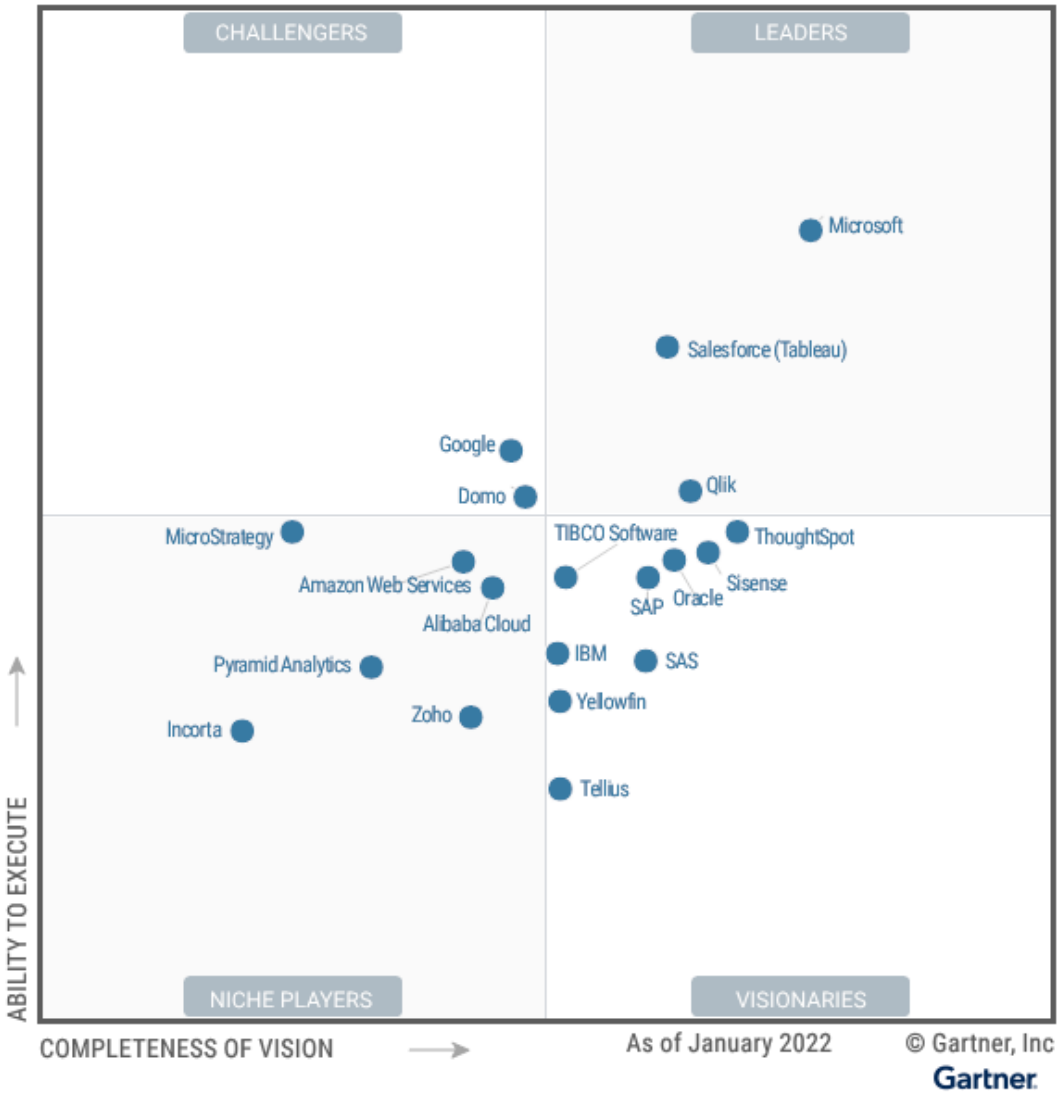
Investigación del mercado actual

La consultora estadounidense Gartner Inc. investigó en el año 2022 las soluciones de analítica e inteligencia de negocios y presentó su informe acompañado de su cuadrante mágico con los proveedores de mayor relevancia a nivel mundial. Las soluciones de los proveedores para grandes empresas son evaluadas en al menos 12 áreas para su calificación. Estas áreas incluyen cuestiones como la usabilidad, visualizaciones, informes, seguridad, análisis en la nube, conectividad de fuentes de datos, preparación de datos, automatización,

soporte de consultas en lenguaje natural y otras. A continuación, se presenta el cuadrante mágico con las empresas Microsoft y Salesforce (Tableau) como líderes del año 2022.

Figura 1

Cuadrante mágico



Nota. Cuadrante mágico de Gartner, por Gartner Inc., 2022, Microsoft (https://info.microsoft.com/ww-landing-2022-gartner-mq-report-on-bi-and-analytics-platforms.html?LCID=EN-US).

9.2 Situación actual de una implementación de BI en una Pyme argentina del ámbito marketing digital

En la última década, las Pyme comenzaron a estar interesadas en la explotación de tecnologías que puedan aportar un mayor valor a la gerencia. Con estas tecnologías esperan poder afrontar con más certeza los cambios en el contexto del negocio y aumentar los beneficios económicos en los mercados donde operan. En el caso de la Pyme analizada, se contrató hace algunos años a una consultora informática para poner en funcionamiento una solución para inteligencia de negocios, con la intención de aprovechar los datos disponibles de clientes que ya están en poder de la empresa.

A continuación, se describe la situación actual de la implementación de la solución de BI.

La Pyme argentina desarrolla sus actividades en el ámbito del marketing digital y es donde el autor ha desempeñado su labor. La empresa cuenta hoy con una oficina propia de tres pisos en Buenos Aires y utiliza una vivienda tipo casa que fue modificada para disponer de varias oficinas. Por una incorrecta organización del área de TI y del equipamiento de telecomunicaciones existente, el único rack grande de telecomunicaciones no tuvo espacio libre para poder alojar el servidor de BI y otro servidor del área Desarrollo. Estos dos servidores fueron colocados en un rack pequeño en una sala que estaba sin uso en planta baja (A4), el resto del equipamiento y servidores está en el primer piso. En la planta baja se encuentra la oficina de recepción (A1), gerencia (A2) y equipo creativo (A3), este último está conformado por diseñadores gráficos y editores de video.

Descripción gráfica de la planta baja

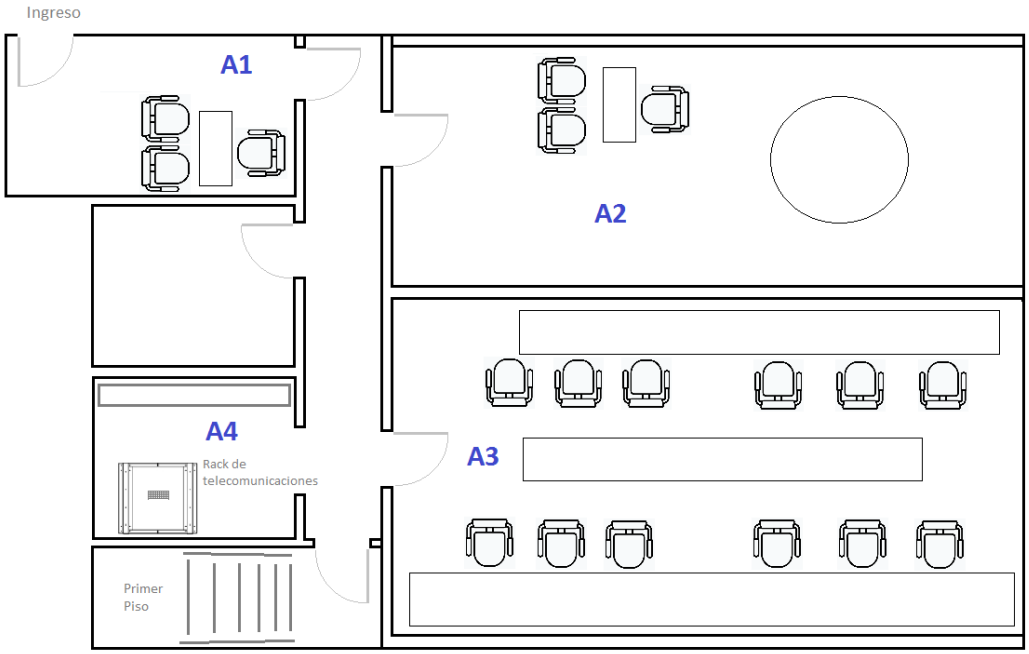


Figura 1. Descripción gráfica de la planta baja de la Pyme.

Fuente: Elaboración propia.

Descripción del servidor de BI

El servidor que fue destinado a la solución de inteligencia de negocios es una computadora de tipo hogareña con hardware potente y gabinete rackeable. El gabinete es una carcasa de metal que protege a la computadora y el término rackeable significa que puede ser colocado en un armario o rack de telecomunicaciones, de manera similar a los cajones de madera de una cajonera o armario en forma horizontal.

El sistema operativo en uso en el servidor de BI es Linux, versión “Debian 6 Squeeze”. Los usuarios acceden al servidor a través de una interface web con su navegador de Internet o se conectan directamente al motor de bases de datos. El acceso al servidor está permitido desde la red interna de la oficina y desde Internet. Además, se puede acceder a través de la red cableada e inalámbrica.

Descripción grafica simplificada de la solución

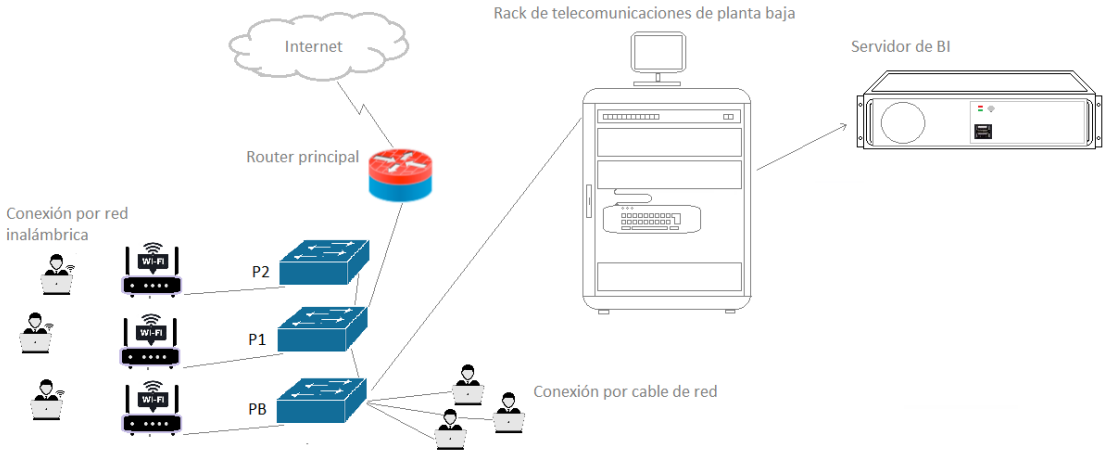


Figura 2. Descripción simplificada de la solución de BI.

Fuente: Elaboración propia.

¿Qué información contiene el servidor de BI?

La solución de BI se implementó para reunir datos disponibles en un solo lugar y posteriormente, realizar un tratamiento de análisis de datos que permita obtener información de valor para la gerencia y dirección.

En este servidor se copian algunos datos de diferentes fuentes, como el sistema de facturación, bases de datos de todos los eventos masivos realizados para clientes, el sistema de gestión de proyectos interno y otros, como métricas de las redes sociales de la Pyme. Las copias han sido automatizadas y son ejecutados a diario en horario nocturno. Para ello, se desarrollaron pequeños programas (en inglés, script) escritos en un lenguaje de programación, que son los encargados de realizar las acciones de copia.

Consecuentemente, algunos de los datos que contiene el servidor de BI son: nombres de clientes, proyectos y responsables, cantidades y montos facturados. Además, datos que se recolectan en eventos masivos, como nombre completo de usuarios, documento nacional de identidad o pasaporte, teléfono, domicilio, email, obra social, empleo actual, educación, salario y opiniones personales. Finalmente, si el evento requiere registración, se crea y almacenan contraseñas de todos los participantes del evento y sus administradores. Los administradores normalmente son gerentes de proyectos o ejecutivos de cuentas de empresas que son clientes de la Pyme.

Por otra parte, el mismo servidor de BI tiene configurado un programa servidor de archivos compartidos compatible con Windows llamado SMBD[14]. Esto fue configurado por la misma consultora que implementó la solución con el objetivo de aprovechar el espacio de almacenamiento ocioso, a fin de compartir archivos y documentos de manera interna dentro de la empresa. El servicio de archivos compartidos no está accesible desde Internet y fue utilizado al menos cinco años por los colaboradores de distintas áreas de la Pyme.

Otros aspectos de la Pyme

Mercado

La Pyme se encuentra prestando servicios de marketing digital a empresas de mediano tamaño de otros países, como Brasil, Estados Unidos, España, Italia y Singapur. La característica más valorada en el mercado de marketing digital es que una empresa pueda dar una rápida respuesta e implementar una solución, siendo lo más requerido como herramienta para realizar eventos online masivos. Así, la Pyme compite con otras agencias de publicidad para hacer funcionar una solución en el menor tiempo posible, generalmente en plazos cortos de tan solo días o semanas.

[14] http://man.sourcentral.org/debian-squeeze/8+smbd

Cultura organizacional

En la empresa se vive una cultura de emprendimiento y cada nuevo cliente o proyecto es un desafío con necesidades únicas que son difícilmente repetibles. Así, el clima organizacional también se muestra día a día con actitud emprendedora en los mandos medios y responsables de gestión comercial. Sin embargo, esto a veces juega en contra al momento de asumir compromisos, ya que, por cuestiones de tiempo, a veces no se evalúan correctamente los riegos en los proyectos o aspectos tecnológicos y el alcance del compromiso por el servicio prestado no es claro. Por último, en la operación diaria son habituales en todos los niveles frases como:

- "Ya lo vendimos, necesitamos implementarlo lo antes posible."
- "Tenemos que sacar esto andando rápido."
- "Ya prometimos que lo íbamos a hacer y lo tenemos que hacer andar."
- "Necesitamos a este cliente, así que hagamos todo lo que podemos hacer."
- "Ya no tenemos más tiempo para cambios, necesitamos salir a vivo."

Todas estas expresiones y otras similares, impactan en la operación diaria y en la manera de trabajar de todos los colaboradores, dado que se terminan aplicando en la manera de gestionar los proyectos que se venden e implementan en producción.

Capital humano de Tecnología

El personal interno de tecnología está compuesto por unos pocos colaboradores que acompañan las necesidades del negocio y clientes. En estos últimos 2 años se decidió conformar una gerencia de TI y definir al menos dos grupos de trabajo con sus responsabilidades, quedando en proceso de formalización el siguiente organigrama de equipos.

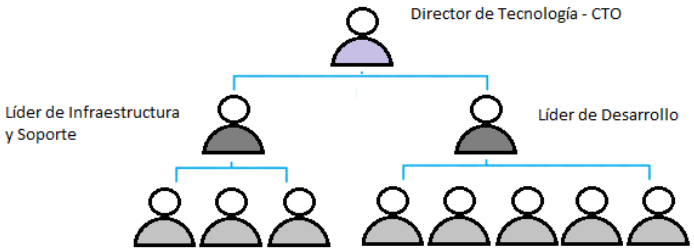


Figura 3. Organigrama del área de TI.

Fuente: Elaboración propia.

Los equipos están conformados mayormente por perfiles junior sin especialización que participan en la creación de proyectos pequeños, como sitios web, páginas web de aterrizaje (en inglés, landing page) y archivos para publicaciones por correo electrónico (en inglés, newsletter). Otros colaboradores del área brindan soporte técnico, conforman la mesa de ayuda y poseen conocimientos básicos de reparación de computadoras. Para todos los proyectos de redes de datos, infraestructura tecnológica, la nube, bases de datos o tecnologías especializadas se contratan consultorías externas, que reportan directamente al director de tecnología.

Observaciones en la seguridad de la información

Vista la situación actual de la implementación de BI en la Pyme, el autor expone algunas cuestiones de seguridad de la información que se descuidaron o no se consideraron en el proyecto implementado por la consultora que estuvo a cargo.

A continuación, se presenta un breve detalle sobre las observaciones en seguridad física, monitoreo, software, red inalámbrica, capacitaciones y copias de respaldo.

Seguridad física

Una de las cuestiones más básicas en seguridad es controlar quién puede acceder físicamente a los servidores. En este caso, el pequeño rack de telecomunicaciones de 20 unidades se encuentra en una sala sin puerta sobre un pasillo con tránsito medio, por el cual accede diariamente el personal de la empresa que trabaja en el primer y segundo piso, incluyendo personal externo dedicado al bufé y maestranza. Aunque el modelo de rack permite usar llaves, no se cuenta con una cerradura instalada. En este pequeño rack se encuentra conectado un monitor y teclado para trabajar en el servidor de pruebas de Desarrollo.

Posible acción malintencionada: Una persona podría conectar una o varias unidades de almacenamiento extraíble USB (en inglés, pendrive), utilizar el monitor y teclado disponible para copiar información almacenada desde el servidor BI. Actualmente, en Argentina se encuentran a la venta unidades de almacenamiento USB de 512 gigas de capacidad por veintinueve mil pesos argentinos, lo cual permite a cualquier usuario contar con herramientas de este tipo a bajo costo para copiar grandes volúmenes de información. También, podría desconectar los servidores, destruirlos o inclusive robar alguno de los componentes de hardware.

Monitoreo

Las cámaras de seguridad o videovigilancia son inexistentes. Estas son necesarias para el registro del acceso físico de personas que ingresen a la sala donde se encuentra el rack.

Por otra parte, el monitoreo en tiempo real del uso de la red de datos, también llamado “monitoreo de tráfico de red”, está ausente. Este tipo de monitoreo es necesario, ya que permite tener visibilidad de la ocupación de la red de datos, por ejemplo, si una persona está realizando copias de grandes volúmenes de información de una computadora a otra o hacia Internet.

Software

Sistema Operativo

La versión del sistema operativo en uso Linux Debian 6 Squeeze ya se encuentra obsoleta. El final del ciclo de vida y soporte oficial de Debian 6 terminó en febrero del año 2016. La pyme no realizó actualizaciones del sistema operativo hasta el año 2023.

Posible acción malintencionada: Un ciberdelincuente podría aprovechar esta situación para distribuir Ransomware en la Pyme, ya que, un sistema operativo desactualizado se ve afectado por técnicas de ataque modernas a través de la red, como, por ejemplo, el Ransomware Ryuk[15], un programa malicioso que se copia a si mismo de manera automática, se transmite en toda la red local de computadoras y cifra unidades de almacenamiento para luego pedir un rescate a través de un pago. Cuando un servidor se ve afectado por un ataque de Ransomware deja indisponible el acceso a la información, para todos los usuarios incluyendo a sus administradores.

Antivirus

Los puestos de trabajo de la Pyme utilizan el sistema operativo Windows en varias versiones, algunas computadoras de escritorio o portátiles utilizan las versiones que ya venían instaladas desde su compra. Estas versiones de Windows en uso incluyen una versión llamada Home, la cual utiliza por defecto las cuentas de usuario con permisos de administrador. Además, la Pyme no cuenta con una solución de antivirus centralizada o estándar en todas las computadoras, muchas de las cuales utilizan antivirus gratuitos y otros sin licencias para actualización. Al mismo tiempo, los servidores que usan Linux como el servidor BI no cuentan con antivirus instalado.

[15] https://www.cloudflare.com/es-es/learning/security/ransomware/ryuk-ransomware/

Posible acción malintencionada: La falta de antivirus facilita que una persona pueda realizar ataques de acceso a la red interna de la empresa, desde Internet o desde otra computadora en la misma red interna. También, permite infecciones de virus informáticos que pueden causar distintos tipos de daños o realizar acciones de espionaje. Por otra parte, el antivirus desactualizado o ausente permite a un ciberdelincuente instalar un pequeño programa portable en la computadora de un colaborador de la Pyme, ya sea que tenga Windows o Linux, para posteriormente tomar el control remoto o ejecutar ordenes de manera remota, tal como si lo estuviera ejecutando el mismo colaborador de la Pyme. De esta manera, se podría fácilmente descubrir los archivos compartidos en la red interna de la empresa, como los archivos compartidos en el servidor de BI y realizar copias de los archivos hacia alguna computadora existente en Internet. Un ejemplo de estos programas para ejecutar ordenes remotas es Shellter[16]. Estas tareas pueden ser llevadas a cabo remotamente desde Internet y sin consentimiento e intervención del usuario.

Cortafuego de sistema operativo

Existen programas que funcionan como un buen complemento de seguridad del sistema operativo. Estos son los programas cortafuegos de sistema operativo (en inglés, host-based firewall). Un cortafuego de este tipo previene que se realicen acciones malintencionadas sobre un sistema operativo como Linux Debian. En este caso, el servidor de BI con Linux no posee instalado ningún programa cortafuego de sistema operativo.

Posible acción malintencionada: Una persona podría realizar múltiples intentos de acceso al servidor de BI, con el uso de un programa que automatiza los intentos de autenticación con usuario y contraseña. Un ejemplo de estos programas es Hydra[17], que permite realizar muchos intentos de autenticación por segundo durante varias horas o incluso días. Estos programas utilizan archivos llamados “diccionarios de contraseñas” que

[16] https://gitlab.com/kalilinux/packages/shellter/-/tree/kali/master/docs
[17] https://www.kali.org/tools/hydra/

contienen miles de contraseñas recolectadas por ciberdelincuentes y son puestos a disposición en Internet de manera gratuita.

El programa Hydra se utiliza para probar una conexión por SSH, un protocolo de administración remota que usan los administradores de servidores para trabajar como si estuvieran parados frente al servidor con un teclado y monitor. Si una persona lograra una conexión por SSH al servidor, podría realizar copias de archivos hacia computadoras de la red interna de la empresa o a Internet.

Otra acción malintencionada podría ser la de realizar intentos de acceso directamente al motor de bases de datos del servidor BI, utilizando una herramienta similar a Hydra llamada MySQL Brute[18]. Esta permite probar la autenticación con usuario y contraseña de manera automatizada haciendo uso de los diccionarios de contraseñas. Si se logra una conexión directamente al motor de bases de datos con el usuario root, se tendrá acceso a toda la información de las bases de datos existentes en el servidor de BI.

Autenticación centralizada

La autenticación de un colaborador para al acceso al servidor BI se realiza utilizando usuarios que fueron creados localmente en el sistema operativo Linux. Aunque el nombre de cada usuario coincide con el mismo usado en otros sistemas de la empresa, la contraseña utilizada solo existe en el servidor de BI y muchas veces nunca se cambia. En este servidor no están configuradas cuestiones básicas de seguridad de contraseña, como el vencimiento por una cantidad limitada de tiempo, el control de contraseñas débiles, la longitud mínima, los bloqueos de usuario por cantidad de intentos fallidos en el acceso y el uso de doble factor de autenticación, como podría ser la recepción de un mensaje de texto al teléfono celular del usuario para confirmar un acceso seguro. Por otra parte, la falta de administración centralizada de contraseñas dificulta que se pueda realizar un bloqueo de usuario, para aquellos colaboradores que ya no pertenecen a la Pyme.

[18] https://github.com/Tinram/MySQL-Brute

Posible acción malintencionada: La situación actual permite que un usuario de la empresa utilice la misma contraseña débil durante años. Esto aumenta las posibilidades de que un ciberdelincuente pueda averiguar las contraseñas de algún usuario activo en esa ventana de tiempo. Así, una persona no autorizada que logre ingresar con contraseñas antiguas podría realizar distintas acciones no autorizadas sobre los datos, como visualizarlos, copiarlos o alterarlos.

Red inalámbrica

La Pyme utiliza una red de datos inalámbrica para conectar a los colaboradores que trabajan con computadoras portátiles. Esta red inalámbrica tiene acceso a la red privada de la empresa y a los servidores internos como el servidor de BI y otros. La red inalámbrica se encuentra siempre encendida, tiene el nombre de la empresa y es visible desde fuera del edificio por los vecinos de la cuadra. Para conectarse solo se necesita la contraseña establecida.

Posible acción malintencionada: Existen varios métodos para ingresar a una red inalámbrica ajena sin conocer la contraseña. Una persona podría realizar intentos de autenticación mediante técnicas de ingeniería social o probando contraseñas aleatorias, utilizando un programa que automatiza el intento de conexión simulando ser un usuario. Estos programas también permiten usar archivos como diccionarios de contraseñas. Algunos de los diccionarios de contraseñas gratuitos más conocidos en Internet son Rockyou[19] y Kaonashi[20].

Otro método posible para ingresar a la red inalámbrica es utilizar un programa como Aircrack-ng, que envía solicitudes de desconexión simulando la desconexión de un usuario ya conectado y luego captura la solicitud de reconexión. La misma herramienta no permite

[19] https://gitlab.com/kalilinux/packages/wordlists/-/blob/kali/master/
[20] https://github.com/kaonashi-passwords/Kaonashi/tree/master/wordlists

ver la contraseña capturada, ya que se mantiene la de reconexión cifrada, aunque permite calcular si alguna contraseña del diccionario, el archivo con miles de contraseñas, sirve para conectarse a la red inalámbrica. Durante este proceso se compara la contraseña cifrada de reconexión capturada y cada contraseña del diccionario de manera cifrada. Las contraseñas del diccionario no se encuentran cifradas, pero el programa Aircrack-ng las calcula cifradas a medida que va realizando las pruebas, una por una. Este proceso suele demorar algunas horas hasta encontrar alguna coincidencia.

Otra alternativa complementaria es usar programas como Naive-hashcat[21] para intentar descifrar directamente la contraseña de reconexión capturada.

A continuación, se presenta una descripción gráfica del proceso de ataque:

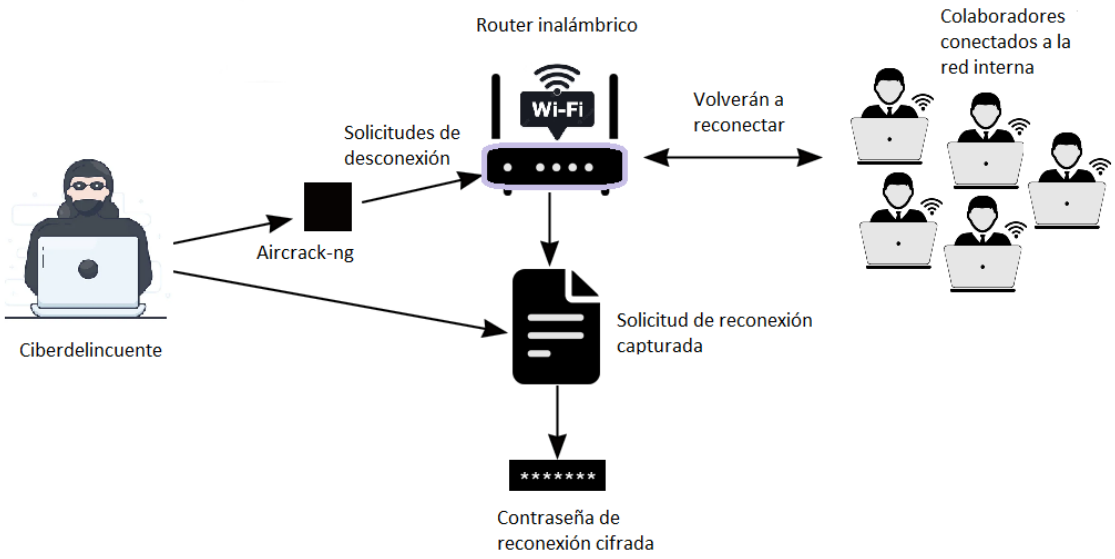


Figura 4. Representación del ataque con Aircrack-ng.

Fuente: Elaboración propia.

[21] https://github.com/brannondorsey/naive-hashcat

Los métodos de acceso a una red inalámbrica ajena de manera malintencionada están disponibles públicamente en Internet de manera gratuita, poseen tutoriales paso a paso y son expuestas en encuentros o seminarios web de seguridad informática, como una muestra de las capacidades de los ciberdelincuentes. Muchos de esos tutoriales pueden seguirse paso a paso teniendo conocimientos mínimos de computación y no requieren contar con habilidades de un experto en seguridad informática. Este escenario resulta peligroso, ya que cualquier persona con intención de acceso podría realizar ataques a la red inalámbrica, incluso desde afuera del edificio, para acceder a los servidores internos.

Capacitaciones

Aunque la Pyme cuenta con varias áreas y personal que ya lleva más de diez años trabajando en la empresa, no se han realizado capacitaciones o campañas de concientización sobre aspectos básicos de seguridad de la información. Además, el personal de tecnología no ha recibido capacitaciones sobre desarrollo seguro o gestión de incidentes de seguridad de la información.

Posible acción malintencionada: Un ciberdelincuente podría manipular a un colaborador de la Pyme con técnicas de persuasión que utilizan correos electrónicos o llamadas telefónicas para lograr algún beneficio a su favor y acceder a información que involuntariamente le sería entregada. Concretamente, podría enviar correos electrónicos falsos (en inglés, Phishing) a cualquier persona de la Pyme, con el objetivo de solicitar datos sensibles, robar sus contraseñas o comunicar que ha ganado un premio y dirigir al usuario a un sitio web malicioso para la descarga de Ransomware. En el caso de utilizar llamadas telefónicas fraudulentas (en inglés, Vishing) podría engañar al usuario que recibe la llamada haciéndose pasar por un proveedor conocido, soporte técnico o cualquier persona cercana al contexto de la Pyme y así llevarlo a entregar información confidencial.

Con el uso de estas técnicas el ciberdelincuente podría lograr que el personal de la Pyme cometa errores involuntarios, que darían pie a la materialización de una amenaza, por desconocimiento de las consecuencias de sus actos.

Copias de respaldo

La solución BI no tiene activa las configuraciones para copias de seguridad de respaldo (en inglés, backup) programadas. Esta situación no permitiría una posible recuperación de la información del servidor, en caso de sufrir algún ataque como un Ransomware, lo que daría como resultado que la solución de inteligencia de negocios no esté disponible para la gerencia y dirección.

9.3 Beneficios de los estándares en seguridad de la información

Aunque existen varios estándares, marcos de referencia o guías de adhesión voluntaria, impulsadas por gobiernos, organizaciones o por la comunidad de expertos en seguridad, el autor destaca el estándar NIST CSF[22] y la ISO/IEC 27001, que permiten gestionar la seguridad de la información en una Pyme.

Estándar del NIST

NIST es el acrónimo de Instituto Nacional de Estándares y Tecnología (en inglés, National Institute of Standards and Technology) dependiente del Departamento de Comercio del gobierno federal de los EE.UU. El marco de ciberseguridad del NIST, también conocido como NIST Cybersecurity Framework o NIST CSF, es una guía que permite a las organizaciones, evaluar y establecer un plan de mejora continua para ciberseguridad. Fue creado en 2013 y plantea cinco funciones principales y continuas para mantener la ciberseguridad, las cuales son: identificación, protección, detección, respuesta y recuperación. Dentro de cada función se determina un conjunto de medidas o controles que producen resultados específicos, que forman parte del ciclo de vida del proceso de gestión de riegos de la seguridad cibernética.

Dicho marco está basado en estándares existentes, como NIST SP 800-53 Rev.4, ISO/IEC 27001:2013 y COBIT 5.

Algunos de los beneficios que aporta el marco del NIST y que además, son similares en las distintas versiones de la ISO/IEC 27001 son los siguientes:

- Describir la postura actual de la empresa, la deseada y su progreso, con relación a la ciberseguridad.

[22] https://www.nist.gov/cyberframework/framework/

- Identificar y priorizar oportunidades de mejora continua en un ciclo repetible.
- Identificar riesgos y activos que requieren protección.
- Disponer de un sistema simple que sirva a las partes interesadas internas y externas en relación con los riesgos de ciberseguridad.

Beneficios que aporta el estándar ISO/IEC 27001:2022 con relación a la seguridad de la información almacenada

¿Por qué considerar la norma ISO/IEC 27001:2022 en las Pyme?

La norma ISO ISO/IEC 27001:2022 es el resultado del trabajo conjunto entre el Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la información y el Subcomité SC 27, Seguridad de la información, ciberseguridad y protección de la privacidad. Su valor radica en constituirse como guía oficial con buenas prácticas recomendadas en consenso por expertos de varios países, para establecer, implementar y mantener un Sistema de Gestión de la Seguridad de la Información o SGSI. El alcance del SGSI se debe documentar y puede variar considerando las características de la organización, las unidades del negocio, los activos de información, los procesos principales y las ubicaciones físicas de la empresa.

El mantenimiento de un SGSI está afectado constantemente por las necesidades de la organización, por sus procesos y por su tamaño. El SGSI ayuda a preservar correctamente la confidencialidad, integridad y disponibilidad de la información, mediante una adecuada gestión del riesgo a lo largo del todo el ciclo de vida de la información. Este ciclo, abarca diferentes fases, como el uso, creación, tratamiento, almacenamiento, transmisión, borrado y destrucción.

Por otra parte, una Pyme argentina puede adquirir la norma completa en español a través de IRAM, aunque por el momento, solo se encuentra disponible la versión IRAM-ISO-IEC 27001:2015[23], que aún es válida por tres años desde el momento de certificación.

[23] https://catalogo.iram.org.ar/#/normas/detalles/10195

Posteriormente se deberá hacer la actualización a la versión 27001:2022. Algo muy importante es que la norma puede ser utilizada tanto de manera interna como externa, para evaluar y comprobar la capacidad de la empresa para cumplir los requisitos de seguridad de la información. Así, sirve como base para el cumplimiento legal y puede ser presentado ante terceras partes interesadas, como auditores del gobierno, proveedores o inversionistas.

Se aclara que no es posible disponer de una guía oficial de este nivel de especialización en español, por un costo más bajo que el ofrecido por IRAM en su sitio web.

Beneficios generales que aporta la norma ISO/IEC 27001:2022 en materia de seguridad

En cualquier organización donde nunca se realizó un trabajo sobre gestión de la seguridad de la información es muy positivo considerar la norma ISO/IEC 27001:2022 como guía, ya que permitirá implementar los pilares fundamentales de la seguridad de la información, que son, integridad, confidencialidad y disponibilidad, de una manera profesional, sobre la base de una adecuada evaluación y gestión de riesgos y con perspectiva de largo plazo.

A continuación, se mencionan algunos beneficios que aporta la norma independientemente del ámbito o sector del negocio, tamaño de la organización o ubicación geográfica:

1. Compresión del contexto: El primer beneficio, es que el estudio de la norma ayuda a comprender cuestiones clave, como el contexto de la organización y su capacidad con relación a la seguridad de la información. Además, hace visibles temas importantes que surgen del análisis e involucran intereses de terceros, especialmente clientes, como las obligaciones legales y requerimientos contractuales.

2. Lineamiento para la implementación de un sistema de gestión de la seguridad de la información: Este sistema será fundamental para contribuir a garantizar que la

seguridad de la información es gestionada correctamente. Además, será sistemático, documentado y conocido por toda la empresa.

3. Identificación de los activos de información y su valor: El uso de la norma permite identificar y evaluar los activos de información más importantes y críticos de la organización, sobre los cuales luego se tomarán medidas de protección. Sin esta información el negocio podría sufrir inconvenientes parciales o totales en su normal funcionamiento y el logro de sus objetivos estratégicos podrían verse afectados. Para estos activos se asignarán responsables y se determinará lo que se considera como su uso aceptable. La aplicación de la norma permitirá mantener el valor de los activos de información y evitar incidentes que puedan afectar la operación normal de la empresa.

4. Creación de una política de seguridad de la información: La norma facilita la creación y definición de una política de seguridad de la información para toda la organización. Esta política proporciona la posibilidad de que se alcancen objetivos concretos y de generar conciencia y compromiso en todos los colaboradores para fomentar una cultura empresarial más favorable.

5. Mejora en la comunicación interna: Con la norma como guía, el ejercicio de mantenimiento y mejora continua de la seguridad de la información facilita una mejora notable en la comunicación entre los colaboradores y el directorio, ya que la dirección asignará roles, responsabilidades y canales de comunicación con una interacción frecuente planificada.

6. Transformación de la cultura organizacional: Indudablemente, a partir de las capacitaciones al personal y campañas de concientización se afectará de manera positiva la manera de hacer las cosas a diario, lo que minimizará el impacto de los riesgos innecesarios en la operación o que pueden evitarse con un mínimo de conciencia respecto a la gestión segura de la información. Así, los colaboradores

entenderán la protección de los activos de información como algo realmente necesario, en lugar de verla como un obstáculo que ralentiza o entorpece sus trabajos.

7. Control de permisos en los sistemas de información: A partir de la optimización de procesos y la separación de responsabilidades recomendadas en la norma, se podrá controlar periódicamente a los usuarios activos y las acciones que realizan los colaboradores en los sistemas de información de la empresa. Con esto, se podría evitar el uso indebido de los sistemas, el fraude y los abusos de privilegios. Incluso, la norma ayuda a crear controles para la correcta gestión de baja y bloqueo de los usuarios que ya no pertenecen a la organización y otros como el bloqueo automático de las computadoras desatendidas.

8. Uso de contraseñas fuertes: El uso de la norma permite establecer lineamientos y requisitos para el uso de contraseñas seguras, con lo que se mantiene un estándar de calidad con contraseñas fuertes. Por ejemplo, las contraseñas serán conformadas por combinaciones de letras, números y símbolos, con una longitud de doce o dieciséis dígitos, en función de la criticidad de los datos a proteger. Además, se logra controlar cuestiones como la rotación temporaria de contraseñas. Consecuentemente, se evita el acceso indeseado a los sistemas internos por parte de personas que no pertenecen a la organización, en caso de que logren descubrir una contraseña débil en uso.

9. Control de accesos físicos: La norma da recomendaciones para analizar y definir una correcta ubicación física de los armarios o racks de telecomunicaciones donde se encuentran los servidores. Se podrá crear una política de control de acceso para gestionar y otorgar accesos físicos a colaboradores que lo requieran y justifiquen adecuadamente. Además, esta política sirve como base para controlar otro tipo de accesos, como los accesos lógicos, por ejemplo, la conexión a la red privada virtual o VPN y los accesos internos a la red inalámbrica.

10. Perfeccionamiento del área de TI: Al utilizar la norma como guía se generará un aumento de conciencia en el área de TI, ya que esta deberá interiorizarse en las capacidades requeridas que debe desarrollar para apoyar al negocio. Algunas de estas cuestiones son la seguridad en la nube, el uso de criptografía y la recuperación de desastres. Además, el área podrá entender el grado de exposición a Internet de los sistemas que administra y las vulnerabilidades existentes en sus sistemas en producción, las cuales podrían ser aprovechadas por ciberdelincuentes.

11. Estandarización de los ambientes de sistemas: La norma permite adaptar buenas prácticas sobre la separación y control de los ambientes de sistemas. Normalmente se utilizará tres ambientes, denominados producción, desarrollo y pruebas. Esto ayuda a evitar cambios y errores no autorizados en los sistemas en producción, ya sea en ambientes propios o de clientes. Además, facilita una correcta gestión y control de los cambios que suceden a diario. Así, las situaciones de cada ambiente estarán controladas, documentas y actualizadas.

12. Gestión del capital humano y recursos: El negocio tendrá la posibilidad de dimensionar o redimensionar las capacidades del capital humano y recursos tecnológicos, para mantener la seguridad de la información en toda la organización, ya que ante la ausencia de una gestión adecuada podría existir una falsa creencia de que no se necesita capital humano concientizado.

13. Estandarización del desarrollo de software: Se tendrá la posibilidad de definir un estándar de desarrollo seguro, que incluya los aspectos técnicos de la seguridad de la información. Así, se logrará implementar un estándar para todos los proyectos de desarrollo de software, que impida el aprovechamiento de errores técnicos y vulnerabilidades ya conocidas por los ciberdelincuentes.

14. Generación de una base de conocimiento: A través de la implementación de la norma se podrá mantener el conocimiento documentado dentro de la empresa y evitar su fuga con la rotación del personal.

15. Continuidad del negocio: Los planes de continuidad del negocio deberán incluir la continuidad de seguridad de la información, habilitando que se encuentre presente y sea considerada en los planes de recuperación de desastres, ya sea puntualmente de la solución de BI, del área de seguridad o cualquier otra área de la empresa.

16. Acuerdos de confidencialidad: Con la norma se podrá proteger la información de la empresa considerando cuestiones legales, a partir de la revisión de contratos con clientes, proveedores y personal interno, a fin de garantizar que se cumplan condiciones legalmente exigibles de confidencialidad, disponibilidad, no divulgación y secretos comerciales.

Beneficios del estándar ISO/IEC 27001:2022 con relación a la seguridad de la información almacenada

La norma ofrece un marco serio para implementar buenas prácticas en el tratamiento y gestión segura de la información almacenada. Incluye lineamientos sobre los procedimientos de recuperación de información y la eliminación de la información obsoleta en poder de las Pyme. Así, el tratamiento de estos temas permitirá que la organización pueda identificar, evaluar, gestionar y ser más consiente de los riesgos relacionados a la gestión de la información almacenada. Por otra parte, se podrá trabajar en los riesgos que se desea tratar y en los que se desea aceptar, con el objetivo de mantener la confidencialidad, integridad y disponibilidad de la información, en cumplimiento de las obligaciones legales, los objetivos definidos por la dirección y sobre la base del principio de costo-beneficio.

Algunos beneficios concretos:

1) Información almacenada: La norma ayuda a definir qué información es importante o crítica para el negocio, controlar el acceso y evitar el uso inapropiado de la información. Además, facilita la prevención de las modificaciones no autorizadas y restringir y auditar el acceso remoto a la información. Por otra parte, permite tener control en la gestión de información confidencial de usuarios utilizada en la autenticación, como las contraseñas. También, ayuda a definir canales de comunicación correctos para las transferencias de información.

2) Recuperación de la información: Asiste en la implementación de controles en los procesos de recuperación y facilita los procesos utilizados para restringir y auditar el acceso a los archivos de copias de seguridad. Además, posibilita implementar prácticas seguras en pruebas de recuperación de información periódicas, en apoyo al plan de recuperación de desastres existente en la organización.

3) Eliminación de la información: Permite implementar control en sus procesos, segregación o separación de funciones, así como buenas prácticas para el borrado seguro y destrucción de medios físicos de almacenamiento. Además, habilita el tratamiento de cuestiones tales como el registro de las acciones de eliminación de información, que luego serán válidas en las auditorías.

Otros beneficios que permite la norma y que son aplicables a los tres puntos anteriores son los siguientes:

- Brinda la posibilidad de tener mediciones periódicas para exponerlas en reportes ejecutivos.
- Permite actualizar el alcance de los procedimientos de gestión, en caso de que la normativa o necesidad del negocio lo requiera.

En resumen, la gestión de la seguridad de la información requiere que se trabaje en un ciclo de mejora continua, que permite la planificación, ejecución y control, que es lo que construye información valiosa y concreta sobre cómo tratar la información en la empresa. Uno de los beneficios más relevantes es que las Pyme podrán mostrar con indicadores concretos la gestión segura de la información en sus entornos a otras personas interesadas, como auditores privados y del gobierno, clientes, nuevos clientes, proveedores e inversionistas. Esto es indudablemente beneficioso para el negocio, ya que tiene un impacto positivo en la obtención de nuevos clientes y en la retención de los actuales y una mejor gestión de los proyectos existentes.

Para el caso puntual de la Pyme analizada, permitirá retomar el contacto con empresas a las que no se pudo prestar servicios de marketing digital años anteriores, ya que se solicitaba demostrar un tratamiento seguro de la información alineado con la ISO 27001, tal como lo demanda actualmente el mercado internacional.

9.4 Riesgos para el negocio cuando no se tiene en cuenta la seguridad de la información en soluciones de BI

Entre los riesgos más relevantes que afectan negativamente al negocio se encuentran los siguientes; accesos no autorizados, fuga de datos interna y divulgación no autorizada, con el consecuente posible daño a la reputación de la marca, retiro de accionistas y deterioro de capacidades en la dirección estratégica. A continuación, se expone un detalle sobre cada uno de estos riesgos.

Accesos no autorizados

Una de las situaciones repetitivas dentro de las Pyme es la de rotar el personal en diferentes proyectos, clientes o posiciones laborales. Desde el punto de vista de la seguridad se deben controlar los privilegios otorgados, ya que en muchas ocasiones un colaborador que fue responsable de un proyecto que ya finalizó, se queda con los permisos en varios sistemas con el rol de gerente, siendo que su función actual es solo operativa. Otro caso similar es el inverso, es decir cuando un colaborador aumenta su jerarquía pasando de un puesto operativo a ser gerente y a estar a cargo de un cliente o cartera de proyectos. En este caso, se deberían retirar los permisos del rol operativo, para poder mantener una correcta segregación de funciones y respetar el flujo de autorizaciones.

Lo mismo aplica en los sistemas para inteligencia de negocios. En este caso, la Pyme ha dejado con accesos activos al servidor de BI a algunos colaboradores que ya no pertenecen al área de TI. Incluso, podría haberlo hecho con otras personas que ya no se encuentran en relación de dependencia con la empresa. La falta de control sobre los usuarios activos de la solución de BI podría permitir acciones indeseadas sobre la seguridad de la información, como los siguientes:

- Accesos no autorizados, ya sea de visualización interna o remota desde Internet. Así, se afecta a la confidencialidad de la información.

- Modificación de la información, que afecta la integridad.
- Visualización o alteración de copias de archivos y bases de datos, que afecta la confidencialidad y la disponibilidad.
- Borrado de información, que afecta la disponibilidad.

Fuga de datos interna

El hecho de no contar con un mapa de datos empresarial imposibilita la visibilidad de la interrelación entre los sistemas. Además, al no existir una clasificación de los activos de información tampoco se sabe con certeza la criticidad de cada fuente de información, por lo que se trata a todas con igual importancia. A todo esto, se le suma la faltante de un sistema de monitoreo en tiempo real, que dificulta poder detectar determinadas acciones que realizan los usuarios que podrían estar relacionadas a la fuga de datos. Esta situación posibilita que una fuga de información pueda no ser detectada, por ejemplo, la acción de conexión de un dispositivo de almacenamiento USB a un servidor, una pérdida intencional de una computadora portátil de la empresa, el gran uso repentino de la red de datos cableada o inalámbrica, una gran actividad de escritura en el disco rígido de una computadora portátil, la conexión de un usuario a VPN en un horario inusual o el uso repentino de la conexión a Internet desde la oficina hacia algún servicio de almacenamiento en la nube. Todas las mencionadas son acciones típicas que pueden revelar conductas indeseadas de usuarios que roban información. En contextos como el descripto, que caracterizan a una Pyme, pueden ocurrir sin ser detectadas y el riesgo estará siempre presente mientras no se tomen medidas de detección y prevención.

Divulgación no autorizada, daño a la reputación de la marca y retiro de accionistas

Para ilustrar este tipo de riesgos, se cita a continuación un caso públicamente conocido que puede ser aplicado, como se verá más adelante, a una Pyme argentina.

Caso Facebook, año 2018.

El problema con Cambridge Analytica hizo caer las acciones de la empresa Facebook, actualmente llamada Meta, el día veintiséis de julio de 2018. La caída de las acciones fue de cerca del 19% en solo 24 horas.

Según el diario estadounidense The New York Times, la compañía perdió aproximadamente 120.000 millones de dólares de su capitalización. El día de la caída comenzó con el precio de sus acciones en 215 dólares y cerró el mismo día a 176 dólares.

A continuación, se presenta el registro de la caída de las acciones en Nasdaq:

Nota. Gráfico de acciones de META en Nasdaq, por Nasdaq, 2023 (https://www.nasdaq.com/market-activity/stocks/meta/advanced-charting).

Nasdaq (en inglés, National Association of Securities Dealers Automated Quotations) es la segunda bolsa de valores electrónica automatizada más importante de Estados Unidos. Se caracteriza por comprender empresas de alta tecnología en electrónica, informática, telecomunicaciones, biotecnología y otras.

Síntesis del problema

La consultora británica Cambridge Analytica, creada en el año 2013, era una empresa privada con sede en Londres que utilizaba análisis de datos para desarrollar campañas para marcas y políticos.

Esta empresa adquirió de forma indebida información de 50 millones de usuarios de la red social Facebook en Estados Unidos.

La obtención de perfiles de 50 millones de usuarios de Facebook no fue obra de Cambridge Analytica, sino que se le atribuye a Aleksandr Kogan, un investigador que trabajaba en la Universidad de Cambridge en Inglaterra. A modo de proyecto personal, Kogan desarrolló en 2013 un test de personalidad en formato de aplicación de Facebook. Luego, unos 265.000 usuarios completaron el test que requería permiso para acceder a su información personal y las de su red de amigos, sin el consentimiento de ellos. Así, Kogan obtuvo todos esos datos con su aplicación.

Después de un tiempo, Facebook aseguró que ya no era posible que una aplicación accediera a la información personal de los amigos de los usuarios, aunque cuando Kogan desarrolló el test, esa opción dependía de la configuración de privacidad de cada usuario. Kogan accedió a actualizaciones de estado, acciones de "me gusta" realizadas por los usuarios y mensajes privados de más del 15% de la población de Estados Unidos. Luego, vendió los datos a la empresa Cambridge Analytica.

Facebook, afirmó que en 2015 cuando se enteró de que la investigación de Kogan había sido entregada a Cambridge Analytica, violando sus condiciones de servicio, retiró la aplicación de Kogan del sitio. Posteriormente, había exigido y recibido una certificación de que los datos habían sido destruidos.

Según las políticas de Facebook, los datos recopilados en su plataforma solo podían ser usados para propósitos de la misma aplicación y no podían ser transferidos o vendidos. Facebook aseguró que no se habían extraído contraseñas ni datos confidenciales, aunque Cambridge Analytica sí disponía de información sobre la ubicación de los usuarios.

Luego del incidente, el director ejecutivo de Facebook, Mark Zuckerberg, publicó en la red social que reconocía que la empresa había cometido errores y asumía la responsabilidad por el hecho.

En los años que siguieron, los fiscales generales de Nueva York y Massachusetts solicitaron a Facebook documentos sobre las violaciones de los términos de servicio y copias de todas las comunicaciones entre Facebook y Cambridge Analytica, entre otros materiales. Los fiscales estimaron que la recolección de datos podría violar las leyes de privacidad en Gran Bretaña y de varios Estados de los Estados Unidos de Norteamérica. Por otra parte, la Agencia de Protección al Consumidor de Estados Unidos[24] (en inglés, Federal Trade Commission o FTC) abrió una investigación para demandar y multar a Facebook.

¿Qué costo tuvo la multa de la Agencia de Protección al Consumidor (FTC)?

En el expediente número 19-cv-2184[25] el juzgado de Estados Unidos ordena a Facebook en junio del año 2019 a pagar una multa de 5.000 millones de dólares, con un plazo de pago de siete días. La FTC alegó que Facebook no realizó una gestión adecuada para trabajar con las aplicaciones de terceros y que la misma compañía sabía que se estaban violando las políticas de su plataforma.

¿Qué puede aprender una Pyme argentina sobre el caso Facebook?

A partir de este caso, las Pyme de Argentina deben aprender que, además de una pérdida económica importante y el daño a la reputación de la marca o empresa, el gobierno puede exigir legalmente el cumplimiento de las normas aplicables en cuanto a la gestión de los datos, en este ejemplo, a los datos personales y su seguridad.

[24] https://www.ftc.gov
[25] https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_stipulated_order_7-24-19.pdf

En este caso, el juzgado exigió a Facebook algunas cuestiones específicas que en realidad son fundamentales en una correcta gestión de seguridad de la información.

Algunas de estas exigencias fueron las siguientes:

- Programa de seguridad de la información: Establecer, implementar y mantener un programa de privacidad integral que proteja la confidencialidad y la integridad de la información, recopilada, utilizada o compartida por el negocio. Debe contener salvaguardas apropiadas para el tamaño, complejidad y el alcance de las actividades del negocio.
- Políticas: Documentar por escrito el contenido, implementación y mantenimiento de la política de privacidad.
- Riesgos: Realizar la evaluación de riesgos y documentarla. Documentar las salvaguardas requeridas para mitigar los riesgos y mantener la confidencialidad e integridad de la información. Además, dejar evidencia de los controles que se identificaron y no fueron implementados y cada razón por las que no se implementaron.
- Capacitación: Describir el entrenamiento requerido para implementar y monitorear el programa de seguridad, incluidos los procedimientos utilizados para evaluar y ajustar su contenido con un ejercicio de mejora continua.
- Concientización: Establecer programas regulares de concientización en privacidad para todos los colaboradores, al menos una vez al año.
- Asignar responsables: Designar uno o más colaboradores que se encuentren calificados para coordinar y ser responsables del programa de seguridad.
- Auditorías: Evaluar y documentar al menos una vez al año los riesgos internos y externos en cada área de su operación.
- Contraseñas: Proteger criptográficamente las contraseñas de usuarios cuando se almacenan y cuando están en tránsito por la red de Internet. Implementar escaneos automáticos regulares diseñados para detectar si alguna contraseña de usuario es almacenada en formato de texto sin cifrado. Utilizar herramientas que determinen la

fortaleza de las claves seleccionadas por los usuarios y rechazar aquellas que no sean acordes con el tipo de acceso a proteger.

- Control de acceso: Utilizar mecanismos que impidan que terceros no autorizados puedan acceder a la información de usuarios almacenada en los servidores.
- Información de usuario: Implementar procedimientos para eliminar de los servidores la información generada por el usuario.
- Teléfonos: No compartir con ningún tercero los números de teléfonos celulares de usuarios que hayan brindado su número para usar el doble factor de autenticación en el acceso a su cuenta.
- Implementaciones: Antes de implementar cada producto, realizar una revisión que evalúe los riesgos para la disponibilidad, confidencialidad e integridad de la información. Documentar lo implementado y los controles de seguridad aplicados.
- Consultores expertos: Consultar y buscar la orientación adecuada de expertos externos e independientes sobre protección, privacidad, implementación, mantenimiento y actualización de seguridad de la información.

Deterioro de capacidades en la dirección estratégica

Aumento de incertidumbre en la Dirección

Con la pérdida de la disponibilidad de una solución de BI que la Dirección está acostumbrada a utilizar para hacer un rápido análisis y tomar decisiones ágiles, indudablemente, el trabajo se verá afectado, ya que quienes deben tomas las decisiones no tendrán a mano información de alto nivel resumida, precisa y actualizada para analizar. Esto puede repercutir en un deterioro de la calidad de las decisiones que se tomen y en un aumento de la incertidumbre en los decisores.

9.5 Plan inicial con recomendaciones para asegurar soluciones de BI en las Pyme de Argentina

El plan para asegurar las soluciones de BI en las Pyme argentinas, que se detalla a continuación, pretende que se puedan implementar y mantener los lineamientos de seguridad de la información expuestos en la norma ISO/IEC 27001:2022. Así, se podrá disponer de controles que protejan la confidencialidad, integridad y disponibilidad de la información.

El autor recomienda abordar el plan en las siguientes etapas:

- Etapa 1. Relevamiento de situación actual: realizar una inspección visual de las instalaciones e infraestructura tecnológica, registro fotográfico, revisión de la documentación de implementación existente o entrevistas al personal de TI que había participado en el proyecto de la solución de BI. Esto permitirá entender el contexto.

- Etapa 2. Documentación: actualizar la existente y generar documentación de la situación actual, si fuera necesario. Considerar la creación de diagramas utilizando algún marco de referencia que permita visualizar relaciones a alto nivel, como, por ejemplo, las primeras cuatro fases de la arquitectura empresarial de TOGAF[26]. Estas cuatro fases son, la de arquitectura de negocios, datos, aplicación y tecnológica. Así, se podrá analizar en su totalidad la solución de BI, sus relaciones con el negocio y reevaluar su nivel de criticidad.

- Etapa 3. Análisis de riesgos: crear o actualizar el inventario de activos de información con todos los elementos pertenecientes a la solución de BI. Realizar un análisis de amenazas y considerar la última versión del informe anual con el top 10 de vulnerabilidades de la fundación OWASP. Realizar una estimación de alto nivel del impacto en el negocio.

[26] https://pubs.opengroup.org/togaf-standard/architecture-content/chap03.html#tag_03

- Etapa 4. Proyectos: lograr una presentación priorizada de todos los proyectos con estimación de recursos, para la mitigación de los riesgos identificados.
  - La presentación o tablero de proyectos debe contener mínimamente: identificador, nombre, tiempo o plazo estimado y responsable.
  - Presentar un detalle por cada proyecto: identificador, nombre, objetivo, responsable, descripción, activos afectados, pilares de seguridad de la información afectados, duración, recursos y costo estimado.

- Etapa 5. Cumplimiento y auditorías: generar la documentación sobre las auditorías realizadas a los proyectos.
  - Presentar un detalle por cada proyecto auditado: fecha, descripción, responsable, identificador de proyecto, hallazgos, no conformidades y oportunidades de mejora, fecha finalización de control y firma del auditor.

- Etapa 6. Informes a la dirección: crear y presentar un informe ejecutivo.

Resumen priorizado de recomendaciones para asegurar soluciones de BI en las Pyme de Argentina

A continuación, se presentan todos los proyectos priorizados en orden a modo de resumen, con una escala de valoración del uno al diez, donde el número uno es el más prioritario. Además, se discriminó cuáles tiene mayor impacto en el control de accesos y cuáles en la protección de la información almacenada. Con la implementación de estos proyectos se espera mitigar los riesgos y asegurar las soluciones de BI en las Pyme de Argentina.

Control de accesos	Prioridad
Protección lógica del servidor	1
Contraseñas	2
Registro de eventos de sistemas	2
Control de administradores	2
Autenticación	3
Garantizar disponibilidad	3
Criptografía	3
Red de datos	4
Seguridad física	5
Monitoreo del servidor	6
Documentación	6
Seguridad en la Nube	7
Puestos de trabajo	8
Pruebas de penetración	9
Revisión independiente del cumplimiento	10

Protección de la información almacenada	Prioridad
Consultoría legal	1
Control de cambios en los sistemas	2
Desarrollo seguro	3
Acuerdos de confidencialidad	3
Recuperación de desastres	3
Criptografía	3
Concientización y entrenamiento	4
Resguardo de información	4
Medios de almacenamiento y borrado seguro	5
Gestionar incidentes de seguridad	6
Documentación	7
Transferencias externas de información	7
Control de licencias	8
Ciclo de vida de los datos	9
Revisión independiente del cumplimiento	10

Tabla 1. Proyectos para la mitigación de riesgos.

Fuente. Elaboración propia.

Detalle de las recomendaciones para los proyectos de control de acceso

Protección lógica del servidor

- Se debe actualizar o reinstalar el sistema operativo, es recomendable dejar en uso la última versión, ya que es la que recibe actualizaciones periódicamente. Para el caso de Linux, se debe utilizar la última versión con soporte oficial conocida por las siglas LTS (en inglés, Long Term Support).
- Se debe implementar un antivirus con detección de tráfico de red, para poder proteger al sistema operativo contra ataques de Malware, Ransomware u otros de carácter similar. Se debe tener en cuenta que será mejor utilizar una consola de antivirus centralizada, que permita administrar todas las computadoras o servidores de la empresa a través de un mismo sistema, generalmente denominado orquestador.
- Se debe implementar un cortafuego a nivel de servidor (en inglés, host-based firewall), este será utilizado para bloquear los intentos de autenticación fallidos. En el caso de Linux, se podría utilizar el programa gratuito Fail2ban[27] o uno de similar propósito. Para Windows existe una versión similar llamada IPban[28].

Contraseñas

- Definir un estándar de contraseña segura, por ejemplo, que incluya una combinación de letras, números y símbolos, con una longitud mínima de doce caracteres.
- Se debe explicar a los usuarios que deben ser conscientes por la responsabilidad individual del secreto de su contraseña y que no deberán divulgarla incluso a personal con mayor autoridad.
- Las contraseñas no deben ser escritas es papel, únicamente será permitido el uso de repositorios de contraseñas indicado por la empresa.

[27] https://www.fail2ban.org/wiki/index.php/FAQ_spanish
[28] https://ipban.com/help/

- La expiración de contraseñas será en un periodo corto, por ejemplo, tres meses. Además, no se podrá reutilizar una misma contraseña antigua.

Estos criterios estrictos para las contraseñas serán principalmente de aplicación en sistemas e información catalogada como crítica.

Registro de eventos de sistemas

- Implementar un servidor o programa que centralice registros de eventos de los sistemas, lo cual será especialmente útil para auditar acciones de usuarios y entender el uso inapropiado de los sistemas, ya sea por software malicioso o por personal interno, incluyendo administradores. Debe ser posible la identificación de los usuarios conectados, la computadora origen, archivos que fueron accedidos y los privilegios utilizados. En Linux se puede utilizar el servidor de registros de eventos gratuito llamado Syslog (en inglés, System Logging Protocol[29]) que cumple con las especificaciones estándar u otras con mejores interfaces visuales como Graylog[30], también gratuito.
- Junto a este servidor se utilizará un programa coordinador de horario utilizando el protocolo estándar (en inglés, Network Time Protocol o NTP) para poder registrar las fechas y horas exactas que se graban en los archivos de registro de eventos. En Internet, existen servidores externos a los que se le puede consultar la hora de manera gratuita, por ejemplo, el servidor llamado 2.ar.pool.ntp.org[31]. Sin la aplicación de tiempo sincronizado en los equipos y registros de eventos, el personal de seguridad no podrá realizar una correcta correlación de eventos, que permita descubrir asociaciones lógicas entre los diferentes hechos, lo que imposibilita descubrir la causa raíz de los problemas y tener precisión en las actividades de auditoría.

29 https://www.rfc-editor.org/rfc/rfc5424
30 https://www.graylog.org/products/source-available/
31 https://www.pool.ntp.org/zone/ar

Control de administradores

- Se debe controlar los accesos y auditar las acciones realizadas de los usuarios con privilegios elevados o administradores de la solución de BI. Además, se debe evitar la utilización de un solo usuario administrador para todo, como por ejemplo las cuentas root o admin. En su lugar se debería asignar usuarios específicos a personas para una mejor auditoria de las acciones. Esto aplica a la Pyme y también se extiende a proveedores o consultores, quienes no deben utilizar una única cuenta de usuario compartida, ya que en caso de tener rotación de personal se podrían divulgar las contraseñas de acceso a terceros sin relación laboral. Es necesario disponer de una lista explicita del personal y otorgar accesos individuales.
- Se debe auditar las actividades de los consultores externos en la solución de BI que utilicen privilegios elevados.
- Los administradores deben estar informados acerca de sus responsabilidades en el uso de los sistemas respecto a la seguridad de la información, antes de que se otorguen sus privilegios elevados.
- Los administradores deben utilizar únicamente el repositorio de contraseñas de la empresa como medio para almacenar contraseñas.

Autenticación

- Se debe utilizar doble factor de autenticación para el acceso a la solución BI, siempre que sea posible. Con esto se logra recibir por otro medio, por ejemplo, un mensaje de texto en un teléfono celular o un código numérico por email, una doble confirmación para lograr el ingreso seguro al sistema. Esto también es llamado “autenticación en dos pasos”.
- Establecer política de bloqueo de usuario por cantidad de intentos de autenticación fallidos, por ejemplo, bloqueo por tres intentos fallidos en un minuto. Además, el bloqueo de un usuario debe registrarse y generar un evento de seguridad que debe ser revisado por personas.

- Establecer una política de expiración de tiempo de sesión, por ejemplo, desconexión de usuario automático si la sesión de usuario permanece inactiva por más de cinco minutos en la solución de BI.
- Las creaciones de usuarios en los sistemas deben ser gestionadas por personal de seguridad en conformidad del procedimiento establecido, por ejemplo, el de solicitud o petición de acceso. Además, dicho personal asignará una contraseña temporal y el sistema solicitará al usuario un cambio de la misma en el primer uso del sistema.

Garantizar disponibilidad

- Es imprescindible que se pueda garantizar la disponibilidad de la solución de BI. Para esto, se pueden considerar cuestiones de hardware como el uso de doble conexión a la red de datos a través de dos interfaces de red, doble conexión a la red eléctrica con dos fuentes de alimentación de servidor, grupo redundante de discos de almacenamiento independientes (en inglés, RAID), etc. La arquitectura tecnológica de la implementación debe estar documentada y actualizada.
- Se debe controlar las condiciones ambientales, humedad y temperatura de la oficina con racks de telecomunicaciones.
- Se debe controlar periódicamente los sistemas de alimentación eléctrica ininterrumpida (en inglés, UPS), las baterías y realizar cortes programados de electricidad para comprobar su correcto funcionamiento.

Criptografía

- Si el servidor tiene instalado el sistema operativo Linux, se debe utilizar criptografía para generar las claves RSA[32], con el fin de autenticar administradores de la solución

[32] https://www.ibm.com/docs/es/sia?topic=kbaula-enabling-rsa-key-based-authentication-unix-linux-operating-systems-2

BI de manera exclusiva. Este proceso es generalmente denominado generación de par de llaves para conexiones SSH. El par de llaves debe ser generado y configurado por el personal de seguridad.

- Los archivos de las claves deben ser almacenadas en el repositorio de contraseñas de la empresa y deben tener un vencimiento definido, por ejemplo, un año.
- Las soluciones de BI que tengan acceso web y utilicen certificados SSL (en inglés, Secure Sockets Layer[33]) deben ser controlados por personal de seguridad, ya que los certificados SSL son emitidos por una entidad o empresa externa y en general, poseen vencimiento anual. Así, se garantiza la correcta creación de una conexión cifrada entre el servidor que tiene el sitio web y el navegador del usuario que visita el sitio web. Sin un certificado SSL vigente, el acceso web podría quedar inaccesible para el usuario que intenta ingresar.

Red de datos

- Se debe establecer un sistema de monitoreo en tiempo real de la red de datos, con el fin de tener visible los volúmenes de tráfico que circulan pudiendo identificar origen y destino. El mismo sistema debe monitorear el servidor de BI.
- Se debe separar las redes en segmentos de red local, a fin de aislar cualquier actividad maliciosa dentro de la red. Esta separación es llamada red de área local virtual o VLAN. Así, quedarán separados los tres ambientes de sistemas, producción, desarrollo y pruebas.
- Los teléfonos celulares no deben tener acceso a la red del servidor de BI, ya que en algunos casos no poseen antivirus y es necesario evitar la propagación de Ramsonware a través de la red inalámbrica.

[33] https://aws.amazon.com/es/what-is/ssl-certificate/

- Restringir el acceso al servidor de BI a través de la red inalámbrica y cableada solo a notebooks específicas a través de su dirección física de red o MAC, a fin de prevenir accesos no autorizados.
- Restringir la conexión del servidor BI a Internet. Solo permitir conexión a los sitios que sean necesarios, por ejemplo, las fuentes de datos.
- Evitar la exposición de la solución de BI a Internet. Para conectarse se deberá utilizar la red privada virtual (en inglés, VPN).
- La red privada virtual que utilicen los consultores de BI deberá estar restringida para acceder únicamente a la dirección de red del servidor de BI. Además, estará limitada en velocidad de conexión ya que si un consultor sube mucha información al servidor de BI usando la conexión por VPN podría saturar la conexión a Internet de la Pyme, provocando una navegación lenta a Internet o cortes en las videoconferencias u otras aplicaciones de streaming.
- Se deberá bloquear los intentos de doble conexión a la VPN a todos los usuarios.
- Los puertos de conexión de área local (en inglés, LAN) que no están siendo utilizados deben ser apagados por el administrador de la red de datos, para evitar conexiones indeseadas que usen un cable de red.

Seguridad física

- Se debe definir la correcta ubicación del equipamiento de TI, rack de telecomunicaciones y del cableado de datos y eléctrico de la solución de BI. Además, se debe lograr la limitación de acceso, registro y control de acceso físico a la oficina donde se encuentre el equipamiento o rack, por ejemplo, utilizando en la puerta una cerradura electrónica con tarjeta magnética y número de identificación personal (en inglés, PIN). Así, la apertura de esta puerta debe generar un evento de seguridad vía correo electrónico para revisión.
- Cada rack de telecomunicaciones debe tener su cerradura correspondiente y no debe permanecer abierto.

- Considerar videocámaras IP o videovigilancia con al menos dos cámaras en la oficina que contiene el rack de telecomunicaciones, las actividades en el sitio, incluso de administradores, deben poder ser supervisadas y auditadas. Las tareas de mantenimiento fuera del horario laboral deben tener autorización previa de la dirección.
- El personal ajeno a TI o Seguridad debe tener autorización de la dirección para el ingreso a la sala de telecomunicaciones y servidores.

Monitoreo del servidor

- Se debe poder monitorear las capacidades del servidor en tiempo real, a través de un programa de monitoreo, el cual debe permitir analizar el uso del hardware, como el procesador, memoria principal, discos, procesos y los programas en ejecución. Cualquier comportamiento fuera de los valores normales debe generar un evento de seguridad para su revisión, por ejemplo, uso del procesador al 100%, cambios en la cantidad de programas en ejecución, discos de almacenamiento sin espacio libre u otros relevantes.
- Si se detectan servicios o procesos activos en el servidor de BI que no están siendo utilizados por usuarios, se deben detener y desactivar desde la configuración del sistema operativo. Así, los servicios sin uso no volverán a activarse tras un reinicio del servidor.

Documentación

- Se debe controlar la información que se imprime en papel que es obtenida del sistema de BI y los documentos utilizados o dejados en salas de reunión y disponer de procedimientos de destrucción segura de las impresiones en papel. Si es posible, se debe configurar el uso de contraseña en las impresoras a fin de evitar la proliferación de documentos impresos sueltos en las impresoras compartidas en la empresa.

Seguridad en la Nube

- Se deben bloquear los grupos de direcciones de red de países considerados conflictivos, a fin de que no puedan descubrir los sistemas de la Pyme en la nube, por ejemplo, utilizando los servicios del cortafuegos que provee Amazon, Google Cloud o Microsoft Azure.
- Si la solución de BI está instalada en un servidor de la nube, se debe monitorear la cantidad de accesos web que recibe el servidor, lo cual permitirá analizar la cantidad y los horarios de los ataques recibidos según el país de origen.
- Se deben escanear vulnerabilidades de la infraestructura de nube y privilegios de credenciales. Además, se debe utilizar credenciales de servicios de nube con el menor privilegio posible.
- Es conveniente deshabilitar los servicios de la nube que no estén siendo utilizados por la solución de BI, por ejemplo, los correspondientes a las API habilitadas por defecto. Si se está utilizando un servicio de almacenamiento de nube para guardar copias de seguridad cifradas de la solución de BI, se debe verificar que la unidad de almacenamiento no tenga una API pública u otra que permita acceder a las copias.

Puestos de trabajo

- Se debe definir una política de puesto de trabajo despejado y pantalla limpia, sin anotaciones en papel y cajoneras con cerradura para dejar el material confidencial o crítico.

Pruebas de penetración

- Se deben realizar pruebas de penetración (en inglés, pentest o pentesting) a las interfaces de acceso del servidor de BI y a los orígenes de datos, mínimamente una

vez al año, con herramientas automáticas y manuales a fin de encontrar vulnerabilidades. Es recomendable que estas tareas sean efectuadas por personal externo especializado en ataques, por ejemplo, consultoras especializadas y con reconocimiento en el mercado.

- Las pruebas de penetración deben generar alertas o eventos de seguridad para revisión. El resultado de las pruebas debe generar reportes con evidencias para proporcionar información a las auditorías.

Revisión independiente del cumplimiento

- Es necesario llevar a cabo revisiones independientes realizadas por entidades o expertos reconocidos, sobre el cumplimiento de la implementación técnica de los controles, en todos los elementos relacionados a la solución de BI.

Detalle de recomendaciones para los proyectos sobre protección de la información almacenada

Consultoría legal

- Se debe contratar una consultoría especializada para identificar posibles incumplimientos legales en materia de seguridad de la información, por ejemplo, en cuanto a la protección y privacidad de la información personal o la ausencia de criptografía en las bases de datos y aplicaciones, desde un punto de vista no solo técnico, sino también jurídico. Además, se debe considerar las exigencias normativas de los países en donde presta servicios digitales.
- Se debe establecer una revisión de los contratos vigentes y nuevos, de colaboradores, proveedores y clientes, a fin de mantener los lineamientos de seguridad de la información. Para cada caso, se podrían considerar los antecedentes y comportamiento ético.

- Se debe definir procedimientos para recopilar registros y evidencias tecnológicas que permitan su utilización en el ámbito legal como elementos válidos. De este modo, se evitará la destrucción accidental o el deterioro de las evidencias, en el caso de ser necesarias o que sean cuestionadas en cuanto a su cadena de custodia o forma de obtención.

Control de cambios en los sistemas

- Se debe implementar procedimientos estándar de control de cambios, para controlar versiones que se implementan en la solución de BI en producción. Estos deberán considerar cuestiones como las autorizaciones de los cambios, revisión de los controles de seguridad, registro de los cambios efectuados y actualización de la documentación existente, entre otras. Siempre que sea posible, se debe documentar el procedimiento para revertir los cambios impactados en la solución de inteligencia de negocios, a fin de evitar cualquier afectación en la disponibilidad para todos los usuarios.

Desarrollo seguro

- Los desarrollos de software deben trabajarse con un sistema de control de versiones que permita realizar una vuelta atrás en caso de ser necesario, por ejemplo, Git[34]. Así, se podrá controlar todos los cambios que se realiza en el código, quién lo hace y en qué fecha y horario.
- Idealmente, las modificaciones o nuevas necesidades de BI deben realizarse sobre un entorno de desarrollo y pruebas. Además, no deben utilizar muestras reales de datos del ambiente de producción, ya que es necesario en todo momento adoptar medidas para proteger la privacidad de los titulares de esos datos.

[34] https://www.atlassian.com/es/git/tutorials/what-is-git

- Se debe implementar un estándar de desarrollo seguro definido como política. Esto permite que se desarrollen y prueben pequeños programas (script) y conectores de la solución de BI de manera segura, sin proporcionar a terceros la posibilidad de aprovechar errores o vulnerabilidades de desarrollo en los accesos a los datos o en las conexiones a bases de datos del ambiente producción. Además, se debe supervisar los desarrollos o complementos realizados por proveedores o terceros, a fin de mantener el estándar de la empresa.
- Los desarrollos web que se realizan para eventos online masivos deben almacenar contraseñas cifradas para evitar que sean reveladas a los usuarios de la solución de BI.

Acuerdos de confidencialidad

- Es necesario realizar acuerdos de confidencialidad y no divulgación de información con las empresas consultoras de la solución de BI, ya que los consultores tienen acceso a información interna y bases de datos de diferentes clientes de la compañía. Estos acuerdos deben permanecer vigentes un tiempo, aun después de que haya finalizado el periodo de contratación.

Recuperación de desastres

- Se debe probar la recuperación de desastres del servidor de BI. El autor considera que esta práctica podría planificarse para ser ejecutada dos veces al año, estimando el peor escenario de recuperación. De esta manera, no solo será posible evaluar la documentación existente y las capacidades del personal para restaurar la solución de BI, sino también medir los tiempos que se requieren para el trabajo en un escenario realista.
- En caso de utilizar una unidad de almacenamiento en la nube para guardar las copias de seguridad cifradas, se debe configurar la infraestructura de la nube para obtener

registros de eventos que serán recolectados por el servidor Syslog con fines de monitoreo, control, análisis y auditorias.

Criptografía

- Se debe utilizar criptografía para proteger las contraseñas almacenadas en las bases de datos y los archivos de copias de respaldo del servidor BI.
- El personal de seguridad deberá analizar e implementar el método de cifrado adecuado, ya que existe criptografía considerada obsoleta o en desuso.

Concientización y entrenamiento

- Es necesario realizar campañas frecuentes de concientización en materia de seguridad a toda la empresa, incluyendo la dirección, por ejemplo, cada tres meses con instancias de evaluación del aprendizaje e impacto. Con relación a la solución de BI, mínimamente se debe capacitar a los administradores y consultores, acerca de sus responsabilidades individuales sobre la confidencialidad de la información y las penalizaciones por el uso indebido de sus usuarios con privilegios elevados.

Resguardo de información

- Se debe realizar copias de respaldo de información y pruebas periódicas de recuperación. Las copias de respaldo deben ser almacenadas al menos en dos lugares físicos distintos. Si se suben a la nube deben estar comprimidas y cifradas con contraseña. Para el caso de cifrar en Linux se puede utilizar el programa gratuito GPG (en inglés, GNU Privacy Guard[35]). Los procedimientos de resguardos deben

[35] https://www.gnupg.org

estar documentados y actualizados y deben incluir los aspectos relacionados al cifrado.

- Se deben realizar ejercicios de recuperación periódicamente para constatar la correcta operación del procedimiento de realización de copias de respaldo de información y su recuperación. Esto será necesario en un escenario real ante una situación de desastre. Además, se deben registrar los tiempos de demora en la maniobra de restauración.
- Los ejercicios de recuperación de desastre de la solución de BI, migraciones, mejoras en la infraestructura o cambios de proveedor de nube, se deben ejecutar cumpliendo los procedimientos establecidos, sin comprometer la seguridad de la información.

Medios de almacenamiento y borrado seguro

- Se debe establecer y controlar qué medios de almacenamiento se utilizarán para trabajar en la solución de BI. Esto incluye discos rígidos del servidor, unidades de almacenamiento extraíble USB y unidades compartidas en la red que se utilizan para copiar temporalmente archivos o bases de datos. Para todos los casos se debe aplicar un procedimiento de borrado seguro que imposibilite la recuperación de datos o información una vez eliminada, en función del nivel de criticidad de la información a destruir. Si es necesario, considerar la destrucción física de los discos.
- Las unidades de almacenamiento extraíble USB ajenas al área de TI o Seguridad estarán prohibidas dentro de la empresa.
- Se debe implementar un procedimiento estándar de borrado seguro de datos, archivos o bases de datos obsoletas, el cual será ejecutado por personal de seguridad con el objetivo de optimizar el espacio libre en discos del servidor de BI.

Gestión de incidentes de seguridad

- Se deben establecer procedimientos que contemplen la identificación de un canal único de contacto, horarios de atención, responsables y cursos de acción para la gestión de incidentes de seguridad de la información relacionados con la solución de BI, por ejemplo, la exposición pública de la información confidencial o contraseñas, el borrado de información intencional o ataques de Ramsonware al servidor. Se debe considerar la documentación para el aprendizaje continuo, su revisión y la generación de evidencias.
- Se debe establecer un procedimiento de escalamiento de incidentes técnicos con responsables y flujo de comunicación definido.
- Los incidentes que han tenido un cierre o una solución deben ser comunicados formalmente con un reporte detallado a la dirección. Se debe evitar y denunciar maniobras de ocultamiento de incidentes de seguridad que suceden.
- Es importante establecer un canal anónimo para reportar conductas inadecuadas, violaciones de acceso, errores humanos, fallos en los controles de seguridad o incumplimiento de las políticas de seguridad existentes y publicadas en la empresa.

Documentación

- Se debe implementar un proceso de control de cambios y versiones documentado en las políticas y procedimientos, para ser utilizados en la gestión de la seguridad de la información de la solución de BI. Esto permitirá mantener la cadena de revisión y aprobaciones, lo que evitaría cambios no deseados.

Transferencias externas de información

- Se debe definir los medios seguros de intercambio o transferencia de información, con el fin de evitar que la información se transmita sin cifrado en la red de Internet. Por ejemplo, se debe controlar que las copias automáticas en horario nocturno se

realicen utilizando un canal cifrado para la transmisión de información. Por ejemplo, se podría utilizar algún estándar de conexión como SSH, HTTP seguro usando certificados SSL, o incluso SFTP[36]. Este último genera primero una conexión de SSH cifrada y dentro de ella una sesión FTP sin cifrado. Estos estándares de conexión están disponibles en Windows y Linux.

Control de licencias

- Se debe implementar o utilizar un repositorio que permita administrar las licencias de software de toda la solución de BI, incluidas la del sistema operativo, motor de bases de datos, antivirus, firewall de host, solución de BI y las que estén en uso en la nube, a fin de garantizar que no se excede el número máximo de licencias permitas, se evite el uso de software ilegal y se mantenga la confidencialidad de las mismas.

Ciclo de vida de los datos

- Se debe crear y mantener un mapa o inventario de fuentes de datos e información de toda la solución de BI. Esto no solo ayuda a mejorar la visibilidad de la interrelación de los sistemas, sino también a planificar tiempos de retención y eliminación de los volúmenes de datos obsoletos.

Revisión independiente del cumplimiento

- Es indispensable realizar revisiones independientes sobre el cumplimiento de políticas, procesos y procedimientos establecidos en materia de seguridad, así como el control de versiones.

[36] https://www.redhat.com/sysadmin/ftp-vs-sftp

- Los auditores externos pueden validar si se implementa la política de desarrollo seguro en los proyectos de desarrollo web y complementos de BI, por ejemplo, el guardado cifrado de las contraseñas almacenadas.
- La dirección será responsable de evaluar los resultados de las auditorías externas. En caso de algún incumplimiento deberá identificar las causas, evaluar e implementar acciones correctivas. Posteriormente, se deberá verificar la efectividad de las acciones correctivas en la protección de la información almacenada.

Ejercicio de proceso continuo

- Al igual que la implementación de un sistema de gestión de seguridad de la información a nivel organizacional, aplicar seguridad en los sistemas de inteligencia de negocios debe permitir un proceso de mejora continua, con sus etapas definidas, planificar, hacer, verificar y actuar (en inglés, PDCA). Además, las propuestas de mejora al finalizar cada periodo de revisión deben quedar documentadas y se debe generar conocimiento a partir de las lecciones aprendidas.
- Considerar la identificación y el registro en los organismos especializados de divulgación de información en materia de seguridad, con el objetivo de recibir avisos de alertas tempranas y asesoramiento sobre nuevos temas descubiertos o amenazas que requieran gestión. En la Ciudad Autónoma de Buenos Aires, existen organismos como por ejemplo el BACsirt[37] o en España, las suscripciones al boletín del INCIBE[38]. Otra opción interesante es considerar las publicaciones de la organización estadounidense MITRE[39], con su boletín de enumeración común de vulnerabilidades (en inglés, CVE). Estos organismos especializados permitirán el acceso a información actualizada en el ámbito de la seguridad de la información y ataques recientes.

[37] https://bacsirt.buenosaires.gob.ar
[38] https://www.incibe-cert.es/suscripciones
[39] https://www.mitre.org/who-we-are/our-story

Estimación para la implementación de los proyectos

El autor estima que el total de los proyectos para asegurar una solución de BI en una Pyme, se podría implementar en cinco meses. En la estimación se consideró necesaria la participación de dos colaboradores con una dedicación de cuatro horas diarias y el apoyo de especialistas externos para temas administrativos y jurídicos puntuales, como la definición de políticas y acuerdos de confidencialidad. En caso de que la dedicación pueda ser completa, los tiempos serían más cortos, aunque este escenario es poco probable, ya que las Pyme argentinas no cuentan con gran cantidad de personal propio y por la demanda en actividades diarias, no podrían dedicar capital humano exclusivamente a estos proyectos durante tanto tiempo.

Al finalizar todas las implementaciones y posterior a la revisión del cumplimiento de los proyectos y auditorias, se deberá realizar una presentación final al directorio.

A continuación, se presenta un gráfico de estimación del tiempo de todos los proyectos para ejecución en la Etapa 4, ordenados de acuerdo con la prioridad más alta.

		Mes 1				Mes 2				Mes 3				Mes 4				Mes 5					
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4		
Proyectos	Prioridad																					Responsable	Auditor
Consultoría legal	1																						
Protección lógica del servidor																							
Contraseñas	2																						
Registro de eventos de sistemas																							
Control de administradores																							
Control de cambios en los sistemas																							
Autenticación	3																						
Garantizar disponibilidad																							
Criptografía accesos e información																							
Recuperación de desastres																							
Acuerdos de confidencialidad																							
Desarrollo seguro																							
Red de datos	4																						
Concientización y entrenamiento																							
Resguardo de información																							
Seguridad física	5																						
Medios de almacenamiento y borrado seguro																							
Monitoreo del servidor	6																						
Gestionar incidentes de seguridad																							
Documentación																							
Transferencias externas de información	7																						
Seguridad en la nube																							
Control de licencias	8																						
Puestos de trabajo																							
Pruebas de penetración	9																						
Ciclo de vida de los datos																							
Revisión independiente del cumplimiento	10																						
Presentación final al directorio																							

Nota. Presentación priorizada de proyectos para la mitigación de riesgos identificados.

Fuente. Elaboración propia.

Otras recomendaciones del autor que se deben tener en cuenta en las Pyme argentinas

El ejercicio de asegurar la solución de inteligencia de negocios posiblemente también permita pensar en alinear la Pyme a la norma. Luego de intervenir puntualmente para asegurar la solución de BI, se deben considerar las siguientes cuestiones para avanzar sobre la seguridad de la información a un nivel general. Muchas de estas recomendaciones fueron implementadas por el autor en escenarios reales para otras empresas y han logrado una mejorar la visibilidad del comportamiento de la red y los sistemas en producción, el control y la capacidad de reacción del equipo de seguridad.

Compromiso de la dirección

- La dirección debe conducir y apoyar en todo momento las iniciativas que se adopten en materia de seguridad de la información, en cumplimiento de la normativa y las necesidades del negocio. Es necesario definir las políticas de la seguridad de la información, publicarlas y revisarlas periódicamente.

Gestión de incidentes de seguridad

- Es necesario establecer procedimientos, responsables y cursos de acción, para la gestión de incidentes de seguridad de la información. Los canales de comunicación deben estar acordados para lograr la gestión interna y externa hacia clientes.

- Una correcta gestión de incidentes permite prepararse, reconocer los incidentes, examinarlos, tomar decisiones, investigar, resolver y ampliar el conocimiento de los colaboradores con las lecciones aprendidas.

Recuperación de desastres

- Se debe acordar por contrato los tiempos de recuperación de desastres para volver a restaurar un proyecto vendido a cliente que se encuentre en la nube, como, por ejemplo, una aplicación para un evento masivo implementada en la nube de Amazon. Se debe estimar un tiempo realista de recuperación, que pueda ser cumplido por el personal de TI de la Pyme o por los consultores contratados para tal fin.
- En caso de armar la infraestructura en la nube con una consultora, se debe informar la criticidad que tendrá el proyecto antes de la creación del ambiente y de la implementación, para considerar de antemano cuestiones de alta disponibilidad en la nube.

Monitoreo

- Se debe monitorear los sistemas que están en producción, los internos de la Pyme y los que son de clientes. Esto incluye, la infraestructura tecnológica de la nube y el comportamiento en tiempo real por el uso de las aplicaciones web. En caso de tener un comportamiento distinto al habitual, el sistema de monitoreo debe generar un aviso de alerta por correo electrónico para la revisión por una persona.

Desarrollo seguro

- Todas las fases de los proyectos de software deben considerar la seguridad de la información. Se deben realizar pruebas de seguridad, como la simulación de ataques

antes de pasar a producción, para comprobar que el software funcione como se espera.

- Se debe controlar que el área Desarrollo cumpla con los estándares de contraseñas seguras, por ejemplo, conformada por letras, número y símbolos, con una longitud de al menos doce caracteres. Las contraseñas débiles en uso en proyectos antiguos de software deben ser reemplazadas por contraseñas que cumplan con el estándar.
- Las contraseñas utilizadas en Desarrollo no deben repetirse o existir en otros proyectos de software. Para cada proyecto y ambiente distinto se debe utilizar contraseñas diferentes.

Teletrabajo

- Se debe crear y comunicar una política de uso aceptable de equipamiento tecnológico, por ejemplo, computadoras de escritorio, notebooks y teléfonos celulares corporativos.
- Es necesario difundir el procedimiento de gestión de incidentes de seguridad, para que el colaborador remoto tenga claro cómo debe proceder en caso de tener una situación o evento que pueda afectar su labor o el negocio, como por ejemplo un incidente por Ransomware, que al estar conectado a la red empresarial por VPN, se podría propagar hacia la red interna en todos los equipos de la empresa, incluyendo el servidor de BI.
- Se debe ingresar a la red la empresa únicamente con equipos empresariales. Los accesos desde las computadoras privadas de los colaboradores deben estar prohibidas ya que no están bajo el control de la empresa y no cumplen o no es posible verificar el cumplimiento de los requisitos básicos de seguridad, como el de tener un antivirus actualizado.
- Se debe monitorear las acciones de los colaboradores conectados remotamente a la red privada virtual de la empresa (VPN) fuera del horario laboral.

- Los colaboradores en modalidad de teletrabajo no deben compartir sus contraseñas personales, incluso durante la solicitud de soporte remoto al área de TI.
- Se debe prohibir el préstamo de las computadoras portátiles a personas ajenas a la compañía, como familiares, amistades u otras.
- Se debe controlar y evitar en la medida de lo posible, el uso de cuentas con privilegios elevados en el sistema operativo Windows. Además, se deben adoptar medidas para impedir la instalación de software no autorizado o ilegal.
- Es necesario mantener actualizado el sistema operativo Windows a través de los parches de seguridad oficiales ofrecidos por la empresa Microsoft.

Verificar la configuración del cortafuegos de la red de datos

- Se debe revisar la configuración del firewall de red, principalmente para bloquear intentos de acceso desde Internet hacia la red interna de la Pyme y para bloquear accesos maliciosos como, por ejemplo, los provenientes de algunos países asiáticos, en los que se originan muchos de los ataques automáticos.
- Para el caso puntual de la Pyme analizada, se decidió realizar un cambio del firewall, debido a que el equipo estaba obsoleto y no tenía soporte oficial en nuestro país. Aunque existen muchos proveedores y marcas en cuestiones de telecomunicaciones, el autor sugiere implementar equipamiento de la marca Mikrotik[40], ya que cuenta con soporte oficial en el país y es de bajo costo. Además, cumple las necesidades requeridas en las Pyme, como los bloqueos de fuentes maliciosas provenientes, entre otros, de países asiáticos; la separación de redes virtuales locales; accesos remotos por red privada virtual; monitoreo del uso en tiempo real y otras funciones de interés para el personal de seguridad. A través de este equipo pasa la conexión a Internet de la Pyme y permite tener un control de todas las conexiones que ingresan y salen a Internet.

[40] https://mikrotik.com

- En caso de que se disponga de un mejor presupuesto para invertir en un firewall y siempre según la consideración del autor, se podría optar por equipamiento de la marca Palo Alto Networks[41], por ejemplo, la serie PA-400 para empresas medianas.

Protección de los sistemas en la nube

- Se debe implementar un cortafuegos de aplicación web (en inglés, WAF) para proteger los sitios web desarrollados para clientes. Un ejemplo de esto, es el producto WAF Pro de la empresa estadounidense Cloudflare[42], que cumple con la protección básica para el TOP 10 de vulnerabilidades de la fundación OWASP a un bajo costo.
- Se debe comprobar que las bases de datos en la nube son únicamente accesibles desde la aplicación que lo requiera.

Acuerdos de confidencialidad

- Es necesario realizar acuerdos de confidencialidad, no divulgación del código de software y derechos de propiedad intelectual, para poder proteger los desarrollos realizados por la Pyme. Estos acuerdos deben permanecer vigentes un tiempo, aun cuando haya finalizado la contratación del personal propio. Se debe definir un alcance legal inicial que podría tomar la empresa, en caso de una violación a los derechos de autor por parte de un colaborador, por ejemplo, trasladar intencionalmente una copia parcial de un programa hacia fuera de la empresa.

[41] https://www.paloaltonetworks.com
[42] https://www.cloudflare.com/plans

Consideraciones generales de alto nivel para alinear una Pyme a la norma ISO/IEC 27001:2022:

- Analizar y tener en cuenta el contexto que rodea a la Pyme e identificar las partes interesadas.
- Obtener el apoyo de la dirección para gestionar la seguridad de la información.
- Planificar los objetivos de la seguridad de la información como lo indica la norma.
- Identificar y realizar un inventario de activos de información. Clasificar el inventario de acuerdo con su tipo e importancia y nombrar propietarios para esos activos.
- Realizar una evaluación de riesgos y documentarla y definir el tratamiento que se le dará a dichos riesgos.
- Estimar el capital humano necesario para mantener la seguridad de la información.
- Asegurar las competencias profesionales del capital humano. Planificar capacitaciones y actualizaciones para periodos definidos.
- Para el equipo operativo de seguridad, definir y documentar qué se hace y con qué recursos. Definir responsables, tiempos y cómo se evalúan los resultados.
- Crear y poner en conocimiento del personal y de terceros involucrados según corresponda, la política de seguridad de la información.
- Concientizar a toda la empresa, explicar responsabilidades y evaluar el grado de aprendizaje. Además, comunicar implicaciones de cualquier incumplimiento.
- Definir los procesos de comunicación interna y externa. ¿Quién comunica? ¿Cuándo? ¿Cómo? ¿Con quién comunicarse?
- Definir y publicar el punto de contacto para canalizar la atención de incidentes de seguridad. Determinar un procedimiento claro para su tratamiento en caso de que ocurran.
- Definir la auditoria interna, su frecuencia y responsabilidades.

Lograr que el SGSI sea pertinente, adecuado y eficaz, tal como lo indica la norma. Trabajar en la obtención de métricas de la seguridad de la información para presentaciones periódicas a la dirección.

10. Conclusiones

Las soluciones de inteligencia de negocios están siendo cada vez más utilizadas por las Pyme como herramienta de apoyo para la gerencia, puesto que permiten disponer de información relevante para mejorar las decisiones, a un costo que es cada año menor. Sin embargo, debido al uso de diferentes tecnologías para la implementación de un sistema de BI en producción, el riesgo en la seguridad de la información aumenta, ya que se deben tomar medidas de precaución para cada uno de los elementos que conforman la solución tecnológica.

Por otra parte, es evidente que la cultura de la empresa influye en cómo se hacen las cosas y cómo se trata la seguridad de la información en todos los niveles. Así, la falta de concientización en las Pyme argentinas complica la perspectiva de seguridad de la información a largo plazo, ya que quienes la conforman carecen de conocimientos básicos para determinar su verdadero valor o se instala una falsa creencia de que proteger la información es algo optativo.

En el mundo de las Pyme de nuestro país, los proyectos que nunca recibieron revisión o mejora continua quedan con faltantes de documentación y en la mayoría de los casos, no se realiza la implementación de medidas para gestionar adecuadamente la seguridad de la información.

En el caso de la Pyme analizada del ámbito marketing digital, la empresa debe ser consciente de que tiene responsabilidades legales y contractuales de proteger la información en su poder. En relación con el servidor de BI, debería ser el primer activo de información en tratarse y protegerse, ya que su interface de conexión web está accesible desde Internet y no cuenta con medidas de protección básicas, lo que imposibilita proteger las bases que contienen datos personales de todos los clientes y las propias que contienen información crítica de la Pyme. Además, se utiliza actualmente el usuario genérico llamado “admin” con privilegios elevados para la administración, lo que facilita la recepción de ataques de fuerza bruta desde países asiáticos y otros, como Rusia y Estados Unidos, utilizando diccionarios

de contraseñas disponibles en Internet. Incluso, al no contar con un cortafuego a nivel servidor, tampoco se logra una limitación en la cantidad de intentos de autenticación por minuto, lo que convierte a la solución de BI en un blanco fácil para los ciberdelincuentes.

En la Pyme argentina bajo análisis, la solución de inteligencia fue un proyecto del área de TI. Como en muchos otros casos, no se consideró la seguridad de la información antes, durante y posteriormente al proyecto. Esto deja en evidencia que, en algunas Pyme, el área de TI carece de un criterio básico en materia de seguridad de la información, lo cual agrava más la situación, ya que se implementan soluciones tecnológicas inseguras. Por el contrario, la situación deseada es evitar siempre que un colaborador o un tercero pueda acceder, modificar o borrar información sin tener autorización previa. Además, las acciones que se realicen en los sistemas deben ser detectables y auditables. Pero como en la Pyme argentina expuesta, la situación de algunas empresas no permite visualizar, encontrar, analizar y prevenir acciones indeseadas en sus sistemas, por lo que el autor considera que a nivel de seguridad estas Pyme se encuentran prácticamente a ciegas.

Aunque las Pyme argentinas como es de esperarse dado el volumen de negocio y los recursos de los que disponen, no cuenten con especialistas de seguridad en su capital humano, los proyectos tercerizados deben estar alineados con las políticas de seguridad de la información que utilice la empresa. En caso de no contar con políticas ya definidas, se debe considerar mínimamente el estándar, en este caso la norma ISO/IEC 27001:2022, de modo que puedan exigir las medidas básicas al proveedor. En este contexto, debe entenderse que una gestión deficiente de la seguridad de la información puede afectar negativamente a los activos de información de la empresa y en consecuencia, a la normal operación del negocio. Posteriormente, también podría afectar negativamente y comprometer los beneficios económicos obtenidos y el logro de los objetivos de la empresa.

Trabajar en la protección de la información en las áreas de todo el negocio, especialmente en aquellas que son críticas, ayuda a diseñar o rediseñar procesos y controles. La norma pretende lograr que la seguridad de la información esté contemplada y presente en todas las fases de la metodología de gestión de proyectos, independientemente del tipo de

proyecto que se esté abordando. Para lograr esto la dirección debe estar involucrada, ya que la implementación de un SGSI y la definición de todas sus políticas es una decisión estratégica de la Pyme.

A pesar de que las Pyme argentinas no consideren dentro de sus objetivos la obtención de una certificación oficial de la norma, proceso que puede ser inalcanzable para la mayoría de este tipo de entidades, se debe trabajar para alcanzar un nivel mínimo de seguridad de la información. Al mismo tiempo, todos los inconvenientes que se presenten deben verse como oportunidades de mejora continua para el negocio y no solo como un problema técnico que debe resolver el área de TI.

La gestión de la seguridad de la información demuestra responsabilidad interna y ante terceros. También, contribuye a que los riesgos se mitiguen correctamente y que toda la estrategia de seguridad de la información esté alineada con los objetivos de la organización, además de satisfacer las regulaciones u obligaciones legales.

En la actualidad, es necesario para cualquier negocio que utilice sistemas de información, poder detectar y prevenir incidentes de seguridad. En los casos que no se pueda lograr, al menos se debe tener capacidades de reacción y recuperación, en los peores casos. Para que las Pyme argentinas puedan hacer frente a los problemas de seguridad de la información modernos, debe haber preparación, respuesta a incidentes y una recuperación probada.

La adecuación de la Pyme a la norma no solo permite preparación y mejora continua, sino que además da una mayor confianza a la imagen del negocio o marca, lo que permite establecer vínculos con nuevos clientes y proveedores ya que mejora la reputación. Parte de dicha imagen confiable está relacionada al desempeño del personal abocado a tareas de protección de la información, que tendrá la capacidad de emitir reportes que permitan visualizar su correcta gestión, con información sobre cantidades, tipos y costos de los incidentes de seguridad de la información que pudieran haberla afectado.

En cuanto al capital humano, como resultado de un cambio de cultura, se tendrá un enfoque proactivo en la gestión de seguridad de la información, en lugar de uno solo reactivo. Además, el uso de la norma ISO/IEC 27001:2022 como una guía, ayudará a evaluar y tratar los riesgos en la seguridad de la información que no son visibles por personal no experto, dado que refleja la experiencia técnica y las recomendaciones de expertos de diferentes países que han contribuido a su redacción, lo cual es muy valioso para el negocio.

Los cuerpos directivos de las Pyme argentinas no deben desestimar el aporte de la norma como una gran ayuda para resolver las necesidades actuales que afectan al desarrollo de sus negocios, independientemente del ámbito y naturaleza de la organización. Es esperable que, en el ejercicio de sus funciones, tengan conocimientos suficientes de la normativa que regula la seguridad de la información dentro del país donde se desempeñan y los estándares y buenas prácticas vigentes, para adoptar decisiones que promuevan el cumplimiento de los aspectos legales que le sean aplicables a la organización, al mismo tiempo de fomentar una fuerte cultura ética, que implique hacer siempre lo que es correcto.

El autor ha presentado un plan inicial con recomendaciones basadas en el estudio de la norma en su última versión, en los conocimientos adquiridos a lo largo de toda la maestría y otros de su experiencia laboral, con la intención de que pueda servir como base para aplicar en una forma efectiva acciones de seguridad de la información en sistemas de inteligencia de negocios en las Pyme argentinas, teniendo en cuenta sus limitaciones de capital humano, el presupuesto con el que cuentan y el contexto en el que desarrollan su actividad. Aunque ha estimado una intervención planificada en cinco meses, hay que tener en cuenta que, si se suman más recursos a los proyectos, estos plazos podrían reducirse significativamente, dando como resultado una rápida respuesta para mitigar los riesgos identificados, con énfasis en el control de acceso y la protección de la información almacenada, tal como lo requiere la situación real.

En resumen, aplicar seguridad a los sistemas de inteligencia de negocios en las Pyme de Argentina produce varios beneficios importantes, como el de prevenir el deterioro de capacidades estratégicas propias para la toma de decisiones apropiadas y evitar otros

relevantes como accesos no autorizados, fuga de datos interna, divulgación no autorizada, daño a la reputación de la marca y el retiro de accionistas. El autor considera que la negligencia puesta de manifiesto en la ausencia de seguridad de la información como un elemento importante en todos los proyectos y desafíos tecnológicos que se aborda resulta perjudicial para el negocio. Efectivamente, si no se invierte lo que es necesario, se adquiere un problema a futuro, que terminará costando más caro para el negocio que el monto requerido para implementar un adecuado programa de seguridad. En definitiva, para muchas situaciones en las Pyme de nuestro país, la utilización de criterios apropiados y una inversión pequeña puede evitar pérdidas millonarias.

Por último, resumiendo el trabajo realizado y teniendo en cuenta las limitaciones de alcance expuestas al inicio, se buscó y el autor entiende que se logró, identificar las tecnologías actuales utilizadas para BI y describir una implementación en una Pyme argentina del ámbito marketing digital. Además, se expuso los beneficios que aporta el estándar ISO/IEC 27001:2022 con relación a la seguridad de la información almacenada. Finalmente, se presentó un plan inicial con recomendaciones que permitan aplicar seguridad de la información en los sistemas de inteligencia de negocios en las Pyme de Argentina.

11. Referencias bibliográficas

Aguilar, L. J. (2019). *Inteligencia de negocios y analítica de datos: Una visión global de Business Intelligence & Analytics.* Barcelona, España: MARCOMBO S.A.

Albuero De Luna, A. (2021). *Principles of Big Data.* Burlington, Canadá: Arcler Press.

Beltrán Pardo, M., & Jaén, F. S. (2014). *Cloud Computing, tecnología y negocio.* Madrid, Ediciones Paraninfo, España.

Brito Pinto, R. P., Sarmiento Barreiro, L. M., Ramírez Hecksher, A. M., Cevallos Gamboa, M. A., Ortiz Chimbo, K. M., & Córdova Aragundi, J. S. (2018). *Aplicaciones, metodologías y tecnologías que permitan transformar datos de los sistemas transaccionales e información desestructurada en información estructurada.* Guayaquil, Ecuador: Grupo Compas.

Comisión Federal de Comercio. (23 de Julio de 2019). Obtenido de https://www.ftc.gov/es/noticias/la-ftc-impone-penalidad-de-5-mil-millones-y-nuevas-restricciones-de-privacidad-de-gran-envergadura

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, 76-105. doi:10.1108/TQM-09-2020-0202

Eduardo, D. V. (2022). *Ciberseguridad para directivos.* Madrid: LID Editorial.

Escuela de Organización Industrial de España. (s.f.). *Norma Española UNE-EN ISO/IEC 27001 (2017).* Obtenido de https://static.eoi.es/inline/une-en_iso-iec_27001.pdf

Estado Argentino. (2000). *Ley 25.326 Protección de los datos personales*. Obtenido de https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

Gartner. (11 de 08 de 2019). *Gartner Glossary.* Obtenido de https://www.gartner.com/en/information-technology/glossary/business-intelligence-bi

Grossmann, W., & Rinderle-Ma, S. (2015). *Fundamentals of Business Intelligence.* Heidelberg, Alemania: Springer-Verlag.

Guardian Media Group. (26 de Julio de 2018). *The Guardian.* Obtenido de https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock

Instituto Nacional de Ciberseguridad de España. (18 de 08 de 2020). *INCIBE.* Obtenido de https://www.incibe.es/aprendeciberseguridad/ransomware

Kenneth, S., & Effy, O. (2018). *Administración de los sistemas de información, séptima edición.* Madrid, España: Igueldo Stud SL.

Luo, Y. (2022). *A general framework of digitization risks in international business.* Obtenido de Journal of International Business Studies: https://doi.org/10.1057/s41267-021-00448-9

Microsoft. (29 de 11 de 2020). *Powerbi : What is business intelligence?* Obtenido de https://powerbi.microsoft.com/en-us/what-is-business-intelligence/

Oracle Corporation. (23 de 01 de 2021). *Oracle Argentina.* Obtenido de https://www.oracle.com/ar/artificial-intelligence/what-is-ai/

OWASP. (2021). *OWASP Top 10.* Obtenido de https://owasp.org/Top10/es/

Pérez Marqués, M. (2015). *Business Intelligence. Técnicas, herramientas y aplicaciones.* Madrid, España: RC Libros.

Ramesh, S., Dursun, D., & Efraim, T. (2017). *Business Intelligence, Analytics, and Data Science: A Managerial Perspective, Fourth edition.* New York, Estados Unidos: Pearson.

Tan, P.-N., Steinbach, M., Kumar, V., & Karpatne, A. (2019). *Introduction to Data Mining* (Segunda edición ed.). New York, Estados Unidos: Pearson Higher Ed.

The New York Times Company. (26 de Julio de 2018). *The New York Times.* Obtenido de https://www.nytimes.com/2018/07/26/business/facebook-stock-earnings-call.html

The New York Times Company. (19 de Marzo de 2018). *The New York Times.* Obtenido de https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Vieites, Á. G. (2011). *Enciclopedia de la seguridad informática - 2ª edición.* Alfaomega, Ra-Ma.

Vmware Inc. (2009). *Vmware.* Obtenido de https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/Virtualization-for-MySQL-on-VMware.pdf