Carrera: Contador Público Nacional y Perito Partidor

SEGURIDAD INFORMÁTICA: LA PROTECCIÓN DE LA INFORMACIÓN EN UNA EMPRESA VITIVINÍCOLA DE MENDOZA, 2019

Trabajo de Investigación

Autor:

María Agustina Sisti

Reg. 29265

m.agussisti@gmail.com

Profesor Tutor:

Pablo David Majowka

M e n d o z a – 2 0 1 9

ÍNDICE

RESUMEN TÉCNICO

La seguridad informática es fundamental para proteger la información en las empresas, que es un recurso estratégico y fuente de toma de decisiones. Los recursos informáticos que forman parte de una empresa son vulnerables a amenazas y riesgos que pueden afectarlos y provocar severos daños y pérdidas.

La presente investigación tiene como finalidad analizar los mecanismos de protección de la información en una empresa vitivinícola de Mendoza, para determinar el nivel de seguridad existente y efectuar las observaciones y recomendaciones que correspondan.

El estudio se realiza a través de un análisis correlacional, descriptivo y transversal. Los datos obtenidos de las encuestas y entrevistas al personal de la empresa como, así también, los que surjan de la observación directa, se interpretan y analizan para determinar el nivel de seguridad informática existente en la empresa vitivinícola.

Los resultados obtenidos demuestran que el nivel de seguridad informática existente en la empresa vitivinícola depende directamente de la calidad y cantidad de mecanismos de seguridad empleados para obtenerla. Es decir, mientras mejores sean dichos mecanismos de seguridad, mayor va a ser el nivel de protección de los recursos informáticos y viceversa. Si bien se aplican ciertos controles y medidas de seguridad en la empresa, los mismos no resultan suficientes y algunos son mejorables, motivo por el cual el nivel de seguridad informática es medio. Esto hace que la entidad se encuentre vulnerable y expuesta a ciertas amenazas y riesgos. Es por ello que precisa un proceso de mejora y fortalecimiento de su seguridad, a fin de obtener una adecuada protección de la información y de todos sus recursos informáticos.

Palabras clave: seguridad informática, sistemas informáticos, información, control, vulnerabilidades, amenazas, riesgos, medidas de seguridad.

INTRODUCCIÓN

La información es uno de los activos más importantes que tienen las empresas. La misma, permite la toma de decisiones y la gestión empresarial, automatiza los procesos operativos y es un factor clave para alcanzar el éxito organizacional, a través de la generación de ventajas competitivas.

Con los avances tecnológicos permanentes, la información empresarial se procesa y almacena en sistemas informáticos, que deben asegurar su protección integral. Estos sistemas, pueden ser vulnerables y, por lo tanto, estar expuestos a riesgos y amenazas. Por este motivo, es fundamental que se realicen controles permanentes que permitan un funcionamiento eficiente y seguro. De esta manera, se garantiza alcanzar un adecuado nivel de seguridad informática.

Existen diversas investigaciones referidas a la importancia seguridad informática como medio de proteger la información empresarial de cualquier evento que pretenda afectarla. Las mismas han sido realizadas mediante análisis documentales, relevamientos bibliográficos, análisis conceptual de diversas teorías y su integración, y también mediante revisiones y experiencias.

La administración, planificación y control de las operaciones desarrolladas en una organización no serían posibles sin información. Cuando esta es de calidad, permite la correcta y eficiente toma de decisiones así como el cumplimiento de los objetivos empresariales. Por todos estos motivos, el principal activo que poseen todas las organizaciones es la información. Actualmente, con el avance de la tecnología, la misma otorga grandes ventajas competitivas y las empresas deben adaptarse y sistematizar sus sistemas constantemente. Pero, a su vez, aparecen nuevas vulnerabilidades que traen aparejadas graves consecuencias, es por ello que la seguridad informática tiene un papel tan importante en las organizaciones (Saroka, R. H., (2002); Peñuela Vasquez, Y. D., (2018)). La información que manejan las empresas tienen un gran valor y debe ser protegida ya que su pérdida, destrucción o alteración implica daños de todo tipo que pueden afectar seriamente la continuidad de las operaciones empresariales. Es importante que las vulnerabilidades, amenazas y riesgos sean identificados para gestionarlos mediante medidas de seguridad y controles que permitan minimizarlos. Esto es imprescindible para garantizar la confidencialidad, integridad y disponibilidad de la información (Laudon, K. C. y Laudon, J. P., (2012); García Pierrat, G. y Vidal Ledo, M. J. (2016)). Sin embargo, resulta fundamental tener en cuenta que la seguridad nunca es total debido a que los riesgos pueden ser reducidos a niveles aceptablemente bajos pero nunca serán nulos. La seguridad informática es un proceso que se debe perfeccionar permanentemente para obtener así un adecuado nivel de seguridad de la información (Voutssas M., J. (2010)).

Por otra parte, es necesario considerar que dentro de los sistemas de información se encuentran los sistemas contables, los cuales deben cumplir con ciertos requisitos para operar de forma legal. Esto conlleva a que los contadores posean una formación académica y profesional que les permita afrontar su labor de la mejor manera y estando siempre preparados para los cambios futuros. Por esta razón, es importante que en las facultades se brinden los conocimientos y prácticas necesarias para formar profesionales que conozcan de tecnología y de seguridad, y que sepan proteger la información con la que trabajan (Escobar, D. S. (2017)). De todas formas, el conocimiento y la consciencia sobre la seguridad informática no se deben circunscribir solo a los profesionales contables sino que abarcan a todas las personas que integran una organización. El bajo nivel de seguridad de la información existente en las empresas se debe a la falta de conocimiento, de cultura, de compromiso y de entendimiento de las personas con respecto a la seguridad informática, y también a la escasa inversión empresarial en seguridad (Peñuela Vasquez, Y. D., (2018)).

Ahora bien, al centrarse específicamente en las empresas vitivinícolas de Mendoza, se puede observar que existe un vacío de estudios referidos a la seguridad informática, motivo por el cual se procede a investigar la relevancia que tiene la protección de la información en una empresa vitivinícola de la provincia y cuál es el nivel de seguridad informática existente en la misma.

Por lo tanto, el objeto del presente trabajo de investigación es identificar los mecanismos de protección de la información utilizados y su impacto en el nivel de seguridad existente en una empresa vitivinícola de Mendoza, para así poder formular observaciones y proponer mejoras. La hipótesis con la que se trabaja, presume que mientras mejores sean los medios utilizados para proteger la información, mayor va a ser el nivel de seguridad existente.

Por su parte, los objetivos específicos que se persiguen consisten en detectar posibles amenazas y riesgos en la información, identificar los controles aplicables en los sistemas informáticos y analizar el rol del contador en la seguridad informática.

Es importante aclarar que, por razones de confidencialidad, el nombre de la empresa vitivinícola estudiada se mantendrá anónimo.

La metodología empleada para realizar la investigación tiene un enfoque cuantitativo, ya que se busca explicar las variables y sus relaciones tal cual son, a través de la recolección de datos, y su medición para establecer patrones de comportamiento. El tipo de investigación según su profundidad, amplitud y alcance temporal es correlacional-sincrónica/transversal. La profundidad es correlacional porque se pretende explicar cómo se vinculan los mecanismos de protección de la información con el nivel de

seguridad existente. De acuerdo con su alcance temporal, la investigación es sincrónica o transversal, ya que se refiere a un periodo específico de tiempo, que es la actualidad.

El tipo de diseño de la investigación es no experimental-transeccional/transversal-correlacional descriptivo. Es no experimental ya que no se manipulan deliberadamente variables, sino que se observan fenómenos tal y cómo se dan en la empresa vitivinícola. No se tiene control directo sobre las variables, ni se puede influir sobre ellas porque ya ocurrieron. Además, es transeccional o transversal porque se recolectan datos y se analiza su incidencia e interrelación en un momento dado; y correlacional descriptivo debido a que se busca especificar las características y propiedades de la seguridad informática.

Los instrumentos y herramientas que se utilizan para la recolección y análisis de datos primarios (obtenidos directamente de la realidad) son entrevistas y encuestas a Directivos y al personal del área informática y contable. Además, se aplica observación directa. Por su parte, para la recolección de datos secundarios (recopilados de forma previa e independiente) se realiza búsqueda bibliográfica de libros, trabajos de investigación, revistas científicas, entre otros. Y, además, búsqueda documental de leyes y normas aplicables.

Por último, la estructura del trabajo de investigación es la descripta a continuación. En el primer capítulo se brindan conceptos fundamentales de los sistemas de información y de la seguridad informática, dando a conocer su importancia. En el segundo capítulo se mencionan las vulnerabilidades, amenazas y riesgos de los sistemas de la empresa vitivinícola y se presenta un análisis estadístico de los delitos informáticos. Luego, en el tercer capítulo se exponen las medidas de seguridad y controles implementados por la empresa y se proporciona una serie de recomendaciones a fin de que pueda elevar su nivel de seguridad informática. En todos estos capítulos se siguen principalmente los lineamientos y estudios de Laudon, K. C. y Laudon, J. P. (2012) y Saroka, H. R. (2002), entre otros autores. Finalmente, en el cuarto capítulo se analiza el rol de los contadores con respecto a la seguridad informática, de acuerdo a Zegarra, O. S. (2014) y Escobar, D. S. (2017), y también se estudia la importancia de una buena formación profesional.

CAPÍTULO I

SEGURIDAD INFORMÁTICA

En este primer capítulo se procederá a definir los sistemas de información y la seguridad informática, brindando conceptos fundamentales, a fin de facilitar la posterior comprensión del trabajo de investigación. También se dará a conocer la importancia de la seguridad informática en las empresas. Se trabaja con los siguientes autores: Laudon, K. C. y Laudon, J. P., Saroka, H. R., Ramió Aguirre, J., entre otros.

1. LOS SISTEMAS DE INFORMACIÓN

La información es un recurso imprescindible en cualquier empresa ya que es la materia prima para la toma de decisiones y, además, genera grandes ventajas competitivas cuando es correctamente utilizada. La misma se obtiene a través de un proceso de retroalimentación que se genera en los sistemas de información.

En la actualidad, con la globalización y los constantes avances tecnológicos, estos sistemas de información se desarrollan en una plataforma digital, lo que da lugar a los sistemas informáticos. Es fundamental para el éxito y supervivencia organizacional que las empresas se adapten a los cambios e incorporen las nuevas tecnologías para llevar a cabo sus negocios. Así también es muy importante que se tomen las medidas adecuadas para proteger los sistemas y, por consiguiente, la información.

1.1.¿QUÉ ES UN SISTEMA DE INFORMACIÓN?

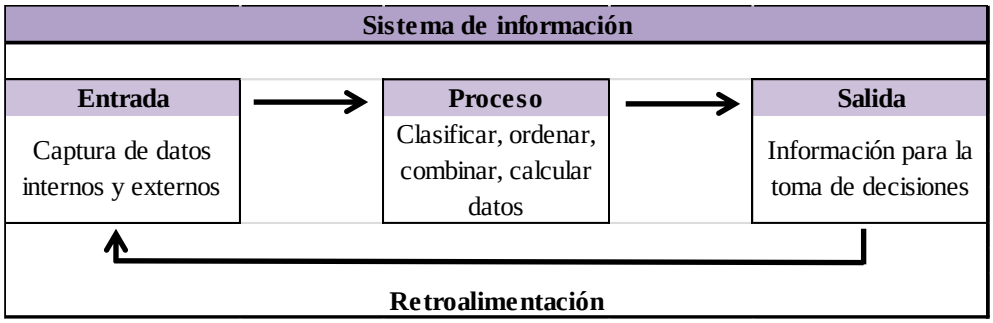
Un sistema es un conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a un determinado objeto, en tanto que, la información es la comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada. (Real Academia Española, 2014, 23° ed.).

Según Laudon, K. C. y Laudon, J. P. (2012), un sistema de información es un conjunto de componentes interrelacionados cuyo objeto es la recolección de datos, su procesamiento y almacenamiento, y la distribución de información para la toma de decisiones y para el control organizacional. Está compuesto por tres actividades: entrada, proceso y salida.

- **Entrada:** donde se captura el elemento primario del sistema de información que es el dato. Los datos recolectados pueden ser internos o externos a la organización.
- **Proceso:** donde los datos se combinan con otros elementos y se vuelven significativos a través de su contextualización, de acuerdo con lo que sucede en la organización.
- **Salida:** donde se obtiene la información útil y significativa para las personas.

Además, se debe contar con la apropiada retroalimentación que permita evaluar o corregir la entrada.

Figura 1: Proceso de la información.



Fuente: Elaboración propia.

Continuando con lo dicho por Laudon, K. C. y Laudon, J. P. (2012), desde una perspectiva de negocios, un sistema de información es una solución organizacional y administrativa basada en tecnología de información para resolver problemas y desafíos del entorno. Es importante comprender las tres dimensiones que le dan forma a los sistemas y permiten que los mismos funcionen efectivamente y generen valor. Estas dimensiones son:

- **Organización:** comprende al personal, estructura, procedimientos, cultura y políticas empresariales. Los sistemas de información forman parte de las organizaciones. No hay sistemas eficientes que se apoyen en organizaciones o estructuras ineficientes.
- **Administración:** comprende la planificación, asignación de recursos financieros y humanos, el establecimiento de estrategias para resolver los desafíos de negocio en el entorno, y la coordinación del trabajo para alcanzar el éxito. Determina cómo debe ser el sistema.
- **Tecnología:** comprende el hardware, software, tecnología de almacenamiento de datos y tecnología de redes y telecomunicaciones. Todos estos elementos, junto con las personas que los operan y administran, constituyen la infraestructura de tecnología de información.

En otras palabras, “un sistema de información es un conjunto de recursos humanos, materiales, financieros, tecnológicos, normativos y metodológicos, organizado para brindar, a quienes operan y a quienes adoptan decisiones en una organización, la información que requieren para desarrollar sus respectivas funciones”, (Saroka, H. R., 2002, p. 33).

El concepto de sistema de información es más amplio que el del sistema informático, ya que el primero engloba al segundo. Los sistemas de información han existido aún antes de la creación de la tecnología de computación. Sin embargo, los avances tecnológicos han potenciado y mejorado la eficiencia y efectividad del procesamiento de datos, otorgando grandes ventajas. Hoy en día, todas las organizaciones utilizan sistemas informáticos basados en tecnología de la información para realizar sus actividades, lo que permite alcanzar los objetivos y metas estratégicas y se traduce en un mayor y mejor control de los procesos, mayor productividad y reducción de costos.

En particular, las empresas vitivinícolas de la provincia de Mendoza desarrollan sus operaciones a través de sistemas informáticos que les permiten obtener las ventajas mencionadas con anterioridad. Estas empresas representan una importante fuente de ingresos y son parte de la cultura mendocina, es por ello que son fundamentales en la provincia ya que la vitivinicultura es una de las actividades económicas más relevantes a nivel local.

La empresa vitivinícola analizada en el presente trabajo de investigación emplea diversos sistemas para captar datos, procesarlos, almacenarlos y obtener información para la toma de decisiones y la realización de sus operaciones y negocios. El principal sistema que se utiliza es de gestión, denominado JD Edwards, mediante el cual se procesan prácticamente el 80% de las operaciones de la empresa, donde se realizan las transacciones de compras, consumo de insumos, pago a proveedores, liquidaciones de impuestos y casi todas las operaciones. Quedan exentas algunas áreas o módulos que no están incluidos en el mismo, como ocurre por ejemplo con el área agrícola que utiliza otras herramientas para poder gestionar. Por su parte, el área de turismo también trabaja con otro sistema que es Tango Gestión. A su vez, en la empresa se utilizan sistemas de explotación de datos, de inteligencia de negocios y sistemas satélites que son desarrollos que se hacen a medida para atender algún aspecto puntual. También se emplean las herramientas de Microsoft Office como Excel, que permiten hacer tareas y realizar el seguimiento de la entidad.

1.2.ESTRATEGIAS DE LOS SISTEMAS DE INFORMACIÓN

Según Porter, M. E. (2008), existen cinco fuerzas competitivas que le dan forma a la estrategia de una empresa: rivalidad entre los competidores existentes, amenaza de nuevos entrantes, poder de

negociación de los proveedores, poder de negociación de los compradores y amenaza de productos o servicios sustitutos.

Laudon, K. C. y Laudon, J. P. (2012) establecen que para que una empresa pueda enfrentarse y contraatacar estas fuerzas competitivas puede utilizar la tecnología y sistemas de información a través de cuatro estrategias genéricas a saber:

- **Liderazgo de bajo costo:** los sistemas de información se pueden utilizar para permitir la reducción de los costos operacionales y para obtener menores y mejores precios. Al utilizar un sistema que brinda una respuesta eficiente al cliente, se enlaza su comportamiento con la empresa.
- **Diferenciación de productos:** es posible utilizar los sistemas de información para habilitar nuevos productos o servicios o para modificar y aumentar la conveniencia del cliente en la utilización de los productos y servicios existentes. Los mismos permiten generar nuevos productos hechos a medida, personalizados según las especificaciones dadas por los clientes.
- **Enfoque en nichos de mercado:** la utilización de los sistemas de información permite a la empresa enfocarse en un mercado específico para brindar un mejor servicio. De esta manera, se pueden analizar más fácilmente los datos para evaluar los gustos, preferencias y patrones de compra de los clientes y así establecer técnicas de marketing precisas que mejoren los niveles de ventas.
- **Fortalecimiento de la intimidad con los clientes y proveedores:** al utilizar sistemas de información es posible estrechar y fortalecer los vínculos con los clientes y proveedores ya que permiten un acceso directo a los mismos. Mantener estos lazos fuertes aumenta la lealtad hacia la empresa y aumenta el costo de cambiar a la misma por la competencia.

Estas estrategias pueden ser aplicadas de manera individual o complementándose entre sí. Cuando una empresa tiene estrategias competitivas establecidas obtiene un mayor crecimiento de sus ingresos, de su productividad y una mayor rentabilidad, ya que le va mejor que a la competencia y posee mejores activos de información y, por ende, tiene un conocimiento superior.

Por su parte, Saroka, H. R. (2002) explica que la información es esencial para descubrir oportunidades a través de los sistemas de información. La misma puede ser utilizada para identificar estrategias que permitan generar ventajas competitivas y también para atacar las posibles amenazas competitivas que se presenten. Para el autor existen dos estrategias básicas que permiten obtener ventajas competitivas y son la reducción de costos y la creación y diferenciación de productos. La reducción de costos aplicando tecnología informática anteriormente se limitaba a obtener mayor eficiencia en la administración global de la empresa. Hoy en día lo que se pretende es la transformación de los métodos de

producción, comercialización y distribución y la innovación en las operaciones internas y externas. En cuanto a la creación y diferenciación de productos, es la tecnología informática la que lo permite y lo hace rentable. Además, toda la infraestructura informática que posee la organización es la que respalda los nuevos productos.

Actualmente en la empresa vitivinícola bajo estudio se utilizan herramientas de inteligencia de negocios pero no se aplican particularmente para lograr la diferenciación con respecto a la competencia, sino más bien para cumplir con los objetivos de venta de la parte comercial. Sin embargo, los sistemas utilizados ayudan con la reducción de costos ya que se redujeron notablemente muchos procesos que anteriormente se llevaban a cabo de manera manual, dependían de más personas y requerían más papeles y trámites más extensos. Además, con la implementación de un sistema informático mejor y más grande, la empresa ha podido crecer y aumentar su volumen en cuanto a ventas, administración y demás sin tener que aumentar el staff, lo que se traduce en una reducción de personal. A su vez, ha aumentado la eficiencia de las operaciones. Por este motivo, se podría decir que la principal ventaja competitiva que posee la empresa vitivinícola es la reducción de los costos de operación a través de la utilización de su sistema informático.

Este sistema es de calidad y está correctamente configurado en relación con los accesos y segregación de funciones, por lo que la organización tiene la seguridad de que la información contenida en la base de datos cumple con los requisitos de existencia (que lo registrado realmente haya ocurrido) e integridad (se ha registrado todo lo ocurrido). Además, el procesamiento de las operaciones se realiza en tiempo oportuno por parte de los usuarios. Todo esto le asegura a la empresa poseer información fidedigna para la toma de decisiones.

La eficiente administración del sistema de información por parte de la empresa vitivinícola, mejora notablemente los tiempos que insume el procesamiento de las operaciones realizado por los operadores. Por otra parte, permite minimizar el tiempo que se requiere para revisar y depurar información al momento de tomar alguna decisión. Esta liberación de tiempo favorece la realización de nuevas tareas e inclusive, en algunos casos, la optimización del número de personas que trabajan en la organización, lo que se traduce en reducción de costos y mayor productividad.

En cuanto a la situación a futuro, la empresa vitivinícola pretende contar concretamente con distintas ventajas competitivas y para ello ha adquirido una nueva herramienta de inteligencia de negocios donde se están definiendo indicadores para todas las gerencias. Estos indicadores se van a desarrollar de manera conjunta con una consultora contratada por la empresa para que posteriormente sean los propios

usuarios de cada área quienes los vayan desarrollando. Con esta herramienta se logrará tener ventajas competitivas como diferenciación de productos y enfoque en nichos de mercado.

1.3.REQUISITOS DE LA INFORMACIÓN

En las organizaciones la toma de decisiones debe ser correcta y de calidad, para ello se requiere información que, a su vez, sea de calidad. Por lo tanto, es necesario contar con sistemas confiables que procesen adecuadamente los datos para transformarlos en información adecuada y oportuna.

Cuando los datos que manejan las empresas son imprecisos, incompletos o inconsistentes, se generan problemas operacionales y financieros; además, las decisiones se tornan imprecisas. Es por esto que las empresas deben tomar acciones para asegurarse de que la información posee un alto nivel de calidad (Laudon, K. C. y Laudon, J. P., 2012).

Saroka, H. R. (2002) establece que para que la información sea eficiente debe cumplir con ciertos requisitos. De esta manera, se asegura que la utilidad que brinde justifique los recursos que se emplean para producirla. Estos requisitos son:

- **Economía:** el costo de producir información no debe ser superior al beneficio que se espera obtener con su utilización. Por ello, se debe analizar la relación costo-beneficio.
- **Oportunidad:** la información debe estar disponible en el momento en que sea requerida.
- **Utilidad:** toda salida de un sistema de información debe satisfacer una necesidad y, por lo tanto, ser útil para los usuarios.
- **Comparabilidad:** la información debe ser comparable en el tiempo, es decir, se debe poder comparar de un periodo a otro. También debe ser comparable en el alcance, lo que sucede cuando las comparaciones corresponden a conceptos semejantes. Por último, debe ser comparable en el espacio, lo que se refiere, por ejemplo, a la comparación de información entre distintas sucursales.
- **Flexibilidad:** todo sistema de información debe adaptarse a los cambios. De esta manera, se satisfacen las cambiantes necesidades de información de la organización.
- **Claridad:** la información debe ser clara y comprensible, teniendo en cuenta el nivel intelectual y técnico del destinatario, así como sus preferencias y su lenguaje. Esto se logra con sistemas de información que gocen de la mayor simplicidad posible.
- **Confiabilidad:** la información debe ser confiable para los usuarios de manera que puedan tomar decisiones basados en ella. La calidad de un sistema de información está determinada, en buena parte, por la calidad y confiabilidad de sus datos primarios.

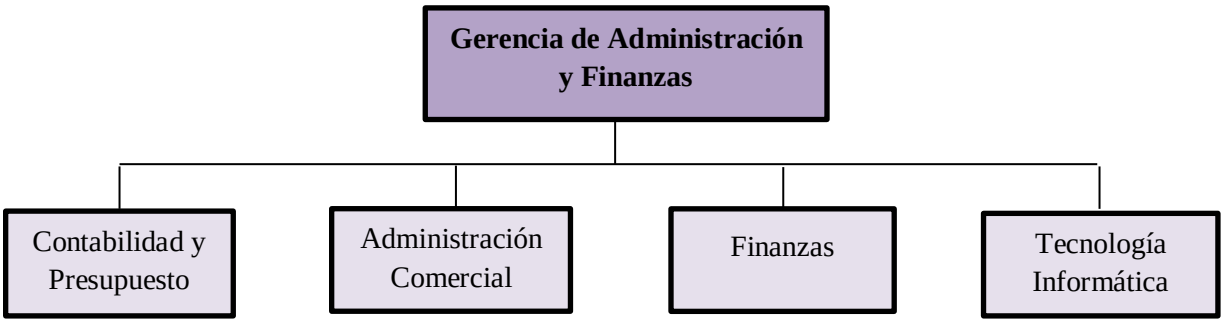
1.4. ADMINISTRACIÓN DE LA INFORMACIÓN

Para que la información cumpla el rol clave que tiene en las organizaciones y permita alcanzar las ventajas competitivas, brindando la mayor utilidad posible, es fundamental que sea adecuadamente administrada. La administración comprende cuatro actividades: planificación, organización, dirección y control. En una empresa debe haber una planificación de cómo se va a capturar, almacenar y utilizar la información. Además, debe ser correctamente organizada para que haya orden y se sepa dónde se encuentra lo que se requiere y quién utiliza cada información. La dirección se requiere para que todos los integrantes de la empresa se dirijan hacia los mismos objetivos, y el control para verificar que la información se utilice correctamente, de acuerdo con lo planificado y con la organización establecida, garantizando de esa manera la seguridad de la misma.

La administración de la información implica, a su vez, la administración del hardware y del software, los sistemas de archivos y comunicaciones, el sistema de administración de formularios, y todo aquello vinculado a la información. Se deben administrar tanto los datos manuales como los digitales, y los procesamientos de datos computarizados como así también los manuales (Saroka, H. R., 2002).

La empresa estudiada posee un Departamento de Tecnología Informática quien se encarga de la administración de los sistemas. En la estructura que presenta la organización, de la Dirección de Gerencias dependen las Gerencias de Administración y Finanzas, Mercado Interno, Mercado Externo, Logística y Abastecimiento, Negocios Especiales, Agrícola, Enología, Planta de Embotellado y Mantenimiento. Al centrarse en la Gerencia de Administración y Finanzas, el organigrama es el siguiente:

Figura 2: Estructura de la Gerencia de Administración y Finanzas



Por lo tanto, el Departamento de Tecnología Informática depende de la Gerencia de Administración y Finanzas por una decisión de la Dirección. Esto es así porque este Departamento se estableció simplemente como un sistema de administración pero la realidad es que es horizontal a toda la

organización, entonces esta ubicación le dificulta mucho la toma de decisiones y demás tareas por no tener una línea directa con la Dirección. Sin embargo, se busca que en el corto o mediano plazo pase a depender directamente de la misma y que sea un Departamento independiente.

Normalmente en la organización de muchas empresas el área de informática o sus especialistas se ubican dependiendo de la parte de administración, finanzas o contabilidad porque todas las empresas necesitan de sistemas que cumplan con las funciones relacionadas, como facturación por ejemplo, por lo que se necesita del informático que haga que dichos sistemas funcionen. Pero esta estructura es válida en empresas chicas. En las empresas que empiezan a ser más grandes el área de sistemas requiere independencia y para ello debe estar ubicada a la misma altura que otras gerencias ya que resulta tan estratégica como cualquier otra área empresarial. Esto se debe a que apoyan todos los proyectos que se llevan a cabo y todo lo que ocurre en la empresa pasa por los sistemas.

En el caso de la empresa vitivinícola, el Departamento de Tecnología Informática se relaciona con el resto de la Gerencia mediante la realización de reuniones y el trabajo en proyectos y obras que hay que llevar a cabo, como remodelación de determinadas cosas o determinar cómo se debe mejorar la seguridad en sitios web, entre otros aspectos. Este Departamento tiene una cantidad de proyectos definidos y cada uno de estos impacta en cada Gerencia. Entonces, se van realizando reuniones formales e informales en las que se va revisando el avance de estos proyectos con las distintas Gerencias.

Los proyectos que se desarrollan se separan en tres aspectos: proyectos relacionados con software, proyectos relacionados con hardware y comunicaciones, y proyectos relacionados con la organización del área. Alguno de estos impactan directamente en una Gerencia y otros impactan en varias. Por ejemplo, el sistema JD Edwards tiene varios módulos, uno de ellos es el de producción y enología que se maneja directamente con la Gerencia de Enología así como todo lo relacionado con el avance de los proyectos que le conciernen.

Actualmente, el Departamento de Tecnología Informática está organizado de la manera que se expone a continuación:

Figura 3: Organigrama del Departamento de Tecnología Informática

Como se puede ver, este Departamento tiene separado lo que es hardware, comunicaciones y software. Las funciones básicas que tiene son las de brindar soporte, elaborar nuevos proyectos y encargarse de las comunicaciones. Dentro de lo que es hardware y comunicaciones, se trabaja en todo lo relacionado a corregir las máquinas. Específicamente en el área de hardware, se controla todo lo referido a cámaras de seguridad, telefonía, estaciones meteorológicas, impresoras y todos los dispositivos periféricos de oficina. Todo esto es administrado por el Departamento de Tecnología Informática. Con respecto a comunicaciones, se trabaja con Internet, telefonía celular y telefonía fija, routers, switches y todo lo que interviene en la comunicación. Además, se realiza el manejo, administración y gestión con los proveedores. Y en cuanto al soporte, se brinda soporte desde el punto de vista técnico cuando los usuarios tienen algún inconveniente con una computadora, teléfono, cámara de seguridad o cuando tienen algún problema referido a comunicaciones. Por lo que se da solución a ese tipo de problemas y, a su vez, se va comprando y adquiriendo nuevo equipamiento.

Por su parte, en lo que es software se poseen distintos sistemas. Para JD Edwards y Tango Gestión se trabaja en equipo con consultoras que dan soporte y dentro de la empresa se va trabajando en los distintos módulos de los mismos. Entonces, el área de sistemas lo que hace es coordinar las tareas con las consultoras, administrar los nuevos requerimientos por un lado y el soporte por otro. Hay nuevos requerimientos de las áreas que deben ser estudiados y evaluados, tener reuniones con los proveedores y tener reuniones con las áreas usuarias para ver si están de acuerdo y aprobar la propuesta y, de esa forma, avanzar. Eso es para todos los sistemas, no sólo para JD Edwards y Tango Gestión, sino también para todos los sistemas satélites. También se trabaja con terceros que complementan la labor realizada con tareas más específicas. Cada persona que trabaja en este Departamento tiene un perfil de puesto donde figuran las funciones básicas que debe llevar a cabo.

Ahora bien, cuando la administración de la información no existe o cuando la existente no es la correcta, se generan una serie de inconvenientes en el manejo de la información ya que los sistemas crecen sin la necesaria planificación. En términos de Laudon, K. C. y Laudon, J. P. (2012) los problemas que surgen son los siguientes:

- **Redundancia e inconsistencia de los datos:** se da cuando un mismo dato es almacenado o archivado en distintos lugares, es decir, es duplicado, lo que genera desperdicio de recursos de almacenamiento e inconsistencia.
- **Dependencia de programa-datos:** los cambios en los programas que se utilizan para actualizar y mantener los archivos de datos requieren cambios en dichos datos, a los que accede ese programa.
- **Falta de flexibilidad:** se refiere a la falta de adaptación a los cambios que puedan surgir.

- **Seguridad defectuosa:** la falta de control hace que se desconozca quién accede a los datos y los modifica.
- **Falta de compartición y disponibilidad de los datos:** la información no puede fluir con libertad por las distintas áreas de la empresa, por lo que se dificulta el poder compartirla o acceder a ella de manera oportuna.

Los mismos se han presentado en la empresa vitivinícola en mayor o menor medida. Se ha dado el caso, por ejemplo, de tener una base de datos fuera de servicio al quedar chico el almacenamiento por no haber un adecuado mantenimiento. También se da la redundancia de datos ya que lo sistemas son independientes y se cargan los mismos datos en distintas bases de datos. Esto es una gran carga pero al emplear distintos sistemas generalmente no comparten la misma base de datos lo que implica necesariamente la duplicidad de datos.

La empresa trabaja de manera correctiva, es decir, los problemas son solucionados una vez que se han producido. El Administrador de Base de Datos es la persona que se encarga de monitorear y controlar constantemente las bases de datos para evitar los problemas. Actualmente, ese perfil no se encuentra en la empresa pero se está evaluando la contratación de una consultora a fin de mejorar en ese aspecto y obtener ese servicio, de esa manera se podría trabajar de forma preventiva y proactiva.

Por otra parte, estos problemas pueden ser resueltos con la aplicación de un sistema de administración de bases de datos, que "es un software que permite a una organización centralizar los datos, administrarlos en forma eficiente y proveer acceso a los datos almacenados mediante programas de aplicación" (Laudon, K. C. y Laudon, J. P., 2012, p. 212). La tecnología informática es la que permite que los datos sean capturados, procesados y almacenados de manera ordenada en archivos y bases de datos para que se pueda contar con la información oportunamente (Saroka, H. R., 2002).

En la empresa vitivinícola la información se administra a través de base de datos, archivos generales, servidores de archivos para compartir, correo electrónico y sistemas propietarios para los diferentes sectores empresariales. Sin embargo, la principal herramienta que posee para la administración de la información es un sistema del tipo Enterprise Resource Planning (ERP) que son sistemas de planificación de recursos empresariales.

Este tipo de sistemas permiten administrar la información a través de bases de datos consolidadas. Además, tienen un tratamiento integral de la información que ingresa al sistema a través de las operaciones que registran los usuarios. Permiten optimizar el tiempo, los recursos y el dinero, por lo que

generan grandes beneficios empresariales, entre ellos, una gestión más eficiente debido a la sincronización entre departamentos.

Los sistemas ERP consolidan la información que cada usuario carga al sistema en su puesto de trabajo y poseen “seguridad de usuario”, es decir, permite limitar las operaciones que cada usuario puede realizar en el sistema y ayuda a optimizar las tareas llevadas a cabo. También dan una visión global de la información lo que permite solucionar los posibles problemas de manera proactiva, lograr la mejora continua y reducir los riesgos. Dentro de este tipo de sistemas, el que es utilizado concretamente por la empresa es JD Edwards EnterpriseOne (JDE), que es un producto de Oracle.

Por otra parte, los sistemas de administración de base de datos utilizados son Structured Query Language (SQL) y My Structured Query Language (MYSQL) que son lenguajes de consulta estructurados, y también se utilizan algunas herramientas POSTGRES.

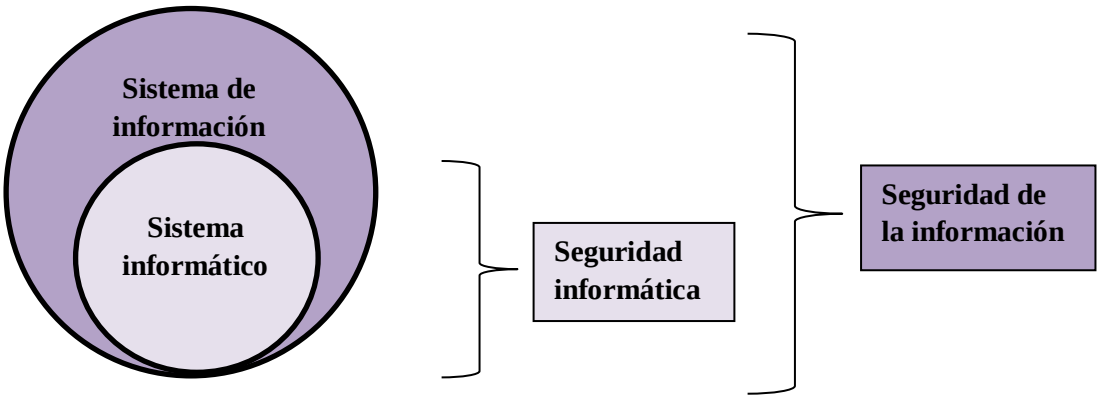
Ahora bien, el presente trabajo de investigación hace foco en el problema de seguridad defectuosa ya que es muy frecuente que se de en las organizaciones debido a la falta de conocimiento y cultura sobre la seguridad informática. Además, es el problema que más afecta la información y el que genera mayores inconvenientes.

2. LA SEGURIDAD INFORMÁTICA

Como se vio anteriormente, la información representa uno de los activos de mayor valor que posee toda empresa y es trascendental ya que se utiliza tanto en las tareas diarias como en la toma de decisiones estratégicas. Cualquier pérdida, daño o alteración de la misma podría provocar serios problemas para el funcionamiento normal de las operaciones y hasta podría significar graves pérdidas económicas. Es de vital importancia que se proteja la información. Por este motivo, como la mayoría de las empresas en la actualidad poseen sistemas informáticos, es necesaria e imprescindible la seguridad informática.

Así como los sistemas de información son más amplios y abarcan a los sistemas informáticos, la seguridad de la información es más amplia que la seguridad informática. La seguridad informática se concentra en la protección de los recursos informáticos. Antiguamente, la información se manejaba sólo en papel por lo que la seguridad era física, pero en la actualidad, además, se maneja de manera electrónica lo que implica que la seguridad se lleve a cabo con un soporte informático (Peñuela Vasquez, Y. D., 2018).

Figura 4: Seguridad informática vs seguridad de la información



2.1. RECURSOS INFORMÁTICOS

Para comprender mejor la seguridad informática es importante conocer cuáles son los recursos que la misma busca proteger. Un sistema informático está conformado por el hardware, software, recursos humanos, datos e información.

El hardware son los recursos físicos y tangibles que se utilizan para las actividades de entrada, proceso y salida en un sistema de información, como las computadoras, los periféricos de entrada y salida, impresoras, lectores de código de barras, entre otros. Por su parte, el software son los recursos lógicos e intangibles, es decir, programas e instrucciones detalladas que controlan, coordinan y permiten a la computadora realizar determinadas tareas. La tecnología de almacenamiento de datos es la que organiza los datos en medios de almacenamiento físicos y la tecnología de redes y telecomunicaciones conecta los distintos elementos del hardware y permite la transmisión de datos de una ubicación física a otra. Cuando dos o más computadoras están interconectadas para compartir recursos se trata de una red, donde las computadoras y el equipo de comunicaciones se conectan. Las redes internas que poseen las empresas y que utilizan la tecnología de internet son las intranets, en tanto que las extranets son las intranets privadas que pueden ser utilizadas por usuarios autorizados fuera de la organización (Laudon, K. C. y Laudon, J. P., 2012). Por último, los recursos humanos son los usuarios de la información, quienes operan y administran los recursos físicos y lógicos. Son todas las personas que forman parte del sistema.

El conjunto de todos estos recursos conforman la infraestructura de tecnología de información de la empresa, que debe adaptarse a los requerimientos específicos de la misma. Cuando se hace un mejor uso de los recursos informáticos aumenta la eficiencia operativa, posibilita la creación de nuevas oportunidades de negocios y se sustentan los procesos clave de la organización, por lo que se genera valor

(Sánchez, E. L. y Lettry, R. N., 2008). La tecnología de información es una poderosa herramienta que permite potenciar y amplificar las capacidades humanas pero para ello es necesario contar con el debido conocimiento de la misma y capacitarse continuamente.

Cada uno de los activos informáticos cumple un rol clave en el desempeño empresarial, por lo que deben ser adecuadamente preservados de cualquier amenaza que pueda afectarlos o dañarlos.

2.2. DEFINICIÓN DE SEGURIDAD INFORMÁTICA SEGÚN DISTINTOS AUTORES

"La seguridad es la situación en la que se está adecuadamente protegido contra pérdidas, de modo tal que los hechos adversos están apropiadamente impedidos, disuadidos, prevenidos, detectados y/o corregidos" (Saroka, R. H., 2002, p. 315).

Según Voutssas M., J. (2010), la seguridad informática es "el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización" (p. 131). Los riesgos y amenazas deben ser administrados para así reducirlos a niveles aceptables, por lo que se garantiza a la empresa el correcto funcionamiento interrumpido de sus actividades y el de los recursos, y de esa manera se permite el logro de sus objetivos.

La preservación de la información puede ser a corto, mediano o largo plazo de acuerdo al periodo de tiempo en el que se requiere su protección y conservación. Además, está ligada al valor que la misma posee. Toda información valiosa debe ser preservada a través de la seguridad informática la que, como se vio anteriormente, busca eliminar o contener los posibles daños y pérdidas que se puedan producir.

En palabras de Ramió Aguirre, J. (2006), la seguridad informática es "un conjunto de métodos y herramientas destinadas a proteger la información y por ende los sistemas informáticos ante cualquier amenaza" (p. 50). Es un proceso en el que intervienen personas y es fundamental que se capaciten y sean conscientes de su importancia. Esta definición coincide con la dada por García Pierrat, G. y Vidal Ledo, M. J. (2016) que establece que la seguridad informática se orienta a la protección de la infraestructura de tecnología de la información, a través de la minimización de los posibles riesgos que puedan afectar dicha infraestructura y la información. Lo que se busca es que el sistema de información sea seguro y confiable, y el objetivo es garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información (Peñuela Vasquez, Y. D., 2018).

Voutssas M., J. (2010) afirma que la seguridad informática tiene un objetivo primario y un objetivo secundario. El objetivo primario consiste en administrar y minimizar los riesgos sobre los recursos informáticos para permitir la continuidad operativa de la empresa. Y el objetivo secundario es brindar y mantener la confiabilidad total de los archivos, registros y documentos informáticos que posea la misma. Para lograr esa confiabilidad total es necesario que se cumplan seis características esenciales:

- **Permanencia:** se refiere a la continuidad del soporte físico y a la existencia de la información por el periodo de tiempo que sea necesario. Se trata de un almacenamiento permanente seguro de la información que permita que las operaciones de la empresa continúen su curso por más que hayan ocurrido daños.
- **Accesibilidad:** los usuarios deben poder acceder a la información y la misma debe ser visible. El acceso a los documentos depende de la capacidad para disponer de programas, sistemas operativos, etcétera, que sean necesarios para ello. En otras palabras, se debe contar con la capacidad tecnológica de acceso.
- **Disponibilidad:** los recursos informáticos deben estar a disposición para su acceso o uso cuando los usuarios autorizados lo requieran. La información debe estar disponible de acuerdo a las condiciones preestablecidas, en los tiempos en que sea requerida y para las personas autorizadas a su acceso y utilización.
- **Confidencialidad (privacidad):** la información debe ser privada y no deben poder acceder a ella personas, entidades o procesos que no cuenten con la debida autorización. Por lo tanto, la información debe estar disponible siempre sólo para los usuarios autorizados, en las circunstancias y bajo las condiciones que hayan sido establecidas. Se debe proteger para que no sea utilizada, observada o divulgada indebidamente.
- **Autenticidad (integridad):** la información debe ser completa y correcta; sólo puede ser creada, modificada o borrada por los usuarios autorizados. La autenticidad es considerada como una característica fundamental para la preservación ya que garantiza que la información no se encuentra corrompida y está libre de alteraciones, es confiable y aceptable.
- **Aceptabilidad (no repudio):** la comunicación de la información entre emisor y receptor debe permitir dar fe de su autenticidad y aceptabilidad de manera que no sea rechazada. Se debe conocer la calidad del proceso de creación de la información y de su conservación y seguridad.

Entonces, cuando la información cumple con todas estas características se puede decir que ha conseguido la confiabilidad total, y de esa manera se logra el objetivo secundario de la seguridad informática. Y, según Ramió Aguirre, J. (2006), cuando se cumplen los principios de confidencialidad,

integridad y disponibilidad los datos están protegidos y seguros, ya que sólo los usuarios autorizados los pueden conocer, crear o modificar, y dichos datos deberán estar disponibles siempre.

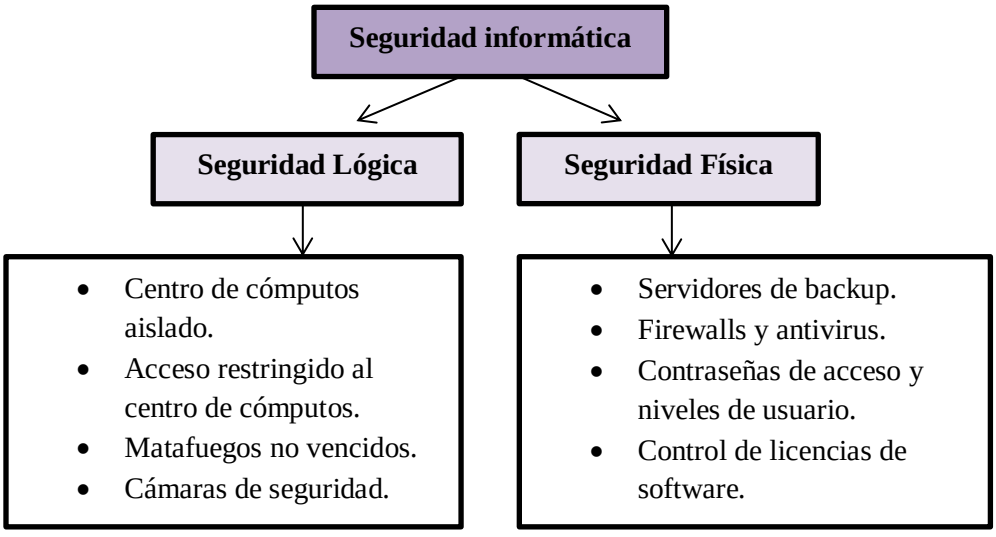
En la empresa vitivinícola se busca que la información cumpla con todos estos requisitos, que son considerados al momento de resguardar los datos para tenerla disponible y que sea confidencial, autentica y aceptable. De esa manera se obtiene la seguridad de que la información en la que se basan los distintos usuarios para la toma de decisiones es confiable y precisa. Sin embargo, estas características de la información pueden verse vulneradas por la ocurrencia de eventos, por lo que en la empresa se utilizan algunas herramientas que ayuden a detectar amenazas o las posibles vulnerabilidades de los sistemas de información de forma preventiva.

Ahora bien, la seguridad informática se puede ver desde dos enfoques complementarios a saber:

- **Seguridad lógica:** protección de los datos, la información y el software. Brinda seguridad en el uso del sistema, procesos, programas, etcétera, y verifica que la información sea utilizada por usuarios autorizados.
- **Seguridad física:** protección del hardware. Preservación del sistema de las amenazas físicas a través del establecimiento de barreras y controles.

En el caso de la empresa analizada algunos ejemplos de estos tipos de seguridad que son aplicados serían los siguientes:

Figura 5: Ejemplos de seguridad informática en la empresa vitivinícola



Es importante recordar que la seguridad nunca es completa o acabada debido a que siempre hay posibilidad de riesgo. Esto es así porque el riesgo se reduce a niveles aceptablemente bajos, lo que no quiere decir que no exista. El proceso de seguridad informática es permanente y evolutivo ya que constantemente surgen nuevas amenazas y riesgos que pueden afectar a la organización. Por ello, siempre debe ser perfeccionado y actualizado para mantener un nivel de seguridad adecuado y una administración del riesgo razonable, teniendo en cuenta la relación costo beneficio de las medidas adoptadas con respecto al valor de los recursos informáticos (Voutssas M., J. 2010).

2.3. IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA

Como ya se ha mencionado, las empresas poseen activos de información sumamente valiosos que deben ser protegidos. Los sistemas pueden contener datos confidenciales, información sobre los procesos y operaciones organizacionales, planes estratégicos y de negocios, secretos comerciales y demás información de vital importancia. Sin embargo, el valor de dicha información se pierde en gran escala si la misma es conocida por personas externas a la empresa. La protección de los sistemas informáticos no debe ser subestimada y dejarse de lado porque es imprescindible para el desarrollo de las operaciones del ente. Por el contrario, se debe invertir en seguridad ya que la información tiene un valor inmensurable y su pérdida, alteración o sustracción pueden generar un impacto devastador. Además, no sólo es la propia información la que está en juego sino también la referida a los empleados, clientes, proveedores y demás personas o entidades que se relacionen con la empresa, lo que podría generarle responsabilidad por los posibles daños ocasionados, pérdida de confianza y podría afectar su imagen. Por este motivo, se debe evitar la fuga y pérdida de información confidencial y la corrupción de los datos adoptando las medidas de seguridad correspondientes (Laudon, K. C. y Laudon, J. P., 2012).

Es sabido que la tecnología avanza a un ritmo sumamente acelerado, en consecuencia las empresas deben adaptarse continuamente a los cambios e incorporarla a sus negocios si pretenden sobrevivir. Así como estos avances en la tecnología traen consigo maravillosas ventajas y oportunidades, también posibilitan un mayor nivel de amenazas para las cuales es fundamental contar con la debida preparación, prevención y capacitación.

Los sistemas informáticos están integrados en las operaciones de las organizaciones, por lo que se genera una dependencia con respecto a la tecnología. Cuando esta falla y no existen procedimientos alternativos se provoca una interrupción en las operaciones y, por lo tanto, no es posible cumplir con los objetivos de la empresa, lo que origina pérdidas que tienen gran impacto. Ante las nuevas amenazas y ataques que van surgiendo día a día, muchas empresas no logran recuperarse y sobrevivir tras la pérdida de su información. Por este motivo, contar con políticas y medidas de seguridad es un factor estratégico

que permite el desarrollo y éxito empresarial. La protección de la información almacenada y procesada a través de los sistemas informáticos es más compleja y se debe preservar no sólo la disponibilidad sino también la integridad y confidencialidad de la misma, lo que da lugar a información de calidad para la toma de decisiones. Todos los usuarios deben ser conscientes de la importancia de la seguridad informática, desde los directivos hasta los empleados, ya que todo aquel que se relaciona con la tecnología de la información va a estar involucrado en su seguridad (García Pierrat, G. y Vidal Ledo, M. J., 2016; Ramió Aguirre, J., 2006).

La falta de cultura, conocimiento y entendimiento sobre la importancia de la seguridad informática es un grave problema que afecta a las organizaciones. En la actualidad, existen grupos de personas organizadas y especializadas en distintos tipos de ataques que buscan obtener información de gran valor para las empresas. Los delitos informáticos son cada vez más frecuentes y de mayor impacto debido a la globalización, la utilización de internet y de nuevas tecnologías que facilitan la ejecución de los mismos. Las personas que se dedican a estas actividades delictivas son conscientes de la importancia y el valor que tiene la información para las empresas y saben que se trata de un negocio sumamente lucrativo. El problema radica en que muchas veces las empresas no están preparadas para contrarrestar los ataques. Por este motivo las medidas de seguridad que se adopten deben integrarse a los planes estratégicos y se debe realizar un seguimiento permanente de las mismas (Peñuela Vasquez, Y. D., 2018). Además, es importante que todos los miembros de la empresa se comprometan y se capaciten en el tema.

Existen tres principios de la seguridad informática que deben ser tenidos en cuenta, según Ramió Aguirre, J. (2006): el acceso más fácil, la caducidad del secreto y la eficiencia de las medidas tomadas.

- **Acceso más fácil:** el atacante va a buscar el punto más débil del sistema de manera de facilitar su acceso y posterior ataque. El mismo puede ser perpetuado desde distintos puntos, tanto internos como externos.
- **Caducidad del secreto:** se debe determinar por cuánto tiempo deben protegerse los datos confidenciales. El sistema de protección caduca cuando ya no es necesario mantener el secreto y confidencialidad de la información.
- **Eficiencia de las medidas tomadas:** las medidas de control establecidas deben ser efectivas, eficientes y apropiadas. Es decir, deben funcionar oportunamente, optimizar la utilización de recursos y pasar desapercibidas por los usuarios.

La empresa vitivinícola considera la seguridad informática como un factor de suma importancia. Para mantener la eficiencia y confianza en la información que se genera día a día en la organización se cuenta con sistemas que se encargan de avalar y administrar dicha seguridad informática. La misma

permite minimizar riesgos relacionados con accesos a datos no autorizados, duplicidad de información en los registros que luego son base de toma de decisiones y malversación de información o fraudes, entre otros.

El problema radica en que en la provincia de Mendoza la seguridad informática todavía no es considerada como algo crítico. Se trata de un tema del que se habla mucho pero todavía no existe consciencia de su importancia y muchas veces los empresarios que gestionan empresas en base a información no lo tienen en consideración. Esto puede deberse a que a nivel local aún no han ocurrido casos de espionaje industrial o ataques dirigidos hacia una empresa de la competencia, por ejemplo. Sin embargo, resulta fundamental que en Mendoza se comience a generar mayor concientización y capacitación con respecto a la seguridad informática no sólo por la criticidad que representa para la continuidad y supervivencia de una empresa, sino también por las ventajas que se consiguen cuando es considerada como un factor estratégico.

Concretamente en la empresa vitivinícola, se ha iniciado una capacitación del personal con respecto a la seguridad para el sistema JD Edwards. Pero la realidad es que no se cuenta con una persona especialista en seguridad informática, tanto física como lógica, por lo que se busca trabajar con consultoras que brinden ese servicio. Respecto a la seguridad física, existe un proyecto de mediano plazo cuyo objetivo es mejorar el data center actual o trasladarlo a otro lugar a fin de que se encuentre más seguro. Actualmente, la estrategia de la empresa es no contar con una persona especializada y dedicada a la seguridad informática, entonces el Departamento de Tecnología Informática busca asesoramiento de las consultoras y complementar sus conocimientos con las mismas para cubrir y coordinar ese trabajo.

La seguridad informática es fundamental y debe abarcar toda la entidad. La empresa vitivinícola es una organización industrial donde hay Gerencias como enología, compras y abastecimiento, fincas, turismo y demás, en las que también se debe aplicar y trabajar con la seguridad informática ya que se maneja información importante. Por más que la información relacionada con facturación, costos y todos los números de la empresa que se encuentran en la Gerencia de Administración y Finanzas sea más sensible, existen otras áreas como enología que tienen desarrollo de nuevos productos que están por lanzar al mercado para lo que se requiere de estudios e investigaciones. Eso precisa de muchas horas de trabajo, compra de equipos y demás requisitos, que si se llega a producir una filtración de seguridad en esos aspectos puede ser tan importante como que salga a la luz cuánto factura la empresa. Por este motivo, resulta importante que se realicen revisiones periódicas de la seguridad informática en toda la empresa, a través de la evaluación de riesgos y la aplicación de controles que permitan proteger la información.

En conclusión, se puede ver que los datos captados, procesados y transformados en información a través de los sistemas informáticos son el centro de poder de las organizaciones y les brindan el conocimiento necesario para poder operar, crecer y competir en el mercado. Sin ellos no es posible la existencia y supervivencia empresarial. Por este motivo resulta tan importante la seguridad informática que busca proteger todos los recursos informáticos de cualquier amenaza, riesgo o ataque que pueda afectarlos. Cuando en las empresas se cuenta con la debida seguridad, la información cumple con todas las características esenciales que permiten la correcta toma de decisiones y el logro de ventajas estratégicas. De esta forma, se logra la mejora en la operatividad y productividad empresarial y se garantiza su supervivencia y competitividad en el mercado.

La empresa vitivinícola cuenta con diversos sistemas informáticos, que son los que permiten realizar las distintas transacciones organizacionales. La implementación de los mismos permite alcanzar las estrategias de una mayor productividad y eficiencia, así como la reducción de costos en las operaciones. Por su parte, la administración de dichos sistemas está a cargo del Departamento de Tecnología Informática, que depende de la Gerencia de Administración y Finanzas, lo que impide que cuente con la debida independencia funcional. Este Departamento se encarga de brindar soporte, elaborar proyectos y de las comunicaciones. Sin embargo, en lo que se refiere a seguridad informática, por decisión de la Dirección, no hay un sector específico que se dedique a la misma, sino que el área de sistemas es quien se encarga en conjunto con consultoras contratadas.

Los sistemas informáticos deben ser protegidos aplicando las medidas de seguridad adecuadas a fin de que la información sea íntegra, confiable y esté oportunamente disponible. De esta manera, se tiene la seguridad de que se toman decisiones correctas, las operaciones se llevan a cabo de la mejor manera y de que los negocios van a ser continuos y exitosos. Por ello, es importante que en Mendoza las empresas comiencen a tener mayor conciencia de la criticidad de la seguridad informática en sus operaciones cotidianas.

CAPÍTULO II

AMENAZAS Y RIESGOS EN LA INFORMACIÓN

El presente capítulo tiene por objeto definir y dar a conocer las vulnerabilidades, riesgos y amenazas en los sistemas informáticos existentes en la empresa vitivinícola bajo estudio. Los autores con los que se trabaja son Laudon, K. C. y Laudon, J. P., Saroka, H. R., Voutssas M., J. y García Pierrat, G. y Vidal Ledo, M. J., entre otros.

1. CONCEPTOS FUNDAMENTALES

Los sistemas informáticos empresariales muy frecuentemente presentan debilidades que los hacen vulnerables a las amenazas, riesgos y ataques. Esto afecta a todos los recursos informáticos y a la organización en su conjunto, pudiendo significar graves pérdidas económicas, daños en la imagen corporativa y hasta la extinción de la empresa si no logra recuperarse adecuadamente. Por este motivo, es fundamental conocer cuáles son las debilidades que presentan los sistemas y contar con los conocimientos necesarios para evitar dichas amenazas, riesgos y ataques que pretenden vulnerarlos a fin de proporcionar la seguridad y los controles necesarios.

Particularmente, en la empresa bajo estudio se considera que el sistema informático presenta ciertas debilidades lo que lo hace medianamente seguro. En la situación actual de la organización se cuenta con el equipamiento necesario a nivel de seguridad pero ha sido actualizado en términos de firewalls, sistemas operativos y aplicativos para mejorarlo.

Como se considera que el nivel de seguridad informática es medio, el Departamento de Tecnología Informática trabaja con consultoras para tener propuestas de mejora en el corto y mediano plazo. También se ha iniciado una capacitación de seguridad porque se creía conveniente. Ya que no se puede tener una persona específica trabajando en seguridad informática la estrategia es la tercerización para que cada sistema pueda contar con una persona que se encargue de administrar su seguridad.

Para lograr el éxito, la competitividad y la continuidad de la empresa vitivinícola, es importante que los sistemas informáticos que utiliza se encuentren debidamente protegidos a través de la seguridad informática para evitar cualquier tipo de amenaza, riesgo o delito informático que pueda afectarlas.

1.1.VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS

Según Saroka, R. H. (2002) y Voutssas M., J. (2010), la vulnerabilidad es la debilidad que presenta cualquier recurso o sistema informático, susceptible de ser explotada por una amenaza. En otras palabras, implica una falta de protección ante las amenazas, que pueden generar un efecto nocivo al fallar la seguridad.

Existen distintos tipos de vulnerabilidades, siendo alguna de ellas más importantes que las otras. Las vulnerabilidades físicas y ambientales implican desastres naturales o situaciones adversas del entorno que pueden afectar el sistema. Por otro lado, las propias de equipos y programas facilitan el acceso a los mismos lo que los hace menos seguros debido a fallas o debilidades. Por último, las humanas son las que surgen de las acciones del personal que trabaja con los sistemas, ya sea que los administre o utilice (García, P. G. y Vidal, L. M. J., 2016).

Como ejemplos de estos tipos de vulnerabilidades se pueden mencionar:

- **Vulnerabilidades físicas y ambientales:** ubicación inadecuada de los sistemas y equipos; infraestructura inapropiada e incapaz de resistir a desastres naturales; cables de energía y red desorganizados; falta de protección contra incendios, inundaciones y cortocircuitos; existencia de suciedad o polvo, contaminación y humedad; roturas de computadoras y equipos.
- **Vulnerabilidades humanas:** falta de concientización y capacitación al personal; ignorancia, negligencia o curiosidad de los usuarios, falta de determinación y seguimiento de responsabilidades; desviaciones en el cumplimiento de buenas prácticas; falta de seguimiento de políticas y procedimientos de seguridad; falta de existencia de planes de contingencia.
- **Vulnerabilidades propias de programas y equipos:** fallas en el diseño o construcción de los programas; cambios frecuentes en la infraestructura de tecnología de la información; equipos, programas y redes “heredados”; inadecuada conservación de los equipos; falta de aplicación de antivirus, firewalls, etc.; falta de actualización de los programas.

En la empresa vitivinícola analizada existen ciertas vulnerabilidades físicas y ambientales por lo que se tienen proyectos que buscan renovar la sala de servidores y mejorarla. El data center cumple con las medidas mínimas de seguridad pero se considera que debe ser acondicionado con nuevas medidas. En la empresa se cuenta con matafuegos pero no con alarmas y otros sistemas contra incendios y eso representa una vulnerabilidad. En cuanto a cortocircuitos, se cuenta con un sistema independiente de energía para los servidores que está protegido con todo lo eléctrico indispensable, con térmica, disyuntores, grupo electrógeno y una instalación independiente del resto de la bodega. También podría

producirse una inundación porque en el lugar donde se encuentra la sala de servidores están próximos unos tanques de agua que, si presentan alguna falla, eso podría afectar de alguna manera el funcionamiento de los servidores. Por otro lado, Mendoza es una zona sísmica y, si bien se cuenta con construcciones antisísmicas, no se tiene seguridad total de que no se produzca algún daño y de que los equipos lo resistan dependiendo del evento que pueda producirse.

Con respecto a las vulnerabilidades humanas, en la empresa no se realizan campañas de concientización a usuarios internos acerca del uso adecuado de las herramientas tecnológicas. Esto representa un punto débil ya que, más allá de que se apliquen restricciones a algunos accesos y demás medidas de seguridad, el personal se conecta con sus dispositivos a las redes empresariales y, por ejemplo, puede conectar su pendrive a una computadora y si se encuentra infectado con algún virus puede significar un riesgo si el antivirus no logra bloquearlo. Es un aspecto que se debe trabajar mucho y de manera continua debido a su gran importancia. En la empresa se trabaja sobre casos muy específicos cuando se detecta algo pero no de manera preventiva.

Por su parte, para minimizar las vulnerabilidades propias de programas y equipos se trabaja mucho en la actualización de sistemas. No sólo se mitiga el riesgo con un buen antivirus sino que es necesario acompañarlo con la debida actualización de los sistemas. Sin embargo, hay algunos que son más fáciles de actualizar que otros. Por ejemplo, los sistemas operativos se actualizan periódicamente en la empresa pero con respecto a los sistemas de gestión es mucho más complicado. Esto es así porque se necesita mucho tiempo y es un trabajo que no solo involucra al área de sistemas sino a toda la organización ya que requiere que se vuelvan a probar las aplicaciones y ver que los procesos funcionen.

Los sistemas informáticos almacenan una gran cantidad de datos en forma electrónica lo que los hace más vulnerables que los manuales a los distintos tipos de amenazas. A través de las redes de comunicación, los sistemas se interconectan en distintas ubicaciones, por lo que los riesgos y ataques pueden aparecer por cualquier punto de acceso a la red. Por otra parte, cuando las organizaciones se asocian entre sí la información reside en redes y computadoras que están fuera del control propio de la empresa lo que provoca una mayor vulnerabilidad ya que se podría perder, alterar o podría caer en manos equivocadas generando graves consecuencias. Además, a los negocios se incorporan los dispositivos móviles de bolsillo que son fáciles de perder o robar y poseen graves debilidades de seguridad, lo que puede desencadenar que intrusos ingresen en las redes internas empresariales. Ahora bien, la utilización de Internet por parte de las empresas es fuente de grandes vulnerabilidades para los sistemas de información. Esto es así debido a que las redes públicas son mucho más peligrosas que las privadas porque casi cualquiera puede acceder a ellas y el impacto de los abusos es mucho más amplio. Otra fuente de

vulnerabilidades es la gran utilización de los correos electrónicos, mensajería instantánea y programas para compartir archivos que son susceptibles a los softwares maliciosos y a que terceros puedan acceder a información confidencial. Por todos estos motivos, los datos digitales son vulnerables a la destrucción, mal uso, error, fraude y a las fallas del hardware o software (Laudon, K. C. y Laudon, J. P., 2012).

Actualmente, las empresas tienen una gran dependencia a los recursos informáticos y la misma crece día a día. Por lo tanto, cualquier vulnerabilidad existente puede dar lugar a una grave crisis. Sin embargo, por más que los violadores externos llamen mucho la atención, la mayor parte de los problemas proviene del interior de la empresa ya sea por las acciones de empleados deshonestos o por errores cometidos en la realización de tareas. Entonces, se torna importante la preocupación de la empresa por protegerse de sí misma. Pero en las organizaciones es muy frecuente la creencia de que no les va a ocurrir ningún percance, por este motivo es fundamental la toma de consciencia de la existencia de potenciales riesgos y la adopción de medidas de seguridad y control. También se debe tener en cuenta que las medidas que se adopten deben adaptarse y actualizarse permanentemente al dinamismo tecnológico para que sean efectivas (Saroka, R. H., 2002).

1.2. AMENAZAS INFORMÁTICAS

De acuerdo a lo dicho por Saroka, R. H. (2002), Voutssas M., J. (2010) y García, P. G. y Vidal, L. M. J. (2016), las amenazas son el conjunto de peligros a los que están expuestos los recursos informáticos de una organización, es decir, son la fuente de incidentes no deseados que pueden dañar dichos recursos y consecuentemente a la propia empresa. Inciden negativamente en los puntos débiles del sistema, lo que implica una potencial violación de la seguridad. En general, son descriptas de acuerdo a su origen y a sus posibles consecuencias.

Continuando con lo explicado por dichos autores, las amenazas pueden ser accidentales o intencionales. Las accidentales pueden deberse a factores naturales, laborales o sociales, incluyendo los desastres naturales o las condiciones medioambientales adversas. En este caso no hay intención de perjudicar a la empresa, pero en caso de existir adecuadas medidas preventivas que podrían haberlas evitado se debe analizar si no hay negligencia o culpa. Por su parte, las amenazas intencionales provienen de personas que pretenden acceder y/o dañar el sistema de manera deliberada. Cuando se materializan este tipo de amenazas se trata de un ataque, que puede ser interno (cuando los usuarios legítimos del sistema actúan de manera no autorizada) o externo (que se producen con frecuencia cuando se permite el acceso remoto destinado a usuarios autorizados).

Según Saroka, R. H. (2002), los peligros se pueden clasificar en cuatro categorías básicas:

- **Ambientales naturales:** incendios, inundaciones, terremotos, cortocircuitos, explosiones, etc.
- **Ambientales operativas:** caída o falla del procesador, periféricos, softwares, comunicaciones, sistema eléctrico, etc.
- **Humanas no intencionales:** falta de documentación actualizada, daño accidental de archivos, errores y omisiones en el ingreso de datos, en el desarrollo de un sistema, en la operación, en el uso de archivos y programas, etc.
- **Humanas intencionales:** fraude, robo, uso indebido de recursos, operación y programación maliciosa, vandalismo, terrorismo, sabotaje, infiltración en líneas, invasión a la privacidad, etc.

Los peligros que más frecuentemente se presentan en las empresas son la existencia de virus, incendios e inundaciones, cortes de electricidad, cortes de gas, agua y demás servicios públicos, fallas mecánicas, sabotaje, empleados descontentos y uso indebido de los recursos.

En cuanto a las amenazas a las que se enfrenta la empresa vitivinícola, se incluyen los terremotos, incendios, cortocircuitos e inundaciones. Si ocurriera alguno de estos eventos y los servidores tuvieran algún problema se tienen copias de seguridad pero no se tiene dónde levantarlas, es decir, no se cuenta con un sitio de respaldo. Con respecto a las roturas de equipos, es posible que se produzcan, sin embargo, los equipos principales prácticamente tienen todo redundante lo que quiere decir que si se rompe una fuente de energía hay una segunda fuente que permite que el equipo funcione mientras se reemplaza la fuente dañada. Y así también si se rompe un disco o cualquier otro componente de ese servidor donde están los datos importantes. A nivel de equipos de puestos de trabajo, se poseen algunos equipos de contingencia por si los que utiliza algún director o gerente se rompen. De esa manera, se les puede entregar rápidamente otro equipo mientras se repara el que sufrió la rotura.

Las amenazas humanas no intencionales también están presentes en la empresa bajo estudio porque el personal puede cometer errores al introducir datos en el sistema o, como se vio anteriormente, puede conectar sus dispositivos a las redes empresariales e infectarlas con algún virus. Además, puede suceder que una persona borre archivos accidentalmente y, por más que se realicen copias de seguridad todas las noches, si la persona borró los datos a la tarde, por ejemplo, para lograr recuperarlos hay que volverse al día anterior lo que implica pérdida de tiempo de trabajo.

Las amenazas humanas intencionales como las anteriores son muy importantes. En la empresa vitivinícola, con los niveles de acceso que tiene cada persona se podría robar información ya que no se cuenta con un sistema de protección en ese aspecto. Por ejemplo, para evitar el robo de información es posible establecer que cierta información como documentos, números de tarjetas de crédito o algunos patrones que sean determinados en alguna herramienta de protección de datos no salgan por correo

electrónico, no se puedan enviar en un chat y demás. La empresa no tiene implementada esta herramienta actualmente. De todas formas, hoy en día resulta muy difícil evitar el robo de información ya que, por ejemplo, con los celulares cualquier persona podría sacarle una foto a la pantalla de la computadora donde figura información importante. Por este motivo, es fundamental contar con personal de confianza que sea íntegro y cuente con valores éticos y hacer que firme un convenio de confidencialidad al momento de ingresar a la empresa.

Por su parte, Ramió Aguirre, J. (2006) explica que las amenazas del sistema afectan principalmente a los recursos informáticos, es decir, al hardware, al software y a los datos. Estas amenazas pueden ser por:

- **Interrupción:** cuando se daña, pierde o inutiliza algún punto del sistema. Afecta la accesibilidad o disponibilidad de la información. Por ejemplo: borrado de programas o datos.
- **Interceptación:** cuando una persona no autorizada consigue acceder a la información, lo que afecta la confidencialidad de la misma. Es difícil de detectar ya que suele no dejar huellas. Por ejemplo: copia de datos sin autorización.
- **Modificación:** cuando una persona no autorizada consigue acceder al sistema y realiza modificaciones para su beneficio. Afecta la integridad. Por ejemplo: cambio de contenidos en una base de datos.
- **Generación:** cuando se crean nuevos objetos en el sistema sin autorización y se falsifican datos e información. Afecta la autenticidad y su detección es difícil. Por ejemplo: generación de registros en una base de datos.

En el presente año, la empresa estudiada no ha sufrido ninguno de estos problemas.

1.3.RIESGOS INFORMÁTICOS

El riesgo es la probabilidad de que un evento nocivo ocurra combinado con su impacto en la organización. Cuantifica la probabilidad de que se produzca una amenaza y cause daño a los recursos informáticos, por lo que se expresa en valores numéricos. El riesgo se materializa cuando una amenaza actúa sobre una vulnerabilidad y genera un impacto (Voutssas M., J., 2010 y García, P. G. y Vidal, L. M. J., 2016).

Según Saroka, R. H. (2002), el impacto o consecuencia es el daño o pérdida provocada por el riesgo que puede afectar cualquiera de los recursos informáticos. Es importante estimar las pérdidas económicas que genera a la hora de evaluar la seguridad. Algunas de estas consecuencias son:

imposibilidad de procesar, pérdidas de archivos y registros, modificación de los registros, lecturas indebidas de información y su divulgación y el uso indebido de los recursos.

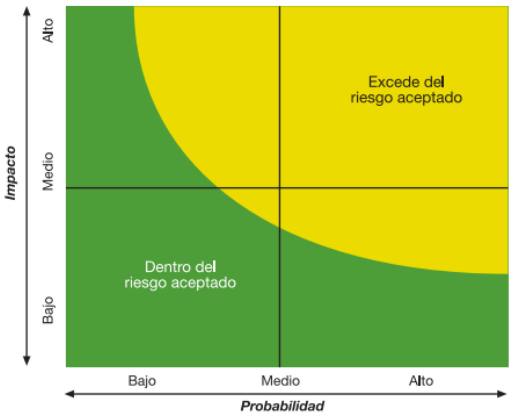
La empresa vitivinícola ha estado expuesta a riesgos, pero los mismos no llegaron a afectarla ni a significar pérdidas económicas ni de ningún otro tipo. Estos riesgos se han manifestado en equipos infectados con virus y correos electrónicos que han tratado de entrar con algún malware que fueron bloqueados oportunamente por el antivirus, por lo que no se convirtieron en un problema para la empresa.

De acuerdo con el Informe COSO II (2004), es fundamental la evaluación de riesgos ya que permite a las organizaciones considerar cuál es el impacto que los potenciales eventos tienen sobre la consecución de los objetivos. Para ello se debe evaluar la probabilidad e impacto de los acontecimientos, donde se pueden utilizar métodos cualitativos, cuantitativos o la combinación de ambos. Además, los riesgos se evalúan con un doble enfoque:

- **Riesgo inherente:** es al que se enfrenta una empresa en ausencia de acciones para modificar su probabilidad e impacto.
- **Riesgo residual:** es el que permanece después de desarrolladas las respuestas a los riesgos.

Una vez realizada la evaluación se debe determinar cómo se va a responder ante los riesgos. Las respuestas pueden ser evitar, reducir, compartir o aceptar el riesgo, considerando el efecto que van a generar en su probabilidad e impacto así como los costos y beneficios que traerán aparejados. La respuesta a seleccionar debe ser aquella que sitúe al riesgo dentro de las tolerancias establecidas por la empresa.

Gráfico 1: Formación del riesgo aceptado



Fuente: Committee of Sponsoring Organizations of the Treadway Commission (COSO II), (2004).

Laudon, K. C. y Laudon, J. P. (2012) explican que la evaluación del riesgo permite saber cuáles son los activos que requieren protección y su grado de vulnerabilidad y, de esta manera, se puede determinar el conjunto más eficiente de controles para brindar protección. Por lo tanto, es importante que la Dirección y los especialistas en sistemas trabajen juntos para conocer el valor de sus activos de información, los puntos más vulnerables y la probabilidad de ocurrencia e impacto que pueden generar los problemas. De esta forma, se adquiere una mejor comprensión de los riesgos a los que se enfrenta la empresa y se concentran los controles en los aspectos más vulnerables y con mayor potencial de daño y pérdida.

En palabras de García, P. G. y Vidal, L. M. J. (2016), una vez que los riesgos fueron evaluados, se los debe gestionar a fin de eliminarlos o reducirlos. Esto se hace a través de la identificación, selección, aprobación y manejo de los controles que permitan reducir la probabilidad de ocurrencia de las amenazas, limitar el impacto de las mismas en caso de que ocurran, reducir o eliminar vulnerabilidades existentes y permitir la recuperación de la empresa ante el impacto. Es decir, se debe determinar cómo se van a tratar los riesgos estableciendo estrategias que permitan tomar decisiones acertadas y efectivas.

Específicamente, para evaluar los riesgos en la empresa estudiada se tiene un informe que fue realizado en base a las normas ISO 27001 donde figuran las distintas áreas con sus riesgos y, además, se cuenta con una matriz de riesgo del área de Tecnología Informática.

Dentro del proyecto de organización del área en el que se trabaja, se acordó con una consultora que la misma se iba a encargar de presentar una propuesta para comenzar a documentar diversos aspectos empresariales. Entre estos aspectos, se encuentra la documentación de todo lo relacionado con la matriz de riesgo y ya se tienen definidos los riesgos más importantes. La consultora ya realizó el relevamiento necesario y ya comenzó a trabajar en la documentación, por lo que se cuenta con una matriz de riesgos que, en realidad, es mejorable.

El Departamento de Tecnología Informática da soporte a todas las necesidades respecto a la seguridad pero, al no haber en la empresa una persona que específicamente se encargue de la misma, este Departamento debe trabajar con consultoras, como se vio anteriormente. El problema radica en que muchas veces las consultoras no llegan a entender lo que realmente necesita la empresa y, en muchos casos, no están preparadas para brindar soluciones. Concretamente, en la empresa vitivinícola sucedió que personal del Departamento de Tecnología Informática se reunió dos veces con ejecutivos de alto nivel de una consultora donde definieron todas las cosas que se debían realizar. Sin embargo, luego volvieron a preguntar lo mismo, por lo que se tuvo que volver a definir lo que se iba a hacer y, finalmente, no brindaron la solución que la empresa necesitaba y quería. Entonces, hay que explicar muchas veces lo que

se requiere y es un asunto muy complejo debido a que no hay una solución que se aplique a todas las empresas por igual sino que hay que ver cada caso concreto para proporcionar una solución satisfactoria.

En la empresa se hizo hacer un informe para tener conocimiento de cuáles son las debilidades a fin de tenerlas en cuenta y estar atentos a las mismas. Se está trabajando en estas debilidades por medio de los distintos proyectos que se están llevando a cabo ya que la empresa se encuentra en un proceso de mejora en cuanto a la seguridad informática.

2. DELITOS INFORMÁTICOS

El delito informático es una actividad ilícita realizada a través de medios informáticos. El mismo es muy atractivo para los delincuentes debido a que representa un negocio en el que el objeto que se busca es pequeño ya que la información se encuentra almacenada en pequeños contenedores. Por otra parte, en la mayoría de los casos el contacto físico es inexistente lo que garantiza al delincuente su integridad física y anonimato. Y además, los datos y la información tienen un valor muy alto. Por este motivo, se deben utilizar herramientas de protección contra este tipo de delitos a fin de evitarlos (Ramió Aguirre, J., 2006).

A continuación se procederá a explicar los principales delitos y amenazas informáticas que pueden afectar a los sistemas a fin de tener un mejor conocimiento y comprensión de los mismos, de acuerdo a lo expuesto por Laudon, K. C. y Laudon, J. P. (2012), Saroka, R. H. (2002), Voutssas M., J. (2010) y Basaes, J.; Godoy, V. A.; Reitano, J. A.; Rojas Gaete, D. B.; Rossel Ortega, V. M. L. y Rossel Ortega, M. L. (2014).

2.1.SOFTWARE MALICIOSO

Los programas de software malicioso o malware se infiltran en los sistemas sin consentimiento de los propietarios para causar daño y alterar su funcionamiento y, por lo tanto, el de la empresa. Incluyen virus, gusanos y caballos de Troya.

2.1.1. Virus y Gusanos

Un virus es un software malintencionado que necesita unirse a otros programas o archivos para ejecutarse, de lo contrario no puede funcionar. Los mismos pueden destruir intencionalmente los datos almacenados en una computadora o pueden ser más inofensivos y sólo generar molestias. El virus necesita de la intervención del usuario para poder propagarse.

Los gusanos son programas independientes que se copian a sí mismos de una computadora a otras a través de una red. Se esparcen con mayor velocidad que los virus ya que no necesitan unirse a otros

programas y archivos y no dependen tanto de la acción humana, es decir, se propagan automáticamente. Lo que hacen es destruir datos y programas y pueden interrumpir o detener la operación de las redes de computadoras.

Tanto los virus como los gusanos pueden ingresar a una computadora a través de Internet, de archivos o software descargados, de archivos adjuntos en los correos electrónicos, y de mensajes de correo electrónico o mensajería instantánea, generalmente sin el conocimiento del usuario. Cuando los malware se dirigen a los dispositivos móviles se esparcen, además de por los medios mencionados anteriormente, a través de Bluetooth, mensajes de texto y por medio de redes Wi-Fi o celulares. Es importante considerar esto ya que los malware que afectan los dispositivos móviles representan una gran amenaza a los sistemas informáticos empresariales debido a su vinculación.

2.1.2. Caballo de Troya

Un caballo de Troya es un programa que parece ser benigno pero finalmente realiza algo distinto a lo que se esperaba. No es un virus en sí porque no se reproduce pero representa un medio para que los virus u otro software malicioso ingresen en el sistema informático.

2.1.3. Ataques de inyección SQL

Los ataques de inyección de SQL introducen un código de programa malicioso en los sistemas y redes corporativas a través de las vulnerabilidades en el software de aplicación Web mal codificado, que se dan cuando dicha aplicación no valida o filtra apropiadamente los datos introducidos por los usuarios en una página Web. Entonces el atacante aprovecha ese error para introducir una consulta SQL falsa y así acceder a la base de datos o a otros sistemas en la red.

2.1.4. Spyware

También actúan como software malicioso algunos tipos de spyware que son pequeños programas que se instalan a sí mismos en las computadoras sin que los usuarios se percaten para monitorear y recopilar información sobre sus actividades, distribuirla a interesados, mostrar anuncios o realizar modificaciones molestas en el equipo para que funcione con lentitud o se bloquee. Los keyloggers son un tipo de spyware que puede registrar las pulsaciones en las teclas de las computadoras para robar números de serie de software, obtener acceso a cuentas de correo electrónico, conseguir contraseñas de sistemas informáticos, realizar ataques a través de internet u obtener información personal.

2.2.TIPOS DE DELITOS INFORMÁTICOS

Según Saroka, R. H. (2002), el perfil del delincuente informático suele presentar ciertas características que surgen de estudios realizados sobre este tipo de delitos. En general, se trata de una persona joven que se encuentra entre los empleados más brillantes y ocupa puestos de confianza, por lo que está familiarizado con los sistemas. A menudo cuenta con la ayuda de alguien más, ya sea un empleado cómplice o alguien externo a la empresa. Aprovecha las variaciones o abandono de las normas para hacer posible sus delitos y le atrae el desafío intelectual que implica violar un sistema informático. Además, muchas veces presenta el "síndrome de Robin Hood" donde es consciente de que es incorrecto perjudicar a un individuo pero no lo toma así cuando la víctima se trata de una organización.

En general, estos delitos son cometidos por hackers o crackers. Los hackers son personas que buscan acceder a los sistemas computacionales sin autorización y obtener el dominio de los mismos. Por su parte, se denomina cracker al hacker que tiene intenciones criminales de violar las medidas de seguridad de los sistemas para irrumpir en ellos. Ambos se aprovechan de las deficiencias encontradas en la seguridad informática para conseguir el acceso y entre las actividades que llevan a cabo luego se encuentran el robo de información, el daño al sistema y el cibervandalismo.

Con la Ley N° 26388 (2008) se modificó el Código Penal de Argentina, incorporando el delito informático. Los distintos tipos de delitos informáticos que están contemplados en esta ley son los siguientes:

- **Artículo 2:** Producción, financiación, comercialización, publicación, distribución, etc. de pornografía infantil por cualquier medio.
- **Artículo 4:** Acceso indebido a una comunicación; apoderación indebida de una comunicación; suprimir o desviar de su destino una comunicación que no le esté dirigida. Intercepción o captación indebida de comunicaciones provenientes de sistemas privados o de acceso restringido. Divulgación o publicación del contenido de la comunicación.
- **Artículo 5:** Acceso sin la debida autorización a excediendo la que se posee a un sistema o dato informático de acceso restringido. Acceso en perjuicio de un sistema o dato informático de un organismo público estatal o proveedor de servicios públicos o financieros.
- **Artículo 6:** Publicación indebida de una comunicación no destinada a publicidad, si el hecho causara o pudiera causar perjuicio a terceros.
- **Artículo 8:** Acceso a banco de datos personales a sabiendas e ilegítimamente o violando sistemas de confidencialidad y seguridad de datos. Proporcionar o revelar a otro información registrada en

un archivo o banco de datos personales cuyo secreto esté obligado a preservar por disposición de la ley. Insertar o hacer insertar datos en un archivo de datos personales.

- **Artículo 9:** Defraudar a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.
- **Artículo 10:** Alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos; o vender, distribuir, hacer circular o introducir en un sistema informático cualquier programa destinado a causar daños.
- **Artículo 12:** Interrumpir o entorpecer una comunicación o resistir violentamente el restablecimiento de la comunicación interrumpida.
- **Artículo 13:** Sustraer, alterar, ocultar, destruir o inutilizar objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público.

Estos delitos informáticos son penados con pena privativa de libertad, multas e inhabilitaciones de acuerdo con el ilícito cometido. Como ejemplos de los mismos se pueden mencionar el robo de identidad (spoofing y sniffing), los ataques de negación de servicio, el spamming, el fraude del clic, la bomba lógica o cronológica, el daño informático y distribución de malwares, entre otros.

En el presente año, la empresa vitivinícola no sufrió ningún tipo de delito informático que pudiera afectarla.

Además, existen otras leyes relacionadas con los delitos informáticos. La Ley N° 24766 (1996) de Confidencialidad busca proteger la información secreta que tiene valor comercial por poseer dicha característica y que está en poder de una persona legitimada para controlarla y para aplicar las medidas necesarias para mantenerla en secreto. Lo que se pretende es evitar que la información sea divulgada, adquirida o utilizada sin consentimiento de manera contraria a los usos comerciales honestos por terceras personas. Por su parte, la Ley N° 25326 (2000) de Protección de los Datos Personales tiene por objeto brindar protección integral a los datos personales para garantizar el honor, la intimidad y el acceso a la información. Entre otros aspectos, contempla los derechos de los titulares de los datos, el control y las sanciones aplicables y las acciones de protección de los datos personales.

Otras leyes que también son aplicables son la Ley N° 11723 de la Propiedad Intelectual, la Ley N° 24481 de Patentes de Invención y Modelos de Utilidad y la Ley N° 22362 de Marcas y Designaciones.

2.3.AMENAZAS INTERNAS

Según Laudon, K. C. y Laudon, J. P. (2012) y Saroka, R. H. (2002), muchas de las debilidades de los sistemas provienen del factor humano más que de aspectos técnicos. Además, si bien gran parte de las amenazas vienen del exterior de la empresa, la mayoría surgen desde el interior de la misma donde los empleados pueden representar un problema en la seguridad. Los trabajadores tienen un acceso privilegiado a la información y a los sistemas, pudiendo robar, modificar o borrar los datos sin dejar rastros cuando la seguridad no es la adecuada.

La falta de conocimiento y capacitación de los usuarios provocan grandes fallas en la seguridad. Son muy frecuentes los errores que se producen cuando se introducen datos incorrectos en los sistemas o cuando se utilizan programas o procedimientos inadecuados y no se siguen las instrucciones correctas en la utilización de los equipos. También se generan fugas de la información cuando los usuarios no cuidan sus contraseñas y se las dan a conocer a cualquier persona, lo que compromete gravemente al sistema.

En el caso de la empresa vitivinícola, no existe una política definida acerca de lo que se debe hacer cuando un empleado utiliza indebidamente la información empresarial, por lo que se debe trabajar y mejorar ese aspecto. De todas formas, con el cambio de firewall que se ha incorporado se obtiene información del registro de navegación, lo que permite conocer y monitorizar la actividad de los usuarios. Por su parte, cuando se trabaja en los sistemas como JD Edwards, algunos módulos tienen habilitada la auditoría lo que permite tener registros de lo que se hace en el mismo. Esta función no está habilitada en todos los sistemas pero si en los más importantes. Muchas veces no se implementa porque el tema de auditoria en los sistemas y en las bases de datos es una carga más, entonces se necesita contar con un mayor almacenamiento, se debe tener equipamiento y demás. Al habilitar la auditoria en todo provoca que el sistema se arrastre en cuanto a performance y eso genera más transacciones en base de datos, más operaciones, afecta el tiempo de procesador y genera una ralentización, entre otros aspectos. También es importante tener cuidado y saber detectar al personal que es potencialmente riesgoso mediante la restricción de accesos, la monitorización de las actividades y datos a los que acceden, el impedimento de realizar instalaciones o la desvinculación en casos más graves.

Por su parte, otras amenazas pueden provenir de los especialistas en sistemas cuando cometen errores en el diseño y desarrollo de software o en el mantenimiento de los programas, entre otras actividades.

Muchas veces sucede que la dirección de la empresa comete la equivocación de pensar que la informática le corresponde sólo a los especialistas y, por lo tanto, no se involucra como correspondería y

no se generan planes estratégicos de sistemas. En general, en la empresa analizada la Dirección se encuentra comprometida con la seguridad informática y trabaja en conjunto con el Departamento de Tecnología Informática. Este Departamento va presentando los distintos proyectos a la Dirección junto con el análisis de riesgo y la cantidad de dinero necesario, y la misma lo evalúa a fin de decidir si se lleva a cabo y hay presupuesto para realizarlo o si no es posible su desarrollo. Entonces, para que la Dirección pueda tomar una decisión, se le pide al Departamento de Tecnología Informática que justifique el proyecto que desea llevar a cabo, contar con dos o tres presupuestos y dar a conocer cuál es el riesgo que asume la organización si no se incorpora el proyecto.

Todas estas cuestiones anteriormente expuestas provenientes tanto de los usuarios finales así como de los especialistas en sistemas, de la dirección y de todos los trabajadores representan importantes amenazas internas que deben ser consideradas a fin de proveer la seguridad necesaria que las prevenga.

2.4.REPORTE DEL OBSERVATORIO DE DELITOS INFORMÁTICOS DE LATINOAMERICA 2017

El Observatorio de Delitos Informáticos de Latinoamérica (ODILA) nace para dar a conocer el problema de la cifra negra de los delitos informáticos. Sus objetivos son combatir dicho problema de la cifra negra en los países de América Latina y generar, sistematizar y difundir información relevante para estudiar, investigar e incidir en la problemática de los delitos informáticos en estos países.

En el último informe realizado por ODILA (2017) se pueden observar una serie de datos y estadísticas interesantes. En primer lugar, se pueden ver las distintas víctimas que utilizan los servicios del Observatorio, donde las personas humanas representan casi el 90% de los reportes que se reciben ya que buscan contar con información adecuada para realizar las denuncias correspondientes. Por su parte, las Pequeñas y Medianas Empresas muchas veces no tienen conocimientos acerca de la manera de actuar ante un incidente y sufren la falta de recursos. En tercer y cuarto lugar se encuentran las grandes empresas y los organismos públicos, quienes tienen mayor facilidad y posibilidades de acceder a asesoramiento profesional para solucionar los hechos delictivos que se presenten. En muchos casos sucede que se decide no hacer públicos los delitos informáticos sufridos para evitar una exposición negativa de la empresa y/o marca ante la opinión pública.

Gráfico 2: Tipos de Víctimas

Víctima	Persona Física	PyME	Empresa + 100 empleados	Organismo Gubernamental	No respondió
Porcentaje	89,8 %	8,16 %	1,02 %	1,02 %	0 %

Fuente: Observatorio de Delitos Informáticos de Latinoamérica (ODILA), (2017).

Por otra parte, se puede observar que la mayor parte de los usuarios no realizan la denuncia de los delitos informáticos sufridos lo que da lugar a una cifra negra superior al 80%. Esto significa que ocho de cada diez delitos no tienen consecuencia penal. También hay denuncias formalmente realizadas que están en curso y otras donde la investigación no logró avanzar. Las denuncias realizadas cuya investigación finalizó y se logró una condena efectiva sobre el imputado sólo representan el 1%, por lo que cada cien delitos informáticos sólo uno llegaría a obtener una condena efectiva. Sin embargo, para la interpretación de las cifras es importante aclarar que muchos de los usuarios que responden las encuestas del Observatorio están en la búsqueda de información para saber si son víctimas de algún delito por lo que lo más probable es que aún no hayan realizado la denuncia. En cambio, quienes ya han realizado la denuncia generalmente se encuentran menos interesados en buscar y aportar datos a ODILA.

Gráfico 3: Denuncia

¿Ha Denunciado?	No, no denuncié porque... (ver siguiente pregunta)	Si, ya denuncie y la investigación está en curso	Si, denuncie pero la investigación no avanzó	Si, denuncié y ya se ha condenado al o los culpables.
Porcentaje	83,67 %	6,12 %	9,18 %	1,02 %

Fuente: Observatorio de Delitos Informáticos de Latinoamérica (ODILA), (2017).

Es importante analizar cuál es el motivo que lleva a un ente a no realizar la denuncia de los delitos informáticos. En la mayoría de los casos se debe a que se cree que la denuncia no va a ser útil ya que no va a solucionar o a cambiar el conflicto social base y se considera que el sistema penal no es apto para combatir este tipo de delitos. En otros casos y como se ha mencionado anteriormente, la denuncia no se realiza debido a que las víctimas no quieren exponer públicamente el hecho ocurrido ya que piensan que la difusión podría generar aún más daño que el ya sufrido y prefieren la confidencialidad. Otro motivo es la falta de información, por lo que muchas veces no se conoce dónde realizar la denuncia formal. También desisten debido a que existe una falta de confianza en la justicia y se cree que la investigación no tendrá éxito o se tiene temor a futuras represalias por parte del autor del delito. Como no se cuenta con información suficiente, sucede que se presentan dudas con respecto a si el hecho se trata o no de un delito y por ese motivo algunas personas no realizan la denuncia.

Gráfico 4: Causas de la No Denuncia

Fuente: Observatorio de Delitos Informáticos de Latinoamérica (ODILA), (2017).

Entre los delitos que más han sido denunciados predominan las amenazas realizadas por medios electrónicos (17,35%). Luego se encuentran las calumnias e injurias a través de estos medios debido a la utilización masiva de redes sociales, la sensación de impunidad y el crecimiento de la libertad de expresión. Por su parte, los fraudes y estafas informáticas son la forma más sencilla que tienen los delincuentes de obtener un beneficio económico por lo que siempre se encuentran entre los cinco delitos más reportados, representando en el 2017 el 12,25%. En los años anteriores el acceso indebido a datos o sistemas (hacking) había sido el delito informático más denunciado, quedando en el 2017 en el séptimo puesto. Ahora bien, entre los delitos menos denunciados se encuentran la denegación de servicio y la difusión de malware y esto puede deberse a que se relacionan con la seguridad de la información

empresarial, por lo que se prefiere no denunciar a fin de que no haya difusión pública y consecuentemente mayores daños.

Gráfico 5: Delitos más denunciados

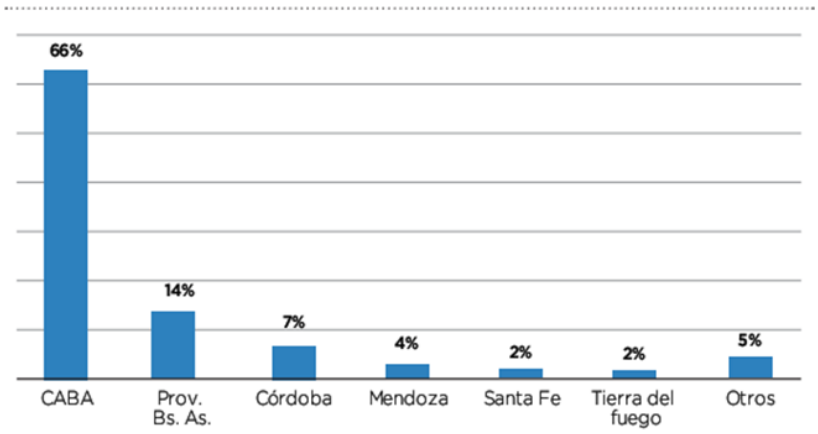
Fuente: Observatorio de Delitos Informáticos de Latinoamérica (ODILA), (2017).

2.5.ESTUDIOS ESTADÍSTICOS SOBRE CIBERCRIMEN: QUINTO MUESTREO DE DENUNCIAS JUDICIALES DE LA REPÚBLICA ARGENTINA, AÑO 2017

Los estudios estadísticos sobre cibercrimen realizados en el país, a través del Quinto muestreo de denuncias judiciales de la República Argentina (2017), tienen por objeto obtener una aproximación de los hechos ilícitos relacionados con la Ley N° 26388 de delitos informáticos y la Ley N° 26904 sobre grooming que llegan a la justicia en los fueros federales y en los penales y contravencionales en los distritos más importantes en cuanto a población del país. Lo que pretende es demostrar qué delitos informáticos son denunciados en los tribunales de los distintos distritos incluidos, pero no representa una muestra del cibercrimen en el país.

Teniendo en cuenta la Ley N° 26388, los delitos investigados en función de las denuncias que se realizaron en la provincia de Mendoza fueron ocho sobre un total de doscientos cinco delitos investigados, lo que representa el 4% de los mismos. Esto coloca a Mendoza en el cuarto distrito con mayor cantidad de denuncias, siendo la Ciudad Autónoma de Buenos Aires la que concentra este tipo de delitos.

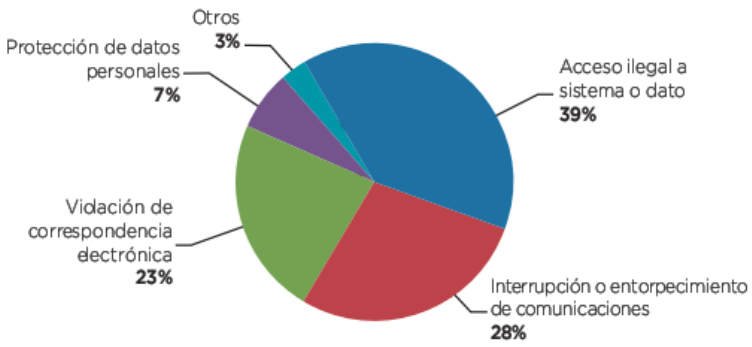
Gráfico 6: Denuncias Ley 26388 por distrito



Fuente: Quinto muestreo de denuncias judiciales de la República Argentina, (2017).

Al analizar las denuncias por figura penal, se puede observar que de doscientas cinco denuncias, las denuncias por acceso ilegal a un sistema o dato fueron ochenta, por lo que representan el 39% del total y se trata del hecho ilícito más denunciado. Luego, sigue la interrupción o entorpecimiento de comunicaciones que representa el 28% con cincuenta y ocho denuncias. Las denuncias por violación de correspondencia electrónica fueron cuarenta y siete lo que significa el 23% del total. Por su parte, la protección de datos personales tuvo catorce denuncias representando el 7%, en tanto que otros delitos como publicación indebida de comunicaciones, daño a bienes intangibles y distribución de virus y alteración de evidencia informática representan sólo el 3% del total.

Gráfico 7: Denuncias Ley 26388 por figura penal



Fuente: Quinto muestreo de denuncias judiciales de la República Argentina, (2017).

3. NIVEL DE RIESGO INFORMÁTICO EN LA EMPRESA VITIVINÍCOLA

Al analizar distintos factores de riesgo informático en la empresa vitivinícola, se pudo determinar y corroborar que el nivel de riesgo existente en general es medio. Es decir, el sistema informático empresarial es medianamente seguro, por lo que requiere reforzar algunas medidas de seguridad y aplicar mayores controles a fin de mejorar la protección de los recursos informáticos.

Tabla 1: Nivel de riesgo en la empresa vitivinícola

Factores de riesgo informático	Nivel
Ubicación inadecuada de sistemas y equipos	Medio
Infraestructura inapropiada incapaz de resistir desastres naturales	Medio
Falta de protección contra incendios, inundaciones, cortocircuitos y terremotos	Alto
Roturas de computadoras y equipos	Medio
Inadecuada seguridad física	Medio
Falta de concientización y capacitación al personal	Alto
Falta de existencia y seguimiento de políticas y procedimientos de seguridad	Medio
Falta de existencia de planes de seguridad y contingencia	Medio
Falta de segregación de funciones y definición clara de responsabilidades	Medio
Falta de control por oposición	Alto
Falta de independencia del Departamento de Tecnología Informática	Alto
Falta de existencia de un área específica dedicada a la seguridad informática	Alto
Errores u omisiones de los usuarios en el ingreso de datos	Medio
Inadecuado archivo y almacenamiento de datos para control	Medio
Fraude informático	Medio
Robo de información	Medio
Robo de activos informáticos	Medio
Manipulación de datos	Medio
Uso indebido de recursos informáticos	Medio
Delitos informáticos	Medio
Falta de realización de auditorías informáticas periódicas	Alto
Falta de control interno informático	Medio
Errores de diseño y programación de sistemas	Medio
Cambios frecuentes en la infraestructura de tecnología informática	Bajo
Falta de flexibilidad de los sistemas	Bajo
Caída o falla del procesador, software, sistema eléctrico, etc.	Medio
Obsolescencia tecnológica	Medio
Falta de actualización de los programas	Medio
Inadecuada seguridad lógica	Medio
Falta de aplicación de antivirus, firewalls, etc.	Bajo
Falta de realización de copias de seguridad periódicamente	Bajo
Falta de existencia de centros de procesamiento alternativos	Alto
Inadecuadas restricciones de acceso	Medio
Inadecuada administración de la identidad y autenticación de los usuarios	Medio
Inadecuada seguridad en la red e Internet	Medio
Inadecuada seguridad en la nube y en dispositivos móviles	Medio

Fuente: Elaboración propia

Las vulnerabilidades, amenazas y riesgos en la información y en los sistemas son aspectos claves a ser evaluados en las empresas a fin de proteger la continuidad de sus operaciones y la supervivencia en el mercado. Es importante que se realicen evaluaciones periódicas de los riesgos informáticos para poder analizar la situación empresarial y darles una adecuada respuesta con la finalidad de reducir su incidencia a niveles aceptablemente bajos. También es necesario tener conocimiento y capacitación acerca de los delitos informáticos para saber cómo evitarlos y qué hacer en caso de que ocurran.

Actuar de manera preventiva es una buena manera de cubrir las vulnerabilidades y debilidades que presentan los sistemas informáticos y que pueden ser explotadas. Sin embargo, en la empresa vitivinícola bajo estudio se trabaja de manera correctiva en la mayoría de los casos, lo que la expone a muchas amenazas y riesgos. Por este motivo, el nivel de seguridad informática empresarial es medio y requiere de una mejora para elevar su nivel y garantizar una adecuada protección de todos los recursos informáticos.

Debido a que en la empresa no se cuenta con todos los recursos y conocimientos necesarios, el Departamento de Tecnología Informática trabaja en conjunto con consultoras para el logro de esa mejora en el corto y mediano plazo. Las consultoras realizan relevamientos y se encuentran documentando las debilidades y evaluando los riesgos a fin de brindar soluciones. A partir del trabajo en conjunto de este Departamento con las consultoras y con el compromiso de la Dirección, la empresa vitivinícola se encuentra en un proceso de mejora de la seguridad informática a fin de elevar su nivel y reducir los riesgos a niveles aceptables.

CAPÍTULO III

MEDIDAS DE SEGURIDAD Y CONTROLES APLICABLES

En este capítulo se procederá a explicar y exponer las medidas de seguridad y controles que se aplican en la empresa vitivinícola a fin de reducir la probabilidad e impacto de los riesgos existentes. A su vez, se presentará una serie de recomendaciones a fin de mejorar el nivel de seguridad informática. Se trabaja con autores tales como Laudon, K. C. y Laudon, J. P., Saroka, H. R. y García Pierrat, G. y Vidal Ledo, M. J., entre otros.

1. MARCO DE TRABAJO PARA LA SEGURIDAD Y EL CONTROL

Como se vio en el capítulo anterior, es fundamental realizar una evaluación y gestión de riesgos para que la empresa conozca la situación en la que se encuentra y pueda determinar qué controles son necesarios con la finalidad de brindar protección a los sistemas de información. Por este motivo, es importante contar con políticas, medidas y planes de seguridad que orienten el accionar de la empresa para tener siempre sistemas confiables, seguros y que operen efectivamente.

Tal como se mencionó en los capítulos anteriores, en la empresa vitivinícola quien se encarga de la seguridad informática y de los controles es el Departamento de Tecnología Informática que trabaja en conjunto con una consultora la cual brinda asesoramiento y ayuda en esos aspectos. Si bien se debería tener una persona definida para encargarse de la seguridad informática, actualmente no se cuenta con la misma. De todas formas, se está llevando a cabo un proceso de fortalecimiento de seguridad informática en el cual se van a tener propuestas formales para mejorar.

La realidad es que la empresa debería contar con un área de seguridad informática separada, es decir, independiente del Departamento de Tecnología Informática. Eso sería lo ideal y es lo que piden los estándares de seguridad aplicables. Sin embargo, como desde la Dirección no se ha decidido tener esta área empresarial, lo asume el Departamento de Tecnología Informática recibiendo ayuda de las consultoras contratadas.

1.1. POLÍTICAS DE SEGURIDAD

Según Laudon, K. C. y Laudon, J. P. (2012) y García Pierrat, G. y Vidal Ledo, M. J. (2016), para garantizar la protección de los activos informáticos de los riesgos identificados es necesario desarrollar una política de seguridad. La misma permite que las tecnologías de la información y comunicaciones sean utilizadas de la manera más eficiente y segura al determinar la forma en la que deben ser empleadas. Las políticas de seguridad establecen las reglas a seguir por el personal que forma parte del sistema informático, determinando el uso aceptable de los recursos informáticos, quién tiene acceso a estos, la administración de la identidad, la política de privacidad de la compañía, la responsabilidad de los usuarios y el uso personal de los equipos y redes corporativas.

Basaes, J. et al. (2014) explican que para diseñar una política de seguridad se requiere, en primer lugar, que el personal técnico conozca las vulnerabilidades y las comunique efectivamente a la gerencia para que pueda comprenderlas y decidir cómo se va a gestionar el riesgo. En segundo lugar, es necesario identificar los activos que necesitan protección a través de la evaluación de las amenazas y riesgos a las que se enfrenta la empresa, implementar las herramientas necesarias para contrarrestarlas y definir una política de uso aceptable, que considera:

- Quién está autorizado a utilizar los recursos.
- Quién está autorizado a conceder acceso y probar los usos.
- Quién administra el sistema.
- Qué tratamiento se le debe dar a la información confidencial.
- Cuáles son los derechos y responsabilidades de los usuarios.

Entonces, el primer paso para proteger la información de la empresa es la elaboración de las políticas de seguridad que brindan educación y capacitación a todo el personal y, a su vez, una explicación detallada de las consecuencias de su violación.

La realidad de la empresa que se estudia es que no se tiene un documento escrito en el que figuren las políticas de seguridad. Es uno de los riesgos a los que se enfrenta la empresa, por lo que se debe trabajar en ello. De todas formas, si se tienen algunos lineamientos que los guían en su labor. Un ejemplo de estos lineamientos es que, cuando se habilitan los accesos a los usuarios, sean personas nuevas que se incorporan o personal que ya se encuentra trabajando en la empresa, siempre se pide la autorización de un gerente o un superior y se cuenta con una ficha de alta para saber qué accesos necesitan, a qué sistemas y qué equipos se les deben entregar. Si se tiene a una persona nueva que va a ingresar en el área de turismo, no tiene ningún sentido que tenga acceso al sistema de gestión empresarial, entonces ciertas cosas se van

viendo desde el sentido común, pero los lineamientos que se siguen no están volcados en un documento como para poder decir que se tiene una política de seguridad y se cumple.

Por este motivo, la empresa vitivinícola se encuentra trabajando con una consultora que se está encargando del armado de todos los documentos y procedimientos. Dentro de eso, se trabaja con el proyecto de definir las políticas de seguridad, en el cual la Dirección se encuentra involucrada.

Las políticas de seguridad son la estrategia general con la que cuenta la empresa, y las medidas y procedimientos son los pasos detallados que se requieren para lograr la seguridad informática. Una buena política de seguridad se debe poder implementar a través de dichas medidas y procedimientos (García Pierrat, G. y Vidal Ledo, M. J., 2016).

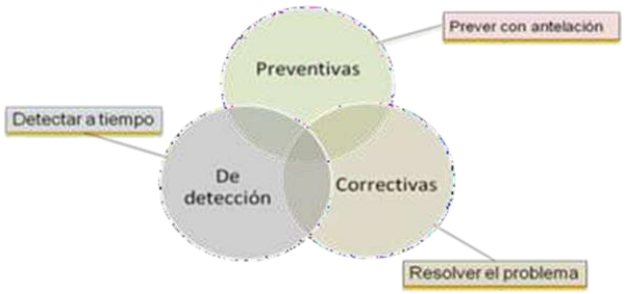
1.2. TIPOS DE MEDIDAS DE SEGURIDAD

A partir de la identificación de los posibles eventos que pueden afectar a la empresa, las medidas y procedimientos de seguridad determinan las acciones que se deben llevar a cabo, los recursos necesarios y las responsabilidades correspondientes. No existe una combinación óptima de controles que sea aplicable a todas las empresas por igual ya que cada una de ellas es un caso particular y, por lo tanto, se debe realizar un análisis del riesgo a fin de identificar los bienes que se encuentran más expuestos en cada caso. Al contrario de las políticas de seguridad generales, las medidas y procedimientos son específicas y se aplican de acuerdo a las necesidades particulares de cada área (García Pierrat, G. y Vidal Ledo, M. J., 2016).

Según Saroka, R. H. (2002), las medidas de seguridad pueden ser de tres tipos:

- **Preventivas:** buscan limitar la posibilidad de que se concreten o materialicen las amenazas a través de acciones que eviten o minimicen su impacto.
- **Detectivas:** buscan limitar los efectos de las amenazas una vez que se han presentado y detectar a tiempo los eventos que puedan producirse.
- **Correctivas:** buscan recuperar la capacidad de operación normal a través de la resolución de los problemas.

Figura 6: Tipos de medidas de seguridad



Fuente: García Pierrat, G. y Vidal Ledo, M. J. (2016).

De acuerdo a lo expuesto por Saroka, R. H. (2002) y Laudon, K. C. y Laudon, J. P. (2012), a continuación se procederá a explicar distintas medidas de seguridad para proteger los recursos informáticos.

1.2.1. Administración de la identidad y la autenticación

La administración de la identidad y la autenticación es fundamental para garantizar que los usuarios que utilizan los recursos informáticos están realmente autorizados para hacerlo. Al implementar un software de administración de identidad se le asigna a cada usuario una identidad digital única que le permite acceder al sistema, por lo que se automatizan los registros de todos los usuarios y sus privilegios. De esta manera, se puede controlar el acceso a los recursos del sistema, se protege la identidad de los usuarios y se puede autenticar a los mismos. La autenticación permite saber que la persona es quien dice ser. Cuando los usuarios están autenticados y cuentan con la debida autorización obtienen el acceso a al sistema.

En cuanto a la posibilidad de acceder al sistema, es posible encontrar dos tipos de controles:

- **Controles de acceso físico:** el acceso físico se da cuando se consigue el control físico directo sobre dispositivos o algún otro elemento del sistema informático. Para evitarlo se deben aplicar controles en el acceso físico y, de esa manera, prevenir los posibles daños, destrucciones o sustracciones de recursos que pueden estar directa o indirectamente implicados en el aseguramiento de la integridad del sistema y de la información. Sin embargo, este control no es suficiente ya que a su vez existen muchos activos no físicos que también requieren protección.

Como ejemplos de este tipo de controles se pueden mencionar la colocación de cámaras de seguridad, uso de tarjetas inteligentes, utilización de candados y alarmas, reconocimiento de la huella digital o de la cara, etc.

- **Controles de acceso lógico:** el acceso lógico se da cuando se realizan operaciones con los datos, programas, archivos y otros recursos del sistema informático. Es necesario otorgar privilegios de acceso a cada usuario de acuerdo a los recursos específicos que se utilizan en las tareas que lleva a cabo. Dichos privilegios de acceso pueden ser otorgados o denegados a los usuarios y/o programas utilizando un software de control de acceso. Los procedimientos de control de privilegios son muy importantes para la seguridad en los sistemas informáticos actuales.

  Como ejemplos de este tipo de controles se pueden mencionar el cifrado de datos, la implementación de firewalls y antivirus, utilización de contraseñas, etc.

1.2.2. Contraseña

Los controles de acceso en su mayoría permiten distinguir entre los usuarios autorizados y los no autorizados para ingresar al sistema. Esta distinción se puede realizar de tres maneras:

- Por algo que la persona tiene. Por ejemplo, credencial de identificación.
- Por algo que la persona es. Por ejemplo, las impresiones digitales.
- Por algo que la persona conoce. Por ejemplo, una contraseña.

Una contraseña es una clave conformada por un conjunto de caracteres que permiten acceder a información restringida. La utilización de contraseñas es la forma más común de autenticar a los usuarios.

A la hora de administrar las contraseñas es importante considerar los siguientes aspectos:

- Deben estar asociadas al tipo de autorización otorgada.
- Deben ser fáciles de memorizar.
- Deben ser cambiadas con frecuencia.
- Nunca deben aparecer representadas en pantalla.
- Debe existir un control automático de repetición de contraseñas.

Sin embargo, las contraseñas presentan importantes debilidades ya que los usuarios tienden a olvidarlas, compartirlas, escribirlas en lugares donde pueden ser vistas o elegir contraseñas inadecuadas que son fáciles de adivinar, todo lo cual compromete la seguridad del sistema. Pero tampoco es bueno utilizar sistemas de contraseñas demasiado rigurosos ya que entorpecen la productividad de los empleados.

En la actualidad existen nuevas tecnologías de autenticación que son más seguras y pueden solucionar estos problemas, como los tokens, las tarjetas inteligentes y la autenticación biométrica. Un token es un dispositivo físico que demuestra la identidad de un solo usuario a través de códigos de contraseñas que cambian con frecuencia, es similar a una tarjeta de identificación. Por su parte, una tarjeta inteligente es un dispositivo que contiene un chip formateado con datos y a través de un dispositivo lector esos datos son interpretados a fin de permitir o negar el acceso. Por último, la autenticación biométrica funciona a través de la medición de un rasgo físico (como huellas digitales, iris de los ojos, rostros o voces) o del comportamiento que hace cada individuo, y se comparan estas características únicas con un perfil almacenado para determinar si existe alguna diferencia entre ellas. El acceso se otorga cuando ambos perfiles coinciden.

1.2.3. Pista de auditoría

La pista de auditoría consiste en un rastro o registro generado por el sistema informático que muestra el historial de las operaciones, por lo que permite su reconstrucción y llegar al documento de origen siguiendo el camino hacia atrás de los procesamientos. Permite saber, a su vez, el modo, el momento y el usuario involucrados en los accesos al sistema.

1.2.4. Backup y recuperación

Cuando se poseen archivos cuyos datos se desean preservar o salvaguardar se realiza una copia de seguridad denominada backup. Esta copia se hace en un medio de almacenamiento distinto al que contiene los datos copiados. El backup también se aplica a los archivos de respaldo y a equipos de computación sustitutos que se utilizan ante fallas de los principales para su reemplazo. Por su parte, la recuperación es un proceso que permite recuperar o restaurar un archivo original que fue alterado, dañado o extraviado. Es decir, es un proceso inverso al backup.

Estas medidas y procedimientos se determinan en función de las necesidades particulares de la empresa. El backup y la recuperación son muy importantes para mantener en funcionamiento las operaciones de la empresa, por lo que es una buena práctica planificar estas medidas de acuerdo al orden de prioridad que se asigna a las actividades que se llevan a cabo. De esta manera se asegura la capacidad de la empresa de continuar desarrollando su negocio.

1.2.5. Criptografía

La criptografía consiste en ocultar lógicamente la información a través de técnicas matemáticas que utilizan algoritmos para transformarla en secuencias de bits ininteligibles para los usuarios no

autorizados. Por lo tanto, la información es encriptada a fin de que no sea alterada y que la comunicación entre personas o entes no se vea interrumpida o modificada. El encriptado permite que sólo los usuarios autorizados puedan acceder a los datos, mensajes, archivos, etc.

Para el cifrado de los datos se utiliza la clave de cifrado que es un código numérico secreto. Para leer el mensaje, el receptor debe descifrarlo. El cifrado se puede realizar utilizando clave simétrica, también conocida como clave secreta, o clave pública. En el cifrado de clave simétrica se utiliza una sola clave que es compartida y sólo debe ser conocida por el emisor y el receptor para mantener la seguridad del sistema. El problema radica en que, al ser necesario compartir de alguna manera la clave secreta entre el emisor y el receptor, esta puede ser interceptada y descifrada por un tercero externo. La forma más segura de cifrado es mediante clave pública. En este caso se emplean dos claves, una pública que es compartida y otra privada que debe mantenerse secreta. Ambas claves están relacionadas, por lo que los datos que han sido cifrados con una clave sólo podrán descifrarse utilizando la otra clave. Entonces, el emisor cifra los datos con la clave pública del receptor y este último los descifra mediante su clave privada.

Al utilizar el cifrado de clave pública, es necesario que la autoridad certificante otorgue un certificado digital para garantizar la autenticidad de las claves y la identidad de los usuarios. Dicho certificado es un documento digital que asegura la vinculación entre una clave pública y una persona o entidad y, de esta manera, se protegen las transacciones.

1.2.6. Medidas de seguridad en la empresa vitivinícola

En la empresa bajo estudio, en cuanto a los controles de acceso físico, los datos se encuentran en una sala de servidores a la que sólo tienen acceso las personas que pertenecen al área de sistemas. No puede acceder cualquier persona y tampoco se encuentra a mano como para que alguien pueda ingresar y llevarse algún recurso con facilidad. Además, hay cámaras de seguridad y se colocan candados y alarmas para evitar cualquier acceso no autorizado. Por su parte, en cuanto a los controles de acceso lógico, se trabaja con perfiles de usuario con distintos niveles de acceso a la información. También se utilizan contraseñas para el acceso de los usuarios a los sistemas, lo que asegura que únicamente realizan transacciones en las áreas que son de su responsabilidad. Es decir, existe seguridad de acceso por usuario con permisos asignados con usuario y contraseña.

La pista de auditoría se tiene en el sistema JD Edwards ya que tiene habilitada la función de auditoría en algunos de sus módulos y eso permite tener el registro de operaciones que fueron realizadas en el mismo. Como ya se vio anteriormente, esta función no se aplica en todos los sistemas debido a la

complejidad que trae aparejada. De todas formas, en las principales operaciones empresariales es posible obtener la pista de auditoría de las transacciones que se realizaron en el sistema.

La empresa vitivinícola posee backup y recuperación entre sus medidas de seguridad. En cuanto a los centros de procesamiento alternativos, se está buscando un proveedor de la nube en la cual se pueda llevar la replicación de los principales sistemas. La réplica sería de los principales sistemas y no de todos por un tema de costos. Además, hay sistemas por los cuales realmente no sirve tener una redundancia de los mismos, como por ejemplo el sistema de reservas del restaurante. Ahora bien, si se trata del sistema de facturación, claramente es importante y de gran utilidad pagar por tener una redundancia ya que la información que genera es clave en la empresa. Entonces, se espera contar con un centro de procesamiento alternativo en el futuro, que será la nube. También puede darse el caso de que sea algo híbrido entre la nube y el data center que se posee actualmente. En la empresa se está evaluando si el centro de procesamiento principal va a ser la nube y el data center va a servir de contingencia o si va a ser algo hibrido.

La encriptación también se aplica en la empresa para proteger la información. Las comunicaciones se realizan a través de Microsoft Office 365 que utiliza protocolos que encriptan la información que viaja entre la computadora y los servidores. El problema es que las computadoras en sí no están encriptadas o sea que, si una computadora es robada, cualquier persona podría tener acceso a la información por el hecho de no estar encriptada, entonces podría acceder al correo y demás información.

Una medida de seguridad que es fundamental es que los usuarios se encuentren capacitados y sean conscientes de la importancia de la seguridad informática. En el caso de la empresa vitivinícola, la capacitación del personal es parcial. Al no existir un área de seguridad informática hay muchas cosas que no se conocen porque es un tema muy amplio. Por su parte, la consciencia en cuanto a la importancia de la seguridad informática también es parcial. En la empresa hay áreas, como las administrativas, que trabajan permanentemente con los sistemas y conocen los riesgos y lo que puede suceder. Pero también hay personas de otras áreas que no tienen conocimientos al respecto, como el caso de un operario que tiene una computadora y la utiliza para imprimir una etiqueta. Este tipo de personas, al no estar capacitadas, no le dan la debida importancia a la seguridad informática. Entonces, al no trabajar con todas las personas en cuanto a este tema es muy difícil que haya consciencia. De hecho, lo ideal sería que desde las áreas informáticas se trabajara en eso con el personal. Además, el empleado se puede llevar la computadora a su casa o incluso en su celular descargar una aplicación que podría ser maliciosa y obtendría acceso a la información. Por este motivo, se trata de un tema que es muy complicado y en el que hay que tener

cuidado con todo, es por ello que las personas deben contar aunque sea con los conocimientos mínimos acerca de la seguridad informática.

1.3. SEGURIDAD EN REDES E INTERNET

Actualmente, todas las empresas utilizan redes e internet para desarrollar sus operaciones, motivo por el cual se deben tener en cuenta a la hora de establecer medidas de seguridad. Continuando con lo dicho por Saroka, R. H. (2002) y Laudon, K. C. y Laudon, J. P. (2012), se explicarán algunas medidas de seguridad aplicables en este aspecto.

1.3.1. Firewalls

Un firewall es una combinación de hardware y software que controla la entrada y protege las redes de la organización, monitoreando el flujo de tráfico de red entrante y saliente e impidiendo que terceros no autorizados accedan a las redes privadas. El firewall busca códigos de seguridad y claves de acceso apropiadas antes de conceder acceso a una red y sólo permite realizar las transferencias autorizadas hacia adentro y afuera de la red, por lo que evita las comunicaciones sin autorización. Verifica información como nombres, direcciones IP o aplicaciones, y las compara con las reglas de acceso programadas en el sistema. Generalmente se colocan entre las redes internas privadas y las redes externas a las cuales no se les tiene demasiada confianza, pero también suelen utilizarse para proteger una parte de la red de una empresa del resto de la red.

Sin embargo, el firewall no impide por completo el acceso no autorizado a las redes. Por esta razón, se debe tener en cuenta como un elemento en un plan de seguridad general además de determinar reglas detalladas acerca de las personas, direcciones o aplicaciones que son aceptadas o rechazadas.

1.3.2. Sistema de detección de intrusos

Los firewalls deben complementarse con un sistema de detección de intrusos. Dicho sistema tiene por objetivo proteger la red corporativa contra el tráfico sospechoso y los intentos de acceder a archivos y bases de datos. Este objetivo se cumple mediante el empleo de herramientas de monitoreo continuo que se colocan en los puntos más vulnerables o activos de las redes, de manera de detectar y evadir a los intrusos en todo momento. El software de exploración busca patrones que indiquen ataques por computadora, controla que los archivos importantes no hayan sido eliminados o modificados y advierte sobre vandalismo o errores de administración del sistema. Además, alerta mediante una alarma en caso de que se encuentre una actividad sospechosa o anormal.

1.3.3. Software antivirus

Es fundamental contar con protección antivirus en los sistemas informáticos empresariales ya que el software realiza una revisión en dicho sistema para detectar la presencia de virus y eliminarlos del área o de las áreas que se encuentran infectadas. El software antivirus debe ser actualizado permanentemente para que sea efectivo debido a que, la mayoría de las veces, sólo resultan efectivos contra los virus que ya se conocían con anterioridad.

También son muy útiles las herramientas antispyware que se integran con el software antivirus y brindan e incluyen protección contra spyware.

1.3.4. Firma digital

La identificación digital de una persona se puede realizar mediante el empleo de la firma digital ya que es una herramienta tecnológica que identifica de forma unívoca a la persona que envía un mensaje y la conecta con el mismo. De esta manera, se garantiza la autoría e integridad de los documentos digitales pero no así la confidencialidad. La firma digital relaciona el documento firmado con información propia del firmante y es encriptada con una clave privada. Cualquier persona que conozca la clave pública del emisor puede verificar la integridad del documento y cuando no se logra desencriptar correctamente la firma significa que el mensaje fue modificado. Por lo tanto, se prueba la autoría de un mensaje cuando es descifrado utilizando la clave pública de una persona, lo que permite asegurar que esa persona lo generó utilizando su clave privada.

De todas formas, para que exista una mayor confianza a la hora de autenticar e identificar a una persona cuando las partes son desconocidas, interviene la autoridad certificante que, como se vio anteriormente, otorga certificados digitales que certifican la propiedad de las claves. Estos contienen el nombre de la persona, su clave pública, demás atributos personales y la identificación de la autoridad certificante así como su firma digital.

La firma digital se encuentra legislada en la Ley N° 25506.

1.3.5. Sistema de administración unificada de amenazas

Los sistemas de administración unificada de amenazas son productos de administración de seguridad que combinan varias herramientas en un solo paquete que contiene firewalls, redes privadas virtuales, sistemas de detección de intrusos y software de filtrado de contenido Web y antispam. Estos sistemas ayudan a las empresas reduciendo costos y mejorando la capacidad de administración.

1.3.6. Seguridad en las redes e Internet empresarial

Las principales medidas de seguridad empleadas en la empresa bajo estudio para proteger sus redes y operaciones llevadas a cabo a través de Internet son firewalls, software antivirus y software de seguridad. Además, los datos no están directamente expuestos a Internet, se necesita la red privada virtual que tiene usuario y contraseña así como un certificado de seguridad para poder acceder.

Por otra parte, el Departamento de Tecnología Informática presentó a la Dirección un proyecto para ampliar el ancho de banda y tener un proveedor de Internet alternativo por cualquier problema que pudiera surgir. Sin embargo, a través de una serie de evaluaciones donde se consideró el tema económico, la Dirección decidió asumir el riesgo de que si se cae el servicio de su proveedor de Internet principal estarán algunos días sin servicio. Estas decisiones exceden al área de sistemas, que simplemente se encarga de presentar las recomendaciones y los riesgos.

1.4. SEGURIDAD EN LA NUBE Y EN LA PLATAFORMA DIGITAL MOVIL

Algunas empresas incorporan a su forma de hacer negocios la computación en la nube y la plataforma digital móvil. Laudon, K. C. y Laudon, J. P. (2012) explican que, por más que estas herramientas generen grandes beneficios, también generan desafíos con respecto a la seguridad y confiabilidad del sistema.

En cuanto a la seguridad en la nube, los usuarios deben verificar que se cumplan los niveles de seguridad establecidos por la organización. A su vez, deben verificar cómo trabaja el proveedor de la nube, la manera en que es segregada la información de la empresa de las de otras compañías, si se utilizan mecanismos sólidos de cifrado y si podrá restaurar la información y en qué tiempo en caso de desastres. También es importante averiguar si el proveedor aceptará que se le realicen auditorías y certificaciones de seguridad externa. De todas formas, cuando las operaciones se llevan a cabo en la nube, la empresa continúa siendo la responsable de brindar protección a los datos confidenciales.

En la empresa analizada todavía no se trabaja en la nube pero en un futuro se va a comenzar a implementar. Se ha demorado su implementación por el tema de la seguridad. Ya se cuenta con todos los accesos y comenzar a trabajar en la nube es algo que se puede hacer rápidamente pero se busca tener bien establecida la plataforma de seguridad en la misma. Para esto, también se ha contratado una consultora a fin de que configure y garantice la seguridad en la nube.

Por su parte, la seguridad en las plataformas móviles debe ser contemplada en las políticas de seguridad empresariales ya que estos dispositivos acceden a sus sistemas y datos. Por este motivo, los

dispositivos móviles requieren protección especial contra malware, robos, pérdidas, hackers, etc. Se deben establecer lineamientos que determinen cómo dar soporte, proteger y utilizar estos dispositivos a fin de evitar problemas y que la seguridad no se vea comprometida.

Actualmente, todos los dispositivos que se entregan que son de la empresa vitivinícola están instalados con una aplicación que se llama Airwatch. Cuando hay algún robo de equipo lo que se hace desde un panel centralizado es el borrado remoto de la información. Si a algún empleado le roban el dispositivo y el área de sistemas ya tiene aviso de que ese dispositivo hay que borrarlo, cuando el ladrón lo prende se borra toda la información. Este sistema también permite determinar cuáles son las aplicaciones que se pueden instalar y cuáles no en los distintos dispositivos móviles pero esta función no se está utilizando en la empresa. Pero perfectamente se podría establecer una lista de las aplicaciones que están autorizadas por el área de sistemas y cuáles se pueden instalar.

Todo el acceso que viene desde equipos móviles se hace a través de la red privada virtual. Por lo tanto, si alguien quiere acceder a los datos desde una computadora y no está dentro de la red de la empresa, va a necesitar una conexión que va encriptada entre la computadora y los servidores de la empresa.

1.5.PLAN DE SEGURIDAD Y PLAN DE CONTINGENCIA

Según Saroka, R. H. (2002), para proveer seguridad al sistema empresarial es fundamental contar con un plan de seguridad y un plan contingencia. Si bien todos los miembros de la organización se ven involucrados, resulta primordial la participación y respaldo de la dirección superior en todas sus etapas para alcanzar el éxito. Laudon, K. C. y Laudon, J. P. (2012) agregan que la dirección debe trabajar en conjunto con los especialistas en tecnología de la información para evaluar qué sistemas y procesos de negocio son los más críticos y tendrían un mayor impacto en caso de fallas.

El plan de seguridad es definido como “un conjunto de medidas preventivas, detectivas y correctivas para enfrentar los riesgos a los que se encuentran expuestas las operaciones de procesamiento o transmisión de datos, así como los archivos, programas y demás recursos informáticos involucrados” (Saroka, R. H., 2002, p.333). Lo que se busca con el plan de seguridad es el resguardo de los recursos informáticos para cumplir con la integridad, confidencialidad, privacidad y continuidad. Para ello se deben identificar los activos expuestos a pérdidas, las vulnerabilidades y amenazas, realizar un análisis del riesgo determinando su impacto e identificar los controles existentes y los faltantes. De esta forma, se pueden seleccionar y establecer las medidas de seguridad que lleven el riesgo a un nivel aceptablemente bajo.

También es imprescindible que se establezca la manera de mantener y mejorar continuamente el plan de seguridad.

Por su parte, el plan de contingencia es “un conjunto de procedimientos que, luego de producido un desastre, pueden ser rápidamente ejecutados para restaurar las operaciones normales con máxima rapidez y mínimo impacto” (Saroka, R. H., 2002, p.334). Forma parte del plan de seguridad y sólo considera e incluye medidas correctivas ya que asume que las contingencias ya han sido estudiadas y resueltas en cuanto a prevención y detección. El plan de contingencia tiene por objetivo proveer la capacidad de continuar el negocio minimizando el impacto de un desastre y lograr una rápida recuperación de las operaciones. Dicho plan debe ser realista y eficiente, estableciendo:

- Los recursos y conocimientos necesarios para enfrentar las contingencias o amenazas.
- Las personas que le deben dar cumplimiento así como sus responsabilidades y roles.
- Los protocolos de actuación, políticas y procedimientos que se deben llevar a cabo.

El plan de contingencia debe ser revisado, probado y aprobado y es fundamental su actualización constante.

La contingencia ideal sería tener todo replicado en algún lugar con accesos, con seguridad y demás, pero cuando se analizan los riesgos y el dinero que implica la inversión puede que no resulte viable. En el caso de la empresa bajo estudio, se está trabajando para tener una contingencia de los principales sistemas en los servicios de la nube. Actualmente, la contingencia que tiene son los backup que se tienen fuera por si surge algún problema. Se tienen equipos que están en otro lugar donde se puede levantar y resguardar información.

En la empresa no se tiene un plan de contingencia como tal sino que se ha escrito un documento con algunas medidas de contingencia que se debe perfeccionar. Entonces, se cuenta con una serie de medidas aisladas que forman parte de un plan de contingencia pero faltan muchos detalles para llegar a ser el plan en sí. Esto es así porque, por ejemplo, no figuran los roles y responsabilidades del personal. Se tiene la copia de seguridad, se tiene el equipamiento necesario pero no está establecido quién se va a encargar de levantar la información y cómo. Tampoco figura si la persona sabe cómo hacerlo y si está capacitada. Por este motivo, no se cuenta con un plan de contingencia completo. Sin embargo, la empresa tiene un proyecto que es la gestión de continuidad del negocio, donde se busca documentar y escribir cada uno de los roles y responsabilidades. Por lo tanto, está encaminada y busca mejorar en este aspecto.

2. ASEGURAMIENTO DE LA CALIDAD DEL SOFTWARE Y DE LA DISPONIBILIDAD DEL SISTEMA

Es sabido que en muchos casos un software puede contener varios errores, por lo que es necesario realizar pruebas constantemente para detectarlos. Cuando se realizan pruebas de manera oportuna, regular y exhaustiva en el software se logra mejorar la calidad y confiabilidad del sistema empresarial (Laudon, K. C. y Laudon, J. P., 2012).

Laudon, K. C. y Laudon, J. P. (2012) afirman que es importante que los sistemas y aplicaciones de las empresas se encuentren siempre disponibles, sobre todo cuando utilizan las redes digitales para realizar sus operaciones. Para esto, existen sistemas de computadora tolerantes a fallas y la computación de alta disponibilidad que buscan minimizar el tiempo en el que el sistema se encuentra inactivo. La computación de alta disponibilidad ayuda a que el sistema se recupere con rapidez ante un desastre, en cambio, la tolerancia a fallas busca la eliminación del tiempo de recuperación y la disponibilidad continua del sistema para proveer un servicio sin interrupciones.

Los sistemas de computación de alta disponibilidad implican la utilización de servidores de respaldo, la existencia de varios servidores en los cuales se distribuya el procesamiento, almacenamiento de alta capacidad y planes de recuperación y continuidad. Este tipo de sistemas computacionales son necesarios en empresas que tienen un gran comercio electrónico o que realizan sus operaciones en redes digitales.

2.1. CONTROL DEL TRÁFICO DE RED: INSPECCIÓN PROFUNDA DE PAQUETES

Existen algunas aplicaciones que consumen el ancho de banda, lo que obstruye y ralentiza las redes empresariales, y por lo tanto, se ve afectado el desempeño. Para resolver este problema se utiliza la inspección profunda de paquetes a través de la cual se examinan los archivos de datos y se asignan prioridades al material en línea, dándole mayor prioridad a los archivos críticos para la empresa y bloqueando o retrasando los paquetes de datos que no son prioritarios para que avance el tráfico más importante de la red.

La inspección profunda de paquetes todavía no se ha implementado en la empresa vitivinícola pero con la aplicación de los nuevos firewalls la idea es que se active esta función y se pueda analizar qué está pasando en la red. Además, contribuiría a la protección de los datos empresariales.

2.2. SUBCONTRATACIÓN DE LA SEGURIDAD

Es posible subcontratar funciones de seguridad con proveedores que brinden estos servicios cuando las empresas no cuentan con recursos, experiencia ni capacidad para generar seguridad en su sistema informático a fin de que este posea una alta disponibilidad. Dichos proveedores se encargan de monitorear la actividad de la red, realizar pruebas de vulnerabilidad y detectar intrusos.

Como ya se ha visto con anterioridad, el Departamento de Tecnología Informática trabaja con diversas consultoras para brindar a la empresa seguridad informática. Por lo tanto, existe una subcontratación de la seguridad al no contar con un área específica que se encargue de la misma en la empresa.

3. CONTROL INTERNO Y AUDITORÍA INFORMÁTICA

De acuerdo con lo explicado por Sánchez Valriberas, G. (2001), el control interno informático verifica que las actividades que se realizan en los sistemas de información se realicen de manera correcta y válida, cumpliendo con las normas y procedimientos fijados en la empresa así como con las normas legales. Lo se busca con el control interno es prevenir o corregir los errores o irregularidades que afectan el funcionamiento del sistema e impiden el logro de sus objetivos y también se busca la protección integral de los recursos informáticos. Estos controles pueden ser manuales (cuando no se utilizan herramientas de computación) o automáticos (cuando se hayan incorporados en el software) y, de acuerdo con los objetivos, a su vez pueden ser controles preventivos, detectivos o correctivos.

Por su parte, la auditoría informática es definida como “el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos” (Sánchez Valriberas, G., (2001), p. 28). Por lo tanto, el auditor debe revisar el funcionamiento de los controles y la fiabilidad de la información e informar a la Dirección de la empresa sobre cualquier inconveniente.

En la empresa vitivinícola no hay control interno informático como tal. Sin embargo, dentro de los proyectos que lleva a cabo el área de sistemas, se trabaja en ese aspecto junto con una consultora. La empresa le paga un paquete de horas pero lo que se hace es simplemente correctivo, es decir, que se corrigen los problemas una vez que pasa algo. La idea es comenzar a trabajar de manera preventiva y siguiendo los lineamientos establecidos por y para la empresa.

Como ya se vio, al no existir un área de seguridad informática, el Departamento de Tecnología Informática asume esas tareas, que son tercerizadas en gran parte, y busca tener una manera de gestionar la seguridad. La estrategia hasta ahora es la de tener un software de administración de pedidos y

planeamiento en conjunto con la documentación que se va a obtener en cada uno de esos aspectos. En base a eso se va a ir planificando y se va a ir teniendo control sobre esos temas.

Este software de administración de pedidos y planeamiento es un proyecto que ha encarado la empresa. Si bien cuenta con un software actualmente, el mismo no es tan eficiente ya que no permite tener estadísticas de qué es lo que más piden o requieren los usuarios. Cuando se tenga el nuevo software, va a permitir la comunicación con todos los usuarios y se van a tener estadísticas de cuáles son los llamados más frecuentes, entonces se van a empezar a tener datos concretos sobre dónde se deben enfocar en la comunicación con el personal. Se trata de un software de desarrollo propio que tendrá dos funcionalidades, la de administración y la de planeamiento de todos los proyectos. Además, la idea es que se vaya actualizando de manera dinámica a medida que van avanzando los proyectos. Este software va a permitir tener datos y medidas cuantitativas para orientar al personal sobre lo que hay que hacer. De esta manera, el Departamento de Tecnología Informática podrá informar a los usuarios sobre lo que realmente necesitan. También permitirá tener una visión global de lo que pasa en la organización, lo que es fundamental para brindar un control adecuado. Entonces, en función a los datos concretos que aportaría este software de administración de pedidos y planeamiento se podrían dar lineamientos en base a lo que realmente necesitan los usuarios.

Algunos controles que se aplican en la empresa estudiada consisten en revisar que las copias de seguridad se estén realizando, entonces todos los días se entra al sistema y se verifica que la copia esté. Además, se cuenta con un monitor donde figuran algunos indicadores de servicios que permite ver que se encuentren operativos y también se está trabajando en incorporar otro tipo de dispositivos. Lo que se busca es poder tener algunas cosas a la vista con el uso de tableros dentro del sistema a través de indicadores que rápidamente indiquen si algo anda mal.

La empresa vitivinícola es muy grande y tiene muchos usuarios, un montón de dispositivos y muy pocas personas en el área de sistemas, por ello se busca el apoyo en diversas herramientas. El enfoque del Departamento de Tecnología Informática, que se ha planteado a la Dirección como estrategia, es que, ya que no se quiere agrandar la organización del área, este departamento se debe fortalecer con consultoras y trabajar con herramientas que permitan que los usuarios sientan que están controlados y que cuenten con políticas claras con respecto a cuáles son los aspectos que deben tener en cuenta para no cometer errores. El personal también tiene que estar involucrado en la seguridad ya que es parte del control interno. El control interno es la base de todo, y todos los integrantes de la organización son responsables, no sólo el área de sistemas. En la empresa se ha comenzado a trabajar para contar con un buen control interno informático. Cuando empiecen a tener indicadores y datos van a poder saber, por ejemplo, si los usuarios

están accediendo a determinada página que representa una amenaza para restringir o reducir el acceso si hace falta y, de esta manera, se va a tener un mayor control y seguridad.

Por su parte, en la empresa hay un área de auditoría pero está orientada a la auditoría de procesos y no de sistemas. Dentro de las auditorías que se realizan, se revisan aspectos más bien funcionales pero no a nivel de seguridad ni de sistemas, por lo que no se realizan auditorías informáticas como tales.

4. GESTIÓN DE LA SEGURIDAD INFORMÁTICA EMPRESARIAL: INFORMES COSO, COBIT E ISO 27001

La empresa vitivinícola estudiada no se encuentra certificada por la norma ISO 27001 pero posee un informe de seguridad elaborado por una consultora en función a la misma y siguiendo directamente todos sus lineamientos. Así mismo, se han tenido en cuenta los informes COSO y COBIT, ya que la norma ISO se basa mucho en temas contemplados en esos informes.

Sin embargo, hoy en día, los informes COSO y COBIT no se están aplicando en la empresa totalmente. De todas formas, los proyectos que se están desarrollando para la organización del área se relacionan con la norma ISO 27001 y los informes COSO y COBIT. La idea es apuntar a estos estándares pero no a nivel de detalle. Pero conceptualmente, en el Departamento de Tecnología Informática son conocidos y se sabe lo que pide cada uno.

En cuanto al Sistema de Gestión de Seguridad de la Información contenido en la norma ISO 27001, actualmente no se aplica en la empresa analizada, pero con la administración de proyectos se está trabajando en eso y se pretende llegar a tener este sistema. Si se logra documentar los riesgos claves de la matriz y documentar demás aspectos relativos a la seguridad, en la empresa se va a conseguir contar con un Sistema de Gestión de Seguridad de la Información. Por más que actualmente no se estén aplicando completamente los lineamientos de la norma ISO 27001 en la empresa, se está trabajando mucho en ello ya que se está en un proceso de mejora de la seguridad informática empresarial.

5. RECOMENDACIONES PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA VITIVINÍCOLA

Con la finalidad de aumentar el nivel de seguridad informática en la empresa vitivinícola bajo estudio, es preciso mejorar las medidas de seguridad aplicadas e incorporar otras medidas nuevas para así lograr un mayor control y protección de todos los recursos informáticos que conforman el sistema informático empresarial.

Al analizar los niveles de los distintos factores de riesgo, es necesario realizar las siguientes recomendaciones:

- Reubicar el centro de cómputos en una zona que sea más segura y adecuada, que permita prevenir y minimizar cualquier riesgo y que posea una mejor y más resistente infraestructura.
- Aplicar alarmas y detectores de incendios, además de matafuegos, en los lugares donde se encuentren las computadoras y demás recursos, que deben ser lugares adecuadamente ventilados. Es muy importante contar con personal que sepa y esté capacitado para usar los extintores en caso de incendio y que exista la adecuada señalización para que estos elementos se puedan localizar con facilidad. También es importante el mantenimiento preventivo y el control regular de las instalaciones eléctricas, lo que también ayuda a prevenir cortocircuitos.
- Colocar las computadoras, cables, equipos y demás recursos informáticos en lugares altos que no puedan ser afectados por inundaciones y aislados de cualquier tanque de agua y de zonas donde el agua puede filtrarse de algún modo. Evitar el consumo de bebidas en las oficinas donde se trabaja con equipos computacionales.
- Asegurarse de que el centro de cómputos se encuentra en un lugar que cuenta con la infraestructura apropiada capaz de resistir temblores.
- Promover para todo el personal el correcto y cuidadoso uso de computadoras y equipos a fin de evitar roturas.
- Brindar capacitaciones a todo el personal al menos una vez al mes acerca de la seguridad informática y su importancia para que se alcance un nivel de concientización apropiado que garantice la utilización correcta y la protección de los recursos informáticos por parte de todos los miembros de la empresa.
- Establecer de manera documentada una política de seguridad que describa los lineamientos y procedimientos de protección de los activos informáticos a seguir por todo el personal. A su vez, realizar un seguimiento para corroborar que se esté cumpliendo y para incorporar actualizaciones y mejoras en caso de que sea necesario.
- Establecer de manera documentada un plan de seguridad que permita saber cómo se debe actuar para prevenir, detectar y corregir cualquier amenaza o riesgo. Del mismo modo, se debe establecer un plan de contingencia que contemple las medidas correctivas a aplicar en caso de desastres, los recursos que serán necesarios y los roles y responsabilidades del personal.
- Tener claramente definidas y, en lo posible, documentadas las funciones que le corresponden a cada persona en materia de seguridad informática, como así también sus responsabilidades. Sería recomendable la elaboración cursogramas y manuales de procedimientos que permitan ver

fácilmente las tareas que corresponden a cada área en cuanto a la protección de los recursos informáticos.

- Es importante que se establezcan controles por oposición de las tareas que se llevan a cabo en los sistemas y de las que son necesarias para su protección. De esta manera, existiría un control cruzado entre distintas áreas empresariales lo que garantizaría un mayor nivel de seguridad.
- El Departamento de Tecnología Informática depende de la Gerencia de Administración y Finanzas y esto no es adecuado debido a que existe un alto riesgo de que la información sea tergiversada y, a su vez, este Departamento no tiene la independencia que necesita para operar. Por este motivo resulta crítico que sea modificada su ubicación en la estructura organizacional. Se sugiere que el Departamento de Tecnología Informática esté ubicado como un staff dependiendo directamente de la Dirección, debido a que brinda apoyo al resto de la organización a través de sus servicios. Es necesario que tenga autoridad para tomar decisiones y proponer sugerencias dada su formación e idoneidad. En la estructura propuesta, este Departamento no posee dependencia funcional en relación con ninguna otra gerencia de la organización, esto es ideal para un buen sistema de control interno ya que minimiza el riesgo de malversación de datos por parte de los integrantes de las gerencias operativas y/o administrativas-contables.
- Si bien la decisión de la Dirección es no tener un área específica dedicada a la seguridad informática, es recomendable que se evalúe esa posibilidad en un futuro. El Departamento de Seguridad Informática se encarga de esta seguridad junto con consultoras en las cuales se terceriza el trabajo pero por el momento el nivel de seguridad es medio y se debe mejorar. Al tener un área de seguridad informática en la empresa se puede contar con personal que esté capacitado en el tema y que pueda brindar soluciones óptimas y oportunas a la empresa al conocer desde adentro su funcionamiento. Además, sería posible brindarles capacitaciones al resto del personal con regularidad para que conozcan sobre el tema y puedan proteger los activos informáticos desde su lugar en la organización.
- Aplicar en los sistemas que se utilizan distintos controles que minimicen el riesgo de introducción de datos incorrectos. Es importante que a la hora de trabajar en los sistemas el personal se encuentre concentrado para evitar errores u omisiones de datos. A su vez es necesario que existan controles a lo largo de todos los procesos que permitan detectar dichos errores u omisiones y evitar la manipulación de datos. También es importante que el almacenamiento y archivo de datos se realice de manera ordenada para permitir su posterior control. Para cumplir con ello, sería recomendable incorporar un administrador de base de datos que se encargue de brindar protección y orden a todos los datos almacenados en la empresa.

- Incorporar al área de auditoría interna auditores informáticos o de sistemas que se encarguen de realizar este tipo de auditorías con regularidad a fin de evaluar la información, los sistemas y los controles aplicables y realizar observaciones y recomendaciones si se detectan debilidades para que puedan ser salvadas. De esa forma, el nivel de seguridad informática existente en la empresa podría mejorar notablemente y se garantizaría una adecuada protección de los recursos informáticos. Si es posible, también se podrían aplicar auditorías continuas que monitorizarían contantemente los sistemas y permitirían detectar a tiempo cualquier problema para que se pueda solucionar con rapidez.
- Al no aplicar control interno informático como tal, sería importante que se revea ese asunto y que se comiencen a implementar este tipo de controles para poder asegurar el funcionamiento correcto y seguro de todos los sistemas informáticos. Estos controles, en combinación con auditorías informáticas, garantizarían un adecuado nivel de seguridad y lo mantendrían en el tiempo si están correctamente realizados. Además, mantendrían los riesgos a un nivel aceptable lo que permitiría a la empresa operar con tranquilidad al contar con información confiable, íntegra y disponible en todo momento.
- A la hora de diseñar y programar sistemas, los especialistas deben realizar pruebas y controles para verificar que funcionan como se espera y que no presentan errores. A su vez, se debe analizar con los usuarios de los sistemas si realmente van a satisfacer las necesidades por las cuales se desarrollan para garantizar que se cumplan eficientemente los objetivos.
- El centro de cómputos, además de ubicarse en un lugar adecuado, debe estar protegido con controles de seguridad y se debe restringir el acceso a las personas autorizadas. Se deben revisar periódicamente los servidores para detectar de manera preventiva cualquier fallo o factor que pueda provocar una caída. Es importante realizar el mantenimiento del hardware, software y del sistema eléctrico con regularidad. También se debe contar con sistemas redundantes donde sus componentes más importantes estén repetidos para poder continuar operando si surge algún problema.
- Capacitarse y actualizarse en cuanto a tecnología para evitar la obsolescencia e ineficiente funcionamiento de los equipos y sistemas que se aplican. Estar atentos en cuanto a los cambios tecnológicos para que la empresa pueda mantenerse competitiva en el mercado y para mejorar constantemente la seguridad informática. Además, los programas que se utilizan deben ser actualizados constantemente para que funcionen de manera óptima.
- Además del backup y recuperación, es fundamental que la empresa cuente con un centro de procesamiento alternativo para que la empresa tenga continuidad operativa ante cualquier riesgo. El proyecto de incorporar la nube como centro de procesamiento alternativo es muy bueno y útil

por lo que se recomienda seguir con su desarrollo. También se debe contar con otros equipos que almacenen todos los datos claves de la empresa, que se ubiquen en un lugar distinto al centro de cómputos y que tengan sus medidas de seguridad.

- Aplicar controles más estrictos en el ingreso a la empresa para corroborar la identidad de las personas. Verificar con regularidad los niveles de acceso de los usuarios a los sistemas y cambiar frecuentemente las contraseñas. Se pueden implementar sistemas de identificación biométrica o tarjetas inteligentes para autenticar con mayor seguridad la identidad de los usuarios. Mantener claramente definido y actualizado a qué sistemas y qué recursos necesita cada usuario para realizar su trabajo y verificar que cuenten con la debida autorización. Por otra parte, es importante que los accesos al sistema queden registrados y se sepa qué usuario accedió, cuándo lo hizo y qué hizo, además de si contaba con la debida autorización.
- Administrar y aplicar adecuadas medidas de seguridad para trabajar en la red e Internet y también para los dispositivos móviles. Es importante que todas las personas en la empresa conozcan los riesgos asociados a los mismos y estén capacitadas para utilizarlos con cuidado y de manera segura. Además de aplicar antivirus y firewalls, se deben controlar las comunicaciones que se realizan a través de estos medios, cifrando la información o aplicando otras medidas que impidan que una persona no autorizada pueda acceder a ella. También se debe cifrar la información crítica almacenada en los equipos. Se debe impedir la descarga de archivos sospechosos y el acceso a sitios que no sean seguros, además de aplicar un software antispiware y mantener el sistema operativo actualizado.

Estas recomendaciones no pretenden agotar las diversas medidas de seguridad que pueden ser aplicadas por la empresa vitivinícola para proteger sus recursos informáticos. Es sabido que la seguridad informática puede implicar un importante gasto de dinero y que la última decisión le corresponde a la Dirección. Sin embargo, se debe tener presente que las medidas de seguridad se tratan siempre de una inversión porque permiten reducir los riesgos a niveles aceptablemente bajos lo que evita cualquier robo, pérdida o alteración de la información así como cualquier delito informático que pueden significar graves problemas y pérdidas económicas en una empresa.

Para que exista una adecuada seguridad informática empresarial, las organizaciones deben evaluar sus riesgos e identificar los activos informáticos expuestos a amenazas para poder establecer adecuados lineamientos que permitan darles tratamiento. Estos lineamientos deben documentarse en políticas y planes de seguridad, así como en planes de contingencia, que contemplen todas las medidas de seguridad

necesarias para mantener los riesgos reducidos a niveles aceptablemente bajos. Estas medidas de seguridad deben ser conocidas por todo el personal, quien debe contar con las capacitaciones correspondientes a fin de poder participar correctamente en la seguridad informática. Además, se debe considerar la seguridad no sólo en los sistemas empresariales sino también en las redes e Internet y en los dispositivos móviles que son utilizados en el trabajo y abren las puertas a muchas amenazas.

En la empresa vitivinícola, existen algunos lineamientos que guían las actividades que se llevan a cabo, pero no existe documentación apropiada de las políticas de seguridad ni de los planes de contingencia. Si bien existen adecuadas medidas de seguridad, no resultan suficientes y es necesario que se mejoren y se incorporen otras nuevas que permitan mejorar el nivel de seguridad informática. A su vez, se requiere la documentación adecuada y completa de los lineamientos que rigen la protección de los recursos informáticos así como la participación y la capacitación de todo el personal.

CAPÍTULO IV

EL ROL DEL CONTADOR EN LA SEGURIDAD INFORMÁTICA

El presente capítulo tiene como objetivo analizar cuál es el rol que tienen los contadores en la seguridad informática dentro de la empresa vitivinícola estudiada. A su vez, se presenta un análisis de la importancia de la formación de los futuros profesionales en la Facultad de Ciencias Económicas de la Universidad Nacional de Cuyo en cuanto a seguridad informática. Los autores con los que se trabaja son Zegarra, O. S., Escobar, D. S. y Fowler Newton.

1. LA INTERVENCIÓN DE LOS CONTADORES EN LA PROTECCIÓN DE LOS SISTEMAS INFORMÁTICOS

Los constantes avances tecnológicos impactan en todos los ámbitos laborales. Actualmente, en todas las profesiones se requiere que las personas posean habilidades informáticas para desarrollar su trabajo. Esto es así debido a los beneficios que las herramientas tecnológicas ofrecen, tales como mayor eficiencia, optimización de tiempo, manejo de grandes volúmenes de datos, entre otros.

Particularmente, la profesión del contador está sumamente ligada a la utilización de estas herramientas ya que su objetivo es la generación de información útil y oportuna para la toma de decisiones de los distintos usuarios que la requieran. Por este motivo, los contadores tienen una gran intervención en el manejo de los sistemas informáticos los cuales les permiten y facilitan el ejercicio de su trabajo. Así también, deben estar capacitados y ser conscientes de la importancia de la seguridad informática a fin de contar con datos e información que cumpla con las características de confidencialidad, integridad y disponibilidad. Esto es de suma importancia porque estos profesionales pueden brindar una gran ayuda a la hora de garantizar la protección de la información y de los sistemas informáticos.

1.1.LOS CONTADORES Y LA TECNOLOGÍA INFORMÁTICA

Tal como ya se mencionó, los contadores tienen una importante intervención en cuanto a la tecnología informática, ya sea como usuarios de los sistemas o como auditores de los mismos, para detectar riesgos y aplicar los controles que brinden la seguridad necesaria.

Según Zegarra, O. S. (2014), cualquiera sea el trabajo que desarrolle el profesional, el mismo se va a ver auxiliado por la tecnología informática. El avance tecnológico ha impactado en los sistemas contables contribuyendo a un mejor y más rápido manejo de grandes cantidades de datos, como así también en la calidad y exactitud de la información y en su presentación oportuna a quien la requiera. Por este motivo, los contadores deben informatizarse para poder llevar a cabo su trabajo. Sin embargo, no es necesario que posean conocimientos profundos referidos al diseño y programación de los sistemas pero sí de sus fundamentos y lógica procesal, lo que les permite un mejor desempeño profesional. Las computadoras y los sistemas contables son las herramientas fundamentales que debe utilizar un contador para cumplir sus funciones de manera eficiente. Estas herramientas permiten la automatización de la contabilidad que es el centro de la información necesaria de una empresa.

Por otra parte, de acuerdo con lo expuesto por Escobar, D. S. (2017), con la adecuada especialización, los contadores pueden planificar, gestionar y controlar los sistemas de información contable o administrativos utilizados en una empresa. Además, deben contribuir a que exista una adecuada seguridad de la información a fin de que se cumplan los requisitos de la información contable y que la misma sea fidedigna. Sin embargo, estas cuestiones no se toman en consideración en la mayoría de las empresas. Pero realmente resulta importante y necesario contar con contadores que sean conscientes del problema y puedan trabajar interdisciplinariamente con los especialistas en sistemas y seguridad para aportar su ayuda y su punto de vista. De esta manera, resulta más sencillo contar con sistemas de información apropiados en cuanto a hardware y software y contar también con políticas de seguridad de la información adecuadas para garantizar la protección de los datos y su confiabilidad. Al aplicar medidas de seguridad se puede evitar la pérdida, modificación, acceso no autorizado a los datos y cualquier otro riesgo que pueda afectar la información que es la base de la toma de decisiones y de la operación empresarial.

1.2.EL ROL DE LOS CONTADORES EN LA EMPRESA VITIVINÍCOLA

En la empresa vitivinícola bajo estudio, la intervención que tienen los contadores a la hora de proteger los sistemas que se emplean es clave. Estos profesionales trabajan en el área de administración y conocen mucho acerca de los procesos empresariales que se llevan a cabo, por lo tanto, tienen un papel fundamental como disparadores de aplicación de buenas prácticas en temas de seguridad informática para toda la organización.

Los contadores son usuarios intensivos de los sistemas informáticos empresariales. La información que los mismos manejan y sobre la cual realizan sus análisis debe ser fidedigna, motivo por el cual deben preocuparse en requerir todas las medidas de seguridad relacionadas con la información. Sin

embargo, también deben contribuir con dichas medidas ya que son responsables, al igual que el resto del personal, de no descargar y/o distribuir archivos que puedan significar amenazas, no prestar o dar a conocer sus contraseñas, no abrir correos electrónicos de dudosa procedencia, entre otros aspectos. Además, tienen la responsabilidad de realizar copias de seguridad de la información. Por todo esto, el rol de los contadores en la empresa es muy importante para brindar un adecuado manejo y protección de todos los recursos informáticos.

En la empresa vitivinícola los contadores actúan como usuarios de los sistemas pero, como se vio en el capítulo anterior, no tienen mucha intervención como auditores de sistemas. Si bien se realizan auditorías internas generales en la organización, no se profundiza ni se aplican específicamente en los sistemas y en su seguridad. De todas maneras, para los contadores resulta muy importante la seguridad informática y es por ese motivo por el cual exigen que se apliquen adecuadas medidas de protección a fin de poder utilizar los sistemas y la información con tranquilidad.

La recomendación que resulta de lo anteriormente expuesto es que sería ideal que hubiera una integración entre el personal del área de sistemas y los contadores. De esta manera, sería más sencillo conocer las necesidades precisas que existen en cuanto a los sistemas y su protección. Estos profesionales pueden trabajar en conjunto para elaborar las políticas y medidas de seguridad, así como los planes de contingencia y así se obtendrían mejores resultados debido a que su visión sería más amplia y abarcativa. Por otra parte, también resulta fundamental que se comiencen a aplicar auditorías informáticas con regularidad para garantizar la confiabilidad, integridad y disponibilidad de los datos y de los sistemas. De esa manera, también se brinda seguridad en la operatividad de la empresa.

2. LA FORMACIÓN DE LOS CONTADORES EN SEGURIDAD INFORMÁTICA

Es de vital importancia que los estudiantes de contabilidad tengan una buena formación académica que les permita convertirse en profesionales competentes y capacitados para enfrentar las diversas situaciones que se les puedan presentar. Además, se trata de una profesión que requiere capacitación y actualización constantes debido a los vertiginosos cambios normativos y tecnológicos que impactan en la actuación y responsabilidad del profesional.

Fowler Newton (2005) define a la contabilidad como “una disciplina técnica que, a partir del procesamiento de datos sobre la composición y evolución del patrimonio de un ente, los bienes de propiedad de terceros en su poder y ciertas contingencias, produce información para la toma de decisiones” (p.9). Además, permite vigilar los recursos y obligaciones de un ente. Por este motivo, los contadores tienen un rol muy importante en las empresas debido a que son los que ayudan a generar esa

información que permite a los administradores o terceros interesados decidir sobre el curso de sus negocios.

De acuerdo con el artículo 13 de la Ley N° 20488 (1973), los contadores tienen incumbencia para elaborar e implantar políticas, sistemas, métodos y procedimientos de trabajo administrativo contable. También tienen incumbencia para aplicar e implantar sistemas de procesamiento de datos y otros métodos para el proceso de información en cuanto a aspectos contables y financieros. Es decir que tienen una gran influencia en los sistemas informáticos que aplican las empresas para la generación de información como así también en su protección.

La forma en la que deben realizar su trabajo los contadores evoluciona permanentemente. Antiguamente la contabilidad se llevaba sólo a través de medios manuales pero en la actualidad es impensable desarrollar el trabajo sin medios informáticos de por medio. Los avances tecnológicos han contribuido enormemente a la rapidez y eficiencia en la labor de los contadores. Sin embargo, así como la tecnología trae innumerables beneficios también aparecen los riesgos que fueron vistos en los capítulos anteriores. Tanto por los beneficios como por los riesgos de la tecnologización, es fundamental que los contadores posean conocimientos sólidos en esta materia para desempeñar su profesión de la mejor manera. Por este motivo, en las facultades se deben impartir materias que aborden la tecnología informática como herramienta de la profesión, dando a conocer la utilización de las computadoras con sus aplicaciones, la utilización de softwares contables y, por supuesto, la seguridad informática, entre otros aspectos.

2.1.LA FORMACIÓN DE LOS CONTADORES EN LA FACULTAD DE CIENCIAS ECONÓMICAS DE LA UNIVERSIDAD NACIONAL DE CUYO

La formación académica que se obtiene en la Facultad de Ciencias Económicas de la Universidad Nacional de Cuyo es de muy buen nivel. En cuanto a seguridad informática, se cuenta con diversas cátedras que brindan conocimientos y preparación al respecto. Sin embargo, sucede que el tiempo de dictado de las materias es acotado por lo que no se llegan a ver todos los temas con la profundidad necesaria. Además, muchas veces no se utilizan los medios informáticos para aplicar los conocimientos lo que limita el aprendizaje de herramientas o aplicaciones informáticas.

Actualmente, en dicha Facultad se está implementando un cambio en el plan de estudios de manera progresiva año a año lo que implica que el plan de estudios del año 1998 se deje de aplicar también de forma progresiva y comience a aplicarse el correspondiente al año 2019.

2.1.1. Plan de estudios del año 1998

En el plan de estudios del año 1998 de la carrera de Contador Público Nacional y Perito Partidor de la Facultad de Ciencias Económicas, las materias que abordan temas referidos a la seguridad informática son Computación, Sistemas Administrativos de Información Contable y Auditoría Operativa y de Sistemas Computarizados. Con el cursado de las mismas se obtienen muy buenos conocimientos referidos a la utilización de las computadoras y algunos de sus aplicativos, los sistemas contables empresariales y el control de los mismos. Pero, como se mencionó anteriormente, no se llegan a ver completamente todos los temas contenidos en los programas de estudio. Y, si bien se estudia el tema de la seguridad informática, no se llega a profundizar lo suficiente como es necesario.

A continuación se procederá a analizar los programas de dichas materias para ver los contenidos que se dictan en cada una de ellas.

- **Computación:**

Computación era un espacio curricular anual obligatorio que se dictaba en primer año de la carrera de Contador Público Nacional y Perito Partidor. Esta materia buscaba que los alumnos utilizaran y lograran un buen dominio de la Tecnología de la Información y Comunicación sobre todo en un entorno económico empresarial y para resolver situaciones profesionales. El programa de estudio contiene las siguientes unidades:

- Unidad I: Introducción a la Tecnología de la Información y Comunicación

El objetivo es que el alumno aprenda a utilizar los recursos computacionales y su sistema operativo. Este aprendizaje se logra mediante la enseñanza de los sistemas de información, la computadora como tecnología de la información, el hardware y software así como los sistemas operativos y la protección de la información.

- Unidad II: Introducción a las Tecnologías de la Comunicación

El objetivo es que se logre una gestión eficiente de las redes de datos e Internet y de las comunicaciones internas y externas organizacionales. El aprendizaje en esta unidad se da mediante la enseñanza de las redes de datos y su seguridad, módems, Internet, búsqueda de información científica y académica y la seguridad en Internet entre otras cosas.

- Unidad III: Procesador de Textos y Herramientas para presentaciones

El objetivo es que el alumno, mediante la utilización del procesador de textos, logre diseñar y elaborar documentación. Además, que logre exponer sus proyectos, ideas o actividades mediante presentaciones multimedia. Estos temas se aprenden a través de la enseñanza de la gestión de imágenes, plantillas y estilos, revisión de documento, formularios y demás aspectos de un procesador de textos. También con la enseñanza del diseño y edición de diapositivas a través de las herramientas correspondientes.

- Unidad IV: Planilla u Hoja de Cálculo

El objetivo de esta unidad es el aprendizaje de la gestión de la información a través del diseño, elaboración y operación eficiente de la planilla de cálculo. Para que el alumno logre dicho aprendizaje se le enseñan los formatos, fórmulas y funciones, creación de gráficos y, también, la integración con el procesador de textos y la creación de base de datos, entre otros aspectos. Además, se enseña a auditar y resolver problemas en las hojas de trabajo así como el análisis de datos.

- Unidad V: Base de Datos

El objetivo es que el alumno logre administrar la información de una organización mediante el diseño y gestión eficiente de base de datos. Esto se aprende a través de la enseñanza de los Sistemas de Gestión de Base de Datos, las características de Access y la creación de base de datos, relación de tablas, consultas, formularios, controles, informes así como exportación de datos y lenguaje de interrogación estándar SQL, entre otros temas. También se pretende la integración de herramientas.

- **Sistemas Administrativos de Información Contable:**

Sistemas Administrativos de Información Contable es un espacio curricular obligatorio que se dicta en el quinto cuatrimestre de la carrera. Esta asignatura busca brindar conocimientos en cuanto a la utilización de tecnologías de información y comunicación como soporte del ejercicio profesional. Además, pretende desarrollar la capacidad para el diseño, implementación y dirección de sistemas de registración e información contable, y la capacidad de aplicar herramientas de tecnología de la información y del procesamiento de datos para resolver situaciones profesionales. Las unidades que conforman esta asignatura son las siguientes:

- Unidad I: Sistemas Administrativos

El objetivo de esta unidad es que el alumno reconozca los sistemas de información e identifique el rol del contador con respecto a los sistemas de información contables, además de que pueda procesar datos contables mediante la utilización de aplicativos. El aprendizaje se logra mediante la enseñanza de los

sistemas de información y el rol del profesional como administrador de la información y de los sistemas de información de la empresa en cuanto a su concepto, dimensiones, jerarquías, sistemas administrativos y contables y los usuarios de la información.

- Unidad II: Herramientas de los Sistemas de Información

El objetivo consiste en lograr el análisis, organización y planificación de procedimientos utilizando las herramientas disponibles y aplicar estas herramientas a los procesos de compras, pagos, ventas y cobranzas. Los temas que son abordados en esta unidad son el uso de métodos gráficos, manuales y formularios, archivos de documentación y registros.

- Unidad III: Tecnología de la Información. Aspectos tecnológicos de los medios de procesamiento y comunicaciones

El objetivo que se busca alcanzar es que el alumno pueda reconocer las tecnologías de la información y comunicación y los beneficios que estas aportan a los sistemas de información. Además, que sean capaces de generar y gestionar bases de datos y definir topologías de red aplicables a distintas organizaciones. Estas cuestiones se aprenden mediante la enseñanza del hardware y software, la comunicación y redes y las bases de datos.

- Unidad IV: Metodologías de incorporación e implementación de sistemas de información

El objetivo es que se logre identificar y seleccionar las metodologías más apropiadas para desarrollar sistemas y para la selección de software. También se busca que como miembro de un equipo multidisciplinario se pueda participar en la planificación, análisis, diseño, e implementación de un sistema de información contable. Los contenidos de esta unidad son la metodología de análisis, diseño e implementación de sistemas de información y la metodología de selección de software y evaluación de sistemas aplicativos.

- Unidad V: Control Interno y gestión de riesgos

El objetivo de esta unidad es que el alumno reconozca la importancia del proceso de control en los sistemas de información identificando sus objetivos y elementos y que tenga la capacidad de evaluar los riesgos asociados a la información e implementar los controles correspondientes. Para ello se enseña el control en general, la gestión de riesgos y el control interno y los aspectos básicos de la seguridad en los sistemas de información.

- **Auditoría Operativa y de Sistemas Computarizados:**

Auditoría Operativa y de Sistemas Computarizados es un espacio curricular obligatorio que se dicta en el décimo cuatrimestre de la carrera. Las competencias que se buscan generar con esta asignatura son la capacidad de diseño, aplicación, evaluación y control de sistemas de gestión y auditoría operativa, la capacidad de describir, analizar, diseñar y auditar procesos de negocios y los sistemas de información asociados y capacidad de emplear las herramientas de tecnología de la información y del procesamiento de datos para resolver situaciones profesionales. Las unidades contenidas en el programa de estudio son:

- Unidad I: Marco General de la Auditoría Interna

El objetivo de esta unidad consiste en lograr que el alumno identifique los principios aplicables a la auditoría interna y conozca el concepto de control interno a través de los modelos que se relacionan con el sistema operativo y de tecnología informática. Para ello se enseña la formación del juicio profesional, los principios y código de ética de los auditores, el Marco Internacional y las Normas Internacionales de auditoría interna, las certificaciones internacionales y los modelos de control como COSO y COBIT, entre otros.

- Unidad II: Auditoría Interna

El objetivo que se persigue es que se alcancen conocimientos y habilidades para desempeñar la auditoría interna con idoneidad y que se desarrollen competencias sociales e intelectuales para un buen trabajo interdisciplinario. Lo que el alumno debe aprender incluye las distintas clases de auditorías, las diferencias con la auditoría externa, definición, objetivos, organización y enfoque moderno de la auditoría interna, su relación con la administración del riesgo empresarial y matrices de riesgo. Además, las etapas de la auditoría y la planificación e informes de la auditoría interna.

- Unidad III: Auditoría Operativa

El objetivo es que el alumno reconozca las amenazas y riesgos en los sistemas de control interno organizacionales a través de los conocimientos y habilidades que se requieren para desempeñarse como auditor operativo. Por este motivo se enseña la definición, objetivos y ejecución de la auditoria operativa, los ciclos auditables y el control interno, los papeles de trabajo y las distintas herramientas para la captura de la información así como las pruebas de auditoría.

- Unidad IV: Aplicación Práctica Auditoría Interna y Operativa

El objetivo que se busca en esta unidad es que se desarrollen habilidades de evaluación y análisis a fin de detectar las debilidades en el sistema de control organizacional y formular observaciones para su

mejora a través de un informe. El alumno incorpora estos conocimientos a través de la enseñanza de la auditoría de procesos, el desarrollo de relevamientos y el informe de auditoría interna.

- Unidad V: Marco Conceptual de Auditoría de Sistemas

El objetivo es que el alumno obtenga conocimientos en seguridad informática y en auditoría de sistemas computarizados para desempeñarse de manera idónea en este tipo de auditoría. El aprendizaje se logra mediante la enseñanza de auditoría de sistemas o tecnología de la información, funciones de control interno informático y auditoría informática, concepto de seguridad informática, plan de contingencia y de recuperación, procedimientos de resguardo y recuperación de datos, seguridad y protección de los activos informáticos.

- Unidad VI: Manejo de Bases de Datos

El objetivo es que se utilicen instrumentos, herramientas y sistemas que permitan obtener evidencia válida y suficiente para cumplir con el objetivo de auditoría y que se logren conocimientos de manejo de bases de datos para analizar grandes volúmenes de información y así llegar a conclusiones que permitan emitir una opinión profesional que agregue valor a la organización. Para ello se enseña el uso de programas de manejo de base de datos y su importancia para el auditor, la administración de datos digitales, el modelo relacional en el manejo de bases de datos, las técnicas de verificación y herramientas aplicables.

- Unidad VII: Aplicación Práctica de Auditoría de Sistemas

El objetivo de esta unidad es que el alumno desarrolle habilidades de evaluación y análisis para determinar debilidades del entorno con respecto a tecnología informática y así detectar debilidades en el sistema de control interno a fin de formular las observaciones para su mejora y elaborar un informe. El aprendizaje se logra mediante la enseñanza de aplicaciones para administrar base de datos, aplicación de pruebas de cumplimiento y pruebas sustantivas estadísticas, casos prácticos sobre el manejo de bases de datos en auditoría y el control interno de tecnología informática en un sistema de gestión empresarial.

- Unidad VIII: Prevención de Lavado de Activos y Financiamiento al Terrorismo

El objetivo consiste en lograr que el alumno obtenga los conocimientos para evaluar los sistemas de control interno de un sujeto obligado en materia de Prevención de Lavado de Activos y Financiamientos al Terrorismo y para asesorar sobre el diseño e implementación de políticas y procedimientos. Por ello se le enseña al alumno la prevención del lavado de dinero, financiación al terrorismo y otras actividades ilícitas, su ámbito de aplicación, organismos de contralor y las implicancias

del contador en esta materia. Además, se enseña la aplicación de controles operativos e informáticos por el auditor interno, fraude interno y externo y detección de operaciones ilícitas por la auditora interna.

2.1.2. Plan de estudios del año 2019

A partir de primer año del ciclo lectivo 2019 se comenzó a aplicar este nuevo plan que busca la formación de los alumnos por competencias, el énfasis de la integración de los conocimientos a lo largo de la carrera, la intensificación de la aplicación práctica de los conocimientos y la incorporación de espacios optativos que faciliten la internacionalización, entre otros aspectos. Además, debido a la globalización y la internacionalización, se hacía necesario un cambio en los planes de estudio para lograr formar profesionales competentes y actualizados que puedan aplicar sus conocimientos sin fronteras (Facultad de Ciencias Económicas, 2018).

El nuevo plan de estudios 2019 para la carrera de Contador Público abarca las siguientes materias relacionadas con la seguridad informática:

- Tecnología de Información I, se imparte en el segundo semestre de primer año de manera obligatoria.
- Tecnología de Información II, se impartirá en el primer semestre de segundo año de manera obligatoria.
- Sistemas y Tecnologías de Información, se impartirá en el primer semestre de tercer año de manera obligatoria.
- Taller de Integración SI/TI, se impartirá en el segundo semestre de tercer año de manera obligatoria.
- Gestión Estratégica de TIC, se impartirá en el segundo semestre de cuarto año de manera optativa.
- Seguridad de Sistemas de Información, se impartirá en el segundo semestre de cuarto año de manera optativa.

Se puede observar que se van a impartir mayor cantidad de materias relacionadas con la tecnología de la información y la comunicación, que seguramente abordarán los temas relacionados con la seguridad informática de manera más específica y profunda. Esto permitirá que los futuros contadores tengan una mejor formación tecnológica a la hora de desempeñarse profesionalmente, lo que traerá innumerables beneficios.

Los cambios en los planes de estudio de la Facultad de Ciencias Económicas mejorarán la formación de los profesionales, quienes estarán más preparados para afrontar el ejercicio profesional,

estarán más capacitados en la utilización tecnologías para desarrollar su labor y tendrán conocimientos internacionales.

La informatización de los contadores y su trabajo interdisciplinario con los especialistas en sistemas resulta fundamental para lograr un adecuado nivel de seguridad informática en una empresa. En el caso particular de la empresa vitivinícola, los contadores se preocupan y trabajan para conseguir adecuadas medidas de seguridad a fin de conseguir la protección de los recursos informáticos. Sin embargo, es necesario que exista una mayor integración del área contable con el área de sistemas con el objetivo de conseguir mejores resultados. También resulta fundamental que se comiencen a realizar auditorías informáticas con cierta regularidad para garantizar que la seguridad existe y mantiene al riesgo en un nivel aceptablemente bajo.

Por otra parte, la formación que obtienen los estudiantes de contabilidad en la Facultad de Ciencias Económicas de la Universidad Nacional de Cuyo es de un muy buen nivel ya que se abordan los temas referidos a seguridad informática desde distintas materias. Con la incorporación del plan de estudios del año 2019 se podrán abordar estos temas con mayor profundidad ya que se incorporan más materias que se refieren exclusivamente a la tecnología de la información, lo que mejorará la preparación de los futuros profesionales.

De todas maneras, además de los conocimientos adquiridos en la formación académica, es bueno que los contadores sientan inquietud y ganas de seguir aprendiendo para mantenerse actualizados y puedan ser cada vez más competitivos. Esto se logra con la asistencia permanente a cursos, conferencias, jornadas contables y también con el autoaprendizaje y la investigación. El conocimiento nunca es suficiente y nunca está de más, es la herramienta más poderosa que poseen los profesionales. Por este motivo, es imprescindible que se siga perfeccionando día a día.

CONCLUSIONES

Para llevar a cabo todas sus operaciones, la empresa estudiada utiliza diversos sistemas informáticos que le permiten captar, procesar y almacenar los datos que son transformados en información para la toma de decisiones. Debido a la importancia que tiene dicha información para el desarrollo de los negocios, resulta imprescindible que la misma sea íntegra, confidencial y se encuentre disponible. Y para el logro de estas características es necesario que exista un nivel de seguridad informática que garantice la protección de todos los recursos informáticos, reduciendo el riesgo a niveles aceptablemente bajos.

En la empresa vitivinícola, la seguridad informática es una función que corresponde al Departamento de Tecnología Informática y que cuenta con el apoyo de la Dirección. Sin embargo, debido a que en la empresa no se poseen todos los conocimientos y recursos necesarios, dicho departamento se ve en la necesidad de trabajar con consultoras para obtener un adecuado nivel de seguridad informática que permita proteger correctamente la información. También cabe destacar que el Departamento de Tecnología Informática no goza de independencia funcional, debido a que su relación con la Dirección no es directa, sino que depende de la Gerencia de Administración y Finanzas. Esto entorpece la toma de decisiones y significa un riesgo en su operatoria.

Entre las distintas amenazas y riesgos que afectan la información empresarial es posible mencionar amenazas climáticas, robo de información por parte de empleados, carga de información falsa al sistema o errores al cargar datos, borrado accidental de archivos, falta de un centro de procesamiento alternativo, correos electrónicos que llegan con malwares, virus, hackeos, fallas del propio sistema, falta de capacitación del personal, falta de controles por oposición y de independencia del Departamento de Tecnología Informática, falta de un área específica dedicada a la seguridad informática en la empresa, falta de realización de auditorías informáticas, entre otros.

Todos los riesgos deben ser evaluados periódicamente a fin de darles una respuesta adecuada y evitar cualquier incidente. La continuidad de las operaciones empresariales y su supervivencia en el mercado se logra cuando las vulnerabilidades, amenazas y riesgos en la información y en los sistemas se someten constantemente a evaluaciones, que permiten determinar la manera correcta de solucionar los problemas. Y, con respecto a los delitos informáticos, se deben brindar capacitaciones que otorguen los conocimientos necesarios para saber evitarlos y tratarlos en caso de que ocurran.

Por su parte, los controles que se aplican en los sistemas informáticos son los siguientes: restricciones de acceso a los servidores, cámaras de seguridad, alarmas y candados para evitar accesos no autorizados, perfiles de usuarios con contraseñas que se renuevan periódicamente, registro de las

operaciones realizadas en el sistema JD Edwards a través de la función de auditoría habilitada en alguno de sus módulos, backup y recuperación, revisión de que las copias de seguridad se estén realizando, encriptación de la información a través de Microsoft Office 365, supervisión a través de indicadores de que los servicios se encuentren operativos. Por otro lado, la seguridad en redes e Internet se maneja a través de firewalls, software antivirus y software de seguridad. Además, se utiliza una red privada virtual con usuario y contraseña y certificado de seguridad para poder acceder, por lo que los datos no están directamente expuestos a Internet. Todo el acceso de dispositivos móviles se realiza a través de dicha red, y los equipos que son entregados por parte de la empresa tienen instalada la aplicación Airwatch que permite el borrado remoto de la información en el caso de robo.

Como se puede ver, los controles que se aplican en la empresa son en su mayoría correctivos, por lo que se implementan una vez que ha ocurrido un problema. Y, si bien existen algunos lineamientos que guían las actividades empresariales, no hay una adecuada documentación de las políticas de seguridad ni de los planes de contingencia. Además, no hay control interno informático como tal y tampoco se realizan auditorías informáticas con regularidad, lo que implica una gran debilidad en la seguridad informática empresarial. Todo esto expone a la empresa vitivinícola a muchas amenazas y riesgos, y la vuelve sumamente vulnerable. Es por ello que el nivel de seguridad informática es medio y precisa de mejoras para elevar su nivel, a fin de que todos los recursos informáticos se encuentren debidamente protegidos. Por más que se aplican medidas de seguridad adecuadas, las mismas deben ser mejoradas ya que no son suficientes y es imprescindible que se incorporen otras nuevas que permitan afrontar todas las vulnerabilidades, amenazas y riesgos que puedan ocurrir y permitan trabajar de manera preventiva. A su vez, es necesaria la adecuada y completa documentación de los lineamientos que rigen la protección de los recursos informáticos, y todo el personal debe ser capacitado para poder participar en la misma de la manera correcta.

En cuanto al rol de los contadores en la seguridad informática empresarial, dichos profesionales son usuarios intensivos de los sistemas informáticos y utilizan la información para realizar su trabajo, por lo que requieren la existencia de adecuadas medidas de seguridad que la protejan y garanticen su calidad. A su vez, son responsables de cumplir con todas esas medidas de seguridad. Los contadores tienen amplios conocimientos de los procesos empresariales, motivo por el cual pueden recomendar buenas prácticas de seguridad informática ya que tienen un papel fundamental en la protección y manejo de los recursos informáticos. Sin embargo, no actúan como auditores de sistemas debido a que en la empresa vitivinícola no se realizan auditorías informáticas. Sería recomendable que se comenzaran a realizar estas auditorías con regularidad y, además, que hubiera una integración entre el Departamento de Tecnología

Informática con el área contable, lo que otorgaría una mayor visión de las necesidades en materia de sistemas y su protección. Esto aumentaría el nivel de seguridad informática existente.

Para que los contadores tengan buenos y sólidos conocimientos en materia de seguridad informática y puedan aportarlos a las empresas, es fundamental que cuenten con una buena formación académica. En el caso de la Facultad de Ciencias Económicas de la Universidad Nacional de Cuyo, los estudiantes obtienen una muy buena formación debido a que el tema de la seguridad informática es abordado en distintas materias. Sin embargo, con el plan de estudios del año 2019 se incorporaron materias que son más específicas y tratan el tema con mayor profundidad y tiempo, lo que mejora la formación de los futuros profesionales. De todas formas, el autoaprendizaje y la actualización constante siempre son necesarios y ayudan a que los contadores sean más competitivos, ya que el conocimiento debe perfeccionarse de manera permanente.

Como conclusión final del trabajo de investigación y teniendo en cuenta el objetivo general perseguido, se observa que el nivel de seguridad informática existente en la empresa vitivinícola depende de la cantidad y calidad de los mecanismos utilizados para proteger la información y los recursos informáticos. Es decir, se cumple la hipótesis, por lo que mientras mejores sean los medios utilizados para proteger la información, mayor va a ser el nivel de seguridad existente. Por el contrario, si los medios que se emplean para la protección de la información no son suficientes o de calidad, el nivel de seguridad informática será menor. En el caso concreto de la empresa, los mecanismos de seguridad empleados son mejorables y no son suficientes, lo que hace que el nivel de seguridad informática sea medio, como ya se ha mencionado anteriormente. La empresa es consciente de sus debilidades en la seguridad informática, motivo por el cual se encuentra en un proceso de fortalecimiento y mejora en ese aspecto.

Resulta imprescindible que se comience a crear una mayor concientización acerca de la importancia de la seguridad informática tanto en la empresa analizada como en todas las empresas mendocinas. Es sabido que la implementación de medidas de seguridad resulta muy oneroso, pero debe ser visto como una inversión que evitará problemas en el corto, mediano y largo plazo y que, además, trae consigo innumerables beneficios. Permite a la empresa operar de manera continua y tranquila, garantizando la protección de todos los recursos informáticos y la supervivencia y competitividad empresarial. Además, al incorporar la seguridad informática a la estrategia empresarial se pueden obtener mejores resultados en el desarrollo de todas las operaciones.

REFERENCIAS

Argentina. Ministerio de Justicia y Derechos Humanos de la Nación. (2019). *Quinto muestreo de denuncias judiciales de la República Argentina: año 2017*. Ciudad Autónoma de Buenos Aires: Ediciones SAIJ.

Basaes, J.; Godoy, V. A.; Reitano, J. A.; Rojas Gaete, D. B.; Rossel Ortega, V. M. L. y Rossel Ortega, M. L. (2014). *El rol del auditor operativo: importancia del contador como auditor operativo en el contexto actual* (Trabajo final de grado). Facultad de Ciencias Económicas, Universidad Nacional de Cuyo, Mendoza.

Committee of Sponsoring Organizations of the Treadway Commission (COSO II). (2004). Gestión de Riesgos Corporativos – Marco Integrado. Técnicas de Aplicación.

Escobar, D. S. (2017). *Formación del Contador Público en Tecnología y Seguridad de la Información: propuesta de reforma curricular* (Tesis de Maestría). Facultad de Ciencias Económicas, Universidad de Buenos Aires. Recuperado de: http://bibliotecadigital.econ.uba.ar/?c=tpos&a=d&d=1502-1116_EscobarDS

Facultad de Ciencias Económicas (2018). Contador Público: Planes de estudio/ Materias. Mendoza, Argentina: Facultad de Ciencias Económicas. Recuperado de: http://fce.uncuyo.edu.ar/estudios/titulo/contador-publico#plan

Facultad de Ciencias Económicas (2018). Nuevos planes de estudio para el 2019. Mendoza, Argentina: Facultad de Ciencias Económicas. Recuperado de: http://fce.uncuyo.edu.ar/nuevo-plan-de-estudios-2019

Fowler Newton, E., (2005). *Cuestiones contables fundamentales,* Buenos Aires, Argentina: La Ley.

García Pierrat, G. y Vidal Ledo, M. J. (2016). La informática y la seguridad. Un tema de importancia para el directivo. *Infodir*, *12*(22), 47-58. Recuperado de: https://www.medigraphic.com/cgi-bin/new/resumen.cgi?IDARTICULO=63722

Laudon, K. C. y Laudon, J. P., (2012). *Sistemas de información gerencial,* México: Pearson educación.

Ley N° 20488 (1973). Ley de Ejercicio Profesional de Ciencias Económicas. Buenos Aires, Argentina.

Ley Nº 24.766 (1996). Ley de Confidencialidad. Buenos Aires, Argentina.

Ley N° 25326 (2000). Ley de Protección de los Datos Personales. Buenos Aires, Argentina.

Ley N° 26388 (2008). Código Penal. Buenos Aires, Argentina.

Observatorio de Delitos Informáticos de Latinoamérica (ODILA). (2017). Informe 2017. Recuperado de: https://www.odila.org/reporte

Peñuela Vasquez, Y. D., (2018). *Análisis e identificación del estado actual de la seguridad informática, dirigido a las organizaciones en Colombia, que brinde un diagnóstico general sobre la importancia y medidas necesarias para proteger el activo de la información* (Monografía de investigación). Universidad abierta y a distancia, Fusagasugá, Colombia.

Porter, M. E. (2008). Las cinco fuerzas competitivas que le dan forma a la estrategia. *Harvard Business Review, 86(*1), 58-77. Recuperado de: https://www.academia.edu/5151135/Las_5_fuerzas_competitivas._Michael_Porter

Programa de la asignatura Auditoría Operativa y de Sistemas Computarizados (2019). Facultad de Ciencias Económicas, Universidad Nacional de Cuyo, Mendoza, Argentina.

Programa de la asignatura Computación (2018). Facultad de Ciencias Económicas, Universidad Nacional de Cuyo, Mendoza, Argentina.

Programa de la asignatura Sistemas Administrativos de Información Contable (2019). Facultad de Ciencias Económicas, Universidad Nacional de Cuyo, Mendoza, Argentina.

Ramió Aguirre, J. (2006). *Libro Electrónico Seguridad Informática y Criptografía*. Madrid, España. 6ª Edición V 4.1.

Real Academia Española (2014). Información. En Diccionario de la lengua española (23° ed.). Recuperado de: https://dle.rae.es/?id=LXrOqrN

Real Academia Española (2014). Sistema. En Diccionario de la lengua española (23° ed.). Recuperado de: https://dle.rae.es/?id=Y2AFX5s

Sánchez, E. L. y Lettry, R. N. (2008). Los sistemas de información de costos en empresas vitivinícolas, *Revista de la Facultad de Ciencias Económicas 2008*, 127, 79-103. Recuperado de: http://bdigital.uncu.edu.ar/8959

Sánchez Valriberas, G. (2001). Control interno y auditoría informática. En Piattini, M. G. y Del Peso, E. (Ed.), *Auditoría informática. Un enfoque práctico* (pp. 25-43). México: Alfaomega.

Saroka, R. H., (2002). *Sistemas de información en la era digital*, Buenos Aires, Argentina: Fundación OSDE.

Voutssas M., J. (2010). Preservación documental digital y seguridad informática. *Investigación Bibliotecológica, 24*(50), 127-155. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008&lng=es&nrm=iso.

Zegarra, O. S. (2014). El impacto de la Informática en la formación del Contador Público: realidades y expectativas. *Quipukamayoc, 1*(2), 63-72. Recuperado de: http://revistasinvestigacion.unmsm.edu.pe/index.php/quipu/article/view/6068

BIBLIOGRAFÍA CONSULTADA

Alfonso Martínez, Y., Blanco Alfonso, B. y Loy Marichal, L. (2012). Auditoría con Informática a Sistemas Contables. *Revista de Arquitectura e Ingeniería, 6*(2), 1-14. Recuperado de: http://www.redalyc.org/articulo.oa?id=193924743004

Aplimedia. [Aplimedia]. (2017, Septiembre 25). Qué es un ERP y para qué sirve - Definición de ERP – Aplimedia [Archivo de video]. Recuperado de: https://www.youtube.com/watch?v=7_r7rGHmh1c

ASMAZEmpresario. [ASMAZEmpresario]. (2012, Noviembre 19). La importancia de una buena administración [Archivo de video]. Recuperado de: https://www.youtube.com/watch?v=Op5zcComvEE

Ley N° 11723 (1933). Ley de la Propiedad Intelectual. Buenos Aires, Argentina.

Ley N° 22362 (1980). Ley de Marcas y Designaciones. Buenos Aires, Argentina.

Ley N° 24481 (1995). Ley de Patentes de Invención y Modelos de Utilidad. Buenos Aires, Argentina.

Ley N° 25506 (2001). Ley de Firma Digital. Buenos Aires, Argentina.

Orellana Benavides, L. A., Hernández Vásquez, R. C. (2003). *Seguridad en redes de datos*. (Tesis de Ingeniería no publicada). Universidad Don Bosco, San Salvador, El Salvador CA. Recuperado de: http://rd.udb.edu.sv:8080/jspui/handle/11715/281

Quiroz-Zambrano, S. M. y Macías-Valencia, D. G. (2017). Seguridad en Informática: consideraciones. *Dominio de las ciencias, 3*(5), 676-688. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824