Seguridad de la Información en una Empresa de Seguridad Privada de Pereira

Alejandra María Aristizábal Arroyave

Diana Carolina Ruiz Arias

Yamileth Valencia Ortiz

Fundación Universitaria del Área Andina

Facultad de Ciencias Administrativas, Económicas y Financieras

Administración de Empresas

Pereira

2018

Seguridad de la Información en una Empresa de Seguridad Privada de Pereira

Proyecto de investigación para optar por el título de Administradoras de Empresas

Alejandra María Aristizábal Arroyave

Diana Carolina Ruiz Arias

Yamileth Valencia Ortiz

Andrés Bayer Agudelo

Administrador de Empresas, Especialista en Gestión del Talento Humano,

Candidato MBA

Fundación Universitaria del Área Andina

Facultad de Ciencias Administrativas, Económicas y Financieras

Administración de Empresas

Pereira

2018

Tabla de contenido

Resumen

La presente investigación tiene como propósito determinar el nivel de seguridad de la información en una empresa de seguridad privada de la ciudad de Pereira, de acuerdo con la norma ISO/IEC 27001:2013, teniendo en cuenta que la información es uno de los activos más importantes dentro de la organización y requiere ser protegida y controlada para evitar el mal uso de esta, por esto se plantean dos objetivos específicos y uno general, con el fin de detectar los factores que impulsaron la creación, implementación y seguimiento de un sistema de seguridad de información a nivel organizacional.

Dentro del marco de antecedentes se plasman aportes relevantes que ayudan a soportar y desarrollar la investigación; además, se adicionan términos que ayudan a la contextualización del tema propuesto, se anexan los instrumentos aplicados a una empresa de seguridad privada como evidencia y se incluyen las conclusiones y recomendaciones generales para contribuir a una mejor comprensión al momento de su lectura.

Palabras claves: seguridad de la información, ISO 27001, sistemas de seguridad de TI, seguridad en TI, ISO 27001 en seguridad privada, protección de la información.

Abstract

This project has as purpose to determine the level of information security in a private security company from Pereira, according to the ISO/IEC 27001:2013, taking into account that the information gather by this company is one of the most important assets they have and it must be protected and control to avoid any misuse. Due to the importance of it, we propose two specific objectives and a general one to detect the factors that lead to the creation, implementation and the follow up of an information security system in the company.

Within the framework of records we evidence some relevant information that help us to back up and develop the information, additionally, we add some terms that can help in the contextualization of this research project. We attach the instruments use by the private security company as evidence and include the final conclusions and general recommendations to contribute to a better understanding by the time of the reading.

Key words: information security, ISO 27001, security systems, security in TI, ISO 27001 in private security, protection of information.

Introducción

Dentro de esta investigación se hace referencia a la importancia que tiene el manejo de información para todas las organizaciones y aún más para las empresas de seguridad privada, donde la responsabilidad de vigilar, defender y proteger los bienes y posesiones de sus clientes es mucho mayor; gracias a esto, suelen convertirse en el blanco de diversas amenazas, por este motivo, se busca determinar el nivel de seguridad de la información dentro de una de estas empresas, de acuerdo con la norma ISO/IEC 27001:2013, analizando los factores que ayudaron a impulsar la implementación del sistema y verificando las condiciones iniciales en las que se encuentra, con el fin de aportar herramientas que serán de ayuda para suplir falencias encontradas, beneficiando de este modo tanto a la organización como a sus usuarios; pues se considera que como administradores de empresas es pertinente conocer los sistemas, métodos y herramientas que existen para proteger la información.

Por lo anterior, se toman como referencia teorías, investigaciones y sucesos con la información necesaria para conseguir los aportes correctos, se explican conceptos y manejos que se evidenciaron en investigaciones previas al desarrollo de esta investigación, con la respectiva aplicación y conclusión de cada una.

Definición del Problema

Planteamiento del Problema

El termino seguridad se asocia a “la propiedad de algo donde no se registran peligros, daños ni riesgos” (Definición.de, 2018); esta se desagrega en varios tipos como son: la seguridad activa, de la información, ciudadana, y jurídica, entre otras. Respecto a la seguridad de la información, Morales (2013, pág. 33) menciona que las empresas de seguridad privada tienen la responsabilidad de vigilar, defender y proteger los bienes y posesiones de sus clientes. Entre sus tareas más comunes, está la de manejar una gran cantidad de información (tanto física como digital) que aporta datos relevantes de clientes y proveedores, información que se describe de forma holística en estados financieros, información contable, bases de datos, manuales de función, información personal e informes acerca de los procesos que se llevan a cabo dentro de esta actividad. En este sentido, las organizaciones de seguridad privada presentan como principal objetivo velar por el cuidado de la información de las empresas u hogares a los cuales prestan sus servicios, ya que son estas las que tienen acceso tanto a sus instalaciones como a la información restringida para el público en general, ya sea accediendo de forma personal o por medio de cámaras de seguridad.

Sin embargo, se evidencian varias connotaciones que enmarcan el mal uso de un sistema de la información, entre las cuales se observan: (1) no dar un uso correcto a la información, (2) no contar con un equipo de trabajo confiable o (3) no tener implementado un sistema de la gestión de la información efectivo y eficiente; cuando se tienen falencias en alguno de los anteriores aspectos, se puede generar el riesgo de perder la ventaja competitiva empresarial y la confianza de los clientes, ocasionando pérdidas monetarias y perjudicando a las personas que se

encuentren involucradas.

Tras lo descrito, las empresas de seguridad privada por su objeto de ser, suelen convertirse en el blanco de diversas amenazas por parte de competidores, clientes y *hacktivistas*, lo que puede generar la alteración, copia o eliminación de dichos datos.

De acuerdo con los datos recopilados en el estudio ESET Security Report 2017, Colombia es el tercer territorio latinoamericano más afectado por actividad maliciosa, con un 46,7% de empresas infectadas. Además, el 74% de las organizaciones de Latinoamérica tienen implementada una política de seguridad, lo que indica que por lo menos 1 de cada 4 empresas no han definido aún este tipo de controles para garantizar la seguridad de la información y solo el 12% de las empresas tiene un área dedicada exclusivamente a la seguridad de la información (ESET, 2017).

Según estudios realizados por la Certicámara en el segundo semestre del 2016, Colombia es considerada una de las naciones más atractivas para los delincuentes informáticos en América Latina; muestra de ello es que el 25% de los ciberataques registrados en el 2015 se originaron en esta parte del mundo (Dinero, 2016); razón por la cual, las empresas de seguridad privada deben trabajar con personal idóneo y contar con sistemas eficientes para la seguridad de la información (Semana, 2014).

Por tanto, se busca determinar el nivel de seguridad de la información en una empresa de seguridad privada, ubicada en la ciudad de Pereira, de acuerdo con la norma ISO/IEC 27001:2013, durante el segundo semestre del año 2017.

Formulación del Problema

Con el desarrollo de la presente investigación, se pretende dar respuesta al siguiente interrogante:

¿Cuál es el nivel de seguridad de la información en una empresa de seguridad privada, ubicada en la ciudad de Pereira, de acuerdo con la norma ISO/IEC 27001:2013, durante el segundo semestre del año 2017?

Objetivos

Objetivo General

Determinar el nivel de seguridad de la información en una empresa de seguridad privada, ubicada en la ciudad de Pereira, de acuerdo con la norma ISO/IEC 27001:2013, durante el segundo semestre del año 2017.

Objetivos Específicos

Analizar los factores que impulsaron la implementación del sistema de seguridad de la información en la empresa.

Verificar las condiciones iniciales del sistema de seguridad de la información, frente a lo que estipula la norma ISO/IEC 27001:2013.

Describir el nivel de seguridad de la información de la empresa, de acuerdo a la norma ISO/IEC 27001:2013.

Justificación

La importancia de la presente investigación, se enmarca en que se analizará el nivel de seguridad de la información en una empresa de seguridad privada de la ciudad de Pereira, de acuerdo con la norma ISO/IEC 27001:2013, con el fin de aportar a esta organización herramientas que sean de ayuda para suplir las falencias que se encuentren, beneficiando de este modo tanto a la organización, como a sus usuarios, ya que la evolución tecnológica hace que la información sea más accesible y este más desprotegida, lo que lleva a pensar de qué manera o a quién se le otorga el poder de manejar dicha información.

Cuando no se tiene un control sobre la información manejada por la organización, se pueden filtrar datos confidenciales acerca de los procesos internos, información de los clientes, colaboradores y más, lo que puede ocasionar estragos económicos y pérdidas de gran consideración para todas las personas involucradas, además de generar controversias a nivel social, personal y posiblemente político.

Cuando los datos de los procesos empresariales caen en manos inescrupulosas, se pueden generar pérdidas, debido a que otras empresas pueden implementar algunos de sus procesos o van a utilizar sus estrategias de venta y de producción a su favor, perdiendo la ventaja competitiva y creando una competencia desleal. Por otro lado, los clientes perderán credibilidad en las organizaciones y optarán por preferir a su competencia.

Además de esto, si se llegan a afectar los derechos o la privacidad de alguien, posiblemente interpongan demandas o medidas que impliquen indemnizar o pagar ciertos dineros que no estaban presupuestados, generando impactos económicos negativos a la organización y problemas personales a quienes se les haya violentado la privacidad.

En las empresas del sector de la seguridad privada debe existir un mayor compromiso y control en el manejo de la información, debido a que estas tienen acceso no solo la información confidencial de su empresa, sino que se desempeñan en el interior de otras organizaciones, conociendo sus procesos y su información confidencial, lo que hace que sean más las personas involucradas en el manejo de los datos, aumentando el riesgo en la seguridad de la información de las empresas a las cuales les prestan sus servicios.

Como administradores de empresas, es pertinente conocer los sistemas, métodos y herramientas que existen para proteger la información, ya que este es uno de los mayores activos de las organizaciones; además, con este conocimiento se podrá ser más estratega y escoger mejor a las personas que tendrán acceso a la misma. Al tener protegida la información o los datos de relevancia en las organizaciones, no solo se tendrá un mayor control acerca de todos los procesos y de todo lo que sucede dentro de esta, sino que será un aspecto que aportará un mayor grado de competitividad y un valor agregado.

Marco Referencial

Marco Teórico

Agustín Cuevas indica que su teoría de la información nace de la técnica de las telecomunicaciones y desborda en la actualidad un dominio de forma muy notable; la información circula en los sistemas físicos, biológicos, sociales y técnicos, en donde la física del siglo pasado ha reconocido un gran número de fenómenos sin enlace aparente (mecánicos, térmicos, eléctricos y químicos), las diferentes formas de una misma entidad, la energía y el progreso que esta visión unitaria ha permitido realizar a las ciencias y técnicas de una forma análoga, un tratamiento unitario de la transmisión de la información, a través de una abstracción y un soporte físico, puede y debe proporcionar a la ciencia y técnica de nuestro tiempo un beneficio comparable (Cuevas Agustín, 1975, pág. 89). Con la aparición del radar surgieron varios problemas; en esencia consistían en que no se trataba con una sola señal, sino con un conjunto de posibles señales (trayectorias de avión), más ruidos impredecibles, donde se busca seleccionar la señal de información eliminando los ruidos; debido a este problema nace la que sería la solución, por Warren Wiener, que en épocas de guerra produjo una abundante documentación muy complicada y escrita en papel amarillo, por lo que afectuosamente se le denominaba “el peligro amarillo”, pero que a su vez resolvía el difícil problema. Durante y después de la guerra surge otro matemático llamado Claude Shannon quien se interesó por el problema de la comunicación y comenzó por estudiar todos los sistemas que habían, buscando un método básico de comparar sus métodos. En el mismo año (1948) en que Wiener publicó su “cibernética”, la cual trata de la comunicación y el control, Shannon publicó un artículo en dos partes, el cual se considera el auténtico fundamento de la teoría de la información. Shannon ha

sido conocido con asuntos tales como mensajes codificados elegidos de un conjunto conocido y que pueden ser transmitidos con precisión y rapidez, en presencia del ruido, mientras que Wiener se ha asociado al campo de la extracción de señales de un conjunto dado, de ruido de tipo conocido; sin embargo tanto Wiener como Shannon trataron el problema, no con una señal simple, sino de forma que se pudiera hacer adecuadamente con cualquier señal seleccionada de un grupo de señales posibles (Cuevas Agustín, 1975, pág. 69).

Por otra parte se observa el principio de fortificación, el cual hace referencia a "una de las disciplinas donde más se dejó sentir la influencia de todas estas importantes innovaciones científico-técnicas. De hecho, fue de tal envergadura el impacto de la nueva mentalidad renacentista en la milicia que, a lo largo del período estudiado, se asiste a la configuración y posterior consolidación de una nueva manera de concebir y afrontar la guerra" (Sánchez Orense, 2012, pág. 23).

Pedro de Lucuze fue un Mariscal de Campo de los Reales Ejércitos y Director de la Real Academia Militar de Matemáticas establecida en Barcelona. Él creó un diccionario acerca de los Principios de Fortificación, el cual contiene las definiciones de los términos principales de las obras de Plaza y de Campaña, con una idea de la conducta regularmente observada en el Ataque y Defensa de las Fortalezas. Este diccionario se utilizó como una estrategia militar para comunicarse y dejar mensajes de señalización que nadie más pudiera entender o descifrar, mediante el uso de abreviaturas y símbolos (Lucuze, 1772).

Del mismo modo se hace referencia a la criptología, debido a que tiene un encanto ligeramente tenebroso en su desarrollo histórico de acuerdo con lo investigado por José María Molina Mateos, donde tiene la facilidad de combinar aspectos como el juego de la inteligencia, la reflexión científica, los problemas de la comunicación lingüística y la transmisión de

mensajes. Pero es, ante todo, una disciplina científica de gran actualidad (Molina Mateos, 2000, pág. 8)**,** donde es considerado seriamente para matemáticos, informáticos, especialistas en estadísticas, ingenieros de telecomunicaciones y se espera que también lo sea para juristas, sociólogos y politólogos, por su incidencia en la sociedad actual. "Además de criptografía, este sistema de escribir ha recibido los nombres de criptología, poligrafía, esteganografía, escritura cifrada, etc." (Molina Mateos, 2000, pág. 10). "No obstante, la norma ISO 7492-2 define a la criptografía como la disciplina que estudia los principios, métodos y medios de transformar los datos, con objeto de ocultar la información contenida en los mismos, detectar su modificación no autorizada y/o prevenir su uso no permitido" (Molina Mateos, 2000, pág. 15).

Para Andrea Sgarro, la criptografía es la disciplina encargada del estudio de los códigos secretos, para diseñar cifrarios que soporten los ataques del criptoanálisis, mientras que para José Pastor, esta es una ciencia que estudia las propiedades tanto de comunicaciones electrónicas como digitales en un ambiente vulnerable y de desconfianza mutua entre los comunicantes (Molina Mateos, 2000, pág. 12).

Uno de los mayores exponentes y grandes autores acerca de la criptografía es Auguste Kerckhoffs, que por medio de sus principios explica cómo un sistema de tipo estratégico debe poseer como característica fundamental la siguiente: la seguridad de un sistema estratégico se basa totalmente o de forma esencial en el secreto de la clave, de forma que si el adversario descubre el tipo de cifrado utilizado, pero ignora la clave empleada para descifrarlo, el secreto del mensaje queda garantizado, no obstante, los principios en los que se basa su teoría son 6. El primero de estos principios indica que el sistema de cifrado debe ser impenetrable, si no en teoría, al menos en la práctica; el segundo menciona que el hecho de que el sistema se vea comprometido no debe dañar a los corresponsales, el tercero es que la clave debe ser fácil de

memorizar y fácil sustituir, el cuarto indica que los criptogramas deben ser idóneos para su transmisión por telégrafo, el quinto menciona que el aparato y los documentos de cifrado deben ser fáciles de transportar, siendo necesario que la operación de cifrado la pueda realizar una sola persona; por último, el sexto principio dice que el sistema debe ser sencillo, no se debe basar en el conocimiento de largas listas de normas ni requerir esfuerzos mentales excesivos. A partir de 1977 se va perdiendo el concepto mítico de secreto atribuido a todo lo relacionado con la criptología, y da paso a "La información sobre la información", que viene a añadir al valor en sí misma, el valor de los soportes, medios tecnológicos que la sustenta, y múltiples acciones de los servicios de inteligencia, creando una situación en la que el secreto no es el instrumento, sino la información que se protege (Molina Mateos, 2000).

Además, está la esteganografía, que es definida por Álvaro Gómez Vieites como la escritura oculta o escritura encubierta, que se encarga de estudiar "todas las posibles técnicas utilizadas para insertar información sensible dentro de otro fichero, denominado "fichero contenedor" (que podría ser un gráfico, un documento o un programa ejecutable), para tratar de conseguir que pueda pasar inadvertida a terceros, y solo pueda ser recuperada por parte de un usuario legítimo empleando para ello un determinado algoritmo de extracción de la información" (Gómez Vieites, 2014, pág. 53). "Las técnicas esteganográficas modernas utilizan aplicaciones informáticas para ocultar la información. Para ello, se utiliza un fichero contenedor como soporte para camuflar una serie de bits con la información sensible que se desea ocultar" (Gómez Vieites, 2014, pág. 54).

La ciencia de la esteganografía lingüística también puede definirse como aquel conjunto de algoritmos robustos que permiten la ocultación de información, típicamente binaria, utilizando textos en lenguaje natural como tapadera. Esta utiliza principios de la esteganografía e

incorpora recursos y métodos de la lingüística computacional como análisis automático del contenido textual, generación automática de texto, análisis morfosintácticos, lexicografía computacional, descripciones ontológicas, etc., para crear procedimientos públicos no triviales según los principios de Kerckhoffs (Consejo superior de investigaciones científicas, 2013).

Con la presente investigación se busca dar a conocer cada uno de los numerales de la Norma Técnica Colombiana ISO/IEC 27001:2013, con el fin de analizar el nivel de seguridad de la información personal en las empresas Seguridad Nacional Ltda. y Estatal de Seguridad Ltda., ubicadas en la ciudad de Pereira.

La Norma Técnica Colombiana ISO/IEC 27001:2013 (ICONTEC, 2013) es un instrumento que se puede aplicar mediante una decisión estratégica a todas las organizaciones de cualquier sector o tamaño, "esta norma especifica los requisitos para establecer implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización" que permite que una empresa sea certificada.

Consta de 10 capítulos de los cuales 3 son generalidades y los demás son lineamientos que se deben seguir para obtener la certificación.

El primer capítulo indica el objetivo y campo de aplicación. Allí se especifican los requisitos necesarios para lograr una mejora continua del sistema de seguridad de la información dentro del contexto de la organización.

El segundo capítulo es el de referencias normativas, donde indican que toda la información que se maneje dentro del documento debe de ser previamente citada y referenciada.

El tercer capítulo de términos y definiciones menciona que se aplican los términos y condiciones especificados en la norma ISO/IEC 27000.

El cuarto capítulo es el del contexto de la organización.

4.1 Conocimiento de la organización y de su contexto: se deben determinar cuestiones internas y externas pertinentes para el propósito y que de alguna manera afecte la capacidad de lograr los resultados propuestos.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas: determinar las partes interesadas y sus requisitos legales y reglamentarios para el sistema de gestión de seguridad de la información.

4.3 Determinación del alcance del sistema de gestión de la seguridad de la información: la organización determina límites y aplicabilidad teniendo en cuenta las especificaciones de los numerales 4.1 y 4.2 documentando toda la información.

4.4 Sistema de gestión de la seguridad de la información: esta norma especifica los requisitos para establecer implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización.

El quinto capítulo habla acerca de liderazgo.

5.1 Liderazgo y compromiso: la dirección de cada organización debe mostrar el compromiso y liderazgo frente al S.G.S.I:

Se deben establecer las políticas y objetivos de la seguridad de la información; además, estos deben ser compatibles con los de la dirección estratégica de cada organización, para asegurar la integración del S.G.S.I en cada proceso de la misma.

Logrando así la disponibilidad de los recursos, difundiendo la importancia de la gestión de seguridad de la información de manera eficaz y conformidad del sistema, las organizaciones deben asegurar mediante la óptima implementación del S.G.S.I los resultados previstos desde el inicio.

Se debe presentar un apoyo y dirigir correctamente a cada integrante de la organización

para que puedan contribuir positivamente con el sistema, alcanzando una mejora continua donde se presente el apoyo a los roles pertinentes de la dirección, para demostrar el liderazgo aplicado a sus áreas de responsabilidad.

5.2 Política: las organizaciones deben de establecer una política de seguridad de la información adecuada con el propósito de cada una, donde se incluyan los objetivos de S.I o proporcionen el marco de referencia para la creación de estos mismos. Debe demostrar el compromiso por cumplir los requisitos relacionados con la seguridad en la información y por lograr la mejora continua de este sistema.

Cada política de seguridad de la información debe estar disponible, como información documentada, difundirse al interior de la organización y estar disponible para las partes interesadas.

5.3 Roles, responsabilidades y autoridades de la organización: la alta dirección debe asegurar que toda responsabilidad y autoridad en cada rol pertinente a la seguridad de la información se asigne y se comunique.

Donde se logre asegurar que el S.G.S.I este conforme a los requisitos de la norma para informar a sus miembros del desempeño del sistema dentro de la organización.

El sexto capítulo habla acerca de planificación.

6.1 Acciones para tratar riesgos y oportunidades.

6.1.1 Generalidades: cada organización al realizar la planeación del S.G.S.I. debe determinar los riesgos y oportunidades que se necesitan tratar; para asegurar que el sistema alcance los resultados previstos, para reducir o prevenir efectos indeseados y alcanzar la mejora continua.

Se deben planificar las acciones que traten dichos riesgos y oportunidades, para

integrarlas e implementarlas dentro del sistema y evaluar su eficacia dentro de cada organización.

6.1.2 Valoración de riesgos de la seguridad de la información: se debe definir y aplicar un proceso que logre la valoración del riesgo de la S.I que mantenga y establezca criterios de aceptación de riesgos del S.G.S.I.

Logrando resultados consistentes, válidos y comparables que ayuden a identificar riesgos de la seguridad de la información.

Para visualizar los riesgos asociados a posibles pérdidas de confidencialidad, integridad y disponibilidad de la información, logrando identificar los dueños de los riesgos.

También identificar las consecuencias potenciales que son el resultado de los riesgos encontrados, realizar una valoración donde se plantee la posibilidad de que ocurran y en qué nivel de riesgo se encuentran.

Comparar los resultados del análisis frente a criterios de riesgos planteados dentro de la norma y priorizar los riesgos que se hallaron para su tratamiento.

6.1.3 Tratamiento de riesgos de la seguridad de la información: se debe lograr la aplicación y definición del proceso de tratamientos de riesgos de la S.I, para seleccionar las ocupaciones más apropiadas, teniendo en cuenta los resultados de valoración; determinando los controles que sean necesarios para implementar las opciones escogidas para el tratamiento del riesgo.

Compararlos con los controles de la norma y los anexos dentro de la misma para que no se vaya a omitir ninguno; aplicar cada uno si es necesario y justificar su inclusión ya sea para su implementación o no.

Formular el plan para el tratamiento del riesgo y obtener por parte de los dueños del

riesgo la aprobación para la mejora de estos dentro de la organización.

6.2 Objetivos de seguridad de la información y planes para lograrlo: se deben establecer los objetivos de S.I en las funciones y niveles pertinentes y estos deben ser coherentes con la política de seguridad de la información, ser medibles (si es posible) teniendo en cuenta los requisitos aplicables y los resultados de la valoración para el tratamiento de los riesgos; ser comunicados y actualizados, según sea apropiado.

La organización debe determinar, mediante la planificación para alcanzar sus objetivos, qué se va a hacer, los recursos requeridos, quién tendrá la responsabilidad, cuándo finalizará y cómo van a realizar la evaluación de los resultados.

El séptimo capítulo es de soporte.

7.1 Recursos: la organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.

7.2 Competencia: determinar y asegurar que las personas que realizan tareas que afecten el desempeño de la seguridad de la información, tengan la competencia necesaria en cuanto a educación, formación y experiencia, lo cual debe estar evidenciado con la información documentada. Se deben tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de estas acciones.

7.3 Toma de conciencia: las personas que trabajan bajo el control de la organización deben tomar conciencia de la política de seguridad de la información, su contribución a la eficacia del SGSI, los beneficios de la mejora del desempeño de la seguridad de la información y las implicaciones de las no conformidades con los requisitos del SGSI.

7.4 Comunicación: determinar las necesidades de comunicación interna y externa relacionadas con el SGSI, como qué, cuándo, quién, a quién y cómo se debe comunicar.

7.5 Información documentada.

7.5.1 Generalidades: el SGSI debe incluir la información documentada requerida por la norma y la que la organización considere necesaria para la eficacia del mismo, además del tamaño de la organización, tipo de actividades, procesos, productos, servicios, la complejidad de sus procesos y sus interacciones y la competencia de las personas.

7.5.2 Creación y actualización: cuando se crea y actualiza la información documentada se debe asegurar que la identificación, descripción, formato, medios de transporte, revisión y aprobación sean apropiados.

7.5.3 Control de la información documentada: se debe asegurar que la información documentada requerida por el SGSI y por esta norma esté disponible y adecuada para su uso, donde y cuando se necesite; además, se debe proteger de forma adecuada. También se deben controlar actividades como distribución, acceso, recuperación, uso, almacenamiento, preservación, control de cambios, retención y disposición.

El octavo capítulo es de operación.

8.1 Planificación y control operacional: se debe planificar, implementar y controlar los procesos para cumplir los requisitos, acciones que se indican dentro de la norma y establecer planes para lograr los objetivos. La información debe estar documentada para tener la confianza en que los procesos se han realizado según lo planificado y tener el control sobre estos. Se deben controlar las consecuencias de los cambios no previstos y tomar acciones para mitigar sus efectos adversos. Se deben controlar los procesos contratados de forma externa.

8.2 Valoración de riesgos de la seguridad de la información: se deben hacer valoraciones de riesgos de la seguridad de la información a intervalos planificados o cuando propongan u ocurran cambios significativos conservando la información documentada de dichas valoraciones.

8.3 Tratamiento de riesgos de la seguridad de la información: se debe implementar el plan de tratamiento de riesgos de la seguridad de la información y conservar la información documentada del mismo.

El noveno capítulo es de evaluación y desempeño.

9.1 Seguimiento medición análisis y evaluación: la organización evaluará la eficacia y el desempeño de la seguridad de la información determinando lo siguiente: medir los procesos y realizar seguimiento a los controles de la seguridad de la información para asegurar resultados válidos que puedan ser comparables y reproducibles conservando la información previamente documentada.

9.2 Auditoría interna: la organización llevará a cabo auditorías internas para proporcionar información acerca de si el sistema de gestión de la información cumple los requisitos de la organización y los requisitos de la norma, y si está implementando eficazmente. También debe planificar e implementar métodos que ayuden a la elaboración de los informes, teniendo en cuenta los procesos involucrados y resultados de auditorías previas.

9.3 Revisión por la dirección: la organización debe revisar el sistema de gestión de la información a intervalos planificados para asegurarse de su conveniencia, adecuación y eficacia continua, siendo consideradas las revisiones previas por la dirección, cambios en cuestiones internas y externas pertinentes al sistema y retroalimentación sobre el desempeño de la seguridad de la información como lo son no conformidades, acciones correctivas, seguimiento y resultados.

El décimo capítulo es de mejora.

10.1 No conformidades y acciones correctivas: cuando se presenta una no conformidad se deben tomar acciones para controlar y corregir, haciendo frente a la consecuencias. Se deben evaluar y determinar las acciones para eliminar las causas de la no conformidad con la idea de

que no vuelva a ocurrir, implementando y desarrollando cualquier acción necesaria que esté dentro de las especificaciones de las no conformidades.

10.2 Mejora continua: la organización debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión de la seguridad de la información.

Marco de Antecedentes

Para el caso del presente apartado se muestra la revisión de literatura que describen en síntesis algunas experiencias, tanto internacionales como nacionales y regionales, con el propósito de tener una visión más holística de los casos evidenciados sobre el tema tratado en el desarrollo del documento.

En el ámbito internacional, se encuentra el Informe de McAfee Labs sobre amenazas hasta junio de 2017, realizada por (Beek, y otros, 2017) por medio de encuestas, en el cual se encontró que la mayor cantidad de incidentes se presentan en América en el sector público, mediante el *malware* Mirai y el país que alberga más servidores de control de redes de bots es Estados Unidos.

En el mismo sentido, (Matalobos Veiga, 2014) realizó un análisis de riesgos de seguridad de la información por medio de una metodología de análisis y gestión de riesgos, gracias a la aplicación de cuestionarios que permitieron identificar cuáles son las áreas que requieren mayor atención, además de las medidas de seguridad necesarias para proteger la información de la organización.

Así mismo, (Sánchez Solá, 2013) utilizó el método inductivo-deductivo y el histórico-lógico para el diseño de un sistema de gestión de la seguridad de la información para comercio electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de Quito, mediante el cual pudo observar el deficiente interés que tienen las gerencias de las empresas privadas respecto al manejo de políticas que ayuden a mantener un adecuado SGSI, además que en Ecuador no existe una cultura organizacional para prevenir incidentes que afecten a la seguridad de la información.

Por su parte, (Panda Security, 2017) realizó el Informe Trimestral Pandalabs T2 2017

mediante unos test, con los que detectó que en los equipos domésticos y de pequeñas empresas está el mayor número de ataques realizados por medio de *malwares* desconocidos, mientras que en las medianas y grandes empresas es de menos de la mitad. Lo anterior se debe a que son más vulnerables y no invierten tanto en *softwares* para su protección. Además, se encontró que el país más atacado a nivel mundial es El Salvador con un 10,85% y Colombia ocupa el séptimo lugar con un 8,29% de ataques. Es necesario extremar las medidas de seguridad utilizadas, ya que cada vez son más avanzados los *malwares* que se utilizan y tienen un mayor alcance. Se recomienda utilizar el *sofware* de seguridad más adecuado de acuerdo con la amenaza a la cual se esté enfrentado; además, es de vital importancia recopilar toda la información que se pueda del *malware* para analizarla y poder elevar el nivel de protección y tener listos diversos planes de contingencia.

De igual forma, (Solarte Solarte, Enríquez Rosero, & Benavides, 2015) realizaron una investigación con el fin de desarrollar habilidades en los ingenieros de sistemas, que les permitan conducir proyectos de diagnóstico, para la implementación e implantación de sistemas de gestión de seguridad de la información alineado con el estándar ISO/IEC 27001 y el sistema de control propuesto en la norma ISO/IEC 27002. Lo anterior lo realizaron por medio de las técnicas de la observación directa mediante visitas programadas y entrevistas aplicadas a los profesionales de sistemas encargados de la administración del área informática, la seguridad informática y usuarios de los sistemas. Posteriormente aplicaron una lista de chequeo basada en la norma, para verificar la existencia de controles de seguridad en los procesos organizacionales. Con base en lo anterior, se evidenció que es imperativo el apoyo y compromiso real de la gerencia o administración para el proceso de diseño, implementación e implantación de un SGSI de acuerdo con los resultados de la auditoria; además, se deben formalizar los procesos y procedimientos

que así lo requieran y documentarlos, en la mayoría de casos se verificó la no existencia de procesos por lo cual se deben definir los procesos y procedimientos faltantes; también es necesario implementar un sistema de control de seguridad informático estableciendo mecanismos que permitan la medición permanente, orientado hacia la mejora de la seguridad de la información y al diseño, implementación e implantación de un SGSI en cada una de las organizaciones de acuerdo a sus necesidades. De todo esto se observó que no existe una cultura de seguridad de la información dentro de las organizaciones, tampoco existen sistemas de control de seguridad informática y de información, y mucho menos, procesos y procedimientos documentados para protección de la información. De los resultados obtenidos se puede concluir que no existe un compromiso real de las directivas, que los empleados no son conscientes de los objetivos que se pretenden con el sistema de control de seguridad de la información y que el personal del área informática no está capacitado para asumir esta responsabilidad.

En línea de lo anterior, (Ware, 2018) llevó a cabo una investigación con la cual buscaba obtener más información sobre el estado de las amenazas internas y las soluciones disponibles para predecirlas y prevenirlas. Esta investigación se llevó a cabo por medio de encuestas aplicadas a compañías de todos los tamaños y sectores, encuestando desde gerentes del área de TI hasta técnicos. A raíz de los problemas encontrados por medio de las encuestas, se concientizó a las empresas acerca de los riesgos a los cuales están expuestos y se desarrolló el programa Constellation que permite tener una postura más dinámica y predictiva para tomar decisiones más rápidas y acelerar la remediación para una protección más efectiva de sistemas, datos, instalaciones y personas críticas. Además, se logró detectar que los datos de los clientes fueron los más vulnerables a ataques internos (63%), seguidos por los datos financieros (55%) y la propiedad intelectual (54%); también se identificó que los usuarios privilegiados representan

la mayor amenaza interna para las organizaciones, seguido por los contratistas y consultores, y los empleados regulares; el 74% de las organizaciones se sienten vulnerables a las amenazas internas, sin embargo, menos de la mitad tienen los controles adecuados en el lugar para evitar un ataque interno.

Seguido de lo anterior, (Pallas & Corti, 2016) buscó dar los lineamientos metodológicos de aplicación sistemática para el diseño, implantación, mantenimiento, gestión, monitoreo y evolución de un SGSI según la norma ISO 27.001, para una empresa perteneciente a un grupo empresarial, la cual además está subordinada con respecto a una empresa principal del grupo, además de ilustrar con un Caso de Estudio, los principales aspectos de aplicación de la misma. Lo anterior lo realizó utilizando tanto el modelo cualitativo como el cuantitativo, mediante observación en campo, entrevistas y test. Gracias a esta investigación, presentó una metodología adecuada a un grupo empresarial, que busca integrar lo mejor de cada uno de los enfoques analizados; se incluye una propuesta de organigrama de Seguridad que compatibiliza la jerarquía estructural del grupo y las necesidades de un SGSI. Adicionalmente se incursiona en la aplicación de técnicas de grafos para la valoración de activos; se formaliza el concepto en términos de propiedades y algoritmia de grafos, y se define con una visión propia del tema, un algoritmo para el ajuste contemplando valoraciones cualitativas y cuantitativas y dependencias parciales y/o totales entre activos. También se describen características y funcionalidades deseables de una herramienta de *software* de apoyo a la metodología. Finalmente se analiza la aplicación de la metodología a un Caso de Estudio, en particular, un \2018Internet Service Provider\2019 (ISP) integrado verticalmente con una \2018TelCo\2019 (empresa de Telecomunicaciones). En el mismo se analizan las particularidades del caso de estudio: los estándares y recomendaciones internacionales específicos, el modelo organizacional aplicable al

negocio, datos estadísticos, y la seguridad requerida para este sector de la industria. De dicha investigación se pudo concluir que en cada etapa del ciclo PHVA del SGSI, cada una de las empresas del grupo debería tener la mayor información posible a los efectos de aplicar criterios y lineamientos corporativos o ajustar los parámetros adecuados para la percepción y estimación de riesgos, y permitir escalar riesgos locales percibidos así como heredar los riesgos percibidos y priorizados desde los estratos superiores, buscando alinear los planes de gestión de seguridad al negocio de la forma más conveniente, en función de los recursos, objetivos concretos y condicionantes.

En el ámbito nacional se encuentra la investigación realizada por (Caceres Goyeneche, 2015), quien postula que al establecer políticas de seguridad informática en los servicios de seguridad privada, se logra obtener mayor confidencialidad con sus clientes y por lo tanto se puede prestar un servicio de mayor calidad, para esto busca fomentar una conciencia de prevención en el aspecto informático de manera estructurada con los lineamientos que aporta la norma ISO 27001. Utilizando fuentes secundarias en la investigación, se concluye que las empresas son víctimas de daño a la integridad de la información y deben hacer una reestructuración para replantear lo que se realiza con la información, estableciendo políticas de seguridad de la misma.

Así mismo, (Aguirre Tobar & Zambrano Ordóñez, 2015) presenta un diagnóstico del área financiera de la Secretaria de Educación Departamental (SED) de Nariño, donde realiza un análisis del sistema de información que soporta la actividad financiera (*software* PCT) y el manejo y control que se le está dando a la información, con la idea de minimizar el impacto y la probabilidad de las amenazas y riesgos potenciales a los que se ve expuesta el área mediante el análisis en el enfoque definido por el estándar COBIT (Control Objectives for Information and

related Technology), debido a que el tema hace necesario establecer las políticas que garanticen la seguridad de la información en la SED y establece puntos críticos de control.

En línea de lo anterior, (Ascanio Arévalo, Trillos Bayona, & Bautista Rico, 2015) realizaron una investigación descriptiva, que consistió en identificar la actividad económica empresarial de la ciudad de Ocaña en sus diversas manifestaciones y en promover la ejecución de prácticas administrativas acordes con referentes nacionales e internacionales, donde proponen la aplicación de herramientas para el análisis de sistemas de información usando la norma ISO 27001:2005, y protegiendo su activo más importante: la información donde se concluye que entenderlos puede contribuir a definir nuevas metas y coordinar acciones para crear un escenario productivo local que responda a los requerimientos de la competitividad.

Del mismo modo, (Perafán Ruiz & Caicedo Cuchimba, 2014) realizan un análisis de riesgos que permite generar controles para minimizar la probabilidad de ocurrencia e impacto de los riesgos asociados con las vulnerabilidades y amenazas de seguridad de la información existentes en la Institución Universitaria Colegio Mayor del Cauca, utilizando fuentes secundarias, debido a que considera muchos de los planteamientos y problemas en seguridad informática. Se encamina a proteger la información contra accesos no autorizados, logrando identificar que La IUCMC actualmente presenta un nivel de riesgo informático considerable, que con el apoyo de las directivas (alta gerencia) y de todo el personal es posible contrarrestar.

Según (Garzón Garzón, 2017), los controles aplicados para Spytech son las mejores prácticas de fácil adaptación, que en conjunto con acciones adicionales implementadas, como el monitoreo, evaluación y mejora continua, minimiza el riesgo y evita que se materialicen las amenazas; esto lo dedujo después de realizar entrevistas de preguntas abiertas, con el fin de dar respuesta a la investigación y de sugerir los controles de acceso para minimizar los riesgos de

seguridad de la información, con el cumplimiento de la confidencialidad, integridad y disponibilidad que define la norma ISO 27001:2013, lo cual permitió a Spytech controlar los riesgos de pérdida, daño y robo de la información.

Por otro lado, (Bueno Bustos, 2016) busca diseñar un Sistema de Gestión de Seguridad de la Información utilizando la norma ISO 27001:2013 en el ICBF Centro Zonal Virgen y Turístico, Regional Bolívar, con la metodología Magerit, donde espera que la empresa implemente los controles y medidas que permitan lograr un nivel aceptable de seguridad para garantizar la confidencialidad, disponibilidad e integridad de los datos, e igualmente, procurando un nivel de riesgo aceptable para la organización, apoyados siempre en el diseño de un Sistema de Gestión de Seguridad de la Información.

En el ámbito regional se evidencia el estudio realizado por (Sierra Jaramillo, 2011), el cual menciona que es pertinente identificar el nivel de utilización de procesos de seguridad de la información de las empresas de Risaralda, donde se toma como referente la norma ISO 27000. Gracias a este referente, se indican las acciones pertinentes que se presentan para que la alta dirección conozca la importancia de invertir recursos económicos para permitir la implementación de la norma y realizar capacitaciones para todo el personal interno; el método para evaluar el estudio es el aleatorio simple a través de encuestas a una pequeña muestra de la población, concluyendo que es de vital importancia la implementación de un modelo de seguridad de seguridad en la información a nivel de cada organización.

Así mismo, (Rico Trejos & Saavedra Rivera, 2015) proponen diseñar un plan de seguridad informática para la Alcaldía de Dosquebradas, logrando encontrar que una de las prioridades para el correcto desempeño y cumplimiento de una política de seguridad, es la renovación del cableado estructurado de la alcaldía, el cual se encuentra obsoleto y este riesgo

evidente no permitirá tener un buen control respecto a la seguridad de la información; la herramienta Microsoft Security Assessment Tool (MSAT) complementa la mejora en la seguridad de la entidad a través de una serie de preguntas, logrando la identificación de las áreas con riesgos de seguridad o vulnerabilidad y las medidas correspondiente para generar una solución en cada una de estas. Como conclusión se identifica la falta de políticas de seguridad informática en la entidad, las cuales son parte fundamental para implementar un proceso de seguridad informática, gracias a esto se definió como punto de partida iniciar de cero con la recolección de la información de forma metodológica para la correcta estructuración de los procesos.

Del mismo modo, (Benavides Sepúlveda & Blandón Jaramillo, 2017) proponen diseñar un modelo de seguridad de la información basado en la norma NTC ISO/IEC 27001 para asegurar la confidencialidad, integridad, disponibilidad y control de la información en instituciones públicas de educación básica de la ciudad de Pereira, comuna Universidad, donde se logran analizar los riesgos asociados a las características particulares de estas instituciones, con el fin de cubrir el 100% de las vulnerabilidades asociadas a temas de mejoramiento y sostenibilidad de su infraestructura, para que el personal pueda tener claridad en el desarrollo de sus funciones y que todo sea acorde con los sistemas de información que se manejan a nivel general; el enfoque cualitativo mediante encuestas en Microsoft Excel logra la búsqueda de las buenas prácticas con base en los lineamientos dados por los organismos participantes (MINTIC, MEN e ISO), tendientes a garantizar la seguridad de la información dentro del contexto escolar. Los resultados de esta investigación se traducen en un modelo expresado en palabras y no en cifras; además, se identificó el grado de madurez del SGSI en cada una estas, logrando definir la importancia que las instituciones educativas de nivel básico del sector público dan a los

mecanismos que permiten garantizar la idoneidad de las personas que son contratadas y enviadas a la institución educativa, pues debido a la falta de control sobre el proceso de selección se maximizan los riesgos de exposición de información, ya sea de manera deliberada o accidental.

Seguido de lo anterior, (Aguirre Cardona & Aristizábal Betancourt, 2013) diseñan una propuesta de un sistema de gestión de seguridad de la información para el Grupo Empresarial La Ofrenda, planteando que una continua evolución, crecimiento y sofisticación de la tecnología, al igual que los ataques cibernéticos en las organizaciones, ponen de manifiesto la necesidad de adoptar medidas y controles que permitan proteger a la compañía ante las amenazas a los activos informáticos. Se aplicaron encuestas y se realizaron entrevistas a personal con manejo de procesos y subprocesos importantes de la empresa, con el fin de identificar los pasos a seguir que permiten diseñar, implementar e implantar adecuadamente el SGSI, además de lograr estándares y buenas prácticas que sean ampliamente aceptados.

De igual forma, (Espinosa Betancur, García Gallo, & Giraldo Restrepo, 2016) diseñaron y desarrollaron un modelo aplicable del SGSI para los 3 procesos misionales de la Corporación Autónoma Regional de Risaralda (gestión ambiental sectorial, gestión integral y ordenamiento ambiental del territorio y gestión ambiental territorial), basados en las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013. Para esta investigación se utilizaron los enfoques cualitativo y cuantitativo, mediante observación directa, entrevistas, encuestas y listas de chequeo. Todo lo anterior sirvió para que la CARDER tomara conciencia de la crítica situación respecto a la seguridad de la información que llevaban y ayudó a que todas las partes que hacen parte de cada proceso se involucraran en la implementación del SGSI.

En línea de lo anterior, (Henao Acosta, 2010) plantea el diseño de la política de seguridad informática para la empresa Apostar S.A.; se lograron establecer las prioridades que en materia

de seguridad informática requería la organización para así poderle dar viabilidad a estas, garantizando la continuidad en sus operaciones en caso de una pérdida generalizada de información a causa de una de las vulnerabilidades detectadas, donde se hace entrega del diseño de la Política de Seguridad Informática de Apostar S.A., con los resultados del análisis obtenidos por medio de encuestas realizadas en entrevistas, identificando la investigación como exploratoria y entregando la propuesta creada para su posterior implementación. Se logra concluir que a nivel nacional y/o regional muchas organizaciones no consideran necesario tener una política de seguridad informática definida formalmente; si bien se considera importante y se ejecutan algunas prácticas tendientes a garantizar la seguridad de la información, la falta de procedimientos formales hace que no se tomen medidas definidas en momentos que así lo requieran.

Marco Conceptual

Hacker. La RAE lo describe como un pirata informático y su traducción recomendada para la voz inglesa *hacker*; es una "persona con grandes habilidades en el manejo de ordenadores, que utiliza sus conocimientos para acceder ilegalmente a sistemas o redes ajenos" (Real Academia Española, 2005).

Además, este término se ha utilizado históricamente para describir a un experto en programación y recientemente para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa (Costas Santos, Seguridad informática, 2014, pág. 33).

A los profesionales de la seguridad de la información que utilizan sus conocimientos de *hacking* con fines defensivos, (Benchimol, 2011, pág. 49) se les llama *Ethical Hacker* o *hacker* ético. Se dedican a determinar lo que un intruso puede hacer sobre un sistema y la información, velando por su protección. Son expertos en informática y sistemas, con certeros conocimientos sobre los sistemas operativos, *hardware*, electrónica, redes, telecomunicaciones y programación en lenguajes de alto y bajo nivel. Además, entienden sobre problemas relacionados con seguridad en temáticas como la criptografía, los sistemas de control de acceso, las aplicaciones, la seguridad física y la seguridad administrativa, siguiendo un estricto código de conducta.

Muchos países poseen legislación relativa a los delitos de seguridad de la información, considerando un crimen el hacking de redes o sistemas. Los *hackers* que pongan en peligro la vida de los demás, pueden someterse a cadena perpetua, de acuerdo con la ley norteamericana, en el *Cyber Security Enhancement Act of 2002* (Benchimol, 2011, pág. 56).

En la actualidad existen varios tipos de *hackers* (San Miguel, 2011), entre los que están:

Black hat hackers. También se les llama *hackers* de sombrero negro o simplemente *hackers*. Son los chicos malos, debido a que se dedican a romper la seguridad de computadoras, *networks* o a crear virus. Suelen buscar el camino de menor resistencia, ya sea por alguna vulnerabilidad, error humano, vagancia o algún nuevo método de ataque y su principal motivación es el dinero (San Miguel, 2011).

White hat hackers. Los *hackers* de sombrero blanco son los chicos buenos y éticos. Se dedican a realizar consultorías de seguridad, a penetrar la seguridad de sistemas para encontrar vulnerabilidades y a proteger los sistemas de los *black hat hackers*. Estos tienen los conocimientos de los *black hats* pero los utilizan para hacer el bien (San Miguel, 2011).

Gray hat hackers. Los *hackers* de sombrero gris juegan a ser buenos y malos, es decir, tienen una ética ambigua. Utilizan sus conocimientos de *black hat hacker* para penetrar en sistemas y buscar vulnerabilidades, con el fin de ofrecer sus servicios para repararlos bajo contrato (San Miguel, 2011).

***Crackers*.** Hacen parte de los *black hats*, ya que entran en sistemas vulnerables y hacen daño, robando información y dejando algún virus o *malware*; además, trojan en el sistema y crean puertas traseras para poder entrar nuevamente cuando les plazca. Algunos *crackers* diseñan programas para romper seguridades de *softwares*, ampliar funcionalidades del *software* o el *hardware* original conocidos como *cracks*, *key generators*, etc., por medio de ingeniería inversa (San Miguel, 2011).

***Script kiddies*.** Así se le conoce a los "*hackers* que utilizan programas escritos de otros para penetrar algún sistema, red de computadora, página *web*, etc. ya que tiene poco conocimiento sobre lo que está pasando internamente en la programación" (San Miguel, 2011).

***Phreaker*.** Se dedica a *hackear* los sistemas telefónicos, telefonía móvil, tecnologías inalámbricas y la voz sobre IP (VoIP). Además, investiga los sistemas telefónicos usando la tecnología por el placer de manipular un sistema tecnológicamente complejo y en ocasiones para poder obtener beneficios como llamadas gratuitas (San Miguel, 2011).

***Newbie*.** El novato es el que se tropieza con una página *web* sobre *hacking* y baja todas las utilidades y programas a su PC, lee y ejecuta los programas para ver qué hacen, sin obtener éxito. Es inofensivo y a veces se les confunde con un *lammer* (San Miguel, 2011).

***Lammer*.** Se cree *hacker* pero no tiene los conocimientos necesarios. Descarga cientos de libros y videos de diversos temas de *hacking* pero no ha leído ni visto ninguno de estos, solamente los almacena y los presume (San Miguel, 2011).

Ransomware. También es llamado criptovirus y se caracteriza por encriptar o hacer inaccesibles determinados ficheros en un ordenador, obligando al usuario víctima a pagar un rescate (ransom en inglés) para poder acceder a su información. Normalmente cifra los ficheros que más utiliza el usuario como documentos de texto, hojas de Excel e imágenes, entre otros (Costas Santos, Seguridad informática, 2014, pág. 133). Este malware se propaga como un gusano y otro de sus fines es el de inutilizar el sistema; el rescate que solicita, por lo general, consiste en el envío de un SMS o en la compra de un programa para restablecer el sistema (Moreno, 2014, pág. 176).

Phishing. El objetivo de esta modalidad de estafa es obtener los datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc., de un usuario, es decir, extraerle todas las referencias posibles para después usarlas con fines fraudulentos. Normalmente se realiza

duplicando las páginas *webs* de entidades bancarias, de forma que el visitante crea que se encuentra en la web original. Cuando está realizada la copia, se envían mensajes falsos que parecen provenir de sitios *web* reconocidos o de su confianza, como su banco o la empresa de su tarjeta de crédito. Estos mensajes y los sitios *web* parecen oficiales, consiguiendo engañar a muchas personas y logrando obtener números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales. Estos delincuentes, usan su información para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad (Bolaños, Simoneau, & Becerra, 2009, pág. 20).

El término *phishing* proviene de la palabra inglesa "*fishing*" (pesca), la cual se refiere al intento de hacer que los usuarios piquen en el anzuelo. Los *phisher* son quieres realizan esta práctica; además, se dice que el término "*phishing*" es la contracción de "*password harvesting fishing*" (cosecha y pesca de contraseñas), lo cual es probablemente un acrónimo retroactivo. El término *phishing* se mencionó por primera vez en enero de 1996 en el grupo de noticias de *hackers* alt.2600, aunque posiblemente ya había aparecido anteriormente en la edición impresa del boletín de noticias hacker "*2600 Magazine*". El término *phishing* se adoptó por quienes buscaban "pescar" cuentas de miembros de AOL (Simoneau & Becerra, 2009).

El *phishing* se produce de varias formas, desde un mensaje a un teléfono celular, una llamada telefónica, una *web* simulada, una ventana emergente, hasta la recepción de un correo electrónico. Las formas de uso más comunes son el SMS solicitando datos personales, supuestamente por motivos de seguridad, mantenimiento de la entidad, mejorar su servicio, encuestas, confirmación de su identidad o cualquier excusa, que propicie la entrega de los datos, incluso, el mensaje puede contener formularios, enlaces falsos, textos originales, imágenes oficiales, etc., con el fin de que se visualice idéntica al sitio *web* original. También se usa la

llamada telefónica, suplantando a una entidad privada o pública para que la persona facilite datos privados. La página *web* o ventana emergente es muy clásica y bastante usada, y los sitios *web* falsos que usan ganchos llamativos como ofertas irreales, para que el usuario facilite todos sus datos (Bolaños, Simoneau, & Becerra, 2009).

Marco Legal

Ley Estatutaria 1581 de 2012 (Octubre 17) - Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto Número 1377 de 2013. Por el cual se reglamenta parcialmente la ley 1581 de 2012.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Por la cual se dictan disposiciones generales para la protección de datos personales.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

The Cyber Security Enhancement Act of 2002, dispone aplicar cadena perpetua a hackers que imprudentemente pongan en peligro la vida de los demás. Los *hackers* maliciosos que ataquen redes y sistemas informáticos relacionados con sistemas de transporte, compañías de energía o cualquier otro servicio público y generen algún tipo de amenaza contra la vida podrían ser procesados por esta ley.

Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), con la intención de establecer las nuevas reglas del juego que indiquen los derechos y deberes de empresas y particulares en el mundo de las transacciones de productos y prestaciones de servicios realizadas a través de Internet.

Norma ISO/IEC 27000. Ofrece una visión general de las normas de toda la serie 27001, una introducción a los SGSI, terminología utilizada, etc.

Norma ISO/IEC 27001. Es la norma principal y contiene los requisitos del sistema de gestión se seguridad de la información. Es la norma utilizada por los auditores externos para certificarlos SGSI de las empresas.

Norma ISO/IEC 27002. Guía de buenas prácticas en la que se describen los objetivos de control y controles recomendables relativos a la seguridad de la información.

Norma ISO/IEC 27003. Se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo a la Norma ISO/IEC 27001.

Norma ISO/IEC 27004. Guía para medir eficacia de un SGSI.

Norma ISO/IEC 27005. Proporciona las directrices para la gestión del riesgo en la seguridad de la información.

Normas ISO/IEC 27007 e ISO/IEC 27008. Guías de auditoría.

Ley 1712 de 2014 de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

Ley 734 de 2002 por la cual se expide el Código Disciplinario Único.

Decreto Ley 356 de 1994 - Estatuto de Vigilancia y Seguridad Privada.

Decreto 2355 de 2006, en algunos de sus apartes al referirse a la información, permite determinar que no toda puede ser dada a conocer en la red pública de datos.

El artículo 15 de la Constitución, modificado por el acto legislativo N° 02 del 18 de diciembre de 2003 dice lo siguiente: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificarlas informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

El artículo 95 de la Ley 270 de 1996 (estatutaria de la administración de justicia). Ordena que los procesos que se tramiten con soporte informático garantizarán la confidencialidad, privacidad y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley.

Literal c del artículo 32 de la ley 527 de 1999. Busca garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor.

Art. 25 del decreto 1747 de 2002. Vela por respetar las condiciones de confidencialidad y seguridad de acuerdo con las normas vigentes respectivas-

Literal 11 del artículo 13 del decreto 1742 de 2002. Busca garantizar la confidencialidad de la información que no figure en el certificado.

Marco Contextual

Pereira una ciudad de Colombia, capital del departamento de Risaralda, ubicada en el Eje Cafetero, fundada el 30 de Agosto 1.863. Se encuentra ubicada en la región centro-occidente del país, en el valle del río Otún en la Cordillera Central de los Andes colombianos. Esta ciudad es conocida también como la querendona, trasnochadora y morena. En el área urbana, los municipios en Colombia están divididos en comunas. Pereira está dividida en 19 comunas, cada una de estas con múltiples barrios. El área municipal es de 702 km²; limita al norte con los municipios de La Virginia, Marsella y Dosquebradas, al este con Santa Rosa de Cabal y el departamento del Tolima, al sur con los departamentos de Quindío y Valle del Cauca, al oeste con el municipio de Balboa y el departamento del Valle del Cauca. Pereira es el primer centro urbano del eje cafetero y el segundo de la región paisa (Alcaldía de Pereira, 2016).

(Google Maps, 2018)

(Google Maps, 2018)

La economía de Pereira depende en gran medida del café; sin embargo, cuenta con una estructura diversificada, siendo el sector primario el representante del 5,7% del producto interno, el sector secundario muestra un peso relativo del 26,2% en el municipio y el sector terciario es el más representativo con una magnitud de 68,1% (Concejo Municipal de Pereira, 2017).

En Pereira, desde el año 1972 se empezaron a presentar fallas en el manejo de la información en las organizaciones, que fueron ocasionadas por la aparición de virus y programas que lograron *hackear* a grandes compañías, gracias a que no previnieron los posibles ataques que podrían sufrir a futuro debido a las falencias que manejan en cuanto a la seguridad en la información. Con el paso de los años las organizaciones encargadas de robar la información a grandes o pequeñas empresas han evolucionado a tal punto, que cuando una empresa implementaba una solución a cada debilidad interna en seguridad en la información, estas organizaciones inmediatamente empezaban a trazar posibles ataques a través de nuevas versiones de virus y programas para nuevamente perjudicar a las empresas dañando, plagiando o

eliminando la información encontrada después del ataque.

En la actualidad se encuentran falencias en el manejo de la información, ya que es mucho más fácil acceder a esta, haciendo necesario que cada empresa implemente un sistema de gestión de la seguridad en la información, el cual se puede construir o mejorar teniendo en cuenta los parámetros estipulados en la norma ISO/IEC 27001, que se pueden adaptar a cada organización, permitiendo proteger sus datos. Cabe destacar que cada empresa debe estar un paso adelante de las organizaciones inescrupulosas que roban la información para perjudicar a estas mismas. Es casi que obligatorio tener un plan B, que contenga las soluciones a ataques futuros, además de ir actualizando su SGSI para prevenir posibles ataques a la información confidencial de cada una con el paso del tiempo.

En la Cámara de Comercio de Pereira se encuentran registradas 10 empresas del sector de seguridad privada, las cuales requieren tener implementado un sistema de gestión de la seguridad en la información con un mayor grado de confiabilidad y desarrollo, para garantizar la protección tanto de su información como la de las demás organizaciones a las cuales les ofrecen sus servicios. Estas empresas son:

- Estatal de Seguridad Ltda.
- Seguridad Nacional Limitada.
- Seguridad Dissel Ltda.
- Seguridad Acin Limitada.
- Coordinar Seguridad y Compañía Ltda.
- Veinticuatro Horas Seguridad Limitada.
- Reaccionar Limitada.
- Strong Security y Compañía Limitada.

- Compañía New Security Propiedad Horizontal Ltda.

Esta investigación toma como referencia la empresa de seguridad privada N.

La empresa de seguridad privada N es una empresa dedicada a buscar soluciones con alta tecnología y personal motivado, contribuyendo a la tranquilidad de los clientes y generando valor a los socios; cuenta con un equipo de profesionales altamente competentes y capacitados, lo que ayuda a que tengan el personal más idóneo para prestar el servicio de seguridad privada, supervisión y control permanente; cuenta con el área de servicio al cliente, la cual está en contacto permanente con cada usuario, para poder atender las necesidades y requerimientos que se generan durante la prestación del servicio, también son los encargados de mantener informados acerca de los riesgos y posibles amenazas que se generan en el sector. Esta empresa actualmente se encuentra certificada en las normas ISO 9001:2015 y BASC; además, tiene como proyecto a corto plazo, certificarse en la norma OHSAS 18001 y después en la norma ISO 27001:2013 (Empresa de seguridad privada N, 2018).

Marco Tecnológico

Algunas de las empresas más conocidas en la realización de antivirus y diferentes sistemas para la protección de la información (Costas Santos, Seguridad informática, 2014), son:

Característica	McAfee	Norton (Symantec)	ESET NOD32	Panda Security
Antivirus	Sí	Sí	Sí	Sí
Antispyware	Sí	Sí	Sí	Sí
Link Scanner	No	No	No	Sí
Antirootkit	Sí	Sí	Sí	Sí
Web Shield	No	Sí	Sí	Sí
ID Protection	Sí	Sí	No	Sí
Firewall	Sí	Sí	Sí	Sí
Antispam	No	No	No	Sí
Sistemas x64	No	Limitado	Sí	Sí
Español	Sí	Sí	Sí	Sí
Soporte técnico	30 días	Sí	Sí	Sí
Mac y Linux	No	Sólo Mac	Sólo Linux	Sólo Linux
Consumo de recursos	Término Medio	Muchos	Pocos	Pocos
Version	2009	2009	4.0	2010

(Costas Santos, Seguridad informática, 2014)

A continuación, se relacionarán algunos de los *softwares*, programas y herramientas más utilizados a la hora de proteger y salvaguardar la información:

Antivirus. Es un programa informático específicamente diseñado para detectar, bloquear y eliminar códigos maliciosos. Aunque se sigue utilizando la palabra antivirus, estos programas han evolucionado y son capaces de detectar y eliminar, no solo virus, sino también otros tipos de códigos maliciosos como gusanos, troyanos y espías **(Costas Santos, Seguridad informática, 2014, pág. 147)**.

Antispyware. Los *spywares* o programas espía **(Costas Santos, Seguridad informática, 2014, pág. 154)** son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad. Todas estas acciones se hacen de forma oculta al usuario o bien se enmascaran tras confusas autorizaciones al instalar terceros programas, por lo que rara vez el usuario es consciente de ello.

Los tipos de *antispyware* que existen son antiespías de escritorio y antiespías en línea.

Antifraude. Estas herramientas nos informan de la peligrosidad de los sitios que visitamos, en algunos casos, nos informan de forma detallada qué enlaces de esas páginas se consideran peligrosos y cuál es el motivo. Existe *Spoofstick*, que es un *software* que se instala como una extensión del navegador que sirve para comprobar que las páginas que visitamos son auténticas y que no son potencialmente peligrosas, y está *Netcraft* que protege de los ataques de *phishing*, encargándose de vigilar dónde se hospeda y proporcionar un índice de riesgo de los sitios que son visitados ayudando a defender a la comunidad internauta de fraudes **(Costas Santos, Seguridad informática, 2014, pág. 156)**.

Antispam. El *spam* se puede definir como el envío masivo de correo electrónico no solicitado; en realidad, un alto porcentaje del correo electrónico que se mueve hoy en día es *spam*. Principalmente se utiliza como complemento a otras técnicas que tienen como un objeto y fin engañar al usuario logrando obtener un beneficio económico. Además, el simple hecho del envío y la recepción de este correo provoca un tráfico de datos que ayudan a saturar el internet; es por ello que se presentarán unas herramientas para tratar de mitigar el efecto *spam*, son programas que filtran los correos electrónicos y tratan de eliminarlos, algunas de estas herramientas son *Time Machine*. Esta herramienta se instala en forma de *plug-in* de navegador y funciona con el correo *web* de *Gmail*, *Windows Live Hotmail* y *Yahoo*, además de con el programa *Outlook Express*. El programa comprueba si el correo recibido corresponde a la empresa que debería, y que no es un intento de *phishing*. Actualmente el programa puede reconocer algunas compañías y entre ellas una cuantas de servicios de Internet, utilizadas muy frecuentemente como ganchos para intentos de robo de identidad mediante técnicas de *phishing*; otra herramienta es *Spamihilator*, donde tiene a disposición de todos los usuarios un programa *antispam*, que se encarga de filtrar los correos electrónicos no deseados (*spam*) que son enviados (Costas Santos, Seguridad informática, 2014, pág. 157).

Anti-Dialer. Son pequeños programas que se encargan de marcar números telefónicos que dan acceso a algún tipo de servicio, en un principio, este tipo de aplicaciones eran distribuidos por proveedores de acceso a Internet para facilitar a sus clientes el proceso de conexión con el servidor (Noticias Universia España, 2003).

Este tipo de herramienta permite controlar a qué números de teléfono está conectado un módem, con el único fin de controlar que no sea utilizado ningún número que no esté en la lista

de contactos o números permitidos, ya que hay algunos programas que cambiaban estos números por otros de tarificación especial, y las llamadas salían mucho más caras. Este tipo de fraude ha quedado reducido a conexiones de 56 kbps, con módem de marcación sobre línea telefónica, conexiones ya en desuso (Costas Santos, Seguridad informática, 2014, pág. 158).

Análisis de ficheros en línea. Son herramientas que ofrecen un servicio gratuito para realizar análisis de ficheros sospechosos mediante el uso de múltiples motores antivirus que busca complementar el mismo, de esta manera se puede comprobar si dichos ficheros contienen o no algún tipo de código malicioso; la herramienta *Dr.Web On-line* para el análisis en línea de direcciones de Internet busca códigos maliciosos que pueden estar inyectado en las páginas HTML. En el caso de ser así, esta herramienta avisa que el acceso a este sitio podría ser peligroso, ya que podría dañar la configuración del sistema (Costas Santos, Seguridad informática, 2014, pág. 158).

Análisis de URL. Son herramientas para el análisis de direcciones de páginas *web*, que sirven para determinar si el acceso a dicha URL puede afectar o no a la seguridad de nuestro sistema. Existen varios tipos de analizadores en función de cómo se accede al servicio: los que realizan un análisis en línea, los que se descargan como una extensión o *plugin* de la barra del navegador y los que se instalan como una herramienta de escritorio. Estos útiles son capaces de categorizar las páginas que se desea visitar, de modo que estando atentos a esa valoración, se puede evitar que el sistema sea infectado por acceder a páginas peligrosas. Estas herramientas pueden detectar, y a veces hasta bloquear, el acceso a páginas que contengan código malicioso, fraude electrónico, contenidos inapropiados e incluso si el código intenta explotar alguna

vulnerabilidad sobre nuestro navegador o sistema. No se asegura que la información que puedan ofrecer sea del todo fiable al 100%, bien porque la página *web* solicitada no haya sido todavía analizada, o porque puedan existir opiniones distantes de diferentes internautas sobre un mismo sitio *web*. En cualquier caso, consideramos que nos aportan una información bastante útil, ya que nos alertan o avisan sobre las posibles amenazas a las que exponemos nuestro sistema al acceder a determinados sitios *web*.

Hoy se cuenta con una herramienta tan fundamental como son las URL que permiten saber qué tan segura es la dirección *web* a la que se ingresara desde determinado computador, para identificar las posibles amenazas que podrá sufrir la información almacenada en el mismo (Costas Santos, Seguridad informática, 2014, pág. 159).

Sistemas biométricos. Se entiende como un sistema automatizado que realiza labores de biometría. Es decir, un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada. En la actualidad existen sistemas biométricos que basan su acción en el reconocimiento de diversas características. Las técnicas biométricas más conocidas son nueve y están basadas en los siguientes indicadores biométricos: rostro, termograma del rostro, huellas dactilares, geometría de la mano, venas de las manos, iris, patrones de la retina, voz y firma (Bancada Cruceña, 2009).

Algunos beneficios que traen estas herramientas (Costas Santos, Seguridad informática, 2014), son eliminar la necesidad de poseer una tarjeta para acceder y de una contraseña difícil de recordar, y al ser utilizando un dispositivo biométrico los costos de administración son más pequeños, ya que se realiza el mantenimiento del lector y una persona se encarga de mantener la

base de datos actualizada. Sumado a esto, las características biométricas de una persona son intransferibles a otra.

Protección electrónica. Se llama así (Costas Santos, Seguridad informática, 2014, pág. 61) a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectados los elementos de señalización, que son los encargados de hacer saber al personal de una situación de emergencia. Cuando uno de los elementos, sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; esta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación, algunos ejemplos de estas son (Borghello, 2016):

Barreras infrarrojas y de micro-ondas. Estas transmiten y reciben haces de luces infrarrojas y de micro-ondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Estas barreras están compuestas por un transmisor y un receptor de igual tamaño y apariencia externa, cuando el haz es interrumpido, se activa el sistema de alarma, y luego vuelve al estado de alerta. Estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc. Las invisibles barreras fotoeléctricas pueden llegar a cubrir áreas de hasta 150 metros de longitud (distancias exteriores). Pueden reflejar sus rayos por medio de espejos infrarrojos con el fin de cubrir con una misma barrera diferentes sectores. Las micro-ondas son ondas de radio de frecuencia muy elevada. Esto permite que el sensor opere con señales de muy bajo nivel sin ser afectado por otras emisiones de radio, ya que están muy alejadas en frecuencia Debido a que estos detectores no utilizan aire como medio de propagación, poseen la ventaja de no ser afectados por

turbulencias de aire o sonidos muy fuertes.

Otra ventaja importante es la capacidad de atravesar ciertos materiales como son el vidrio, lana de vidrio, plástico, tabiques de madera, revoques sobre madera, mampostería y hormigón.

Detector ultrasónico. Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, generará una perturbación en dicho campo que accionará la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas. La cobertura de este sistema puede llegar a un máximo de 40 metros cuadrados.

Detectores pasivos sin alimentación. Estos elementos no requieren alimentación extra de ningún tipo, solo van conectados a la central de control de alarmas para mandar la información de control.

Sonorización y dispositivos luminosos. Dentro de los elementos de sonorización se encuentran las sirenas, campanas, timbres, etc. Algunos dispositivos luminosos son los faros rotativos, las balizas, las luces intermitentes, etc. Estos deben estar colocados de modo que sean efectivamente oídos o vistos por aquellos a quienes están dirigidos. Los elementos de sonorización deben estar bien identificados para poder determinar rápidamente si el estado de alarma es de robo, intrusión, asalto o aviso de incendio. Se pueden usar transmisores de radio a corto alcance para las instalaciones de alarmas locales. Los sensores se conectan a un transmisor que envía la señal de radio a un receptor conectado a la central de control de alarmas encargada de procesar la información recibida.

Circuitos cerrados de televisión. Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos

deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizada como medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad). Todos los elementos anteriormente descritos poseen un control contra sabotaje, de manera que si en algún momento se corta la alimentación o se produce la rotura de alguno de sus componentes, se enviará una señal a la central de alarma para que esta accione los elementos de señalización correspondientes.

Diseño Metodológico

Tipo de Investigación

Se aplica la investigación exploratoria y descriptiva para definir los problemas de investigación. La investigación descriptiva se usa para conocer cómo está estructurado y desarrollado el sistema de seguridad de la información, teniendo en cuenta de una forma más detallada y concreta cada uno de los procesos y procedimientos que se llevan a cabo en la organización. La investigación exploratoria se usa para realizar una verificación de las condiciones iniciales del sistema de seguridad de la información de la empresa objeto de investigación, respecto a la norma ISO 27001:2013, para que posteriormente, pueda suplir las falencias que tiene y certificarse en dicha norma (Hernández Sampieri, Collado, & Baptista Lucio, 2014).

Se utiliza la investigación concluyente descriptiva, en un corte transversal para dar solución a los interrogantes planteados, ya que se busca establecer qué está ocurriendo, cómo se está actuando, cuándo se realiza y dónde está sucediendo. Con esta investigación se generarán datos de primera mano con el fin de realizar un análisis general y presentar un panorama del problema, ayudando de esta manera a una empresa de seguridad privada, ubicada en la ciudad de Pereira, a implementar estrategias que ayuden a mejorar y reforzar sus sistemas de seguridad de la información (Benassini, 2009).

Métodos, Técnicas e Instrumentos

Método según la selección de datos. La recolección de los datos se realiza mediante el método primario, dado a que la información es obtenida directamente de la empresa objeto de investigación por medio de una visita a la misma.

Método según enfoque. Se utiliza el método según enfoque cuantitativo, empleando la técnica de entrevista dirigida. Para el primer objetivo se utiliza un cuestionario de preguntas cerradas como instrumento y para el segundo objetivo se utiliza una lista de chequeo.

Método según selección de la muestra. Para esta investigación se emplea muestreo no probabilístico por conveniencia para elegir la empresa objeto de investigación.

Método según la aplicación. Se aplica al mercado industrial del sector socioeconómico terciario, debido a que se realiza directamente a la empresa involucrada y no a los clientes finales de esta.

Recolección de Información

Muestra. Para llevar a cabo la presente investigación, se seleccionó una de las empresas más representativas del sector de seguridad privada de la ciudad de Pereira, con el fin de dar respuesta a los objetivos planteados.

Validación de experto. La validación de los instrumentos utilizados para esta investigación, fue realizada por el ingeniero Jesús Aníbal Baena Arcila, quien consideró que no era necesario realizarles modificaciones, pero indicó que si se hubiera tenido un mayor conocimiento o una mejor investigación previa a cerca del contexto de la empresa objeto de investigación, se hubieran podido mejorar los instrumentos, caracterizándolos hacia la misma.

El experto que validó los instrumentos, es ingeniero en sistemas con énfasis en telecomunicaciones, egresado de la UNAD en el año 2008; cuenta con más de 20 años de experiencia en la industria en la parte de las telecomunicaciones y ha trabajado como encargado, director y gerente en varias organizaciones; además, fue la persona encargada de implementar la política de seguridad de la información en la primera certificación de la ISO 9001:2003 en la empresa Telemark Spain S.L., participó en la certificación de la ISO 9001:2015 para la empresa GTI, realizando la caracterización del área de ingeniería en sistemas e implementó la política de seguridad de la información en Chevrolet Caminos, la cual se encuentra en proceso de divulgación.

Aplicación del instrumento. La presente investigación se lleva a cabo por medio de la aplicación de un cuestionario de preguntas cerradas para dar respuesta al primer objetivo y una lista de chequeo para dar respuesta al segundo objetivo, los cuales se encuentran adjuntos en apéndices. Los dos instrumentos son aplicados en la empresa de seguridad privada N los días 6 y 7 de abril del 2018, por medio de una entrevista dirigida y se utiliza la observación directa para verificar la aplicación de los numerales de la lista de chequeo.

Análisis de la Información

De acuerdo con el cuestionario de preguntas cerradas aplicado a la empresa de seguridad privada N, se logra identificar que esta es una empresa muy bien estructurada y fuerte en todos sus procesos de T.I., debido a que le dan una gran importancia a la seguridad de su información.

Hasta la fecha, dicha empresa no ha presentado ningún ataque o amenaza interna, mientras que a nivel externo han recibido múltiples ataques, aunque ninguno de estos ha sido efectivo. Todas las áreas de esta empresa manejan información sensible, pero la información que ellos más procuran proteger son las bases de datos que contienen la información de sus clientes.

Además, se logra identificar que a pesar de que la empresa de seguridad privada N no es nada vulnerable a ataques a la información, trabajan arduamente para proteger la seguridad de sus servidores de archivos y de las redes utilizadas, pues consideran que la forma que se utiliza más frecuentemente para robar información, es mediante la captura de paquetes en las redes.

Ellos son conscientes de que la tecnología se vuelve cada vez más compleja y que los *malware* evolucionan constantemente, por este motivo, consideran de vital importancia garantizar la seguridad de la información, realizando análisis predictivos y enfocándose completamente en la prevención, pero dejando de lado la corrección. En la parte preventiva a nivel interno, se utilizan métodos como el monitoreo de la actividad de todos los usuarios, permitiendo realizar seguimiento a todos los movimientos realizados dentro de las aplicaciones centrales, de acuerdo con las políticas establecidas dentro de la organización; además, no es permitida la reproducción parcial ni total de ningún tipo de información y todo se maneja mediante copias controladas, realizadas desde el área de gestión de calidad, se utilizan programas de gobernanza de la seguridad de la información, se realizan capacitaciones constantes a los

usuarios para reforzar conocimientos, se emplean aplicaciones y dispositivos especializados de terceros, se verifican los antecedentes de cada una de las personas que se encuentran en proceso de selección, se maneja autenticación secundaria y cuentan con funciones de seguridad nativas del sistema operativo subyacente y herramientas personalizadas, junto con las aplicaciones desarrolladas en la misma empresa. Adicionalmente, para la detección y protección contra amenazas externas se utilizan dos herramientas de defensa perimetral de seguridad: una versión premium del antivirus y un equipo encargado de hacer el perímetro.

La detección de ataques tanto internos como externos es inmediata, gracias a las herramientas de protección que bloquean las amenazas de forma automática, pero no tienen conocimiento del tiempo que les tomaría recuperarse de un ataque, debido a que hasta la fecha ninguno ha sido efectivo, de igual forma, tampoco saben con exactitud el costo promedio que tendría la remediación de una ataque, pero manifiestan que no sería nada difícil determinar el tamaño del daño real dentro de empresa. Actualmente, la empresa no presenta barreras que impidan una mejor administración de las amenazas internas y externas.

En los próximos 12 meses, la empresa espera un aumento en el presupuesto para poder cambiar el servidor de correo, el cual se encuentra en buenas condiciones pero con su cambio mejorarían notablemente en el desarrollo de este proceso.

En cuanto al análisis correctivo, la empresa no lo considera necesario, debido a que están muy seguros de que sus sistemas de prevención son completamente efectivos, motivo por el cual, no tienen bien desarrollado su marco de gestión de riesgos, el cual no incluye ataques cibernéticos ni procesos documentados para el momento en que se lleguen a ver afectados por algún tipo de ataque o amenaza. Lo anterior, se considera una debilidad en el sistema de seguridad de la información, por lo cual se recomienda fortalecer su marco de gestión de riesgos,

incluyendo el análisis correctivo; además, se sugiere realizar simulacros de ataques programados para saber cómo actuarían los usuarios frente a una amenaza o si tienen la suficiente consciencia para no leer correos infectados que se puedan llegar a pasar el filtro automático que realizan los sistemas de detección, ya que por las restricciones que tienen, no se conoce qué tan efectivas son las capacitaciones que se han realizado a los colaboradores.

Objetivos de control y controles	Ponderación (%)	Nivel de implementación 0-100%	Resultado
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	**10,00%**	**80,00%**	**8,000%**
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información	**10,00%**	**80,00%**	**8,000%**
A.5.1.1 Políticas para la seguridad de la información	6,00%	80,00%	4,800%
A.5.1.2 Revisión de las políticas para la seguridad de la información	4,00%	80,00%	3,200%
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	**10,00%**	**100,00%**	**10,000%**
A.6.1 Organización interna	**10,00%**	**100,00%**	**10,000%**
A.6.1.1 Roles y responsabilidades para la seguridad de la información	3,00%	100,00%	3,000%
A.6.1.2 Separación de deberes	2,00%	100,00%	2,000%
A.6.1.3 Contacto con las autoridades	1,00%	100,00%	1,000%
A.6.1.4 Contacto con grupos de interés especial	2,00%	100,00%	2,000%
A.6.1.5 Seguridad de la información en la gestión de proyectos	2,00%	100,00%	2,000%
A.6.2 Dispositivos móviles y teletrabajo	**0,00%**	**100,00%**	**0,000%**
A.6.2.1 Política para dispositivos móviles	0,00%	100,00%	0,000%
A.6.2.2 Teletrabajo	0,00%	100,00%	0,000%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	**10,00%**	**100,00%**	**10,000%**
A.7.1 Antes de asumir el empleo	**4,00%**	**100,00%**	**4,000%**
A.7.1.1 Selección	2,00%	100,00%	2,000%
A.7.1.2 Términos y condiciones del empleo	2,00%	100,00%	2,000%
A.7.2 Durante la ejecución del empleo	**4,00%**	**100,00%**	**4,000%**

A.7.2.1 Responsabilidades de la dirección	1,50%	100,00%	1,500%
A.7.2.2 Toma de conciencia, educación y la formación en la seguridad de la información	1,50%	100,00%	1,500%
A.7.2.3 Proceso disciplinario	1,00%	100,00%	1,000%
A.7.3 Terminación y cambio de empleo	**2,00%**	**100,00%**	**2,000%**
A.7.3.1 Terminación o cambio de responsabilidades de empleo	2,00%	100,00%	2,000%
A.8 GESTIÓN DE ACTIVOS	**5,00%**	**100,00%**	**5,000%**
A.8.1 Responsabilidad por los activos	**2,00%**	**100,00%**	**2,000%**
A.8.1.1 Inventario de activos	0,50%	100,00%	0,500%
A.8.1.2 Propiedad de los activos	0,50%	100,00%	0,500%
A.8.1.3 Uso aceptable de los activos	0,50%	100,00%	0,500%
A.8.1.4 Devolución de los activos	0,50%	100,00%	0,500%
A.8.2 Clasificación de la información	**2,00%**	**100,00%**	**2,000%**
A.8.2.1 Clasificación de la información	0,70%	100,00%	0,700%
A.8.2.2 Etiquetado de la información	0,70%	100,00%	0,700%
A.8.2.3 Manejo de activos	0,60%	100,00%	0,600%
A.8.3 Manejo de medios	**1,00%**	**100,00%**	**1,000%**
A.8.3.1 Gestión de medios removibles	0,34%	100,00%	0,340%
A.8.3.2 Disposición de los medios	0,33%	100,00%	0,330%
A.8.3.3 Transferencia de medios físicos	0,33%	100,00%	0,330%
A.9 CONTROL DE ACCESO	**10,00%**	**100,00%**	**10,000%**
A.9.1 Requisitos del negocio para control de acceso	**2,50%**	**100,00%**	**2,500%**
A.9.1.1 Política de control de acceso	1,25%	100,00%	1,250%
A.9.1.2 Acceso a redes y a servicios en red	1,25%	100,00%	1,250%
A.9.2 Gestión de acceso de usuarios	**2,50%**	**100,00%**	**2,500%**
A.9.2.1 Registro y cancelación del registro de usuarios	0,41%	100,00%	0,410%
A.9.2.2 Suministro de acceso de usuarios	0,45%	100,00%	0,450%
A.9.2.3 Gestión de derechos de acceso privilegiado	0,41%	100,00%	0,410%
A.9.2.4 Gestión de información de autenticación secreta de usuarios	0,41%	100,00%	0,410%
A.9.2.5 Revisión de los derechos de acceso de usuarios	0,41%	100,00%	0,410%
A.9.2.6 Retiro o ajuste de los derechos de acceso	0,41%	100,00%	0,410%
A.9.3 Responsabilidades de los usuarios	**2,50%**	**100,00%**	**2,500%**

A.9.3.1 Uso de información de autenticación secreta	2,50%	100,00%	2,500%
A.9.4 Control de acceso a sistemas y aplicaciones	**2,50%**	**100,00%**	**2,500%**
A.9.4.1 Restricción de acceso a la información	0,50%	100,00%	0,500%
A.9.4.2 Procedimiento de ingreso seguro	0,50%	100,00%	0,500%
A.9.4.3 Sistema de gestión de contraseñas	0,50%	100,00%	0,500%
A.9.4.4 Uso de programas utilitarios privilegiados	0,50%	100,00%	0,500%
A.9.4.5 Control de acceso a códigos fuente de programas	0,50%	100,00%	0,500%
A.10 CRIPTOGRAFÍA	**5,00%**	**0,00%**	**0,000%**
A.10.1 Controles criptográficos	**5,00%**	**0,00%**	**0,000%**
A.10.1.1 Política sobre el uso de controles criptográficos	2,50%	0,00%	0,000%
A.10.1.2 Gestión de llaves	2,50%	0,00%	0,000%
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	**5,00%**	**100,00%**	**5,000%**
A.11.1 Áreas seguras	**2,50%**	**100,00%**	**2,500%**
A.11.1.1 Perímetro de seguridad física	0,80%	100,00%	0,800%
A.11.1.2 Controles de acceso físicos	0,80%	100,00%	0,800%
A.11.1.3 Seguridad de oficinas, recintos e instalaciones	0,30%	100,00%	0,300%
A.11.1.4 Protección contra amenazas externas y ambientales	0,30%	100,00%	0,300%
A.11.1.5 Trabajo en áreas seguras	0,30%	100,00%	0,300%
A.11.1.6 Áreas de despacho y carga	0,00%	100,00%	0,000%
A.11.2 Equipos	**2,50%**	**100,00%**	**2,500%**
A.11.2.1 Ubicación y protección de los equipos	0,27%	100,00%	0,270%
A.11.2.2 Servicios de suministro	0,27%	100,00%	0,270%
A.11.2.3 Seguridad del cableado	0,27%	100,00%	0,270%
A.11.2.4 Mantenimiento de equipos	0,27%	100,00%	0,270%
A.11.2.5 Retiro de activos	0,27%	100,00%	0,270%
A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones	0,30%	100,00%	0,300%
A.11.2.7 Disposición segura o reutilización de equipos	0,30%	100,00%	0,300%
A.11.2.8 Equipos de usuario desatendido	0,28%	100,00%	0,280%
A.11.2.9 Política de escritorio limpio y pantalla limpia	0,27%	100,00%	0,270%

A.12 SEGURIDAD DE LAS OPERACIONES	**10,00%**	**76,07%**	**7,690%**
A.12.1 Procedimientos operacionales y responsabilidades	**1,40%**	**100,00%**	**1,400%**
A.12.1.1 Procedimientos de operación documentados	0,40%	100,00%	0,400%
A.12.1.2 Gestión de cambios	0,40%	100,00%	0,400%
A.12.1.3 Gestión de capacidad	0,30%	100,00%	0,300%
A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operaciones	0,30%	100,00%	0,300%
A.12.2 Protección contra códigos maliciosos	**1,40%**	**100,00%**	**1,400%**
A.12.2.1 Controles contra códigos maliciosos	1,40%	100,00%	1,400%
A.12.3 Copias de respaldo	**1,60%**	**100,00%**	**1,600%**
A.12.3.1 Respaldo de la información	1,60%	100,00%	1,600%
A.12.4 Registro y seguimiento	**1,40%**	**32,50%**	**0,490%**
A.12.4.1 Registro de eventos	0,30%	20,00%	0,060%
A.12.4.2 Protección de la información de registro	0,40%	0,00%	0,000%
A.12.4.3 Registros del administrador y del operador	0,30%	10,00%	0,030%
A.12.4.4 Sincronización de relojes	0,40%	100,00%	0,400%
A.12.5 Control de software operacional	**1,40%**	**100,00%**	**1,400%**
A.12.5.1 Instalación de software en sistemas operativos	1,40%	100,00%	1,400%
A.12.6 Gestión de la vulnerabilidad técnica	**1,40%**	**100,00%**	**1,400%**
A.12.6.1 Gestión de las vulnerabilidades técnicas	0,70%	100,00%	0,700%
A.12.6.2 Restricciones sobre la instalación de software	0,70%	100,00%	0,700%
A.12.7 Consideraciones sobre auditorías de sistemas de información	**1,40%**	**0,00%**	**0,000%**
A.12.7.1 Controles de auditorías de sistemas de información	1,40%	0,00%	0,000%
A.13 SEGURIDAD DE LAS COMUNICACIONES	**7,50%**	**100,00%**	**7,500%**
A.13.1 Gestión de la seguridad de las redes	**3,75%**	**100,00%**	**3,750%**
A.13.1.1 Controles de redes	1,25%	100,00%	1,250%
A.13.1.2 Seguridad de los servicios de red	1,25%	100,00%	1,250%
A.13.1.3 Separación en las redes	1,25%	100,00%	1,250%
A.13.2 Transferencia de información	**3,75%**	**100,00%**	**3,750%**

A.13.2.1 Políticas y procedimientos de transferencia de información	0,94%	100,00%	0,940%
A.13.2.2 Acuerdos sobre transferencia de información	0,94%	100,00%	0,940%
A.13.2.3 Mensajería electrónica	0,93%	100,00%	0,930%
A.13.2.4 Acuerdos de confidencialidad o de no divulgación	0,94%	100,00%	0,940%
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	**7,50%**	**99,63%**	**7,472%**
A.14.1 Requisitos de seguridad de los sistemas de información	**3,00%**	**100,00%**	**3,000%**
A.14.1.1 Análisis y especificación de requisitos de seguridad de la información	1,00%	100,00%	1,000%
A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas	1,00%	100,00%	1,000%
A.14.1.3 Protección de transacciones de los servicios de las aplicaciones	1,00%	100,00%	1,000%
A.14.2 Seguridad en los procesos de desarrollo y de soporte	**2,50%**	**98,89%**	**2,472%**
A.14.2.1 Política de desarrollo seguro	0,28%	100,00%	0,280%
A.14.2.2 Procedimientos de control de cambios en sistemas	0,28%	100,00%	0,280%
A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	0,28%	100,00%	0,280%
A.14.2.4 Restricciones en los cambios a los paquetes de software	0,28%	100,00%	0,280%
A.14.2.5 Principios de construcción de los sistemas seguros	0,28%	90,00%	0,252%
A.14.2.6 Ambiente de desarrollo seguro	0,28%	100,00%	0,280%
A.14.2.7 Desarrollo controlado externamente	0,28%	100,00%	0,280%
A.14.2.8 Pruebas de seguridad de sistemas	0,27%	100,00%	0,270%
A.14.2.9 Prueba de aceptación de sistemas	0,27%	100,00%	0,270%
A.14.3 Datos de prueba	**2,00%**	**100,00%**	**2,000%**
A.14.3.1 Protección de datos de prueba	2,00%	100,00%	2,000%
A.15 RELACIONES CON LOS PROVEEDORES	**5,00%**	**100,00%**	**5,000%**
A.15.1 Seguridad de la información en las relaciones con los proveedores	**2,50%**	**100,00%**	**2,500%**

A.15.1.1 Política de seguridad de la información para las relaciones con proveedores	0,84%	100,00%	0,840%
A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores	0,83%	100,00%	0,830%
A.15.1.3 Cadena de suministro de tecnología de información y comunicación	0,83%	100,00%	0,830%
A.15.2 Gestión de la prestación de servicios de proveedores	**2,50%**	**100,00%**	**2,500%**
A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	1,25%	100,00%	1,250%
A.15.2.2 Gestión de cambios en los servicios de los proveedores	1,25%	100,00%	1,250%
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	**5,00%**	**97,14%**	**4,857%**
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información	**5,00%**	**97,14%**	**4,857%**
A.16.1.1 Responsabilidades y procedimientos	0,72%	100,00%	0,720%
A.16.1.2 Reporte de eventos de seguridad de la información	0,72%	90,00%	0,648%
A.16.1.3 Reporte de debilidades de seguridad de la información	0,72%	100,00%	0,720%
A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos	0,71%	90,00%	0,639%
A.16.1.5 Respuesta a incidentes de seguridad de la información	0,71%	100,00%	0,710%
A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	0,71%	100,00%	0,710%
A.16.1.7 Recolección de evidencia	0,71%	100,00%	0,710%
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	**5,00%**	**50,00%**	**2,000%**
A.17.1 Continuidad de seguridad de la información	**3,00%**	**0,00%**	**0,000%**
A.17.1.1 Planificación de la continuidad de la seguridad de la información	1,00%	0,00%	0,000%
A.17.1.2 Implementación de la continuidad de la seguridad de la información	1,00%	0,00%	0,000%
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1,00%	0,00%	0,000%
A.17.2 Redundancias	**2,00%**	**100,00%**	**2,000%**

A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	2,00%	100,00%	2,000%
A.18 CUMPLIMIENTO	**5,00%**	**67,83%**	**3,395%**
A.18.1 Cumplimiento de requisitos legales y contractuales	**2,50%**	**64,00%**	**1,600%**
A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	0,50%	20,00%	0,100%
A.18.1.2 Derechos de propiedad intelectual	0,50%	100,00%	0,500%
A.18.1.3 Protección de registros	0,50%	100,00%	0,500%
A.18.1.4 Privacidad y protección de información de datos personales	0,50%	100,00%	0,500%
A.18.1.5 Reglamentación de controles criptográficos	0,50%	0,00%	0,000%
A.18.2 Revisiones de seguridad de la información	**2,50%**	**71,67%**	**1,795%**
A.18.2.1 Revisión independiente de la seguridad de la información	0,83%	15,00%	0,125%
A.18.2.2 Cumplimiento con las políticas y normas de seguridad	0,84%	100,00%	0,840%
A.18.2.3 Revisión del cumplimiento técnico	0,83%	100,00%	0,830%
TOTAL	**100,00%**	**83,62%**	**85,914%**

En la empresa de seguridad privada N se verificaron las condiciones en las que se encuentra actualmente, frente a la norma ISO/IEC 27001:2013, en todo lo relacionado con los numerales, políticas de la seguridad de la información y demás aspectos, logrando observar cómo llevan a cabo los procesos de implementación, revisión y control, que realizan por medio de una política integral.

En esta organización, el marco de gestión de seguridad se realiza definiendo completamente las responsabilidades y deberes de cada área involucrada. Además, se logró evidenciar que no aplican los controles de políticas de dispositivos móviles y teletrabajo, ya que no lo utilizan.

En cuanto a la seguridad de los recursos humanos, la organización maneja estrictos

procedimientos y controles para la selección y vinculación del personal, realizando previamente la revisión de cada uno de los ítems del numeral como antecedentes, visitas domiciliarias, acuerdos contractuales y responsabilidades para los futuros colaboradores.

La empresa de seguridad privada N implementa completamente todos los parámetros necesarios para la identificación de activos, definiendo claramente las responsabilidades y deberes a todos los colaboradores. Respecto a la clasificación de la información, la organización lo realiza de acuerdo con la criticidad de la información, desarrollando procedimientos para el etiquetado previo con fecha, nombre de quién lo realizó y quién lo tiene a cargo, entre otros datos relevantes.

En manejo de medios de gestión removible, disposición de medios y la transferencia de estos, se implementa de forma que no se permiten medios removibles como lo son los dispositivos USB, bloqueando los puertos correspondientes para evitar el robo de información.

El control de acceso es muy minucioso, de forma que solo se tiene acceso a la información estrictamente necesaria, de acuerdo con los perfiles de cada cargo; además, cuando se finaliza contrato a un colaborador o cambia de responsabilidades, se realiza tanto la cancelación de la huella de acceso como la cancelación de su usuario y cambio de contraseñas de sus correos, para que posteriormente sean asignados a un nuevo responsable.

Uno de los requisitos que especifica la norma es la criptografía como método para proteger la confidencialidad de la información, en lo cual la organización no ha implementado ningún control, ya que únicamente hacen uso del antivirus; por lo tanto, se recomienda analizar la posible implementación apropiada y eficaz de esta.

Esta empresa, aplica los controles necesarios para proteger la información en cuanto a seguridad física y del entorno se refiere, contando con un archivo externo para conserva de forma

física todos los documentos, los cuales también se encuentran de forma digital. Para los equipos desatendidos utilizan bloqueos automáticos tras 5 minutos de inactividad, con el fin de garantizar la seguridad de sus operaciones.

Adicionalmente, la organización realiza copias de seguridad diariamente a nivel interno y mensualmente realizan copias de seguridad en dos equipos diferentes a nivel externo, con el fin de protegerse contra la pérdida de datos, pero no existe un registro de eventos debido a que la organización confía completamente en las medidas predictivas que aplica. En la parte de las telecomunicaciones se aplican controles muy radicales, como el bloqueo total de correos que provienen de dominios poco confiables, páginas webs que no son relacionadas con el trabajo, sistemas de red o archivos que no correspondan al perfil del cargo del trabajador y panel de control, entre otros; además, no es permitida la instalación o modificación de ningún *software* ni configuración de los sistemas, ya que todo esto está habilitado únicamente para los usuarios administradores del área de TI.

Todas las modificaciones que se hagan a cualquier archivo, procedimiento, *software* y demás, se registran en un formato de control de cambios y todos los archivos están debidamente relacionados en una matriz de documentación.

En las relaciones con los proveedores, la organización cuenta con unas políticas muy estrictas y todos los acuerdos y las condiciones son incluidas dentro del contrato de prestación de servicios, con el fin de asegurar el cumplimiento de dichas condiciones y garantizar así el uso apropiado de la información.

La gestión de los incidentes en dicha organización, presenta varias falencias, debido a que los reportes de eventos se realizan de forma automática por medio de los programas de protección de la información, pero no se revisan de forma periódica ni se registran debidamente;

además, se revisa únicamente el tipo de amenazas que se han presentado de forma informativa pero no se toma ninguna acción respecto a estas, ya que lo consideran innecesario por el hecho de no haberse visto afectados por ninguna de estas. De igual forma, la empresa de seguridad privada N no cuenta con una continuidad de seguridad plenamente identificada, debido a que nunca han tenido la necesidad de hacerlo, pues la organización no ha presentado ningún tipo de crisis y no consideran necesario establecerlo, ya que no contemplan la posibilidad de que pueda llegar a ocurrir una situación adversa.

Para el cumplimiento de los requisitos legales, se identifica y documenta el sistema y las políticas dentro de la política integral, de acuerdo con los parámetros establecidos por la norma BASC, pero no se realiza de forma individual y especifica, ni se realiza de acuerdo con los requisitos establecidos por la norma ISO/IEC 27001:2013.

Conclusiones

De acuerdo con el objetivo que se había planteado de analizar los factores que impulsaron la implementación del sistema de seguridad de la empresa, se llega a la conclusión de que fue la constante evolución que presenta la tecnología, la cual demanda actualización constante de los sistemas dentro de las organizaciones de este sector , para fortalecer internamente la protección de la información crítica que manejan y contrarrestar las nuevas formas de realizar amenazas, para lograr fortalecer la protección de las bases de datos que contienen la información de sus clientes.

De acuerdo a los objetivos de verificar las condiciones y describir el nivel de seguridad de la información frente a la norma se logra concluir que la empresa de seguridad N, aplica controles estrictos, basándose en los requisitos exigidos por la norma BASC lo que ha contribuido a que cumplan en un 85,91% con los numerales estipulados en la norma ISO/IEC 27001:2013, logrando dar respuesta al objetivo general planteado en esta investigación.

Recomendaciones

La presente investigación sirve como soporte para futuras investigaciones basadas en la norma ISO/IEC 27001, relacionadas con el manejo y la seguridad de la información, por este motivo, se recomienda realizar un análisis minucioso a la organización u organizaciones objeto de investigación y a su área de seguridad de la información, debido que este campo es muy amplio y complejo. En el presente documento, se encuentran conceptos y procedimientos que se aplican de forma muy técnica, los cuales tienen sus respectivas contextualizaciones, con el fin de facilitar el entendimiento de la misma.

De igual forma, se recomienda que los instrumentos a aplicar se elaboren de manera muy detallada, para identificar más fácilmente el enfoque principal que tiene la organización en el manejo de información.

Por otra parte, para las empresas que deseen iniciar su proceso de implementación o certificación de la norma ISO/IEC 27001, se recomienda realizar una verificación del estado inicial en el que se encuentra la organización, con el fin de saber cuáles son los requisitos que aún no se están cumpliendo y poder implementar los planes de mejora necesarios; así, será más sencillo cumplir a cabalidad con los requisitos, lineamientos y políticas que establece dicha norma y el proceso de evaluación y diagnóstico se realizará con una mayor eficacia.

A la empresa de seguridad privada N, se recomienda desarrollar y definir un marco de gestión de riesgos que incluya e identifique las posibles amenazas y ataques que puedan sufrir, para fortalecer la protección interna y conocer las dificultades que presenten frente a cualquier ataque o amenaza efectivo dentro de estas; y poder aplicar las soluciones establecidas para cada caso.

Bibliografía

© Estatal de Seguridad. (18 de Enero de 2018). *Estatal de Seguridad ::: Seguridad y Confianza*. Obtenido de Estatal de Seguridad ::: Seguridad y Confianza: http://estataldeseguridad.com.co/web/

Aguirre Cardona, J. D., & Aristizábal Betancourt, C. (2013). *0058A284.pdf.* Obtenido de 0058A284.pdf: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

Aguirre Tobar, R. A., & Zambrano Ordóñez, A. F. (26 de Octubre de 2015). *Estudio para la implementación del sistema de gestión de seguridad de la información para la secretaria de educación departamental de Nariño basado en la norma ISO/IEC 27001.* Obtenido de Estudio para la implementación del sistema de gestión de seguridad de la información para la secretaria de educación departamental de Nariño basado en la norma ISO/IEC 27001: http://repository.unad.edu.co/bitstream/10596/3655/1/13039116.pdf

Alcaldía de Bogotá. (01 de Octubre de 2017). *Consulta de la Norma:*. Obtenido de Consulta de la Norma:: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Alcaldía de Pereira. (20 de Diciembre de 2016). *Información del Municipio*. Obtenido de Información del Municipio: http://www.pereira.gov.co/MiMunicipio/Paginas/Informacion-del-Municipio.aspx

Álvarez, C. (22 de Abril de 2014). *El análisis morfosintáctico de una oración*. Obtenido de unProfesor: https://www.unprofesor.com/lengua-espanola/el-analisis-morfosintactico-de-una-oracion-111.html

Ascanio Arévalo, J. G., Trillos Bayona, R. A., & Bautista Rico, D. W. (1 de Diciembre de 2015). *Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información | Arévalo Ascanio | Tecnura.* Obtenido de Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información | Arévalo Ascanio | Tecnura: https://revistas.udistrital.edu.co/ojs/index.php/Tecnura/article/view/9551/10782

Bancada Cruceña. (13 de Abril de 2009). *Que son los Sistemas Biométricos*. Obtenido de eju.tv: http://eju.tv/2009/04/que-son-los-sistemas-biometricos/

Beek, C., Dinkar, D., Gund, Y., Lancioni, G., Minihane, N., Moreno, F., . . . Weafer, V. (3 de Julio de 2017). *Informe trimestral de McAfee Labs sobre amenazas, junio de 2017.* Obtenido de Informe trimestral de McAfee Labs sobre amenazas, junio de 2017: https://www.mcafee.com/es/resources/reports/rp-quarterly-threats-jun-2017.pdf

Benassini, M. (2009). *Introducción a la investigación de mercados: enfoque para América Latina* (Segunda edición ed.). México: Pearson Educación.

Benavides Sepúlveda, A. M., & Blandón Jaramillo, C. A. (24 de Julio de 2017). *INFORME FINAL ALEJANDRA & CARLOS V5.pdf.* Obtenido de INFORME FINAL ALEJANDRA & CARLOS V5.pdf: http://repositorio.autonoma.edu.co/jspui/bitstream/11182/1117/1/INFORME%20FINAL%20AL

Benchimol, D. (2011). *Hacking.* Buenos Aires: Fox Andina.

Bolaños, J., Simoneau, V., & Becerra, H. (2009). *Giga. No. 3, 2005.* La Habana: COPEXTEL.

Borghello, C. F. (1 de Julio de 2016). *Seguridad Informatica / Seguridad Física - Protección Electrónica*. Obtenido de Segu.Info: http://www.segu-info.com.ar/fisica/electronica.htm

Bueno Bustos, S. S. (27 de Abril de 2016). *45593318.pdf.* Obtenido de 45593318.pdf: http://repository.unad.edu.co/bitstream/10596/6169/1/45593318.pdf

Caceres Goyeneche, A. D. (3 de Octubre de 2015). *Políticas de seguridad informática como herramienta para la preservación e integridad de la información en las empresas de seguridad privada en Bogotá.* Obtenido de Políticas de seguridad informática como herramienta para la preservación e integridad de la información en las empresas de seguridad privada en Bogotá: http://repository.unimilitar.edu.co/bitstream/10654/7164/1/POLITICAS%20DE%20SEGURIDAD%20ensayo.pdf

Concejo Municipal de Pereira. (28 de Mayo de 2017). *Historia*. Obtenido de Concejo Municipal de Pereira: http://www.concejopereira.gov.co/wp/ipaginas/ver/63/historia/

Consejo superior de investigaciones científicas. (2013). *Arbor: ciencia, pensamiento y cultura. Vol. 189. Nro. 760.* Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas.

Costas Santos, J. (2014). *Seguridad informática.* Madrid: RA-MA Editorial.

Costas Santos, J. (2014). *Seguridad informática.* Madrid: RA-MA Editorial.

Cuevas Agustín, G. (1975). *Teoría de la información, codificación y lenguajes.* Madrid: Servicio de Publicaciones del Ministerio de Educación y Ciencia.

Definición.de. (18 de Enero de 2018). *Concepto de seguridad — Definicion.de.* Obtenido de Concepto de seguridad - Definición, Significado y Qué es: https://definicion.de/seguridad/

Dinero. (4 de Agosto de 2014). *Empresas colombianas se preocupan por su seguridad informática*. Obtenido de Empresas colombianas se preocupan por su seguridad informática: http://www.dinero.com/empresas/articulo/virus-males-ciberneticos-empresas-colombianas/199331

Dinero. (5 de Enero de 2016). *El 2015 fue un año de “altas y bajas” para la seguridad informática*. Obtenido de El 2015 fue un año de “altas y bajas” para la seguridad informática: http://www.dinero.com/pais/articulo/informe-certicamara-sobre-seguridad-informatica-colombia-para-2016/217635

Dinero. (15 de Septiembre de 2016). *'Hacktivistas' tienen a las empresas en alerta*. Obtenido de 'Hacktivistas' tienen a las empresas en alerta: http://www.dinero.com/edicion-impresa/tecnologia/articulo/los-riesgos-empresariales-por-los-ciberataques/231868

Dinero. (19 de Enero de 2017). *Las empresas colombianas escatiman en gastos y se rajan en ciberseguridad*. Obtenido de Las empresas colombianas escatiman en gastos y se rajan en ciberseguridad: http://www.dinero.com/empresas/articulo/encuesta-anual-de-seguridad-de-la-informacion-de-la-firma-ey/241201

Dix, J. (12 de Abril de 2016). *Encuesta Global de Seguridad de la Información 2015.* Obtenido de Encuesta Global de Seguridad de la Información 2015: http://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2015/$FILE/ey-encuesta-global-seguridad-informacion-2015.pdf

eldiario.es. (16 de Mayo de 2013). *Grandes robos informáticos de la historia*. Obtenido de Grandes robos informáticos de la historia: http://www.eldiario.es/turing/Grandes-robos-informaticos-historia_0_132986921.html

Empresa de seguridad privada N. (18 de Enero de 2018). *Servicios de Seguridad Humana Escoltas Guardas en Colombia*. Obtenido de Servicios de Seguridad Humana Escoltas Guardas en Colombia: http://www.seguridadnacional.co/servicio/seguridad-humana/

ESET. (27 de Abril de 2017). *ESET Security Report Latinoamérica 2017.* Obtenido de eset-security-report-2017.pdf: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

Espinosa Betancur, J. G., García Gallo, R. S., & Giraldo Restrepo, A. (9 de Julio de 2016). *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS TRES PROCESOS MISIONALES DE LA CORPORACIÓN AUTÓNOMA REGIONAL DE RISARALDA (CARDER) - SGSI CARDER - Informe Final.pdf.* Obtenido de SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS TRES PROCESOS MISIONALES DE LA CORPORACIÓN AUTÓNOMA REGIONAL DE RISARALDA (CARDER) - SGSI CARDER - Informe Final.pdf: http://repositorio.autonoma.edu.co/jspui/bitstream/11182/976/1/SGSI%20CARDER%20-

Garzón Garzón, M. (7 de Julio de 2017). *Diseñar los controles de acceso aplicables a la empresa Spytech S.A.S para su posterior implementación, de acuerdo con el dominio A9 de la norma ISO 27001:2013.* Obtenido de 52355641.pdf: http://repository.unad.edu.co:8080/bitstream/10596/11990/1/52355641.pdf

Gómez Vieites, Á. (2014). *Sistemas seguros de acceso y transmisión de datos.* Madrid: RA-MA Editorial.

Google Maps. (2018). *Pereira - Google Maps*. Obtenido de Pereira - Google Maps: https://www.google.com.co/maps/place/Pereira,+Risaralda/@4.804771,-75.7487832,13z/data=!4m5!3m4!1s0x8e388748eb56c1fd:0x95b39410f9f1dfbc!8m2!3d4.808717 4!4d-75.690601

Henao Acosta, C. (2010). *CDPEIST14.pdf.* Obtenido de CDPEIST14.pdf: http://repositorio.ucp.edu.co:8080/jspui/bitstream/10785/3056/1/CDPEIST14.pdf

Hernández Sampieri, R., Collado, C. F., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6 ed.). México D.F.: Mc Graw Hill Education.

ICONTEC. (2013). *Norma Técnica Colombiana NTC-ISO-IEC 27001.* Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

INCIBE. (s.f.). *INCIBE*. Obtenido de INCIBE: https://www.incibe.es/

Lucuze, P. d. (1772). *Principios de fortificación.* Barcelona: Thomas Piferrer.

Matalobos Veiga, J. M. (22 de Septiembre de 2014). *Trabajo de fin de carrera - PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf.* Obtenido de Trabajo de fin de carrera - PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf: http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

Medina, E. (14 de Julio de 2017). *LeakerLocker es un ransomware para Android que filtra información privada del usuario - MuySeguridad*. Obtenido de MuySeguridad: http://muyseguridad.net/2017/07/14/leakerlocker-ransomware-android-filtra-informacion-privada/

Molina Mateos, J. M. (2000). *Seguridad de la información. Criptología.* Córdoba: El Cid Editor.

Morales, G. I. (2013). Responsabilidad civil de las empresas de seguridad privada. *Revista de la Asociación Española de Abogados Especializados en Responsabilidad Civil y Seguro, (46)*, 33.

Moreno, J. C. (2014). *Reparación de equipamiento microinformático.* Madrid: RA-MA Editorial.

Noticias Universia España. (22 de Noviembre de 2003). *NUEVAS AMENAZAS DE INTERNET: DIALERS*. Obtenido de Noticias Universia España: http://noticias.universia.es/ciencia-nn-tt/noticia/2003/11/22/615922/nuevas-amenazas-internet-dialers.html

Pallas, G., & Corti, M. E. (22 de Febrero de 2016). *Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica.* Obtenido de CIBSI-Dia2-Sesion3(4).pdf: http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-

Panda Security. (2017). *PandaLabs Report Q2 2017 - Pandalabs-2017-Q2-ES.pdf.* Obtenido de PandaLabs Report Q2 2017 - Pandalabs-2017-Q2-ES.pdf: https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/08/Pandalabs-2017-Q2-ES.pdf

Panda Security. (27 de Junio de 2017). *Petya: Nuevo ataque global de ransomware - Panda Security*. Obtenido de Petya: Nuevo ataque global de ransomware - Panda Security: http://www.pandasecurity.com/spain/mediacenter/malware/petya-ataque-ransomware/

Perafán Ruiz, J. J., & Caicedo Cuchimba, M. (10 de Noviembre de 2014). *Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca.* Obtenido de PROYECTOSEGURIDADINFORMATICA_1.docx.docx - 76327474.pdf: http://repository.unad.edu.co:8080/bitstream/10596/2655/3/76327474.pdf

Pérez Hernández, C., Moreno Ortiz, A., & Fáber, P. (1999). Lexicografía computacional y lexicografía de corpus. *Revista española de lingüística aplicada*, 175-214. Obtenido de http://tecnolengua.uma.es/doc2/resla98.pdf

Portafolio. (27 de Febrero de 2017). *Qué es el 'phishing' delito informático*. Obtenido de Qué es el 'phishing' delito informático: http://www.portafolio.co/mis-finanzas/que-es-el-phishing-delito-informatico-503702

Real Academia Española. (19 de Junio de 2005). *DPD 1.ª edición, 2.ª tirada*. Obtenido de Diccionario panhispánico de dudas: http://lema.rae.es/dpd/srv/search?id=HTm1EjFzPD6zs66ao6

Rico Trejos, W., & Saavedra Rivera, S. (2015). *PROPUESTA PARA LA IMPLEMENTACION DE UN PLAN DE SEGURIDAD EN LA ALCALDIA DE DOSQUEBRADAS - CDMIST126.pdf.* Obtenido de PROPUESTA PARA LA IMPLEMENTACION DE UN PLAN DE SEGURIDAD EN LA ALCALDIA DE DOSQUEBRADAS - CDMIST126.pdf: http://repositorio.ucp.edu.co:8080/jspui/bitstream/10785/3658/1/CDMIST126.pdf

San Miguel, A. (3 de Octubre de 2011). *8 Tipos De Hackers Que Debes Conocer*. Obtenido de AxelSanMiguel.com: http://axelsanmiguel.com/8-tipos-de-hackers-que-debes-conocer/

Sánchez Orense, M. (2012). *La fortificación y el arte militar en los tratados renacentistas en lengua castellana: estudio lexicológico y lexicográfico.* Salamanca: Ediciones Universidad de Salamanca.

Sánchez Solá, Á. P. (Noviembre de 2013). *Diseño de un sistema de gestión de la seguridad de la información para comercio electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de Quito.* Obtenido de Diseño de un sistema de gestión de la seguridad de la información para comercio electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de Quito: http://repositorio.puce.edu.ec/handle/22000/6293

Semana. (28 de Abril de 2014). *Seguridad privada al día*. Obtenido de Seguridad privada al día: http://www.semana.com/especiales-comerciales/seguridad/articulo/seguridad-privada-al-dia/385267-3

Sierra Jaramillo, O. A. (2011). *ESTUDIO DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN DIGITAL EN LAS EMPRESAS DEL DEPARTAMENTO DE RISARALDA - 0058S572.pdf.* Obtenido de ESTUDIO DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN DIGITAL EN LAS EMPRESAS DEL DEPARTAMENTO DE RISARALDA - 0058S572.pdf: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2370/0058S572.pdf?sequence=1

Simoneau, V., & Becerra, H. (2009). *Giga. No. 1, 2010.* La Habana: COPEXTEL.

Solarte Solarte, F. N., Enríquez Rosero, E. R., & Benavides, M. d. (Diciembre de 2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001.* Obtenido de Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001: http://www.rte.espol.edu.ec/index.php/tecnologica/article/viewFile/456/321

Tecnósfera con Información de Agencias. (27 de Junio de 2017). *Un nuevo ataque cibernético mundial afecta a varias multinacionales*. Obtenido de Un nuevo ataque cibernético mundial afecta a varias multinacionales: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/nuevo-ataque-cibernetico-afecta-a-empresas-en-el-mundo-103092

Ware, B. (13 de Enero de 2018). *Insider_Threat_Report_2017_Haystax_FINAL.pdf.* Obtenido de Insider_Threat_Report_2017_Haystax_FINAL.pdf: http://haystax.com/wp-content/uploads/2017/03/Insider_Threat_Report_2017_Haystax_FINAL.pdf

Apéndices

Apéndice N.° 1. Cuestionario de Preguntas Cerradas.

FUNDACIÓN UNIVERSITARIA DEL ÁREA ANDINA, SECCIONAL PEREIRA

CUESTIONARIO PARA DETERMINAR EL NIVEL DE SEGURIDAD DE LA INFORMACIÓN

El propósito del presente cuestionario es analizar los factores que impulsaron la implementación del sistema de seguridad de la información.

Fecha:	Día		Mes		Año		Nombre de la empresa:
Teléfono:							E-mail:
Dirección:							Área encargada del control del SGSI:
Nombre del responsable del SGSI:							Cargo:
Persona a quien se entrevista:							Cargo:

1. ¿Cuántos ataques a la información experimentó su organización en los últimos 12 meses?

1.1 Ninguno		1.2 Entre 1 y 5		1.3 Entre 6 y 10		1.4 Entre 11 y 15	
1.5 Entre 15 y 20		1.6 Más de 20		1.7 No sabe			

2. ¿Por cuántos de estos ataques se han visto afectados?

2.1 Ninguno		2.2 Entre 1 y 5		2.3 Entre 6 y 10		2.4 Entre 11 y 15	
2.5 Entre 15 y 20		2.6 Más de 20		2.7 No sabe			

3. ¿Cree que los ataques generalmente se han vuelto más frecuentes en los últimos 12 meses?

3.1 Sí		3.2 No		3.3 No sabe	

4. ¿Qué tipo de amenazas le preocupan más?

4.1 Filtración o fuga de datos inadvertida		4.2 Infracción de datos por negligencia	
4.3 Infracciones maliciosas de datos		4.4 Otra (indique cuál)	

5. ¿Qué grupos de usuarios representan el mayor riesgo de seguridad para las organizaciones?

5.1 Usuarios privilegiados de TI y administradores con acceso a información confidencial					
5.2 Contratistas y consultores temporales		5.3 Empleados regulares			
5.4 Usuarios de negocios privilegiados		5.5 Gerentes ejecutivos			
5.6 Socios comerciales		5.7 Otro personal de TI			
5.8 Clientes		5.9 Otro (indique cuál)			

6. ¿Qué motivaciones para las amenazas maliciosas le preocupa más?

6.1 Monetizar datos confidenciales		6.2 Fraude		6.3 Sabotaje		6.4 Robo de IP	
6.5 Espionaje		6.6 Otra (indique cuál)					

7. ¿Qué activos de TI son más vulnerables a los ataques?

7.1 Bases de datos		7.2 Servidores de archivos		7.3 Dispositivos móviles	
7.4 Endpoints		7.5 Aplicaciones comerciales		7.6 Infraestructura en la nube	
7.7 Aplicaciones en la nube		7.8 Redes		7.9 Otro (indique cuál)	

8. ¿Qué tipos de datos son más vulnerables a los ataques?

8.1 Datos de los clientes		8.2 Datos financieros		8.3 Propiedad intelectual	
8.4 Datos de la planeación estratégica de la compañía					
8.5 Datos de los empleados		8.6 Datos de ventas y mercadeo		8.7 Datos de la salud	
8.8 Otro (indique cuál)					

9. ¿Qué activos de TI se usan con más frecuencia para lanzar ataques?

9.1 Aplicaciones comerciales		9.2 Dispositivos móviles		9.3 Redes		9.4 Servidores de archivos	
9.5 Endpoints		9.6 Bases de datos		9.7 Infraestructura o aplicaciones en la nube			
9.8 Otro (indique cuál)							

10. ¿Cuáles cree que son las principales razones por las cuales las amenazas están aumentando?

10.1 Insuficientes estrategias y soluciones de protección de datos	

10.2 Número creciente de dispositivos con acceso a datos confidenciales	
10.3 Proliferación de datos sensibles que se mueven fuera del firewall en dispositivos móviles	
10.4 Más empleados, contratistas y socios que acceden a la red	
10.5 Aumento de la cantidad de datos confidenciales	
10.6 Mayor conocimiento público o visibilidad de amenazas internas que no fueron reveladas	
10.7 La tecnología se vuelve más compleja	
10.8 Uso creciente de aplicaciones e infraestructuras en la nube	
10.9 Otra (indique cuál)	

11: ¿Qué tan vulnerable es su organización a las amenazas?

11.1 Extremadamente vulnerable		11.2 Muy vulnerable		11.3 Moderadamente vulnerable	
11.4 Ligeramente vulnerable		11.5 Nada vulnerable			

12: ¿Su organización tiene los controles apropiados para prevenir un ataque?

12.1 Sí		12.2 No		12.3 No sabe	

13: ¿Qué tan difícil es detectar y prevenir los ataques internos en comparación con los ciberataques externos?

13.1 Más difícil que detectar y prevenir ciberataques externos	
13.2 Tan difícil como detectar y prevenir ciberataques externos	
13.3 Menos difícil que detectar y prevenir ataques cibernéticos externos	

14: ¿Qué hace que la detección y prevención de ataques sea cada vez más difícil en comparación con hace un año?

14.1 Personas con acceso a sistemas e información confidencial	
14.2 El uso incrementado de aplicaciones en la nube que pueden filtrar datos	
14.3 El aumento en la cantidad de datos que está dejando el perímetro de la red protegida	
14.4 Más dispositivos de usuario final capaces de robo	
14.5 Dificultad para detectar dispositivos fraudulentos introducidos en la red o sistemas	
14.6 Ausencia de un programa de gobernanza de la seguridad de la información	
14.7 Los empleados son más sofisticados	
14.8 Migración de datos confidenciales a la nube junto con la adopción de aplicaciones en la nube	

14.9 Otro (indique cuál)	

15: ¿Monitorea el comportamiento de los usuarios?

15.1 Sí, pero solo acceso a registros	
15.2 Sí, utilizamos herramientas automatizadas para monitorear el comportamiento del usuario	
15.3 Sí, pero solo bajo circunstancias específicas	
15.4 Sí, pero solo después de un incidente	
15.5 No, no supervisamos el comportamiento del usuario en absoluto	
15.6 No sabe	

16: ¿Qué nivel de visibilidad tiene usted sobre el comportamiento del usuario dentro de las aplicaciones centrales?

16.1 Sistema/función de auditoría en la aplicación		16.2 Registros del servidor	
16.3 Se implementó el monitoreo de la actividad del usuario		16.4 Sin visibilidad en absoluto	
16.5 Han implementado el registro de claves			

17: ¿Su organización aprovecha los análisis para determinar las amenazas?

17.1 Sí, gestión de actividades e informes resumidos		17.2 Sí, acceso a datos y análisis de movimiento	
17.3 Sí, análisis de comportamiento del usuario		17.4 Sí, análisis predictivo	
17.5 No		17.6 No sabe	

18: ¿Incluye ataques cibernéticos en su marco de gestión de riesgos?

18.1 Sí		18.2 No		18.3 No sabe	

19: ¿Qué controles de riesgo utilizan para gestionar el riesgo de ocurrencias de ciberataques?

19.1 Tableros de eventos de seguridad		19.2 Herramientas de defensa perimetral de seguridad	
19.3 Sistema de monitoreo de registros		19.4 Procesos de remediación de eventos de seguridad	
19.5 Herramientas de base de datos y monitoreo de archivos			
19.6 Violaciones de acceso (indicadores clave de riesgo por base de datos o sistema)			
19.7 Pérdida de datos y corrupción (principales indicadores de riesgo)			
19.8 Tiempo de inactividad del sistema (indicadores clave de riesgo)			

19.9 Otro (indique cuál)	

20: ¿Cuáles son las principales barreras para una mejor administración de amenazas?

20.1 Falta de capacitación y experiencia		20.2 Falta de colaboración entre los departamentos			
20.3 Falta de tecnología adecuada		20.4 Falta de personal		20.5 Presupuestos insuficientes	
20.6 No tienen barreras		20.7 Otro (indique cuál)			

21: ¿Cómo combate su organización las amenazas hoy?

21.1 Programa de gobernanza de la seguridad de la información		21.2 Capacitación del usuario			
21.3 Aplicaciones y dispositivos especializados de terceros		21.4 Verificaciones de antecedentes			
21.5 Proveedor de servicios de seguridad administrados		21.6 Autenticación secundaria			
21.7 Monitoreo de actividad de base de datos		21.8 Actividad de monitoreo del usuario			
21.9 Funciones de seguridad nativas del sistema operativo subyacente					
21.10 Herramientas personalizadas y aplicaciones desarrolladas en la casa					
21.11 Todas las anteriores		21.12 No usan nada		21.13 Otro (indique cuál)	

22: ¿En qué aspectos de la gestión de amenazas se concentra su organización principalmente?

22.1 Tácticas de disuasión		22.2 Tácticas de detección		22.3 Análisis y análisis forense	
22.4 Engaño (por ejemplo, honeypots, etc.)				22.5 Ninguna	
22.6 Otro (indique cuál)					

23: ¿Cómo cambiará su presupuesto de seguridad en los próximos 12 meses?

23.1 Esperan un aumento en el presupuesto de seguridad en los próximos 12 meses		
23.2 El presupuesto se mantendrá plano		23.3 El presupuesto disminuirá

24: ¿Cuánto tiempo le tomaría a su organización detectar un ataque?

24.1 En minutos		24.2 En cuestión de horas		24.3 Dentro de un día	

24.4 Dentro de una semana		24.5 Dentro de un mes		24.6 Dentro de tres meses	
24.7 Más de tres meses		24.8 Sin capacidad de detectar			

25: ¿Cuánto tiempo le tomaría a su organización recuperarse de un ataque?

25.1 En una semana		25.2 Dentro de un mes		25.3 Dentro de tres meses	
25.4 Más de tres meses		25.5 Sin capacidad para recuperar		25.6 No sabe	

26: ¿Cuál es el costo promedio estimado de remediación después de un ataque?

26.1 Menos de 100.000 dólares		26.2 Entre 100.000 y 500.000 dólares	
26.3 Entre 500.000 y 1’000.000 dólares		26.4 Entre 1’000.000 y 2’000.000 dólares	
26.5 Más de 2’000.000 dólares		26.6 No sabe	

27: Dentro de su organización, ¿qué tan difícil es determinar el daño real de una amenaza?

27.1 Muy difícil		27.2 Moderadamente difícil		27.3 Nada difícil	

Gracias por su amable colaboración. Que tenga un excelente día.

Apéndice N.° 2. Lista de Chequeo.

FUNDACIÓN UNIVERSITARIA DEL ÁREA ANDINA, SECCIONAL PEREIRA

LISTA DE CHEQUEO PARA DETERMINAR EL NIVEL DE SEGURIDAD DE LA INFORMACIÓN

El propósito de la presente lista de chequeo es verificar las condiciones iniciales del sistema de seguridad de la información, frente a lo que estipula la norma ISO/IEC 27001:2013.

Fecha:	Día		Mes		Año		Nombre de la empresa:
Teléfono:							E-mail:
Dirección:							Área encargada del control del SGSI:
Nombre del responsable del SGSI:							Cargo:
Persona a quien se entrevista:							Cargo:

Objetivos de control y controles					
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN					
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información					
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.					
A.5.1.1	Políticas para la seguridad de la información	*Control* Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	***Se realiza***	***No se realiza***	***No aplica***
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	***Se realiza***	***No se realiza***	***No aplica***
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					
A.6.1 Organización interna					
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.					
A.6.1.1	Roles y responsabilidades para la seguridad	*Control* Se deben definir y asignar todas las responsabilidades de la seguridad de la	***Se realiza***	***No se realiza***	***No aplica***

	de la información	información.			
A.6.1.2	Separación de deberes	*Control* Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	***Se realiza***	***No se realiza***	***No aplica***
A.6.1.3	Contacto con las autoridades	*Control* Se deben mantener contactos apropiados con las autoridades pertinentes.	***Se realiza***	***No se realiza***	***No aplica***
A.6.1.4	Contacto con grupos de interés especial	*Control* Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	***Se realiza***	***No se realiza***	***No aplica***
A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyectos.	***Se realiza***	***No se realiza***	***No aplica***
A.6.2 Dispositivos móviles y teletrabajo					
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.					
A.6.2.1	Política para dispositivos móviles	*Control* Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	***Se realiza***	***No se realiza***	***No aplica***
A.6.2.2	Teletrabajo	*Control* Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	***Se realiza***	***No se realiza***	***No aplica***
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS					
A.7.1 Antes de asumir el empleo					
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.					
A.7.1.1	Selección	*Control* Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	***Se realiza***	***No se realiza***	***No aplica***

A.7.1.2	Términos y condiciones del empleo	*Control* Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	***Se realiza***	***No se realiza***	***No aplica***
A.7.2 Durante la ejecución del empleo					
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.					
A.7.2.1	Responsabilidades de la dirección	*Control* La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	***Se realiza***	***No se realiza***	***No aplica***
A.7.2.2	Toma de conciencia, educación y la formación en la seguridad de la información	*Control* Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	***Se realiza***	***No se realiza***	***No aplica***
A.7.2.3	Proceso disciplinario	*Control* Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	***Se realiza***	***No se realiza***	***No aplica***
A.7.3 Terminación y cambio de empleo					
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.					
A.7.3.1	Terminación o cambio de responsabilidades de empleo	*Control* Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	***Se realiza***	***No se realiza***	***No aplica***
A.8 GESTIÓN DE ACTIVOS					
A.8.1 Responsabilidad por los activos					
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección apropiadas.					
A.8.1.1	Inventario de activos	*Control* Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe	***Se realiza***	***No se realiza***	***No aplica***

		elaborar y mantener un inventario de estos activos.			
A.8.1.2	Propiedad de los activos	*Control* Los activos mantenidos en el inventario deben tener un propietario.	***Se realiza***	***No se realiza***	***No aplica***
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	***Se realiza***	***No se realiza***	***No aplica***
A.8.1.4	Devolución de los activos	*Control* Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	***Se realiza***	***No se realiza***	***No aplica***
A.8.2 Clasificación de la información					
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.					
A.8.2.1	Clasificación de la información	*Control* La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada.	***Se realiza***	***No se realiza***	***No aplica***
A.8.2.2	Etiquetado de la información	*Control* Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	***Se realiza***	***No se realiza***	***No aplica***
A.8.2.3	Manejo de activos	*Control* Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	***Se realiza***	***No se realiza***	***No aplica***
A.8.3 Manejo de medios					
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios.					
A.8.3.1	Gestión de medios removibles	*Control* Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	***Se realiza***	***No se realiza***	***No aplica***

A.8.3.2	Disposición de los medios	*Control* Se debe disponer de forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	***Se realiza***	***No se realiza***	***No aplica***
A.8.3.3	Transferencia de medios físicos	*Control* Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	***Se realiza***	***No se realiza***	***No aplica***
A.9 CONTROL DE ACCESO					
A.9.1 Requisitos del negocio para control de acceso					
Objetivo: Limitar el acceso a información a instalaciones de procesamiento de información.					
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	***Se realiza***	***No se realiza***	***No aplica***
A.9.1.2	Acceso a redes y a servicios en red	*Control* Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	***Se realiza***	***No se realiza***	***No aplica***
A.9.2 Gestión de acceso de usuarios					
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.					
A.9.2.1	Registro y cancelación del registro de usuarios	*Control* Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	***Se realiza***	***No se realiza***	***No aplica***
A.9.2.2	Suministro de acceso de usuarios	*Control* Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	***Se realiza***	***No se realiza***	***No aplica***
A.9.2.3	Gestión de derechos de acceso privilegiado	*Control* Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	***Se realiza***	***No se realiza***	***No aplica***
A.9.2.4	Gestión de información de autenticación secreta de usuarios	*Control* La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	***Se realiza***	***No se realiza***	***No aplica***
A.9.2.5	Revisión de los	*Control*	***Se***	***No se***	***No***

	derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	***realiza***	***realiza***	***aplica***
A.9.2.6	Retiro o ajuste de los derechos de acceso	*Control* Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	***Se realiza***	***No se realiza***	***No aplica***
A.9.3 Responsabilidades de los usuarios					
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.					
A.9.3.1	Uso de información de autenticación secreta	*Control* Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	***Se realiza***	***No se realiza***	***No aplica***
A.9.4 Control de acceso a sistemas y aplicaciones					
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.					
A.9.4.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	***Se realiza***	***No se realiza***	***No aplica***
A.9.4.2	Procedimiento de ingreso seguro	*Control* Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	***Se realiza***	***No se realiza***	***No aplica***
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	***Se realiza***	***No se realiza***	***No aplica***
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	***Se realiza***	***No se realiza***	***No aplica***
A.9.4.5	Control de acceso a códigos fuente de programas	*Control* Se debe restringir el acceso a los códigos fuente de los programas.	***Se realiza***	***No se realiza***	***No aplica***
A.10 CRIPTOGRAFÍA					
A.10.1 Controles criptográficos					
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad,					

la autenticidad y/o la integridad de la información.					
A.10.1.1	Política sobre el uso de controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	***Se realiza***	***No se realiza***	***No aplica***
A.10.1.2	Gestión de llaves	*Control* Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	***Se realiza***	***No se realiza***	***No aplica***
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO					
A.11.1 Áreas seguras					
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.					
A.11.1.1	Perímetro de seguridad física	*Control* Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	***Se realiza***	***No se realiza***	***No aplica***
A.11.1.2	Controles de acceso físicos	*Control* Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.	***Se realiza***	***No se realiza***	***No aplica***
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	*Control* Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	***Se realiza***	***No se realiza***	***No aplica***
A.11.1.4	Protección contra amenazas externas y ambientales	*Control* Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	***Se realiza***	***No se realiza***	***No aplica***
A.11.1.5	Trabajo en áreas seguras	*Control* Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	***Se realiza***	***No se realiza***	***No aplica***
A.11.1.6	Áreas de despacho y carga	*Control* Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	***Se realiza***	***No se realiza***	***No aplica***
A.11.2 Equipos					
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las					

operaciones de la organización.					
A.11.2.1	Ubicación y protección de los equipos	*Control* Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	***Se realiza***	***No se realiza***	***No aplica***
A.11.2.2	Servicios de suministro	*Control* Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	***Se realiza***	***No se realiza***	***No aplica***
A.11.2.3	Seguridad del cableado	*Control* El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	***Se realiza***	***No se realiza***	***No aplica***
A.11.2.4	Mantenimiento de equipos	*Control* Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	***Se realiza***	***No se realiza***	***No aplica***
A.11.2.5	Retiro de activos	*Control* Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	***Se realiza***	***No se realiza***	***No aplica***
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	*Control* Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	***Se realiza***	***No se realiza***	***No aplica***
A.11.2.7	Disposición segura o reutilización de equipos	*Control* Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reuso.	***Se realiza***	***No se realiza***	***No aplica***
A.11.2.8	Equipos de usuario desatendido	*Control* Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	***Se realiza***	***No se realiza***	***No aplica***
A.11.2.9	Política de escritorio limpio y pantalla limpia	*Control* Se debe adoptar una política de escritorio limpio para los papeles y medios de	***Se realiza***	***No se realiza***	***No aplica***

		almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.			
A.12 SEGURIDAD DE LAS OPERACIONES					
A.12.1 Procedimientos operacionales y responsabilidades					
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de la información.					
A.12.1.1	Procedimientos de operación documentados	*Control* Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	***Se realiza***	***No se realiza***	***No aplica***
A.12.1.2	Gestión de cambios	*Control* Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	***Se realiza***	***No se realiza***	***No aplica***
A.12.1.3	Gestión de capacidad	*Control* Se debe hacer seguimiento al uso de recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	***Se realiza***	***No se realiza***	***No aplica***
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operaciones	*Control* Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	***Se realiza***	***No se realiza***	***No aplica***
A.12.2 Protección contra códigos maliciosos					
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.					
A.12.2.1	Controles contra códigos maliciosos	*Control* Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	***Se realiza***	***No se realiza***	***No aplica***
A.12.3 Copias de respaldo					
Objetivo: Proteger contra la pérdida de datos.					
A.12.3.1	Respaldo de la información	*Control* Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	***Se realiza***	***No se realiza***	***No aplica***
A.12.4 Registro y seguimiento					

Objetivo: Registrar eventos y generar evidencia.					
A.12.4.1	Registro de eventos	*Control* Se deben elaborar, conservar y revisar regularmente los requisitos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	***Se realiza***	***No se realiza***	***No aplica***
A.12.4.2	Protección de la información de registro	*Control* Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	***Se realiza***	***No se realiza***	***No aplica***
A.12.4.3	Registros del administrador y del operador	*Control* Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	***Se realiza***	***No se realiza***	***No aplica***
A.12.4.4	Sincronización de relojes	*Control* Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	***Se realiza***	***No se realiza***	***No aplica***
A.12.5 Control de software operacional					
Objetivo: Asegurarse de la integridad de los sistemas operacionales.					
A.12.5.1	Instalación de software en sistemas operativos	*Control* Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	***Se realiza***	***No se realiza***	***No aplica***
A.12.6 Gestión de la vulnerabilidad técnica					
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.					
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	***Se realiza***	***No se realiza***	***No aplica***
A.12.6.2	Restricciones sobre la instalación de software	*Control* Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	***Se realiza***	***No se realiza***	***No aplica***
A.12.7 Consideraciones sobre auditorías de sistemas de información					
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.					
A.12.7.1	Controles de auditorías de sistemas de	*Control* Los requisitos y actividades de auditoría que involucran la verificación de los	***Se realiza***	***No se realiza***	***No aplica***

	información	sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.			
A.13 SEGURIDAD DE LAS COMUNICACIONES					
A.13.1 Gestión de la seguridad de las redes					
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de soporte.					
A.13.1.1	Controles de redes	*Control* Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	***Se realiza***	***No se realiza***	***No aplica***
A.13.1.2	Seguridad de los servicios de red	*Control* Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	***Se realiza***	***No se realiza***	***No aplica***
A.13.1.3	Separación en las redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	***Se realiza***	***No se realiza***	***No aplica***
A.13.2 Transferencia de información					
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.					
A.13.2.1	Políticas y procedimientos de transferencia de información	*Control* Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	***Se realiza***	***No se realiza***	***No aplica***
A.13.2.2	Acuerdos sobre transferencia de información	*Control* Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	***Se realiza***	***No se realiza***	***No aplica***
A.13.2.3	Mensajería electrónica	*Control* Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	***Se realiza***	***No se realiza***	***No aplica***
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	*Control* Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no	***Se realiza***	***No se realiza***	***No aplica***

		divulgación que reflejen las necesidades de la organización para la protección de la información.			
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
A.14.1 Requisitos de seguridad de los sistemas de información					
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que presentan servicios sobre redes públicas.					
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	*Control* Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	***Se realiza***	***No se realiza***	***No aplica***
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	*Control* La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	***Se realiza***	***No se realiza***	***No aplica***
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	*Control* La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada.	***Se realiza***	***No se realiza***	***No aplica***
A.14.2 Seguridad en los procesos de desarrollo y de soporte					
Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.					
A.14.2.1	Política de desarrollo seguro	*Control* Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	***Se realiza***	***No se realiza***	***No aplica***
A.14.2.2	Procedimientos de control de cambios en sistemas	*Control* Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	***Se realiza***	***No se realiza***	***No aplica***
A.14.2.3	Revisión técnica de las aplicaciones	*Control* Cuando se cambian las plataformas de operación, se deben revisar las	***Se realiza***	***No se realiza***	***No aplica***

	después de cambios en la plataforma de operación	aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.			
A.14.2.4	Restricciones en los cambios a los paquetes de software	*Control* Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	***Se realiza***	***No se realiza***	***No aplica***
A.14.2.5	Principios de construcción de los sistemas seguros	*Control* Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	***Se realiza***	***No se realiza***	***No aplica***
A.14.2.6	Ambiente de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprenden todo el ciclo de vida de desarrollo de sistemas.	***Se realiza***	***No se realiza***	***No aplica***
A.14.2.7	Desarrollo controlado externamente	*Control* La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	***Se realiza***	***No se realiza***	***No aplica***
A.14.2.8	Pruebas de seguridad de sistemas	*Control* Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	***Se realiza***	***No se realiza***	***No aplica***
A.14.2.9	Prueba de aceptación de sistemas	*Control* Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	***Se realiza***	***No se realiza***	***No aplica***
A.14.3 Datos de prueba					
Objetivo: Asegurar la protección de los datos usados para pruebas.					
A.14.3.1	Protección de datos de prueba	*Control* Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	***Se realiza***	***No se realiza***	***No aplica***
A.15 RELACIONES CON LOS PROVEEDORES					
A.15.1 Seguridad de la información en las relaciones con los proveedores					
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.					

A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	*Control* Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	***Se realiza***	***No se realiza***	***No aplica***
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	*Control* Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	***Se realiza***	***No se realiza***	***No aplica***
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	*Control* Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	***Se realiza***	***No se realiza***	***No aplica***
A.15.2 Gestión de la prestación de servicios de proveedores					
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.					
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	*Control* Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	***Se realiza***	***No se realiza***	***No aplica***
A.15.2.2	Gestión de cambios en los servicios de los proveedores	*Control* Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.	***Se realiza***	***No se realiza***	***No aplica***
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN					
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información					
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.					
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer las responsabilidades y procedimientos de gestión para asegurar	***Se realiza***	***No se realiza***	***No aplica***

		una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.			
A.16.1.2	Reporte de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	***Se realiza***	***No se realiza***	***No aplica***
A.16.1.3	Reporte de debilidades de seguridad de la información	*Control* Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	***Se realiza***	***No se realiza***	***No aplica***
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	*Control* Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	***Se realiza***	***No se realiza***	***No aplica***
A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	***Se realiza***	***No se realiza***	***No aplica***
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	*Control* El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	***Se realiza***	***No se realiza***	***No aplica***
A.16.1.7	Recolección de evidencia	*Control* La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	***Se realiza***	***No se realiza***	***No aplica***
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO					
A.17.1 Continuidad de seguridad de la información					
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.					
A.17.1.1	Planificación de la continuidad de la seguridad de la	*Control* La organización debe determinar sus requisitos para la seguridad de la	***Se realiza***	***No se realiza***	***No aplica***

	información	información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.			
A.17.1.2	Implementación de la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	***Se realiza***	***No se realiza***	***No aplica***
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	***Se realiza***	***No se realiza***	***No aplica***
A.17.2 Redundancias					
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.					
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	*Control* Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir con los requisitos de disponibilidad.	***Se realiza***	***No se realiza***	***No aplica***
A.18 CUMPLIMIENTO					
A.18.1 Cumplimiento de requisitos legales y contractuales					
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.					
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	*Control* Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.	***Se realiza***	***No se realiza***	***No aplica***
A.18.1.2	Derechos de propiedad intelectual	*Control* Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	***Se realiza***	***No se realiza***	***No aplica***
A.18.1.	Protección de	*Control*	***Se***	***No se***	***No***

3	registros	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	***realiza***	***realiza***	***aplica***
A.18.1.4	Privacidad y protección de información de datos personales	*Control* Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	***Se realiza***	***No se realiza***	***No aplica***
A.18.1.5	Reglamentación de controles criptográficos	*Control* Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	***Se realiza***	***No se realiza***	***No aplica***
A.18.2 Revisiones de seguridad de la información					
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.					
A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	***Se realiza***	***No se realiza***	***No aplica***
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	*Control* Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	***Se realiza***	***No se realiza***	***No aplica***
A.18.2.3	Revisión del cumplimiento técnico	*Control* Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	***Se realiza***	***No se realiza***	***No aplica***

Gracias por su amable colaboración. Que tenga un excelente día.

Apéndice N.° 3. Cuestionario de Preguntas Cerradas Aplicado en la Empresa de Seguridad Privada N.

FUNDACIÓN UNIVERSITARIA DEL ÁREA ANDINA, SECCIONAL PEREIRA

CUESTIONARIO PARA DETERMINAR EL NIVEL DE SEGURIDAD DE LA INFORMACIÓN

El propósito del presente cuestionario es analizar los factores que impulsaron la implementación del sistema de seguridad de la información.

Fecha:	Día	06	Mes	04	Año	2018	Nombre de la empresa: Empresa de seguridad privada N
Teléfono: *Confidencial*							E-mail: *Confidencial*
Dirección: *Confidencial*							Área encargada del control del SGSI: Área de tecnología de información y área de calidad
Nombre del responsable del SGSI: *Confidencial* *Confidencial*							Cargo: Director del área de tecnología de información Directora del área de calidad
Persona a quien se entrevista: *Confidencial* *Confidencial*							Cargo: Director del área de tecnología de información Directora del área de calidad

1. ¿Cuántos ataques a la información experimentó su organización en los últimos 12 meses?

1.1 Ninguno		1.2 Entre 1 y 5		1.3 Entre 6 y 10		1.4 Entre 11 y 15	
1.5 Entre 15 y 20		1.6 Más de 20	X	1.7 No sabe			

2. ¿Por cuántos de estos ataques se han visto afectados?

2.1 Ninguno	X	2.2 Entre 1 y 5		2.3 Entre 6 y 10		2.4 Entre 11 y 15	
2.5 Entre 15 y 20		2.6 Más de 20		2.7 No sabe			

3. ¿Cree que los ataques generalmente se han vuelto más frecuentes en los últimos 12 meses?

3.1 Sí	X	3.2 No		3.3 No sabe	

4. ¿Qué tipo de amenazas le preocupan más?

4.1 Filtración o fuga de datos inadvertida		4.2 Infracción de datos por negligencia			
4.3 Infracciones maliciosas de datos		4.4 Otra (indique cuál)	Robo de información		

5. ¿Qué grupos de usuarios representan el mayor riesgo de seguridad para las organizaciones?

5.1 Usuarios privilegiados de TI y administradores con acceso a información confidencial					X
5.2 Contratistas y consultores temporales		5.3 Empleados regulares			
5.4 Usuarios de negocios privilegiados		5.5 Gerentes ejecutivos			
5.6 Socios comerciales		5.7 Otro personal de TI			
5.8 Clientes		5.9 Otro (indique cuál)			

6. ¿Qué motivaciones para las amenazas maliciosas le preocupa más?

6.1 Monetizar datos confidenciales	X	6.2 Fraude		6.3 Sabotaje		6.4 Robo de IP	
6.5 Espionaje		6.6 Otra (indique cuál)					

7. ¿Qué activos de TI son más vulnerables a los ataques?

7.1 Bases de datos	X	7.2 Servidores de archivos		7.3 Dispositivos móviles	
7.4 Endpoints		7.5 Aplicaciones comerciales		7.6 Infraestructura en la nube	
7.7 Aplicaciones en la nube		7.8 Redes		7.9 Otro (indique cuál)	

8. ¿Qué tipos de datos son más vulnerables a los ataques?

8.1 Datos de los clientes	X	8.2 Datos financieros		8.3 Propiedad intelectual	
8.4 Datos de la planeación estratégica de la compañía					
8.5 Datos de los empleados		8.6 Datos de ventas y mercadeo		8.7 Datos de la salud	
8.8 Otro (indique cuál)					

9. ¿Qué activos de TI se usan con más frecuencia para lanzar ataques?

9.1 Aplicaciones comerciales		9.2 Dispositivos móviles		9.3 Redes	X	9.4 Servidores de archivos	
9.5 Endpoints		9.6 Bases de datos		9.7 Infraestructura o aplicaciones en la nube			
9.8 Otro (indique cuál)							

10. ¿Cuáles cree que son las principales razones por las cuales las amenazas están aumentando?

10.1 Insuficientes estrategias y soluciones de protección de datos	
10.2 Número creciente de dispositivos con acceso a datos confidenciales	
10.3 Proliferación de datos sensibles que se mueven fuera del firewall en dispositivos móviles	
10.4 Más empleados, contratistas y socios que acceden a la red	
10.5 Aumento de la cantidad de datos confidenciales	
10.6 Mayor conocimiento público o visibilidad de amenazas internas que no fueron reveladas	
10.7 La tecnología se vuelve más compleja	X
10.8 Uso creciente de aplicaciones e infraestructuras en la nube	
10.9 Otra (indique cuál)	

11: ¿Qué tan vulnerable es su organización a las amenazas?

11.1 Extremadamente vulnerable		11.2 Muy vulnerable		11.3 Moderadamente vulnerable	
11.4 Ligeramente vulnerable		11.5 Nada vulnerable	X		

12: ¿Su organización tiene los controles apropiados para prevenir un ataque?

12.1 Sí	X	12.2 No		12.3 No sabe	

13: ¿Qué tan difícil es detectar y prevenir los ataques internos en comparación con los ciberataques externos?

13.1 Más difícil que detectar y prevenir ciberataques externos	
13.2 Tan difícil como detectar y prevenir ciberataques externos	X
13.3 Menos difícil que detectar y prevenir ataques cibernéticos externos	

14: ¿Qué hace que la detección y prevención de ataques sea cada vez más difícil en comparación con hace un año?

14.1 Personas con acceso a sistemas e información confidencial	
14.2 El uso incrementado de aplicaciones en la nube que pueden filtrar datos	
14.3 El aumento en la cantidad de datos que está dejando el perímetro de la red protegida	
14.4 Más dispositivos de usuario final capaces de robo	
14.5 Dificultad para detectar dispositivos fraudulentos introducidos en la red o sistemas	

14.6 Ausencia de un programa de gobernanza de la seguridad de la información	
14.7 Los empleados son más sofisticados	
14.8 Migración de datos confidenciales a la nube junto con la adopción de aplicaciones en la nube	
14.9 Otro (indique cuál)	Las amenazas están evolucionando constantemente

15: ¿Monitorea el comportamiento de los usuarios?

15.1 Sí, pero solo acceso a registros	
15.2 Sí, utilizamos herramientas automatizadas para monitorear el comportamiento del usuario	X
15.3 Sí, pero solo bajo circunstancias específicas	
15.4 Sí, pero solo después de un incidente	
15.5 No, no supervisamos el comportamiento del usuario en absoluto	
15.6 No sabe	

16: ¿Qué nivel de visibilidad tiene usted sobre el comportamiento del usuario dentro de las aplicaciones centrales?

16.1 Sistema/función de auditoría en la aplicación		16.2 Registros del servidor	
16.3 Se implementó el monitoreo de la actividad del usuario	X	16.4 Sin visibilidad en absoluto	
16.5 Han implementado el registro de claves			

17: ¿Su organización aprovecha los análisis para determinar las amenazas?

17.1 Sí, gestión de actividades e informes resumidos		17.2 Sí, acceso a datos y análisis de movimiento	
17.3 Sí, análisis de comportamiento del usuario		17.4 Sí, análisis predictivo	X
17.5 No		17.6 No sabe	

18: ¿Incluye ataques cibernéticos en su marco de gestión de riesgos?

18.1 Sí		18.2 No	X	18.3 No sabe	

19: ¿Qué controles de riesgo utilizan para gestionar el riesgo de ocurrencias de ciberataques?

19.1 Tableros de eventos de seguridad		19.2 Herramientas de defensa perimetral de seguridad	X
19.3 Sistema de monitoreo de registros		19.4 Procesos de remediación de eventos de seguridad	

19.5 Herramientas de base de datos y monitoreo de archivos	
19.6 Violaciones de acceso (indicadores clave de riesgo por base de datos o sistema)	
19.7 Pérdida de datos y corrupción (principales indicadores de riesgo)	
19.8 Tiempo de inactividad del sistema (indicadores clave de riesgo)	
19.9 Otro (indique cuál)	

20: ¿Cuáles son las principales barreras para una mejor administración de amenazas?

20.1 Falta de capacitación y experiencia		20.2 Falta de colaboración entre los departamentos			
20.3 Falta de tecnología adecuada		20.4 Falta de personal		20.5 Presupuestos insuficientes	
20.6 No tienen barreras	X	20.7 Otro (indique cuál)			

21: ¿Cómo combate su organización las amenazas hoy?

21.1 Programa de gobernanza de la seguridad de la información		21.2 Capacitación del usuario			
21.3 Aplicaciones y dispositivos especializados de terceros		21.4 Verificaciones de antecedentes			
21.5 Proveedor de servicios de seguridad administrados		21.6 Autenticación secundaria			
21.7 Monitoreo de actividad de base de datos		21.8 Actividad de monitoreo del usuario			
21.9 Funciones de seguridad nativas del sistema operativo subyacente					
21.10 Herramientas personalizadas y aplicaciones desarrolladas en la casa					
21.11 Todas las anteriores	X	21.11 No usan nada		21.12 Otro (indique cuál)	

22: ¿En qué aspectos de la gestión de amenazas se concentra su organización principalmente?

22.1 Tácticas de disuasión		22.2 Tácticas de detección	X	22.3 Análisis y análisis forense	
22.4 Engaño (por ejemplo, honeypots, etc.)				22.5 Ninguna	
22.6 Otro (indique cuál)					

23: ¿Cómo cambiará su presupuesto de seguridad en los próximos 12 meses?

23.1 Esperan un aumento en el presupuesto de seguridad en los próximos 12 meses			X
23.2 El presupuesto se mantendrá plano		23.3 El presupuesto disminuirá	

24: ¿Cuánto tiempo le tomaría a su organización detectar un ataque?

24.1 En minutos	X	24.2 En cuestión de horas		24.3 Dentro de un día	
24.4 Dentro de una semana		24.5 Dentro de un mes		24.6 Dentro de tres meses	
24.7 Más de tres meses		24.8 Sin capacidad de detectar			

25: ¿Cuánto tiempo le tomaría a su organización recuperarse de un ataque?

25.1 En una semana		25.2 Dentro de un mes		25.3 Dentro de tres meses	
25.4 Más de tres meses		25.5 Sin capacidad para recuperar		25.6 No sabe	X

26: ¿Cuál es el costo promedio estimado de remediación después de un ataque?

26.1 Menos de 100.000 dólares		26.2 Entre 100.000 y 500.000 dólares	
26.3 Entre 500.000 y 1’000.000 dólares		26.4 Entre 1’000.000 y 2’000.000 dólares	
26.5 Más de 2’000.000 dólares		26.6 No sabe	X

27: Dentro de su organización, ¿qué tan difícil es determinar el daño real de una amenaza?

27.1 Muy difícil		27.2 Moderadamente difícil		27.3 Nada difícil	X

Gracias por su amable colaboración. Que tenga un excelente día.

Apéndice N.° 4. Lista de Chequeo Aplicada en la Empresa de Seguridad Privada N.

FUNDACIÓN UNIVERSITARIA DEL ÁREA ANDINA, SECCIONAL PEREIRA

LISTA DE CHEQUEO PARA DETERMINAR EL NIVEL DE SEGURIDAD DE LA INFORMACIÓN

El propósito de la presente lista de chequeo es verificar las condiciones iniciales del sistema de seguridad de la información, frente a lo que estipula la norma ISO/IEC 27001:2013.

Fecha:	Día	06 y 07	Mes	04	Año	2018	Nombre de la empresa: Empresa de seguridad privada N
Teléfono: *Confidencial*							E-mail: *Confidencial*
Dirección: *Confidencial*							Área encargada del control del SGSI: Área de tecnología de información y área de calidad
Nombre del responsable del SGSI: *Confidencial* *Confidencial*							Cargo: Director del área de tecnología de información Directora del área de calidad
Persona a quien se entrevista: *Confidencial* *Confidencial*							Cargo: Director del área de tecnología de información Directora del área de calidad

Objetivos de control y controles					
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN					
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información					
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.					
A.5.1.1	Políticas para la seguridad de la información	*Control* Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					
A.6.1 Organización interna					

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.					
A.6.1.1	Roles y responsabilidades para la seguridad de la información	*Control* Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.6.1.2	Separación de deberes	*Control* Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.6.1.3	Contacto con las autoridades	*Control* Se deben mantener contactos apropiados con las autoridades pertinentes.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.6.1.4	Contacto con grupos de interés especial	*Control* Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyectos.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.6.2 Dispositivos móviles y teletrabajo					
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.					
A.6.2.1	Política para dispositivos móviles	*Control* Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	***Se realiza***	***No se realiza***	***No aplica*** **X**
A.6.2.2	Teletrabajo	*Control* Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	***Se realiza***	***No se realiza***	***No aplica*** **X**
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS					
A.7.1 Antes de asumir el empleo					
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.					
A.7.1.1	Selección	*Control* Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes,	***Se realiza*** **X**	***No se realiza***	***No aplica***

		reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.			
A.7.1.2	Términos y condiciones del empleo	*Control* Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.7.2 Durante la ejecución del empleo					
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.					
A.7.2.1	Responsabilidades de la dirección	*Control* La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.7.2.2	Toma de conciencia, educación y la formación en la seguridad de la información	*Control* Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.7.2.3	Proceso disciplinario	*Control* Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.7.3 Terminación y cambio de empleo					
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.					
A.7.3.1	Terminación o cambio de responsabilidades de empleo	*Control* Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.8 GESTIÓN DE ACTIVOS					
A.8.1 Responsabilidad por los activos					
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección					

apropiadas.					
A.8.1.1	Inventario de activos	*Control* Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.8.1.2	Propiedad de los activos	*Control* Los activos mantenidos en el inventario deben tener un propietario.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.8.1.4	Devolución de los activos	*Control* Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.8.2 Clasificación de la información					
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.					
A.8.2.1	Clasificación de la información	*Control* La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.8.2.2	Etiquetado de la información	*Control* Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.8.2.3	Manejo de activos	*Control* Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.8.3 Manejo de medios					
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios.					

A.8.3.1	Gestión de medios removibles	*Control* Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.8.3.2	Disposición de los medios	*Control* Se debe disponer de forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.8.3.3	Transferencia de medios físicos	*Control* Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9 CONTROL DE ACCESO					
A.9.1 Requisitos del negocio para control de acceso					
Objetivo: Limitar el acceso a información a instalaciones de procesamiento de información.					
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9.1.2	Acceso a redes y a servicios en red	*Control* Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9.2 Gestión de acceso de usuarios					
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.					
A.9.2.1	Registro y cancelación del registro de usuarios	*Control* Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9.2.2	Suministro de acceso de usuarios	*Control* Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9.2.3	Gestión de derechos de acceso privilegiado	*Control* Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9.2.4	Gestión de	*Control*	***Se***	***No se***	***No***

	información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	***realiza*** **X**	***realiza***	***aplica***
A.9.2.5	Revisión de los derechos de acceso de usuarios	*Control* Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9.2.6	Retiro o ajuste de los derechos de acceso	*Control* Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9.3 Responsabilidades de los usuarios					
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.					
A.9.3.1	Uso de información de autenticación secreta	*Control* Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9.4 Control de acceso a sistemas y aplicaciones					
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.					
A.9.4.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9.4.2	Procedimiento de ingreso seguro	*Control* Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.9.4.5	Control de acceso	*Control*	***Se***	***No se***	***No***

	a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	***realiza*** **X**	***realiza***	***aplica***
A.10 CRIPTOGRAFÍA					
A.10.1 Controles criptográficos					
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.					
A.10.1.1	Política sobre el uso de controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	***Se realiza***	***No se realiza*** **X**	***No aplica***
A.10.1.2	Gestión de llaves	*Control* Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	***Se realiza***	***No se realiza*** **X**	***No aplica***
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO					
A.11.1 Áreas seguras					
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.					
A.11.1.1	Perímetro de seguridad física	*Control* Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.11.1.2	Controles de acceso físicos	*Control* Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	*Control* Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.11.1.4	Protección contra amenazas externas y ambientales	*Control* Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.11.1.5	Trabajo en áreas seguras	*Control* Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.11.1.6	Áreas de despacho y carga	*Control* Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible,	***Se realiza***	***No se realiza***	***No aplica*** **X**

		aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.			
A.11.2 Equipos					
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.					
A.11.2.1	Ubicación y protección de los equipos	*Control* Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.11.2.2	Servicios de suministro	*Control* Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.11.2.3	Seguridad del cableado	*Control* El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.11.2.4	Mantenimiento de equipos	*Control* Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.11.2.5	Retiro de activos	*Control* Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	*Control* Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.11.2.7	Disposición segura o reutilización de equipos	*Control* Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reuso.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.11.2.8	Equipos de usuario	*Control* Los usuarios deben asegurarse de que a los	***Se realiza***	***No se realiza***	***No aplica***

	desatendido	equipos desatendidos se les da protección apropiada.	**X**		
A.11.2.9	Política de escritorio limpio y pantalla limpia	*Control* Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.12 SEGURIDAD DE LAS OPERACIONES					
A.12.1 Procedimientos operacionales y responsabilidades					
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de la información.					
A.12.1.1	Procedimientos de operación documentados	*Control* Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.12.1.2	Gestión de cambios	*Control* Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.12.1.3	Gestión de capacidad	*Control* Se debe hacer seguimiento al uso de recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operaciones	*Control* Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.12.2 Protección contra códigos maliciosos					
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.					
A.12.2.1	Controles contra códigos maliciosos	*Control* Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.12.3 Copias de respaldo					
Objetivo: Proteger contra la pérdida de datos.					
A.12.3.1	Respaldo de la información	*Control* Se deben hacer copias de respaldo de la	***Se realiza***	***No se realiza***	***No aplica***

		información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	**X**		
A.12.4 Registro y seguimiento					
Objetivo: Registrar eventos y generar evidencia.					
A.12.4.1	Registro de eventos	*Control* Se deben elaborar, conservar y revisar regularmente los requisitos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	***Se realiza***	***No se realiza*** **X**	***No aplica***
A.12.4.2	Protección de la información de registro	*Control* Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	***Se realiza***	***No se realiza*** **X**	***No aplica***
A.12.4.3	Registros del administrador y del operador	*Control* Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	***Se realiza***	***No se realiza*** **X**	***No aplica***
A.12.4.4	Sincronización de relojes	*Control* Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.12.5 Control de software operacional					
Objetivo: Asegurarse de la integridad de los sistemas operacionales.					
A.12.5.1	Instalación de software en sistemas operativos	*Control* Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.12.6 Gestión de la vulnerabilidad técnica					
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.					
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.12.6.2	Restricciones sobre la instalación de software	*Control* Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	***Se realiza*** **X**	***No se realiza***	***No aplica***

A.12.7 Consideraciones sobre auditorías de sistemas de información					
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.					
A.12.7.1	Controles de auditorías de sistemas de información	*Control* Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	***Se realiza***	***No se realiza*** **X**	***No aplica***
A.13 SEGURIDAD DE LAS COMUNICACIONES					
A.13.1 Gestión de la seguridad de las redes					
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de soporte.					
A.13.1.1	Controles de redes	*Control* Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.13.1.2	Seguridad de los servicios de red	*Control* Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.13.1.3	Separación en las redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.13.2 Transferencia de información					
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.					
A.13.2.1	Políticas y procedimientos de transferencia de información	*Control* Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.13.2.2	Acuerdos sobre transferencia de información	*Control* Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.13.2.3	Mensajería electrónica	*Control* Se debe proteger adecuadamente la información incluida en la mensajería	***Se realiza*** **X**	***No se realiza***	***No aplica***

		electrónica.			
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	*Control* Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
A.14.1 Requisitos de seguridad de los sistemas de información					
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que presentan servicios sobre redes públicas.					
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	*Control* Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	*Control* La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	*Control* La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.14.2 Seguridad en los procesos de desarrollo y de soporte					
Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.					
A.14.2.1	Política de desarrollo seguro	*Control* Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.14.2.2	Procedimientos de control de cambios en sistemas	*Control* Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de	***Se realiza*** **X**	***No se realiza***	***No aplica***

		procedimientos formales de control de cambios.			
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	*Control* Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.14.2.4	Restricciones en los cambios a los paquetes de software	*Control* Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.14.2.5	Principios de construcción de los sistemas seguros	*Control* Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.14.2.6	Ambiente de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprenden todo el ciclo de vida de desarrollo de sistemas.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.14.2.7	Desarrollo controlado externamente	*Control* La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.14.2.8	Pruebas de seguridad de sistemas	*Control* Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.14.2.9	Prueba de aceptación de sistemas	*Control* Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.14.3 Datos de prueba					
Objetivo: Asegurar la protección de los datos usados para pruebas.					
A.14.3.1	Protección de datos de prueba	*Control* Los datos de prueba se deben seleccionar,	***Se realiza***	***No se realiza***	***No aplica***

		proteger y controlar cuidadosamente.	**X**		
A.15 RELACIONES CON LOS PROVEEDORES					
A.15.1 Seguridad de la información en las relaciones con los proveedores					
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.					
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	*Control* Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	*Control* Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	*Control* Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.15.2 Gestión de la prestación de servicios de proveedores					
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.					
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	*Control* Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.15.2.2	Gestión de cambios en los servicios de los proveedores	*Control* Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN					
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información					

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.					
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.16.1.2	Reporte de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.16.1.3	Reporte de debilidades de seguridad de la información	*Control* Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	*Control* Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	*Control* El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.16.1.7	Recolección de evidencia	*Control* La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO					
A.17.1 Continuidad de seguridad de la información					

Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.					
A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.	***Se realiza***	***No se realiza*** **X**	***No aplica***
A.17.1.2	Implementación de la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	***Se realiza***	***No se realiza*** **X**	***No aplica***
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	***Se realiza***	***No se realiza*** **X**	***No aplica***
A.17.2 Redundancias					
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.					
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	*Control* Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir con los requisitos de disponibilidad.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.18 CUMPLIMIENTO					
A.18.1 Cumplimiento de requisitos legales y contractuales					
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.					
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	*Control* Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.	***Se realiza***	***No se realiza*** **X**	***No aplica***
A.18.1.2	Derechos de propiedad intelectual	*Control* Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de	***Se realiza*** **X**	***No se realiza***	***No aplica***

		reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.			
A.18.1.3	Protección de registros	*Control* Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.18.1.4	Privacidad y protección de información de datos personales	*Control* Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.18.1.5	Reglamentación de controles criptográficos	*Control* Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	***Se realiza***	***No se realiza*** **X**	***No aplica***
A.18.2 Revisiones de seguridad de la información					
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.					
A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	***Se realiza***	***No se realiza*** **X**	***No aplica***
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	*Control* Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	***Se realiza*** **X**	***No se realiza***	***No aplica***
A.18.2.3	Revisión del cumplimiento técnico	*Control* Los sistemas de información se deben revisar periódicamente para determinar el	***Se realiza*** **X**	***No se realiza***	***No aplica***

		cumplimiento con las políticas y normas de seguridad de la información.			

Gracias por su amable colaboración. Que tenga un excelente día.